ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΛΕΤΗ ΚΕΝΩΝ ΑΣΦΑΛΕΙΑΣ LAMP ΣΥΣΤΗΜΑΤΩΝ

Αρβανιτάκη Γεωργία

Πτυχιακή Εργασία

που αφορά τη μελέτη κενών ασφάλειας των λογισμικών
Apache και Mysql, καθώς και των scripting γλωσσών
προγραμματισμού PHP-Perl-Python

Πειραιάς

Ιούλιος 2011

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι διαδικτυακές εφαρμογές συνήθως εκπροσωπούν ένα δημόσιο πρόσωπο στις επιχειρήσεις ανά τον κόσμο. Αντίθετα με τις εκτός δικτύου ή εσωτερικές εφαρμογές , οι διαδικτυακές εφαρμογές είναι πιθανότερο να έρθουν σε επαφή με κακόβουλους χρήστες. Συνεπώς , η ασφάλεια είναι μεγάλης σημασίας για τις διαδικτυακές εφαρμογές και η αποτυχία ενίσχυσης της επαρκούς ασφάλειας μπορεί να αποτελέσει σοβαρό πρόβλημα.

Μερικές από τις πιο συνήθεις επιθέσεις σε διαδικτυακές εφαρμογές είναι η πλαστογράφηση στοιχείων, η εισαγωγή Sql ερωτημάτων , η άρνηση υπηρεσίας, η υπερχείλιση buffer. Η σοβαρότητα των επιθέσεων ποικίλει από παραβίαση προσωπικών πληροφοριών και δεδομένων, κλοπή ταυτότητας , σε απώλεια ή και τροποποίηση δεδομένων (συγκεκριμένα με την εισαγωγή Sql ερωτήματος) ακόμα και πειρατεία σε μηχάνημα host. Επειδή οι διαδικτυακές εφαρμογές είναι προσβάσιμες σε δημόσιο τομέα (το διαδίκτυο), οι επιθέσεις συμβαίνουν δημόσια με αποτέλεσμα σοβαρές επιπτώσεις.

Αν και πρέπει να κατανοήσουμε και να εφαρμόσουμε την προστασία, σημαντικό ρόλο παίζουν επίσης η επίδοση, ο σχεδιασμός και η χρηστικότητα . Το επίπεδο ασφαλείας που θα πρέπει να υιοθετηθεί είναι ανάλογα το project , αλλά θα πρέπει να δοθεί προσοχή στα λιγότερο σωστά δεδομένα και να εφαρμοστεί η αυθεντικότητα. Επίσης θα πρέπει να δοθεί προσοχή και σε άλλες τυπικές διαδικασίες για την ασφάλεια του κώδικα όπως το φιλτράρισμα δεδομένων χρησιμοποιώντας την whitelist approach, δηλαδή τη μέθοδο όπου όλα τα δεδομένα είναι ανακριβή μέχρι να κριθούν σωστά, την ασφαλή αποθήκευση των μυστικών και των ευαίσθητων λεπτομερειών (όπως οι λεπτομέρειες αυθεντικοποίησης των βάσεων δεδομένων), χρησιμοποιώντας αληθείς , εμπορικά τυποποιημένες και γνωστές μεθόδους κρυπτογραφίας και hashing και τρέχοντας σε ελάχιστα δικαιώματα οπότε να μειωθεί η σοβαρότητα των επιθέσεων εάν και εφόσον συμβούν. Ακόμα θα πρέπει να υπογραμμιστεί η σημαντικότητα του απαραίτητου ελέγχου ασφαλείας των εφαρμογών , για να σιγουρέψουμε ότι υπάρχει επαρκής και σωστός χειρισμός των λαθών και ότι οι εφαρμογές δεν είναι ευαίσθητες για να διαπραγματευτούν όταν τους δίνονται απρόσμενα δεδομένα ή δραστηριότητες . Όταν αναπτύσσουμε εφαρμογές είναι σημαντικό τα λάθη να αντιμετωπίζονται και εάν είναι δυνατόν να καταστέλλονται , γιατί συχνά αποκαλύπτουν χρήσιμες πληροφορίες , οι οποίες μπορούν να κάνουν το χακάρισμα ευκολότερο . Επιπλέον , εφόσον μια εφαρμογή παραγωγής είναι πιθανότερο να αντιμετωπίσει προβλήματα διαφορετικά από μια εφαρμογή ανάπτυξης (όπως προβλήματα που τυχαίνουν λόγω συναγωνισμού θεμάτων η υψηλούς φόρτωσης) , είναι συνετό να υπάρχουν εργαλεία για τη παρακολούθηση του μόνιτορ και του ιστορικού (monitoring και logging tools) ή ακόμα και να αποτελούν κομμάτια της εφαρμογής.

2. Ο ΟΡΟΣ ΕΥΠΑΘΕΙΑ

Στην ασφάλεια των υπολογιστών , ο όρος ευπάθεια είναι μία αδυναμία η οποία επιτρέπει σε έναν εισβολέα να μειώσει την ασφάλεια ενός συστήματος πληροφοριών. Η ευπάθεια αποτελείται από τρία στοιχεία : την ευαισθησία ή το ελάττωμα ενός συστήματος, την πρόσβαση του εισβολέα στο ελάττωμα και την ικανότητα του εισβολέα να εκμεταλλευτεί το ελάττωμα.

Για να είναι το σύστημα ευάλωτο πρέπει ο εισβολέας να έχει ένα τουλάχιστον το εργαλείο ή τη τεχνική για να μπορέσει να συνδεθεί με μία αδυναμία του συστήματος. Σε αυτό το πλαίσιο, η ευπάθεια είναι γνωστή επίσης ως Επίθεση Επιφάνειας (Attack Surface).

Περιπτώσεις κενών ασφαλείας πολλές φορές βασίζονται σε θέματα ευπάθειας. Πολλές είναι οι περιπτώσεις όπου κάποιος μπορεί να εκμεταλλευτεί κάποιο κενό ασφαλείας για να κάνει επίθεση.

Σαν παράθυρο ευπάθειας ορίζεται ο χρόνος από όταν το κενό ασφαλείας δημιουργήθηκε στο λογισμικό , έως και τη στιγμή που αφαιρέθηκε η πρόσβαση , έγινε διόρθωση του προβλήματος η απενεργοποιήθηκε ο εισβολέας.

3. ΤΑ LAMP ΣΥΣΤΗΜΑΤΑ

Το LAMP είναι ένα αποδεδειγμένα αποτελεσματικό σύνολο λογισμικού ανοιχτού κώδικα, το οποίο δουλεύει όπως ένα σύστημα . Η ανοιχτή αρχιτεκτονική καθενός από τα στοιχεία του επιτρέπουν μια συνεχώς ομαλή ενοποίηση μεταξύ τους, με αποτέλεσμα ένα δυνατό συνδυασμό.

Οι πρώτοι που υιοθέτησαν αυτές τις τεχνολογίες το 1997 είχαν αντιμετωπιστεί ως ριζοσπαστικοί , αλλά σήμερα το κίνημα του ανοιχτού κώδικα είναι αυξανόμενο. Μικρές και μεγάλες επιχειρήσεις υιοθετούν την μέθοδο ανάπτυξης του LAMP.

Κατευθυνόμενο μακριά από τα υψηλά κόστη, η εφαρμογή του λογισμικού σε διακομιστές και πελάτες με αδειοδότηση γίνεται αυξανόμενα απαραίτητη , γιατί η σταθερότητα κάθε εφαρμογής ξεπερνάει τις πιο ακριβές.

Σε πρόσφατες εκδηλώσεις , κάποιες κυβερνήσεις αποφάσισαν να κάνουν το βήμα στον ανοιχτό κώδικα , λαμβάνοντας υπόψη την αξιοπιστία του, την αποτελεσματικότητά του και το σημαντικά χαμηλό κόστος σε σύγκριση με συμβατικές λύσεις.

Πέρα από το κατόρθωμα της επίτευξης αυτού του επιπέδου της ανεξαρτησίας, ικανό να το αποδεχτούν ολόκληρες κυβερνήσεις, το κύριο πλεονέκτημα που έχουν δει όσοι χρησιμοποιούν τα LAMP συστήματα είναι η ταχύτητα. Ο συνδυασμός Linux και Apache είναι ικανός να «υπηρετεί» περισσότερες σελίδες από οποιαδήποτε άλλη εμπορική ή ανοιχτού κώδικα λύση.

Η Mysql είναι η γρηγορότερη βάση δεδομένων ανοιχτού κώδικα με ταχύτητα η οποία συγκρίνεται με την βάση δεδομένων της Oracle. Αυτό και μόνο το γεγονός επηρέασε τη NASA να αλλάξει σε Mysql το 2000. Με την Mysql το επίπεδο λειτουργικότητας το οποίο προσφέρεται στους καταναλωτές της , αυξάνεται σε leaps και bounds – με κυριότερο σημείο την προσφορά αποθηκευμένων διαδικασιών, ένα σύστημα το οποίο συναντάται μόνο σε ανεπτυγμένες βάσεις δεδομένων.

Πράγμα το οποίο μας φέρνει στη δύναμη της Php. Η Php είναι το γρηγορότερο scripting πρόγραμμα για διακομιστές στον πλανήτη. Λειτουργεί με Active Server Pages (ASP), Java, .Net και ColdFusion, επιτρέποντας ένα μεγαλύτερα δυνατό αριθμό χρηστών ανά διακομιστή , ενώ παράλληλα παρέχει το ίδιο ποσό λειτουργικότητας – λαμβάνοντας φυσικά υπόψη τις κατάλληλες μεθόδους προγραμματισμού.

3.1 L – ΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ LINUX

Το Linux είναι το λειτουργικό σύστημα στο οποίο τρέχουν οι εφαρμογές. Είναι ιδιαίτερα αξιοσημείωτο για την ταχύτητά του, τις ελάχιστες απαιτήσεις υλικού, την ασφάλεια και την απομακρυσμένη σύνδεση που προσφέρει. Ένα άλλο ακόμα σημαντικό στοιχείο είναι ότι το Linux είναι δωρεάν. Το Linux είναι ένα πλήρες λειτουργικό σύστημα το οποίο δε στοιχίζει τίποτα στη χρήση του. Ο χρήστης μπορεί να το κατεβάσει κατευθείαν από το διαδίκτυο , να το εγκαταστήσει και να το χρησιμοποιήσει.

Ένα άλλο σημαντικό πλεονέκτημα είναι η ικανότητα να το χρησιμοποιήσεις με ή χωρίς γραφικό περιβάλλον (GUI) , ανάλογα τις ανάγκες του χρήστη.

Το Linux είναι ένα project που ξεκίνησε ως χόμπι από τον Linus Torvalds όταν ήταν φοιτητής στο πανεπιστήμιο του Ελσίνκι στην Φιλανδία. Εκεί δουλεύοντας με το Minix (ένα μικρό σύστημα Unix) , αποφάσισε να δημιουργήσει ένα λειτουργικό σύστημα το οποίο θα ξεπερνούσε τα πρότυπα του Minix .Ξεκίνησε την ανάπτυξη του το 1991 και η πρώτη δημοσίευση στο κοινό ήταν η έκδοση 0.002. Η ανάπτυξη του Linux συνεχίζεται μέχρι και σήμερα με αναβαθμίσεις, οι οποίες γίνονται όλο και πιο συχνά.

3.2 A – Ο ΔΙΑΔΙΚΤΥΑΚΟΣ ΔΙΑΚΟΜΙΣΤΗΣ APACHE

Ο διαδικτυακός διακομιστής Apache αναπτύχθηκε από την εταιρεία Apache Software Foundation και αποτελεί μία λύση για τους διαδικτυακούς διακομιστές ανοιχτού κώδικα. Είναι εξαιρετικά γρήγορος και συνδυάζεται πολύ καλά με το λειτουργικό σύστημα Linux . Χρησιμοποιώντας τον διακομιστή Apache μπορούμε να δημιουργήσουμε εικονικούς διακομιστές (hosts) που μας επιτρέπουν να τρέχουμε πολλαπλές ιστοσελίδες σε έναν μόνο διακομιστή. Ο διακομιστής Apache είναι διαθέσιμος και για το περιβάλλον των Windows , παρόλα αυτά στο σύστημα των Windows η επίδοση δεν θα είναι η ίδια λόγω της διαχείρισης μνήμης της Microsoft και της αρχιτεκτονικής της δομής. Μια γρήγορη ματιά στα χαρακτηριστικά γνωρίσματα του Apache , θα περιελάμβανε αντικείμενα όπως παρακολούθηση ιστορικού ενεργειών (enhanced logging), ρύθμιση εύρους ζώνης (bandwidth throttling), προστασία πρόσβασης καταλόγου (directory access protection), υποστήριξη CGI (Common Gateway Interface (CGI) support), υποστήριξη SSL (Secure Sockets Layer (SSL) support) και πολλές ακόμα χρήσιμες ενσωματωμένες μονάδες .

Ο διακομιστής Apache γίνεται όλο και πιο γρήγορα δημοφιλής και είναι στη πρώτη θέση των διακομιστών που χρησιμοποιούνται σύμφωνα με τις έρευνες του netcraft (http://news.netcraft.com/archives/2011/05/02/may-2011-web-server-survey.html). Είναι στη πρώτη θέση εδώ και 15 χρόνια με μεγάλη διαφορά. Έχοντας τη πρώτη θέση από το 1996 με ποσοστό πάνω από από 60% ανά χρόνο , ακολουθεί η Microsoft με 16% ανά χρόνο και η Google με 12% .

3.3 M – Ο ΔΙΑΚΟΜΙΣΤΗΣ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ MYSQL

Ο διακομιστής βάσης δεδομένων Mysql είναι ένας ισχυρός διακομιστής διαχείρισης βάσεων δεδομένων, ο οποίος επιτρέπει στο χρήστη να αποθηκεύει και να ανακτά δεδομένα μέσω της γλώσσας Php. Υπάρχει η δυνατότητα αποθήκευσης διαφόρων τύπων δεδομένων όπως Boolean Operators, κείμενο, ακέραιους αριθμούς, εικόνες, δυαδικά δεδομένα και BLOBs(binary large objects) γρήγορα και αποτελεσματικά με ελάχιστη προσπάθεια. Σημαντικό ρόλο παίζει επίσης στη δημιουργία δυναμικών ιστοσελίδων. Με τον όρο δυναμική ιστοσελίδα εννοείται η δυνατότητα χρησιμοποίησης μιας και μοναδικής σελίδας κώδικα για την παρουσίαση διαφορετικών πληροφοριών βασισμένες στην αλληλεπίδραση του χρήστη. Αυτό εικονικά θα ήταν απίθανο χωρίς τη χρήση μίας βάσης δεδομένων και μιας scripting γλώσσας όπως η Php για να διαχειριστεί τα δεδομένα.

Η Mysql περιέχει χαρακτηριστικά όπως δημιουργία αντιγράφων, κλείδωμα πίνακα, οριοθέτηση των ερωτημάτων, λογαριασμούς χρηστών, πολλαπλές βάσεις δεδομένων, επίμονες συνδέσεις, αποθηκευμένες διαδικασίες, triggers, όψεις.

3.4 P – Η SCRIPTING ΓΛΩΣΣΑ PHP

Η PHP (προέρχεται από τις λέξεις Hypertext PreProcessor) είναι μια γλώσσα προγραμματισμού για την ανάπτυξη δυναμικών ιστοσελίδων. Είναι ευρέως διαδεδομένη γλώσσα και είναι ειδικά διαμορφωμένη για την ανάπτυξη κώδικα για το διαδίκτυο. Μπορεί να ενσωματωθεί σε αρχεία html και να μεταφραστεί από έναν διαδικτυακό διακομιστή με έναν Php επεξεργαστή , ο οποίος και θα παράγει την ιστοσελίδα. Αποτελεί ελεύθερο λογισμικό που διατίθεται βάσει της άδειας PHP.

Έχει εξελιχθεί σε μία από τις πιο δημοφιλείς server-side γλώσσες προγραμματισμού για τη δημιουργία διαδικτυακών εφαρμογών και αποτελεί μια από τις δημοφιλέστερες scripting γλώσσες που αναπτύσσεται συνεχώς. Σύμφωνα με μια πρόσφατη έρευνα [1], η PHP χρησιμοποιείται από το 76,7 % των ιστότοπων, ποσοστό αρκετά μεγάλο. Αν και η γλώσσα PHP έχει υποστεί δύο σημαντικές αλλαγές την τελευταία δεκαετία, διατηρεί μια Perl μορφή στη σύνταξη και στη δυναμική, η οποία συμβάλλει στο πιο ισχυρό της πλεονέκτημα, του να είναι απλή και ευέλικτη.

3.5 P – Η SCRIPTING ΓΛΩΣΣΑ PERL

Η Perl είναι μία υψηλού επιπέδου γλώσσα προγραμματισμού για τη δημιουργία δυναμικών ιστοσελίδων. Αναπτύχθηκε αρχικά ως μία γλώσσα προγραμματισμού για το λειτουργικό Unix για την επεξεργασία των reports. Από τότε, έχει υποστεί πολλές αλλαγές και αναθεωρήσεις για να γίνει ευρέως δημοφιλής μεταξύ των προγραμματιστών.

Η Perl δανείζεται στοιχεία από άλλες γλώσσες προγραμματισμού , συμπεριλαμβανομένης της C, της Shell Scripting, της AWK, και της Sed. Η γλώσσα Perl παρέχει ισχυρές δυνατότητες επεξεργασίας κειμένου χωρίς τα αυθαίρετα μήκη των ορίων των στοιχείων, που έχουν πολλά από τα σύγχρονα εργαλεία του Unix, πετυχαίνοντας την εύκολη επεξεργασία των κειμένων. Χρησιμοποιείται επίσης για τη δημιουργία γραφικών, τη διαχείριση του συστήματος, τον προγραμματισμό του δικτύου, για εφαρμογές που απαιτούν πρόσβαση σε βάσεις δεδομένων και για το προγραμματισμό του CGI για το διαδίκτυο.

Βασικά χαρακτηριστικά της γλώσσας αυτής αποτελούν το δυναμικό σύστημα τύπων (μία μεταβλητή αποκτά τύπο μόνο μετά από την ανάθεση μιας τιμής σε αυτή, μπορεί να διαχειριστεί αριθμούς και συμβολοσειρές, πίνακες απλούς και συσχετικούς , να δημιουργήσει δυναμικές δομές όπως δέντρα, στοίβες, ουρές) , η ιδιότητα ότι μια συνάρτηση ή μια διαδικασία δεν έχουν προκαθορισμένο αριθμό ορισμάτων και μπορούν να οριστούν αναδρομικά, η παροχή εργαλείων για ταυτόχρονη επεξεργασία δεδομένων μέσω νημάτων ή κάνοντας χρήση της κλήσης συστήματος fork, η παροχή υποδομών για δικτυακό προγραμματισμό και τέλος η δημιουργία CGI scripts.

[1] http://w3techs.com/technologies/overview/programming_language/all

3.6 P – Η SCRIPTING ΓΛΩΣΣΑ PYTHON

Η Python είναι μια διαδραστική αντικειμενοστραφής γλώσσα προγραμματισμού. Είναι σημαντική και για shell scripting αλλά και για web scripting και λειτουργεί με αυτό τον τρόπο από το Google μέχρι και τα video games. Έχει ως στόχο το συνδυασμό «αξιοσημείωτης δύναμης με πολύ σαφή σύνταξη», και η πρότυπη της βιβλιοθήκη είναι ευρεία και ολοκληρωμένη.

Η Python υποστηρίζει πολλά παραδείγματα προγραμματισμού , αλλά δεν περιορίζεται μόνο σε αντικειμενοστραφείς λύσεις αλλά και σε μικρότερου βαθμού λειτουργικό στυλ προγραμματισμού. Διαθέτει ένα πλήρως δυναμικό τύπο συστήματος και αυτόματη διαχείριση μνήμης , παρόμοια με εκείνη του συστήματος της Ruby, της Perl και της Tcl . Όπως και άλλες δυναμικές γλώσσες , η Python χρησιμοποιείται συχνά ως γλώσσα δέσμης ενεργειών , αλλά χρησιμοποιείται επίσης και σε ένα ευρύ φάσμα σε μη scripting πλαίσια.

Σχεδιάστηκε ώστε να είναι εξαιρετικά επεκτάσιμη. Νέες μονάδες μπορούν εύκολα να ενσωματωθούν γραμμένες σε C , C + + . Η Python μπορεί επίσης να χρησιμοποιηθεί ως γλώσσα για την επέκταση των υφιστάμενων μονάδων και εφαρμογών που απαιτούν μια προγραμματιζόμενη διεπαφή. Αυτός ο σχεδιασμός ενός μικρού πυρήνα γλώσσας με μεγάλη βιβλιοθήκη και εύκολα επεκτάσιμο διερμηνέα προέρχεται από τον Van Rossum .

4. ΕΙΣΑΓΩΓΗ ΣΤΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ

4.1 ΕΙΣΑΓΩΓΗ SQL ΕΡΩΤΗΜΑΤΟΣ (SQL INJECTION)

Η εισαγωγή Sql ερωτήματος είναι μια τεχνική παραβίασης, η οποία προσπαθεί να «περάσει» Sql εντολές μέσα από μία διαδικτυακή εφαρμογή για να τις εκτελέσει σε μια βάση δεδομένων. Αυτό συμβαίνει όταν ο προγραμματιστής δέχεται την είσοδο του χρήστη η οποία τοποθετείται απευθείας σε μια δήλωση Sql και δεν φιλτράρει σωστά τους επικίνδυνους χαρακτήρες.

Αυτό μπορεί να επιτρέψει σε ένα επιτιθέμενο όχι μόνο να κλέψει δεδομένα από τη βάση δεδομένων αλλά επίσης και να τα τροποποιήσει ή ακόμα και να τα διαγράψει. Οι επιτιθέμενοι συνήθως εισάγουν single quotes στο αλφαριθμητικό του ερωτήματος του URL , ή σε ένα πεδίο εισαγωγής της φόρμας, για να ελέγξουν εάν μπορούν να πραγματοποιήσουν εισαγωγή Sql ερωτήματος. Αν ο επιτιθέμενος δεχθεί μήνυμα λάθους υπάρχει μεγάλη πιθανότητα η εφαρμογή να είναι ευάλωτη σε ευπάθειες εισαγωγής Sql ερωτημάτων.

Οι διαδικτυακές εφαρμογές επιτρέπουν στους νόμιμους επισκέπτες της ιστοσελίδας να υποβάλουν και να ανακτούν δεδομένα σε ή από μια βάση δεδομένων μέσω του διαδικτύου χρησιμοποιώντας τον περιηγητή ιστού τους.

Οι βάσεις δεδομένων είναι κεντρικής σημασίας για τις σύγχρονες ιστοσελίδες. Αποθηκεύουν τα δεδομένα που απαιτούνται για τους ιστότοπους για να παραδώσουν συγκεκριμένο περιεχόμενο στους επισκέπτες και να προσφέρουν πληροφορίες στους πελάτες, τους προμηθευτές, τους εργαζόμενους και τους μετόχους. Οι πιστοποιήσεις του χρήστη, τα οικονομικά στοιχεία μιας πληρωμής, τα στατιστικά στοιχεία της εταιρείας μπορεί όλα να είναι σε μια βάση δεδομένων και είναι προσβάσιμα από νόμιμους χρήστες, μέσω off-the-shelf και προσαρμοσμένες διαδικτυακές εφαρμογές.

Σελίδες login, υποστήριξη και έντυπα αίτησης προϊόντων, φόρμες επικοινωνίας, σελίδες αναζήτησης, καροτσάκια online αγορών και η γενική παράδοση δυναμικού περιεχομένου είναι τα χαρακτηριστικά της ιστοσελίδας και είναι όλα παραδείγματα των διαδικτυακών εφαρμογών. Αυτά τα χαρακτηριστικά της ιστοσελίδας είναι όλα ευπαθή σε επιθέσεις SQL Injection.

Μόλις ένας εισβολέας αντιληφθεί ότι ένα σύστημα είναι ευάλωτο σε εισαγωγή Sql ερωτήματος, είναι σε θέση να εισάγει ένα ερώτημα ή εντολή Sql μέσω ενός πεδίου της φόρμας εισόδου. Αυτό ισοδυναμεί με παράδοση στον εισβολέα τη βάση δεδομένων του χρήστη και επιτρέποντάς του να εκτελέσει οποιαδήποτε εντολή Sql, συμπεριλαμβανομένων και της διαγραφής πίνακα (drop table) στη βάση δεδομένων.

Ένας εισβολέας μπορεί να εκτελέσει αυθαίρετα Sql ερωτήματα σε ένα ευάλωτο σύστημα. Αυτό μπορεί να θέσει σε κίνδυνο την ακεραιότητα της βάσης δεδομένων του χρήστη και να εκθέσει ευαίσθητες πληροφορίες. Ανάλογα με τη back-end βάση δεδομένων κατά τη χρήση, οι ευπάθειες εισαγωγής Sql ερωτήματος μπορεί να οδηγήσουν σε διαφορετικά επίπεδα δεδομένων / πρόσβασης στο σύστημα για τον εισβολέα. Μπορεί να είναι δυνατό να χειραγωγήσουν υπάρχοντα ερωτήματα, να ενώσουν αυθαίρετα δεδομένα, να κάνουν χρήση subselects ή και να προσθέσουν επιπλέον ερωτήματα.

4.2 ΑΡΝΗΣΗ ΥΠΗΡΕΣΙΑΣ (DENIAL OF SERVICE - DoS)

Μια επίθεση άρνησης υπηρεσίας (DoS) είναι μία ευπάθεια στην οποία ο χρήστης ή ο οργανισμός στερείται των υπηρεσιών ενός πόρου, που είναι το αναμενόμενο να έχουν, με την πρόθεση να καταστήσει την νόμιμη χρήση αδύνατη.

Χρησιμοποιεί τα χαρακτηριστικά και τη λειτουργικότητα ενός διαδικτυακού ιστότοπου για να καταναλώσει, να εξαπατήσει ή και να παρακάμψει τους ελέγχους πρόσβασης του ιστότοπου.

Σε μια επίθεση άρνησης υπηρεσίας, ο εισβολέας προσπαθεί να αποτρέψει νόμιμους χρήστες από την πρόσβαση σε πληροφορίες ή υπηρεσίες. Με στόχο τον υπολογιστή και τη σύνδεση με το δίκτυο του, ή τους υπολογιστές και το δίκτυο των ιστότοπων που προσπαθεί ο χρήστης να χρησιμοποιήσει, ένας εισβολέας μπορεί να αποτρέψει το χρήστη από την πρόσβαση του σε e-mail, ιστοσελίδες, ηλεκτρονικούς λογαριασμούς (τράπεζες, κλπ.) ή και άλλες υπηρεσίες που βασίζονται στον υπολογιστή που επηρεάζεται.

Οι πόροι περιλαμβάνουν τον χρόνο της CPU, την κατανάλωση μνήμης , το εύρος ζώνης, το χώρο στο δίσκο κλπ. Όταν οποιοσδήποτε από αυτούς τους πόρους φτάσει σε πλήρη χωρητικότητα, το σύστημα λογικά θα είναι μη προσβάσιμο για τις συνήθεις δραστηριότητες του χρήστη.

Το πιο κοινό και προφανές είδος επίθεσης άρνησης υπηρεσίας συμβαίνει όταν ένας εισβολέας "πλημμύρίζει" ένα δίκτυο με πληροφορίες. Όταν ο χρήστης πληκτρολογεί μια διεύθυνση URL για μια συγκεκριμένη ιστοσελίδα στον περιηγητή σας, στέλνει ένα αίτημα στον διακομιστή του ιστότοπου για να δει τη σελίδα. Ο διακομιστής μπορεί να επεξεργαστεί μόνο ένα συγκεκριμένο αριθμό των αιτήσεων με τη μία, έτσι ώστε αν ένας εισβολέας επιβαρύνει το διακομιστή με αιτήματα, δεν μπορεί να επεξεργαστεί το αίτημα του χρήστη. Ο εισβολέας μπορεί να χρησιμοποιήσει μηνύματα spam e-mail για να ξεκινήσει μια παρόμοια επίθεση στο λογαριασμό e-mail του χρήστη. Είτε έχει ένα λογαριασμό e-mail που παρέχεται από τον εργοδότη του ή αυτόν που διατίθεται μέσα από μια δωρεάν υπηρεσία όπως το Yahoo ή το Hotmail και του έχει δοθεί ειδικό ποσοστό χωρητικότητας, κάτι το οποίο περιορίζει την ποσότητα των δεδομένων που μπορεί να έχει στο λογαριασμό του ο χρήστης ανά πάσα στιγμή. Με την αποστολή πολλών ή και μεγάλων μηνυμάτων στο λογαριασμό, ένας εισβολέας μπορεί να καταναλώσει ποσοστό χωρητικότητας , και έτσι να εμποδίζει το χρήστη να λάβει νόμιμα μηνύματα.

Συμπτώματα Άρνησης Υπηρεσίας

- Ασυνήθιστα αργή απόδοση του δικτύου (άνοιγμα αρχείων ή πρόσβαση σε διαδικτυακούς τόπους)
- Έλλειψη ενός συγκεκριμένου διαδικτυακού τόπου
- Αδυναμία πρόσβασης σε οποιαδήποτε ιστοσελίδα
- Δραματική αύξηση στον αριθμό των spam e-mails που λαμβάνονται (αυτό το είδος της επίθεσης άρνησης υπηρεσίας θεωρείται ένα μήνυμα βόμβα(e-mail bomb))

Οι επιθέσεις άρνησης υπηρεσίας μπορούν επίσης να οδηγήσουν σε προβλήματα στο δίκτυο και στους κλάδους γύρω από τον υπολογιστή στον οποίο έχει γίνει η επίθεση. Π.χ. το εύρος ζώνης ενός δρομολογητή μεταξύ του διαδικτύου και ενός τοπικού δικτύου μπορεί να καταναλωθεί από μία επίθεση και να θέσει σε κίνδυνο όχι μόνο τον υπολογιστή για τον οποίο σχεδιάστηκε η επίθεση, αλλά και ολόκληρο το δίκτυο. Αν η επίθεση πραγματοποιείται σε αρκετά μεγάλη κλίμακα , ολόκληρες γεωγραφικές περιοχές με σύνδεση στο διαδίκτυο μπορεί να τεθούν σε κίνδυνο .

Οι δράστες των επιθέσεων συνήθως στοχοποιούν τοποθεσίες ή υπηρεσίες που φιλοξενούνται σε διακομιστές «υψηλού προφίλ», όπως τράπεζες, πύλες πληρωμής πιστωτικών καρτών κλπ. Ο όρος χρησιμοποιείται γενικά με ό,τι αφορά τα δίκτυα υπολογιστών αλλά δεν περιορίζεται σε αυτόν τον τομέα, μπορεί επίσης να χρησιμοποιηθεί σε συνάρτηση και με τη διαχείριση πόρων της CPU.

Μέθοδοι επίθεσης

Μια επίθεση άρνησης υπηρεσίας χαρακτηρίζεται από μια ρητή προσπάθεια του εισβολέα να αποτρέψει τους νόμιμους χρήστες της υπηρεσίας να χρησιμοποιήσουν την υπηρεσία αυτή. Οι επιθέσεις μπορεί να απευθύνονται σε οποιαδήποτε συσκευή του δικτύου, συμπεριλαμβανομένων των επιθέσεων σε συσκευές δρομολόγησης και διαδικτύου, ηλεκτρονικού ταχυδρομείου ή DNS διακομιστές .

Η επίθεση μπορεί να γίνει με διάφορους τρόπους. Τα πέντε βασικά είδη επίθεσης είναι τα εξής:

1. Κατανάλωση των υπολογιστικών πόρων όπως το εύρος ζώνης, ο χώρος στο δίσκο ή ο χρόνος του επεξεργαστή.
2. Διαταραχή των πληροφοριών ρύθμισης παραμέτρων, όπως η δρομολόγηση των πληροφοριών.
3. Διαταραχή των κρατικών πληροφοριών, όπως η εκούσια αναστοιχειοθέτηση των TCP συνόδων.
4. Διατάραξη των φυσικών στοιχείων του δικτύου.
5. Παρεμπόδιση των μέσων επικοινωνίας μεταξύ των χρηστών για τους οποίους προορίζονται και το θύμα, έτσι ώστε να μην μπορούν πλέον να επικοινωνούν επαρκώς.

Μια επίθεση DoS μπορεί να περιλαμβάνει την εκτέλεση κακόβουλου λογισμικού που προορίζεται για :

Κατανάλωση μνήμης, λανθασμένο dereference δείκτη διεύθυνσης, κρασάρισμα δαίμονα, διακοπή λειτουργίας συστάδων, διακοπή λειτουργίας δαιμόνων, κρασάρισμα διαδικασιών, outage εφαρμογών, outage διακομιστή, εκτέλεση εντολών, κωδικοποίηση χαρακτήρων πολλών byte, «υπερανάγνωση» του buffer, κατανάλωση CPU και bandwidth, κρασάρισμα εφαρμογής, καταστροφή μνήμης, αλλοίωση δεδομένων, αποκοπή δεδομένων, μη αρχικοποίηση δείκτη διεύθυνσης dereference, αποτυχία ανάκτησης, μη έγκυρη πρόσβαση μνήμης, τερματισμός εφαρμογών μέσω συνδέσεων δικτύου, κρέμασμα συστήματος, use-after-free, διακοπή όλων των λειτουργιών εντοπισμού αρχείων, outage δαίμονα, σφάλμα κατάτμησης.

4.3 ΥΠΕΡΧΕΙΛΙΣΗ BUFFER (BUFFER OVERFLOW)

Ως υπερχείλιση buffer ορίζεται η περίπτωση αποθήκευσης δεδομένων σε ένα buffer εκτός της μνήμης που θα έπρεπε να αποθηκευτούν κανονικά. Τα επιπλέον στοιχεία αντικαθιστούν την παρακείμενη μνήμη, τα οποία μπορεί να περιέχουν άλλα στοιχεία, όπως στοιχεία μεταβλητών του προγράμματος και τα δεδομένα προγράμματος ελέγχου ροής. Αυτό μπορεί να οδηγήσει σε ασταθή συμπεριφορά του προγράμματος , συμπεριλαμβανομένων των σφαλμάτων πρόσβασης στη μνήμη, τα λανθασμένα αποτελέσματα , τη λήξη του προγράμματος ή την παραβίαση ασφαλείας του συστήματος.

Οι υπερχειλίσεις buffer είναι μια κοινή αιτία δυσλειτουργίας του λογισμικού. Ένας εισβολέας μπορεί να είναι σε θέση να χρησιμοποιήσει μια κατάσταση υπερχείλισης buffer για να αλλάξει τη ροή της διαδικασίας της εφαρμογής του. Η υπερχείλιση του buffer και η επανεγγραφή των memory-stack δεικτών θα μπορούσαν να χρησιμοποιηθούν για να εκτελέσει αυθαίρετα οποιοσδήποτε κακόβουλος εντολές του λειτουργικού συστήματος. Αποτελούν σημαντικό πρόβλημα σε συστήματα που βασίζονται σε λογισμικό και σε εφαρμογές για μεγάλο χρονικό διάστημα.

Μια υπερχείλιση buffer συμβαίνει όταν ένα πρόγραμμα ή μια διαδικασία προσπαθεί να αποθηκεύσει περισσότερα δεδομένα σε ένα buffer, από ό,τι επρόκειτο να κρατήσει. Δεδομένου ότι οι buffers έχουν δημιουργηθεί για να περιέχουν ένα πεπερασμένο αριθμό στοιχείων, οι επιπλέον πληροφορίες - οι οποίες πρέπει να πάνε κάπου - μπορεί να υπερχειλίσουν σε γειτονικούς buffers, διαφθείροντας ή «υπερεγγράφοντας» τα έγκυρα δεδομένα που φυλάσσονται σε αυτούς.

Αν και μπορεί να συμβεί κατά λάθος, λόγω σφάλματος προγραμματισμού, η υπερχείλιση buffer είναι ένα ολοένα και συχνότερο είδος επίθεσης ασφάλειας στην ακεραιότητα δεδομένων. Σε επιθέσεις υπερχείλισης buffer, τα επιπλέον στοιχεία που μπορεί να περιέχουν κωδικούς που σχεδιάστηκαν για να ενεργοποιήσουν συγκεκριμένες ενέργειες , στην πραγματικότητα στέλνουν νέες οδηγίες για την επίθεση υπολογιστή κάτι που θα μπορούσε, για παράδειγμα, να καταστρέψει τα αρχεία του χρήστη, να αλλάξει τα δεδομένα του ή να αποκαλύψει εμπιστευτικές πληροφορίες.Λέγεται ότι οι επιθέσεις υπερχείλισης buffer έχουν προκύψει διότι η γλώσσα προγραμματισμού C παρείχε το πλαίσιο και οι κακές πρακτικές προγραμματισμού παρείχαν την ευπάθεια.

4.4 ΥΠΟΧΕΙΛΙΣΗ BUFFER (BUFFER UNDERFLOW)

Η υποχείλιση του buffer είναι μια κατάσταση που προκύπτει όταν ένας buffer που χρησιμοποιείται για την επικοινωνία μεταξύ δύο συσκευών ή διαδικασιών, τροφοδοτείται με δεδομένα σε χαμηλότερη ταχύτητα από ότι τα δεδομένα που διαβάζονται από αυτό. Αυτό απαιτεί το πρόγραμμα ή τη συσκευή που διαβάζουν από το buffer, να σταματήσουν την επεξεργασία τους, ενώ ο buffer ξαναγεμίζει. Αυτό μπορεί να προκαλέσει ανεπιθύμητες και μερικές φορές σοβαρές παρενέργειες. Η απλούστερη λύση είναι φυσικά η αύξηση του μεγέθους του buffer.

4.5 ΥΠΕΡΧΕΙΛΙΣΗ ΑΚΕΡΑΙΩΝ (INTEGER OVERFLOW)

Υπερχείλιση ακεραίου είναι το αποτέλεσμα της προσπάθειας τοποθέτησης στη μνήμη του υπολογιστή. ενός ακέραιου που είναι πολύ μεγάλος για τον τύπο δεδομένων του ακέραιου σε ένα δεδομένο σύστημα.

Υφίσταται όταν ένας ακέραιος αριθμός, που δεν έχει ελεγχθεί σωστά, χρησιμοποιείται για τον προσδιορισμό της offset ή του μεγέθους στη κατανομή μνήμης, στην αντιγραφή, στην αλληλουχία. Αν ο εν λόγω ακέραιος αυξάνεται πέρα από τη μέγιστη δυνατή αξία, μπορεί να αναδιπλωθεί ώστε να γίνει ένας πολύ μικρός, ή αρνητικός αριθμός, και παρέχοντας έτσι μια πολύ λανθασμένη τιμή.

Μια υπερχείλιση ακεραίου είναι ένα πιθανό πρόβλημα σε ένα πρόγραμμα, που βασίζεται στο γεγονός ότι η αξία που μπορεί να κρατηθεί σε ένα αριθμητικό τύπο δεδομένων περιορίζεται από το μέγεθος του τύπου δεδομένων σε bytes.

Συνέπειες

Διαθεσιμότητα : Οι υπερχειλίσεις ακεραίου οδηγούν γενικά σε απροσδιόριστη συμπεριφορά και ως εκ τούτου σε συντριβές. Στην περίπτωση των υπερχειλίσεων που αφορούν μεταβλητές δεικτών βρόχου, η πιθανότητα του άπειρου βρόγχου είναι επίσης υψηλή.

Ακεραιότητα : Εάν η εν λόγω τιμή είναι σημαντική για τα δεδομένα (σε αντίθεση με τη ροή), η απλή καταστροφή δεδομένων έχει συμβεί. Επίσης, αν η υπερχείλιση ακεραίου έχει οδηγήσει σε μια κατάσταση υπερχείλισης μνήμης, είναι πολύ πιθανό να αλλοιωθούν τα δεδομένα.

Έλεγχος πρόσβασης : Οι υπερχειλίσεις ακεραίων μπορούν μερικές φορές να ενεργοποιήσουν υπερχειλίσεις buffer, οι οποίες μπορούν να χρησιμοποιηθούν για την αυθαίρετη εκτέλεση κώδικα. Αυτό είναι συνήθως έξω από το πεδίο εφαρμογής της πολιτικής ασφάλειας ενός προγράμματος.

4.6 ΠΕΡΑΣΜΑ ΚΑΤΑΛΟΓΟΥ (DIRECTORY TRAVERSAL)

Η ευπάθεια περάσματος καταλόγου είναι μια μορφή αδυναμίας που επιτρέπει στους επιτιθέμενους την πρόσβαση σε απόρρητους καταλόγους, την εκτέλεση εντολών και την προβολή των δεδομένων εκτός του κανονικού κατάλογου του διαδικτυακού διακομιστή όπου το περιεχόμενο της εφαρμογής είναι αποθηκευμένο.

Είναι μια μορφή εκμετάλλευσης του HTTP με την οποία ένας χάκερ χρησιμοποιεί το λογισμικό σε έναν διαδικτυακό διακομιστή, για να αποκτήσει πρόσβαση στα δεδομένα σε έναν κατάλογο, εκτός από τον κατάλογο root του διακομιστή. Εάν η προσπάθεια είναι επιτυχής, ο χάκερ μπορεί να δει τα απόρρητα αρχεία ή ακόμα και να εκτελέσει εντολές στον διακομιστή. Οι επιθέσεις περάσματος καταλόγου συνήθως εκτελούνται χρησιμοποιώντας προγράμματα περιήγησης στο διαδίκτυο. Κάθε διακομιστής στον οποίο τα δεδομένα εισόδου από προγράμματα περιήγησης στο διαδίκτυο δεν είναι επικυρωμένα, τότε είναι ευάλωτος σε αυτό το είδος της επίθεσης. Ένας εξειδικευμένος χάκερ μπορεί εύκολα να πραγματοποιήσει αυτόν τον τύπο επίθεσης σε διακομιστές με ανεπαρκή προστασία με την αναζήτηση μέσω του δέντρου καταλόγου. Ο κίνδυνος από τέτοιες επιθέσεις μπορεί να μειωθεί με προσεκτικό προγραμματισμό του διαδικτυακού διακομιστή, με την εγκατάσταση των ενημερώσεων λογισμικού και των patches, με το φιλτράρισμα των εισροών από προγράμματα περιήγησης, καθώς και τη χρήση των σαρωτών ευπάθειας.

Τα αρχεία των διαδικτυακών διακομιστών μπορούν να είναι στατικά όπως εικόνες και αρχεία HTML, ή δυναμικά όπως ASP και JSP αρχεία. Όταν το πρόγραμμα περιήγησης ζητά ένα δυναμικό αρχείο, ο διαδικτυακός διακομιστής εκτελεί πρώτα το αρχείο και στη συνέχεια επιστρέφει το αποτέλεσμα στο πρόγραμμα περιήγησης. Ως εκ τούτου, τα δυναμικά αρχεία είναι στην πραγματικότητα αρχεία που εκτελούνται στο διαδικτυακό διακομιστή.

Για να αποτραπούν οι χρήστες από την πρόσβαση σε μη εξουσιοδοτημένα αρχεία στο διαδικτυακό διακομιστή, οι διαδικτυακοί διακομιστές παρέχουν δύο κύριους μηχανισμούς ασφαλείας :

Ο κατάλογος root ελαχιστοποιεί την πρόσβαση του χρήστη σε συγκεκριμένο κατάλογο στο σύστημα αρχείων του διαδικτυακού διακομιστή. Όλα τα αρχεία τοποθετούνται στον κατάλογο root και σε υπο-καταλόγους του που είναι προσβάσιμοι στους χρήστες.

Για να περιορίσει την πρόσβαση των χρηστών σε συγκεκριμένα αρχεία στο root κατάλογο , οι διαχειριστές χρησιμοποιούν λίστες ελέγχου πρόσβασης. Χρησιμοποιώντας λίστες ελέγχου πρόσβασης, οι διαχειριστές μπορούν να καθορίσουν αν ένα αρχείο μπορεί να προβληθεί ή να εκτελεστεί από τους χρήστες, καθώς και άλλα δικαιώματα πρόσβασης.

Η ευπάθεια περάσματος καταλόγου είναι επίσης γνωστή ως .. / (τελεία τελεία κάθετος) επίθεση.

4.7 CROSS-SITE SCRIPTING (XSS)

Με τον όρο Cross-site scripting ή XSS αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών των υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστότοπο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει κώδικα σε έναν ιστότοπο, μέσω ενός κειμένου εισόδου για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστότοπο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή στον επισκέπτη του ιστότοπου.

Ο κακόβουλος χρήστης θα μπορούσε να επιτύχει κλοπή κωδικών/λογαριασμών και προσωπικών δεδομένων, αλλαγή ρυθμίσεων του ιστότοπου, κλοπή των cookies, ψεύτικη διαφήμιση (μέσω π.χ. ενός συνδέσμου).

Αναγκάζει μια ιστοσελίδα να δώσει στην οθόνη δεδομένα που αφορούν τον πελάτη, τα οποία εκτελούνται στον διαδικτυακό περιηγητή του χρήστη. Όταν ένας χρήστης κάνει χρήση του κακόβουλου κώδικα, τότε ο εισβολέας θα αποκτήσει πρόσβαση σε όλο το περιεχόμενο του προγράμματος περιήγησης στο διαδίκτυο (ιστορικό, έκδοση της εφαρμογής, κλπ).

Οι επιτιθέμενοι πετυχαίνουν το XSS με διάφορους τρόπους, όπως για παράδειγμα με την εισαγωγή κώδικα σε ένα σύνδεσμο σε ένα μήνυμα forum ή σε ένα μήνυμα spam. Ο εισβολέας μπορεί να χρησιμοποιήσει e-mail spoofing για να προσποιηθεί ότι είναι μια αξιόπιστη πηγή.

Όπως και άλλες ευπάθειες που σχετίζονται με το διαδίκτυο, όπως η εισαγωγή ερωτήματος Sql, μεγάλο μέρος της ευθύνης για το cross-site scripting οφείλεται στις μη ασφαλείς εφαρμογές που το επιτρέπουν. Οι εφαρμογές των διαδικτυακών διακομιστών , που δημιουργούν σελίδες δυναμικά, είναι ευάλωτοι σε ευπάθειες cross-site scripting αν αποτύχουν να επικυρώσουν την είσοδο των χρηστών και να εξασφαλίσουν ότι οι σελίδες που δημιουργούνται είναι σωστά κωδικοποιημένες. Μια ευπάθεια που επιτρέπει την cross-site scripting ευπάθεια μερικές φορές αναφέρεται ως XSS τρύπα.

4.8 ΠΑΡΑΠΟΙΗΣΗ CROSS-SITE ΑΙΤΗΜΑΤΩΝ (CROSS-SITE REQUEST FORGERY - CSRF)

Η παραποίηση Cross-site αιτημάτων (CSRF) είναι μια μέθοδος επίθεσης σε μια τοποθεσία Web στην οποία ένας εισβολέας μεταμφιέζεται ως νόμιμος και αξιόπιστος χρήστης. Μια επίθεση CSRF μπορεί να χρησιμοποιηθεί για να τροποποιήσει τις ρυθμίσεις του τείχους προστασίας, να κοινοποιήσει μη εξουσιοδοτημένα δεδομένα σε ένα forum ή να πραγματοποιήσει παράνομες οικονομικές συναλλαγές. Ένας χρήστης σε κίνδυνο δεν μπορεί ποτέ να ξέρει ότι μια τέτοια επίθεση έχει συμβεί. Εάν ο χρήστης μάθει για την επίθεση, μπορεί μόνο να αφού η ζημιά έχει πραγματοποιηθεί και η αποκατάσταση μπορεί να είναι αδύνατη.

Μπορεί να εκτελεστεί με τη κλοπή της ταυτότητας ενός υπάρχοντος χρήστη και στη συνέχεια να εισβάλλει σε ένα διαδικτυακό διακομιστή χρησιμοποιώντας αυτή την ταυτότητα. Ένας εισβολέας μπορεί επίσης να εξαπατήσει ένα νόμιμο χρήστη για να στείλει χωρίς να το ξέρει αιτήματα Hypertext Transfer τα οποία επιστρέφουν ευαίσθητα δεδομένα του χρήστη στον εισβολέα.

Είναι λειτουργικά το αντίθετο μίας cross-site scripting (XSS) επίθεσης, στην οποία ο χάκερ εισάγει κακόβουλο κώδικα σε μια σύνδεση σε μια τοποθεσία Web που φαίνεται να προέρχεται από αξιόπιστη πηγή. Όταν ένας τελικός χρήστης κάνει κλικ στη σύνδεση, το ενσωματωμένο πρόγραμμα υποβάλλεται σαν μέρος του διαδικτυακού αιτήματος του πελάτη και μπορεί να εκτελεστεί στον υπολογιστή του χρήστη.

Οι CSRF επιθέσεις είναι πιο δύσκολο να αντιμετωπιστούν σε σχέση με τις επιθέσεις XSS. Εν μέρει, αυτό οφείλεται στο γεγονός ότι οι CSRF επιθέσεις είναι λιγότερο συχνές και δεν έχουν λάβει την ίδια προσοχή. Ένα άλλο πρόβλημα είναι το γεγονός ότι μπορεί να είναι δύσκολο να καθοριστεί εάν ή όχι μια αίτηση HTTP από ένα συγκεκριμένο χρήστη στην πραγματικότητα είναι από τον ίδιο τον χρήστη. Ενώ αυστηρά προληπτικά μέτρα μπορούν να παρθούν για την επαλήθευση της ταυτότητας του χρήστη που προσπαθεί να αποκτήσει πρόσβαση σε μια τοποθεσία Web, οι χρήστες μπορεί να μην ανεχθούν συχνά αιτήματα για έλεγχο ταυτότητας. Η χρήση των κρυπτογραφημένων tokens μπορεί να προσφέρει περιοδική αυθεντικοποίηση ταυτότητας στο παρασκήνιο, ώστε ο χρήστης να μην δέχεται συνεχώς αιτήσεις ελέγχου ταυτότητας.

4.9 ΜΗ ΕΜΠΙΣΤΗ ΑΝΑΖΗΤΗΣΗ ΜΟΝΟΠΑΤΙΟΥ (UNTRUSTED SEARCH PATH)

Μη έμπιστη αναζήτηση μονοπατιού ορίζεται η επίθεση στην οποία ο εισβολέας τροποποιεί μια διαδρομή αναζήτησης της εφαρμογής του χρήστη, για να τον μεταφέρει σε ένα κακόβουλο πρόγραμμα, το οποίο έπειτα θα εκτελούσε η στοχευόμενη εφαρμογή. Το πρόβλημα επεκτείνεται σε οποιοδήποτε είδος πόρων που η εφαρμογή εμπιστεύεται.

Η εφαρμογή ψάχνει για πόρους χρησιμοποιώντας μια εξωτερικά τροφοδοτημένη διαδρομή αναζήτησης που μπορεί να δείξει σε πόρους που δεν είναι υπό τον άμεσο έλεγχο της εφαρμογής. Αυτό μπορεί να επιτρέψει σε επιτιθέμενους να εκτελέσουν τα δικά τους προγράμματα, να έχουν πρόσβαση σε μη εξουσιοδοτημένα αρχεία δεδομένων, ή να τροποποιήσουν τη διαμόρφωση με απροσδόκητους τρόπους.

Μερικές από τις πιο κοινές παραλλαγές των μη αξιόπιστων διαδρομών αναζήτησης είναι οι εξής:

- Το πρόγραμμα θα μπορούσε να κατευθυνθεί προς τα λάθος αρχεία, προκαλώντας ενδεχομένως ένα κρασάρισμα ή κρέμασμα του συστήματος όταν το αρχείο προορισμού είναι πολύ μεγάλο σε μέγεθος ή δεν έχει την αναμενόμενη μορφή.

- Το πρόγραμμα θα μπορούσε να στείλει την έξοδο μη εξουσιοδοτημένων αρχείων στον εισβολέα.

- Πιθανότητα επίθεσης άρνησης υπηρεσίας (DoS)

4.10 ΕΠΙΘΕΣΗ ΩΜΗΣ ΒΙΑΣ (BRUTE FORCE ATTACK)

Η επίθεση ωμής βίας αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Τέτοιου είδους επιθέσεις, οι οποίες χρησιμοποιούν όλα τα δυνατά κλειδιά, μπορούν πάντοτε να πραγματοποιηθούν. Συχνά, όμως, ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας πιο "πιθανά", κατά την άποψή του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών.

Στην ακαδημαϊκή βιβλιογραφία η μέθοδος ωμής βίας είναι μέτρο ασφάλειας ενός αλγόριθμου κρυπτογράφησης. Ένας αλγόριθμος κρυπτογράφησης θεωρείται "σπασμένος" αν υπάρχει αλγόριθμος κρυπτανάλυσης, ο οποίος μπορεί να βρει το κλειδί με μικρότερη πολυπλοκότητα από τη μέθοδο ωμής βίας, ανεξαρτήτως εάν αυτή η προσπάθεια υπολογισμού είναι εφικτή στην πράξη.

Συνήθως, το μήκος των κρυπτογραφικών κλειδιών επιλέγεται με τρόπο τέτοιο, ώστε να απαιτείται υπερβολικά μεγάλος χρόνος υπολογισμών (με βάση τις τρέχουσες υπολογιστικές δυνατότητες) και άρα να μην έχει χρηστική αξία μία τέτοιου είδους επίθεση. Ωστόσο, πολλά υπολογιστικά συστήματα έχουν κατά καιρούς γίνει στόχος επίθεσης ωμής βίας, με περισσότερο γνωστά τα συστήματα του Πενταγώνου και αστυνομικών αρχών των ΗΠΑ.

Επίσης η επίθεση στον κωδικό πρόσβασης μπορεί να μην προσπαθεί να αποκρυπτογραφήσει τα στοιχεία, αλλά να συνεχίζει να δοκιμάζει διαφορετικούς κωδικούς πρόσβασης. Για παράδειγμα, μια επίθεση ωμής βίας μπορεί να έχει ένα λεξικό όλων των λέξεων ή μια λίστα των κωδικών πρόσβασης που χρησιμοποιούνται συνήθως. Για να αποκτήσει πρόσβαση στο λογαριασμό χρησιμοποιώντας μια επίθεση ωμής βίας, το πρόγραμμα θα εισάγει όλες τις διαθέσιμες λέξεις για να αποκτήσει πρόσβαση στο λογαριασμό. Μια άλλη επίθεση ωμής βίας είναι ένα πρόγραμμα που τρέχει μέσα από όλα τα γράμματα ή γράμματα και αριθμούς, μέχρι να πάρει ένα αποτέλεσμα.

Αν και μια επίθεση ωμής βίας μπορεί εν τέλει να αποκτήσει πρόσβαση σε ένα λογαριασμό, αυτές οι επιθέσεις μπορεί να διαρκέσουν αρκετές ώρες, ημέρες, μήνες ακόμα και χρόνια για να τρέξει. Ο χρόνος που χρειάζεται για να ολοκληρώσει αυτές τις επιθέσεις είναι εξαρτάται από το πόσο περίπλοκος είναι ο κωδικός πρόσβασης.

Για να βοηθήσουν στην πρόληψη επιθέσεων ωμής βίας πολλά συστήματα επιτρέπουν στο χρήστη να κάνει συγκεκριμένο αριθμό λαθών, εισάγοντας το όνομα χρήστη ή τον κωδικό τους τρεις ή τέσσερις φορές. Αν ο χρήστης υπερβεί αυτές τις προσπάθειες το σύστημα κλειδώνει για να αποτρέψει οποιαδήποτε μελλοντική προσπάθεια.

4.11 ΕΥΠΑΘΕΙΑ ΣΥΝΥΠΟΛΟΓΙΣΜΟΥ (REMOTE FILE INCLUSION - RFI)

Η ευπάθεια συνυπολογισμού (RFI) είναι ένας τύπος επίθεσης που συναντάται πιο συχνά στις ιστοσελίδες. Επιτρέπει σε έναν εισβολέα να συμπεριλάβει ένα απομακρυσμένο αρχείο, συνήθως μέσα από μια δέσμη ενεργειών, στο διαδικτυακό διακομιστή. Το θέμα ευπάθειας προκύπτει λόγω της χρήσης της εισόδου που παρέχεται από τους χρήστες χωρίς την κατάλληλη επικύρωση.

Αυτό μπορεί να οδηγήσει σε κάτι μικρό όπως η γνωστοποίηση των περιεχομένων του αρχείου, αλλά μπορεί να οδηγήσει και σε εκτέλεση κώδικα στο διαδικτυακό διακομιστή, σε εκτέλεση κώδικα στο πελάτη, όπως η JavaScript , που μπορεί να οδηγήσει και σε άλλες επιθέσεις, όπως σε cross-site scripting (XSS), σε άρνηση υπηρεσίας (DoS), σε κλοπή και εκμετάλλευση δεδομένων.

Με την αξιοποίηση αμφίβολων «χαρακτηριστικών» της γλώσσας PHP, ένας εισβολέας μπορεί να εισάγει κώδικα σε ένα PHP πρόγραμμα στο διακομιστή. Αφού μπορεί να το κάνει αυτό, μπορεί να έχει πρόσβαση σε ότι και ο χρήστης του προγράμματος θα μπορούσε (βάσεις δεδομένων, αρχεία κωδικού πρόσβασης, κλπ). Έπειτα να εγκαταστήσει το δικό του κέλυφος που τρέχει με τα προνόμια του χρήστη του διαδικτυακού διακομιστή (όπως Apache ή httpd) και αν ο διακομιστής δεν έχει θωρακίσει ορισμένα τοπικά προνόμια του χρήστη, το κέλυφος θα μπορούσε να χρησιμοποιηθεί για να γίνει ο χρήστης root. Η Php είναι ιδιαίτερα επιρρεπής σε αυτού του είδους την ευπάθεια, επειδή η εγκατάσταση του προεπιλεγμένου συστήματος αρχείων επιτρέπει τις ενέργειες του αυτόματου ανοίγματος URLs σαν να ήταν τοπικά.

4.12 ΕΠΙΘΕΣΗ MAN-IN-THE-MIDDLE (MAN-IN-THE-MIDDLE ATTACK)

Ο όρος επίθεση man-in-the-middle αναφέρεται στο είδος της επίθεσης όπου ο επιτιθέμενος εισβάλει στην επικοινωνία μεταξύ των τελικών σημείων σε ένα δίκτυο, για να εισάγει ψευδείς πληροφορίες και να υποκλέψει τα δεδομένα που μεταφέρονται μεταξύ τους.

Στην συγκεκριμένη επίθεση, ο επιτιθέμενος παρακολουθεί μια ανταλλαγή ενός δημόσιου κλειδιού και στη συνέχεια την αναμεταδίδει, αντικαθιστώντας το δικό του δημόσιο κλειδί για την αιτούμενη, έτσι ώστε τα δύο πρωτότυπα μέρη να φαίνεται ότι εξακολουθούν να επικοινωνούν μεταξύ τους.

Οι man-in-the-middle επιθέσεις έχουν δύο κοινές μορφές , είτε ο επιτιθέμενος κρυφακούει, είτε αλλοιώνει κατάλληλα το μήνυμα. Είναι κοινός κίνδυνος για τις διαδικτυακές χρηματοπιστωτικές συναλλαγές - για παράδειγμα, το ηλεκτρονικό εμπόριο ιστοσελίδων, οι πύλες πληρωμής, οι ηλεκτρονικές τραπεζικές συναλλαγές καθώς και οι πλατφόρμες εξυπηρέτησης πιστωτικών καρτών.

Οι επιθέσεις man-in-the-middle μπορεί να οδηγήσουν σε κλοπές ταυτότητας και σε οικονομικές απάτες. Σε ένα τέτοιο σενάριο, ένας εισβολέας man-in-the-middle μπορεί να υποκλέψει την επικοινωνία των δημόσιων κλειδιών που ανταλλάσσονται από τον πελάτη και το διακομιστή, και να τροποποιήσουν τα δημόσια κλειδιά για κακόβουλο σκοπό. Για να αποφευχθεί κάθε υποψία και από τα δυο ενδιαφερόμενα μέρη , ο επιτιθέμενος θα πρέπει επίσης να διακόψει τα σχετιζόμενα κρυπτογραφημένα μηνύματα και απαντήσεις , και να χρησιμοποιήσει τα σωστά δημόσια κλειδιά για να αποκρυπτογραφήσει και να τα κρυπτογραφήσει ξανά για όλα τα τμήματα της επικοινωνίας σε κάθε στιγμιότυπο. Τέτοιες επιθέσεις, αν και φαινομενικά είναι πολύ δύσκολο να επιτευχθούν, αποτελούν πραγματικό κίνδυνο για τα επισφαλή δίκτυα (π.χ., το Διαδίκτυο, και ασύρματα δίκτυα).

4.13 ΕΥΠΑΘΕΙΕΣ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

Η μεγάλη ευαισθησία των κωδικών πρόσβασης είναι δεδομένη. Υπάρχουν αρκετοί διαφορετικοί τρόποι με τους οποίους ένα άτομο μπορεί να "αποδείξει" την ταυτότητά του. Με το να παρέχει κάτι που ξέρει (όπως ο κωδικός πρόσβασης), με το να παρέχει κάτι που έχει στην κατοχή του (όπως μια κάρτα), με το να παρέχει κάτι που είναι (ένα φυσιολογικό χαρακτηριστικό, όπως ένα δακτυλικό αποτύπωμα), με το να παρέχει κάτι που κάνει (όπως η ομιλία για την ανάλυση μοτίβου φωνής). Επειδή ο κωδικός πρόσβασης είναι κάτι που ο χρήστης γνωρίζει, αυτή η γνώση μπορεί να αποκτηθεί με διάφορους τρόπους.

Η αξιοποίηση ενός αδύναμου κωδικού πρόσβασης είναι ένας τρόπος. Οι χρήστες συχνά επιλέγουν εύκολους κωδικούς πρόσβασης - αυτούς που μπορούν να θυμηθούν, χωρίς πολύ κόπο. Αυτό σημαίνει ότι χρησιμοποιούν μια λέξη, φράση ή αριθμό που έχει ειδική σημασία για αυτούς, όπως το όνομα του συζύγου τους, τα γενέθλιά τους ή τον αριθμό κοινωνικής ασφάλισης. Ένας εισβολέας που γνωρίζει κάτι σχετικά με τον χρήστη μπορεί να είναι σε θέση να μαντέψει τον κωδικό πρόσβασης. Η χρήση κάθε λέξης που υπάρχει στο λεξικό δημιουργεί ευπάθεια, επειδή η επίθεση ωμής βίας και το «λεξικό» μπορούν να τα σπάσουν.

Η αξιοποίηση της συμπεριφοράς των χρηστών είναι επίσης ένας τρόπος. Εάν ο κωδικός πρόσβασης είναι πιο περίπλοκος και μη διαισθητικός (είναι ένας τυχαίος συνδυασμός γραμμάτων και αριθμών), ο χρήστης μπορεί να έχει πρόβλημα να το θυμάται, και αυτό μπορεί να οδηγήσει στο να το γράψει κάπου. Οι χρήστες μπορούν επίσης να μοιραστούν τους κωδικούς τους με άλλους χρήστες σε ένα ανεπίσημο περιβάλλον εργασίας.

Ακόμα και όταν οι χρήστες ασκούν τη δέουσα επιμέλεια, οι χάκερς μπορούν να χρησιμοποιήσουν συχνά τη «κοινωνική μηχανική» ώστε να πείσουν τους χρήστες να αποκαλύψουν τους κωδικούς πρόσβασής τους, παρουσιάζοντας τον εαυτό τους ως άτομα από τη τεχνική υποστήριξη ή το διοικητικό προσωπικό.

Ακόμα και όταν είναι ισχυροί οι κωδικοί πρόσβασης που χρησιμοποιούνται και οι χρήστες κρατούν τους κωδικούς πρόσβασης για τον εαυτό τους, οι εισβολείς μπορεί να είναι σε θέση να συλλάβουν τα διαπιστευτήρια όταν αποστέλλονται μέσω του δικτύου, σε περίπτωση που τα μέτρα ασφαλείας δεν είναι σε θέση να το αποτρέψουν.

Επειδή υπάρχουν τόσοι πολλοί τρόποι ένα μη εξουσιοδοτημένο άτομο με λίγη τεχνική γνώση και άνθρωποι με την ικανότητα να μαθαίνουν τους κωδικούς πρόσβασης των νόμιμων χρηστών, είναι πολύ σημαντικό οι διαδικτυακές εφαρμογές να ξεκινήσουν μια πολύπλευρη άμυνα κατά τη παραβίαση των κωδικών πρόσβασης. Αυτό αρχίζει με την εντολή ότι μόνο ασφαλείς κωδικοί πρέπει να χρησιμοποιούνται.

5. ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ APACHE

5.1 ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ APACHE

CVE-2011-1571

Η αδιευκρίνιστη ευπάθεια στο XSL Content portlet στο Liferay Portal Community Edition (CE) (εκδόσεις 5.x and 6.x), και όταν χρησιμοποιείται ο Apache Tomcat, επιτρέπει σε απομακρυσμένους χρήστες να εκτελέσουν εντολές αυθαίρετα μέσω ακαθόριστων παραγόντων.

Εκδόθηκε : 07/05/2011

Σοβαρότητα: Υψηλή

CVE-2010-0010

Ένα μειονέκτημα μιας λανθασμένης μετατόπισης μεταξύ αριθμητικών τύπων βρέθηκε στο μονάδα mod_proxy , το οποίο επηρεάζει μερικά αρχιτεκτονικά συστήματα των 64-bit. Ένας κακόβουλος HTTP διακομιστής στον οποίο οι αιτήσεις περνάνε από τον proxy διακομιστή , θα μπορούσε να χρησιμοποιήσει αυτό το μειονέκτημα για να ενεργοποιήσει μια υπερχείλιση heap buffer σε μια httpd διαδικασία - παιδί μέσω μιας επεξεργασμένης απάντησης.

Εκδόθηκε : 03/02/2010

Σοβαρότητα: Υψηλή

CVE-2010-0219

Ο Apache Axis2, έχει ένα προεπιλεγμένο κωδικό πρόσβασης του axis2 για το λογαριασμό του διαχειριστή, το οποίο κάνει ευκολότερη την εκτέλεση κώδικα αυθαίρετα για τους απομακρυσμένους χρήστες που θέλουν να επιτεθούν, με το ανέβασμα μίας επεξεργασμένης διαδικτυακής υπηρεσίας .

Εκδόθηκε : 18/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-2076

Ο Apache CXF 2.0.x, δεν απορρίπτει σωστά το DTDs στα SOAP μηνύματα, το οποίο επιτρέπει σε απομακρυσμένους χρήστες που θέλουν να επιτεθούν να διαβάσουν αρχεία αυθαίρετα, να στείλουν HTTP αιτήματα στους ενδοδίκτυους διακομιστές, ή να προκαλέσουν μία άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και cpu) μέσω του επεξεργασμένου DTD, όπως παρουσιάστηκε από τη δήλωση μιας οντότητας σε ένα αίτημα στο samples/wsdl_first_pure_xml.

Εκδόθηκε: 19/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-1632

Ο Apache Axis2 , δεν απορρίπτει σωστά τα DTDs στα SOAP μηνύματα, το οποίο επιτρέπει απομακρυσμένους χρήστες να επιτεθούν διαβάζοντας αυθαίρετα αρχεία, στέλνοντας HTTP αιτήματα σε ενδοδίκτυους διακομιστές, η δημιουργώντας άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και cpu) μέσω ενός επεξεργασμένου DTD, όπως παρουσιάστηκε από τη δήλωση μίας οντότητας σε ένα αίτημα για το Synapse SimpleStockQuoteService.

Εκδόθηκε: 22/06/2010

Σοβαρότητα: Υψηλή

CVE-2009-3095

Η μονάδα mod_proxy_ftp στον HTTP διακομιστή Apache επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης και να στείλουν εντολές αυθαίρετα σε έναν διακομιστή FTP μέσω παραγόντων που σχετίζονται με την ενσωμάτωση αυτών των εντολών στην επικεφαλίδα έγκρισης HTTP .

Εκδόθηκε: 08/09/2009

Σοβαρότητα: Υψηλή

CVE-2009-2412

Οι πολλαπλές υπερχειλίσεις ακεραίων στην βιβλιοθήκη του Apache Portable Runtime (APR) και στην βιβλιοθήκη του Apache Portable Utility (δηλ. APR-util) (εκδόσεις 0.9.x και 1.3.x), επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) ή για να εκτελέσουν κώδικα αυθαίρετα μέσω παραγόντων, πράγμα το οποίο ενεργοποιεί επεξεργασμένες κλήσεις στις λειτουργίες allocator_alloc, apr_palloc στην memory/unix/apr_pools.c στην APR, ή επεξεργασμένες κλήσεις στις λειτουργίες apr_rmm_malloc, apr_rmm _calloc, apr_rmm_realloc στην misc/apr_rmm.c στην APR-util, οδηγόντας σε υπερχειλίσεις του buffer.

Εκδόθηκε: 08/06/2009

Σοβαρότητα: Υψηλή

CVE-2009-1955

Η διεπαφή apr_xml_* του κατατμητή expat XML στο xml/apr_xml.c στην βιβλιοθήκη Apache APR-util, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να δημιουργήσουν μια άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης) μέσω ενός επεξεργασμένου XML έγγραφου που περιέχει ένα μεγάλο αριθμό από «φωλιασμένες» αναφορές οντοτήτων, όπως παρουσιάζονται από ένα PROPFIND αίτημα.

Εκδόθηκε: 08/06/2009

Σοβαρότητα: Υψηλή

CVE-2009-1462

Ο διαχειριστής ασφάλειας στο razorCMS (πριν την έκδοση 0.4) δεν πιστοποιεί τις άδειες κάθε αρχείου του λογαριασμού χρήστη του apache, κάτι το οποίο είναι ασυμβίβαστο με την τεκμηρίωση και επιτρέπει σε τοπικούς χρήστες να έχουν απροσδιόριστη επίδραση.

Εκδόθηκε: 28/04/2009

Σοβαρότητα: Υψηλή

CVE-2009-1012

Απροσδιόριστη ευπάθεια στα plug-ins για τον Apache και τους δικτυακούς διακομιστές IIS στον διακομιστή Oracle BEA WebLogic 7.0 Gold επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα.

Εκδόθηκε: 15/04/2009

Σοβαρότητα: Υψηλή

CVE-2009-0486

Ο Bugzilla (εκδόσεις 3.2.1, 3.0.7, και 3.3.2) όταν τρέχει κάτω από το mod_perl, καλεί τη λειτουργία srand όταν ξεκινάει ,κάτι το οποίο προκαλεί στα «παιδιά» του Apache να έχουν το ίδιο seed και να μη παράγουν επαρκείς τυχαίους αριθμούς για τυχαία tokens, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να υπερβούν τους μηχανισμούς ασφάλειας για την παραποίηση cross-site αιτημάτων (CSRF) για να κάνουν ενέργειες για τις οποίες δεν έχουν αδειοδότηση ενώ φαίνονται σαν άλλοι χρήστες.

Εκδόθηκε: 09/02/2009

Σοβαρότητα: Υψηλή

CVE-2008-2384

Η ευπάθεια εισαγωγής ερωτήματος Sql στο mod_auth_mysql.c στη μονάδα mod-auth-mysql (δηλ. libapache2-mod-auth-mysql) για τον HTTP διακομιστή Apache 2.x επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν εντολές Sql αυθαίρετα, μέσω κωδικοποίησης χαρακτήρων πολλών byte για να μπορέσουν να εισάγουν ακαθόριστα στοιχεία.

Εκδόθηκε : 22/01/2009

Σοβαρότητα: Υψηλή

5.2 ΣΥΝΗΘΙΣΜΕΝΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ APACHE

CVE-2011-1752

Η μονάδα mod_dav_svn του HTTP διακομιστή Apache (πριν την έκδοση 1.6.17), επιτρέπει σε απομακρυσμένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποίηση δείκτη διεύθυνσης dereference και κρασάρισμα δαίμονα) μέσω ενός αιτήματος για τους βασικούς πόρους της WebDAV.

Εκδόθηκε : 06/06/2011

Σοβαρότητα: Μέτρια

CVE-2011-1077

Οι πολλαπλές ευπάθειες cross-site scripting (XSS) στον Apache Archiva (εκδόσεις 1.0 μέχρι την 1.2.2 και από την 1.3.x μέχρι και πριν την 1.3.5), επιτρέπουν σε απομακρυσμένους χρήστες να εισάγουν αυθαίρετα web script ή HTML μέσω ακαθόριστων παραγόντων.

Εκδόθηκε : 02/06/2011

Σοβαρότητα: Μέτρια

CVE-2011-1026

Οι πολλαπλές ευπάθειες παραποίησης cross-site αιτημάτων (CSRF) στον Apache Archiva (εκδόσεις 1.0 μέχρι την 1.2.2 και από την 1.3.x μέχρι και πριν την 1.3.5), επιτρέπουν σε απομακρυσμένους χρήστες να υποκλέψουν την αυθεντικοποίηση των διαχειριστών.

Εκδόθηκε : 02/06/2011

Σοβαρότητα: Μέτρια

CVE-2010-3863

Το Apache Shiro, δεν κανονικοποιεί τα μονοπάτια URI πριν τα συγκρίνει με εισαγωγές στο αρχείο shiro.ini, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να υπερβούν τους προοριζόμενους περιορισμούς πρόσβασης μέσω ενός επεξεργασμένου αιτήματος, όπως παρουσιάζεται από το /./account/index.jsp URI.

Εκδόθηκε: 05/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-3700

Το VMware SpringSource Spring Security 2.x, όπως χρησιμοποιείται στην εφαρμογή του διακομιστή IBM WebSphere (WAS) 6.1 και 7.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να υπερβούν τους περιορισμούς ασφαλείας μέσω μιας παραμέτρου μονοπατιού.

Εκδόθηκε: 29/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4007

Το Oracle Mojarra χρησιμοποιεί ένα κωδικοποιημένο View State χωρίς Message Authentication Code (MAC), το οποίο διευκολύνει τους απομακρυσμένους χρήστες ώστε να επιτεθούν για να πραγματοποιήσουν επιτυχημένες μετατροπές του View State μέσω μιας επίθεσης padding oracle.

Εκδόθηκε: 20/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-2057

Το shared/util/StateUtils.java στο Apache MyFaces 1.1.x χρησιμοποιεί ένα κωδικοποιημένο View State χωρίς Message Authentication Code (MAC), το οποίο διευκολύνει τους απομακρυσμένους χρήστες ώστε να επιτεθούν για να εκτελέσουν επιτυχείς μετατροπές του View State μέσω μιας επίθεσης padding oracle.

Εκδόθηκε: 20/10/2010

Σοβαρότητα: Μέτρια

CVE-2009-5006

Στο στοιχείο C++ Broker στο Apache Qpid, μια λειτουργία (SessionAdapter:: ExchangeHandlerImpl::checkAlternate στο broker/SessionAdapter.cpp), επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν μια άρνηση υπηρεσίας (DoS) (λανθασμένο dereference δείκτη διεύθυνσης, κρασάρισμα δαίμονα και διακοπή λειτουργίας συστάδων) με το να επιχειρήσουν να τροποποιήσουν την εναλλαγή μιας ανταλλαγής .

Εκδόθηκε: 18/10/2010

Σοβαρότητα: Μέτρια

CVE-2009-5005

Μια λειτουργία (Cluster::deliveredEvent στο στοιχείο cluster/Cluster.cpp) στον Apache Qpid, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να δημιουργήσουν μια άρνηση υπηρεσίας (DoS) (κρασάρισμα δαιμόνων και διακοπή λειτουργίας συστάδων) μέσω λανθασμένων AMQP δεδομένων.

Εκδόθηκε: 18/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3083

Το sys/ssl/SslSocket.cpp στο qpidd στον Apache Qpid, όταν το πρωτόκολλο SSL είναι ενεργοποιημένο, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μία άρνηση υπηρεσίας DoS (διακοπή λειτουργίας δαιμόνων) με το να συνδεθούν στη θύρα SSL αλλά χωρίς να συμμετέχουν στην χειραψία SSL.

Εκδόθηκε: 12/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3315

Το authz.c στη μονάδα mod_dav_svn για τον HTTP διακομιστή Apache, όταν ενεργοποιείται το SVNPathAuthz short_circuit, δεν χειρίζεται σωστά μία ονομασμένη αποθήκη σαν ένα rule scope (αν μια οντότητα είναι ορατή ή προσπελάσιμη σε συγκεκριμένα μέρη του κώδικα), το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να υπερβούν τους προοριζόμενους περιορισμούς ασφαλείας μέσω svn εντολών.

Εκδόθηκε: 04/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-1623

Η διαρροή μνήμης στην λειτουργία apr_brigade_split_line στο στοιχείο buckets/apr_brigade.c στο εργαλείο της βιβλιοθήκης Apache Portable Runtime, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μια άρνηση υπηρεσίας DoS (κατανάλωση μνήμης) μέσω απροσδιόριστων παραγόντων που σχετίζονται με την καταστροφή ενός APR κάδου.

Εκδόθηκε: 04/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-2952

Ο διακομιστής κυκλοφορίας του Apache, δεν επιλέγει σωστά τις πηγές των θυρών DNS και των συναλλαγών των IDs και δεν χρησιμοποιεί σωστά τα πεδία ερωτημάτων των DNS για να επικυρώσει τις απαντήσεις , κάτι το οποίο διευκολύνει τους επιτιθέμενους που χρησιμοποιούν την επίθεση man-in-the-middle για να δηλητηριάσουν την εσωτερική DNS cache μέσω μίας επεξεργασμένης απάντησης.

Εκδόθηκε: 13/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-1325

Η ευπάθεια παραποίησης Cross-site αιτημάτων (CSRF) στο πακέτο apache2-slms στον διακομιστή SUSE Lifecycle Management 1.0 στον SUSE Linux Enterprise (SLE) 11, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να χακάρουν την αυθεντικότητα των ανυποψίαστων θυμάτων μέσω παραγόντων που σχετίζονται με την λανθασμένη αναφορά των παραμέτρων .

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2234

Η ευπάθεια παραποίησης Cross-site αιτημάτων (CSRF) στον Apache CouchDB 0.8.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να χακάρουν την αυθεντικότητα των διαχειριστών για να κατευθύνουν αιτήματα σε ένα κακόβουλο URL εγκατάστασης.

Εκδόθηκε: 19/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-2791

Το mod_proxy στο httpd στον HTTP διακομιστή Apache 2.2.9, όταν τρέχει στα Unix, δεν κλείνει την backend σύνδεση, όταν συμβεί ένα timeout και διαβάζει μία απάντηση από μία επίμονη σύνδεση, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες σε ευκαιριακές περιστάσεις να επιτεθούν για να κερδίσουν μία πιθανή ευαίσθητη απάντηση, η οποία προοριζόταν για ένα διαφορετικό πελάτη μέσω ενός κανονικού HTTP αιτήματος.

Εκδόθηκε: 05/08/2010

Σοβαρότητα: Μέτρια

CVE-2009-2696

Η ευπάθεια του Cross-site scripting (XSS) στην εφαρμογή του ημερολογίου στην δικτυακή εφαρμογή στον Apache Tomcat στα Red Hat Enterprise Linux 5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα δικτυακό script ή HTML μέσω της παραμέτρου του χρόνου , που σχετίζεται με το "invalid HTML."

Εκδόθηκε: 05/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-1452

Οι μονάδες (1) mod_cache και (2) mod_dav στον HTTP διακομιστή Apache 2.2.x , επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα διαδικασιών) μέσω ενός αιτήματος που δεν έχει μονοπάτι.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Μέτρια

CVE-2010-2227

Ο Apache Tomcat 5.5.0, δεν χειρίζεται κατάλληλα μια μη έγκυρη Transfer-Encoding επικεφαλίδα , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μια άρνηση υπηρεσίας (DoS) (outage εφαρμογών) ή να αποκτήσουν ευαίσθητες πληροφορίες μέσω μιας επεξεργασμένης επικεφαλίδας η οποία αλληλεπιδρά με "την ανακύκλωση ενός buffer."

Εκδόθηκε: 13/07/2010

Σοβαρότητα: Μέτρια

CVE-2010-2068

Το mod_proxy_http.c στον HTTP διακομιστή Apache 2.2.9, σε συγκεκριμένες τροποποιήσεις με proxy worker pools, δεν εντοπίζει επιτυχώς τα timeouts, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν μία πιθανώς ευαίσθητη απάντηση η οποία προορίζεται για ένα διαφορετικό πελάτη σε ευκαιριακές συνθήκες μέσω ενός HTTP αιτήματος.

Εκδόθηκε: 18/06/2010

Σοβαρότητα: Μέτρια

CVE-2010-1587

Το Jetty ResourceHandler στον Apache ActiveMQ 5.xζ, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν JSP source κώδικα μέσω ενός αρχικού substring (//) σε ένα URI για το admin/index.jsp, το admin/queues.jsp ή το admin/topics.jsp.

Εκδόθηκε: 28/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-1157

Ο Apache Tomcat 5.5.0, μπορεί να επιτρέψει σε απομακρυσμένους χρήστες να επιτεθούν για να ανακαλύψουν το hostname του διακομιστή ή την διεύθυνση IP, με την αποστολή ενός αιτήματος για ένα πόρο που απαιτεί basic ή digest αυθεντικοποίηση , και έπειτα διαβάζει το πεδίο realm στην επικεφαλίδα WWW-Authenticate στην απάντηση.

Εκδόθηκε: 23/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-1151

Η κατάσταση Race στη μονάδα mod_auth_shadow για τον HTTP διακομιστή Apache, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την αυθεντικοποίηση, να διαβάσουν και πιθανώς να μετατρέψουν δεδομένα μέσω παραγόντων που σχετίζονται με κακόβουλη αλληλεπίδραση με μία εξωτερική εφαρμογή βοηθείας για επικύρωση των πιστοποιητικών.

Εκδόθηκε: 20/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-0432

Οι πολλαπλές ευπάθειες cross-site scripting (XSS) στο στοιχείο Apache Open For Business Project 09.04 (δηλ. OFBiz), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να τοποθετήσουν αυθαίρετα web script ή HTML μέσω των παραμέτρων productStoreId στο control/expntProductListing, partyId στο partymgr/control/ viewprofile, start στο myportal/control/showPortalPage, contentId στο ecommerce /control/ ViewBlogArticle,entityName στο webtools/control/FindGeneric, subject, content σε ένα ακαθόριστο στοιχείο κάτω από το ecommerce/control/contactus.

Εκδόθηκε: 15/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-1244

Η ευπάθεια παραποίησης Cross-site αιτήματος (CSRF) στο στοιχείο createDestination.action στον Apache ActiveMQ, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να χακάρουν την αυθεντικότητα των ακαθόριστων θυμάτων, για αιτήματα τα οποία δημιουργούν ουρές μέσω της παραμέτρου JMSDestination σε μια ενέργεια στην ουρά.

Εκδόθηκε: 05/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-0009

Ο Apache CouchDB (εκδόσεις από 0.8.0 μέχρι 0.10.1), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες με την μέτρηση του χρόνου ολοκλήρωσης των διαδικασιών που ελέγχουν τα hashes ή τον κωδικό πρόσβασης.

Εκδόθηκε: 04/05/2010

Σοβαρότητα: Μέτρια

CVE-2010-0434

Η λειτουργία ap_read_request στο στοιχείο server/protocol.c στον HTTP διακομιστή Apache 2.2.x, όταν ένα multithreaded MPM χρησιμοποιείται, δεν χειρίζεται κατάλληλα τις επικεφαλίδες στα υποαιτήματα σε συγκεκριμένες περιστάσεις που περιέχουν ένα αίτημα γονιού, το οποίο μπορεί να επιτρέψει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες μέσω ενός επεξεργασμένου αιτήματος, το οποίο δίνει πρόσβαση σε θέσεις μνήμης που σχετίζονται με ένα προηγούμενο αίτημα.

Εκδόθηκε: 05/03/2010

Σοβαρότητα: Μέτρια

CVE-2010-0408

Η λειτουργία ap_proxy_ajp_request στο στοιχείο mod_proxy_ajp.c στον HTTP διακομιστή Apache 2.2.x, δεν χειρίζεται κατάλληλα συγκεκριμένες περιπτώσεις στις οποίες ο πελάτης δεν στέλνει αίτημα, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (outage διακομιστή) μέσω ενός επεξεργασμένου αιτήματος ,σχετικό με τη χρήση ενός κώδικα για σφάλματα 500 αντί για το κατάλληλο κώδικα για σφάλματα 400.

Εκδόθηκε: 05/03/2010

Σοβαρότητα: Μέτρια

CVE-2010-0010

Η υπερχείλιση ακεραίων στην λειτουργία ap_proxy_send_fb στο στοιχείο mod_proxy στον HTTP διακομιστή Apache, επιτρέπει σε απομακρυσμένους διακομιστές να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) ή να εκτελέσουν κώδικα αυθαίρετα μέσω ενός μεγάλου μεγέθους κομματιού, το οποίο θα ενεργοποιήσει μια υπερχείλιση buffer.

Εκδόθηκε: 02/02/2010

Σοβαρότητα: Μέτρια

CVE-2009-2902

Η ευπάθεια του περάσματος ενός καταλόγου στον Apache Tomcat 5.5.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαγράψουν τα αρχεία του καταλόγου work μέσω ακολουθιών μετατροπής του καταλόγου σε ένα όνομα αρχείου WAR.

Εκδόθηκε: 28/01/2010

Σοβαρότητα: Μέτρια

6. ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ MYSQL

6.1 ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ MYSQL

CVE-2011-0432

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στην μέθοδο get_userinfo στη κλάση MySQLAuthHandler στο PyWebDAV, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω των ορισμάτων user ή pw.

Εκδόθηκε: 14/03/2011

Σοβαρότητα: Υψηλή

CVE-2010-1865

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο ClanSphere 2009.0.3 , επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της IP διεύθυνσης στην λειτουργία cs_getip στο generate.php στη μονάδα Captcha, της παραμέτρου s_email στην λειτουργία cs_sql_select στον driver της βάσης δεδομένων MySQL (mysql.php).

Εκδόθηκε : 07/05/2010

Σοβαρότητα: Υψηλή

CVE-2010-1583

Η ευπάθεια εισαγωγής ερωτήματος Sql στην λειτουργία loadByKey στην κλάση TznDbConnection στο Tirzen Framework 1.5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν Sql εντολές αυθαίρετα μέσω του πεδίου ονόματος του χρήστη στη προσπάθεια σύνδεσης.

Εκδόθηκε: 06/05/2010

Σοβαρότητα: Υψηλή

CVE-2009-4484

Οι πολλαπλές υπερχειλίσεις των stack-based buffers στην λειτουργία CertDecoder:: GetName στο TaoCrypt στο yaSSL, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν κώδικα αυθαίρετα ή να προκαλέσουν άρνηση υπηρεσίας (DoS) (καταστροφή μνήμης και κρασάρισμα των δαιμόνων) με την καθιέρωση μιας SSL σύνδεσης και στέλνοντας ένα πιστοποιητικό πελάτη X.509 με ένα επεξεργασμένο όνομα πεδίου , όπως παρουσιάζεται από το mysql_overflow1.py και από το vd_mysql5 στο VulnDisco Pack Professional 8.11.

Εκδόθηκε: 30/12/2009

Σοβαρότητα: Υψηλή

CVE-2009-2942

Οι συνδέσεις mysql-ocaml 1.0.4 για την MySQL δεν υποστηρίζουν κατάλληλα την λειτουργία mysql_real_escape_string, πράγμα το οποίο μπορεί να επιτρέψει σε απομακρυσμένους χρήστες να επιτεθούν για να αυξήσουν τα ζητήματα απόδρασης που έχουν να κάνουν με την κωδικοποίηση χαρακτήρων πολλών bytes.

Εκδόθηκε: 22/10/2009

Σοβαρότητα: Υψηλή

CVE-2009-3102

Η υπορουτίνα doHotCopy στο socket-server.pl στο Zmanda Recovery Manager (ZRM) για την MySQL 2.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν εντολές αυθαίρετα μέσω παραγόντων που αφορούν μια επεξεργασμένη μεταβλητή $MYSQL_BINPATH .

Εκδόθηκε: 08/09/2009

Σοβαρότητα: Υψηλή

CVE-2009-2929

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο TGS Content Management 0.x, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα εντολές Sql μέσω αρκετών παραμέτρων του (tgs_language_id, του tpl_dir, referer, user-agent, site, option, db_optimization, owner, admin_email, select_language, db_host για cms/index.php, cmd, s_dir, minutes, s_mask, test3_mp, test15_file1, submit, brute_method, ftp_server_port, userfile 14, subj, mysql_l, action, userfile 1 για cms/frontpage_ception.php) .

Εκδόθηκε: 21/08/2009

Σοβαρότητα: Υψηλή

CVE-2008-6992

Το τείχος προστασίας GreenSQL, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για παρακάμψουν τον μηχανισμό προστασίας για την εισαγωγή ερωτήματος Sql , μέσω μίας πρότασης WHERE η οποία περιέχει μία έκφραση όπως "x=y=z", η οποία επιτυχώς αναλύεται από την MySQL.

Εκδόθηκε: 19/08/2009

Σοβαρότητα: Υψηλή

CVE-2009-2446

Οι ευπάθειες διαμόρφωσης αλφαριθμητικών στη λειτουργία dispatch_command στην libmysqld/sql_parse.cc στην MySQL, επιτρέπουν σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) και πιθανώς να έχουν και άλλες απροσδιόριστες επιρροές μέσω format string specifiers , σε ένα όνομα βάσης δεδομένων COM_CREATE_DB ή σε ένα αίτημα COM_DROP_DB .

Εκδόθηκε: 13/07/2009

Σοβαρότητα: Υψηλή

CVE-2008-6813

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο phpWebNews 0.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετες εντολές Sql μέσω της παραμέτρου id_kat.

Εκδόθηκε: 22/05/2009

Σοβαρότητα: Υψηλή

CVE-2008-6812

Η ευπάθεια εισαγωγής ερωτήματος Sql στο bukutamu.php στο phpWebNews 0.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν εντολές Sql αυθαίρετα μέσω της παραμέτρου det.

Εκδόθηκε: 22/05/2009

Σοβαρότητα: Υψηλή

CVE-2009-1246

Οι πολλαπλές ευπάθειες περάσματος καταλόγου στο Blogplus 1.0, επιτρέπει σε απομακρυσμένους χρήστες να περιλάβουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω της .. (τελεία τελεία)

Εκδόθηκε: 06/04/2009

Σοβαρότητα: Υψηλή

CVE-2009-1208

Η ευπάθεια εισαγωγής ερωτήματος Sql στο auth2db 0.2.5, χρησιμοποιεί την λειτουργία addslashes αντί για τη mysql_real_escape_string λειτουργία, η οποία επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν επιθέσεις εισαγωγής ερωτήματος Sql χρησιμοποιώντας κωδικοποίηση χαρακτήρων πολλών byte.

Εκδόθηκε: 01/04/2009

Σοβαρότητα: Υψηλή

CVE-2009-0919

Το XAMPP εγκαθιστά πολλαπλά πακέτα με μη ασφαλή προεπιλεγμένο κωδικό πρόσβασης, πράγμα το οποίο διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν πρόσβαση μέσω του "lampp" προεπιλεγμένου κωδικού πρόσβασης για τον λογαριασμό "nobody" με την συμπεριλαμβανόμενη ProFTPD εγκατάσταση, του κενού προεπιλεγμένου κωδικού πρόσβασης για τον λογαριασμό "root" με την συμπεριλαμβανόμενη MySQL εγκατάσταση, του κενού προεπιλεγμένου κωδικού πρόσβασης για τον λογαριασμό "pma" με την phpMyAdmin εγκατάσταση, και πιθανώς και άλλους απροσδιόριστους κωδικούς πρόσβασης .

Εκδόθηκε: 16/03/2009

Σοβαρότητα: Υψηλή

CVE-2009-0617

Η εφαρμογή διαχείρισης δικτύου της Cisco (ANM), χρησιμοποιεί ένα προεπιλεγμένο root κωδικό πρόσβασης στη MySQL, ο οποίος διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετες εντολές λειτουργίας του συστήματος ή να αλλάξει αρχεία του συστήματος.

Εκδόθηκε: 26/02/2009

Σοβαρότητα: Υψηλή

CVE-2008-6287

Πολλαπλές ευπάθειες συνυπολογισμού σε απομακρυσμένα αρχεία PHP στο Broadcast Machine 0.1, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο baseDir για το MySQLController.php, το SQLController.php, το SetupController.php, το VideoController.php και το ViewController.php .

Εκδόθηκε: 25/02/2009

Σοβαρότητα: Υψηλή

CVE-2008-2384

Η ευπάθεια εισαγωγής ερωτήματος Sql στο mod_auth_mysql.c στη μονάδα mod-auth-mysql για τον HTTP διακομιστή Apache 2.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα εντολές Sql μέσω κρυπτογράφησης χαρακτήρων πολλών byte για να κάνουν απροσδιόριστη εισαγωγή δεδομένων.

Εκδόθηκε: 22/01/2009

Σοβαρότητα: Υψηλή

CVE-2008-5738

Το ημερολόγιο Nodstrum MySQL (εκδόσεις 1.1 και 1.2) , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την αυθεντικοποίηση και να κερδίσουν τη πρόσβαση που έχει και ο διαχειριστής ρυθμίζοντας το nodstrumCalendarV2 cookie για 1.

Εκδόθηκε: 26/12/2008

Σοβαρότητα: Υψηλή

CVE-2008-5737

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο ημερολόγιο Nodstrum MySQL (εκδόσεις 1.1 και 1.2) , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετες εντολές SQL μέσω της παραμέτρου του ονόματος χρήστη.

Εκδόθηκε: 26/12/2008

Σοβαρότητα: Υψηλή

CVE-2008-5069

Η ευπάθεια εισαγωγής ερωτήματος Sql στο go.php στο Panuwat PromoteWeb MySQL, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα εντολές Sql μέσω της παραμέτρου id.

Εκδόθηκε: 14/11/2008

Σοβαρότητα: Υψηλή

CVE-2008-3090

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο index.php στο BlognPlus της MySQL, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν εντολές Sql αυθαίρετα μέσω παραμέτρων .

Εκδόθηκε: 09/07/2008

Σοβαρότητα: Υψηλή

CVE-2008-0226

Οι πολλαπλές υπερχειλίσεις buffer στην yaSSL 1.7.5, όπως χρησιμοποιείται στην MySQL, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω της λειτουργίας ProcessOldClientHello στο handshake.cpp ή του "input_buffer& operator>>" στο yassl_imp.cpp.

Εκδόθηκε: 10/01/2008

Σοβαρότητα: Υψηλή

CVE-2008-0227

Το yaSSL 1.7.5 όπως χρησιμοποιείται στην MySQL, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα) μέσω ενός πακέτου Hello που περιέχει μια αξία μεγάλου μεγέθους , πράγμα το οποίο ενεργοποιεί μια διαδικασία «υπερανάγνωσης» του buffer στην λειτουργία HASHwithTransform::Update στην hash.cpp.

Εκδόθηκε: 10/01/2008

Σοβαρότητα: Υψηλή

CVE-2007-6345

Η ευπάθεια εισαγωγής ερωτήματος Sql στο aurora framework , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν εντολές Sql αυθαίρετα μέσω απροσδιόριστων παραγόντων, πιθανόν την παράμετρο αξίας για την λειτουργία pack_var στη μονάδα/db.lib/db_mysql.lib.

Εκδόθηκε: 13/12/2007

Σοβαρότητα: Υψηλή

6.2 ΣΥΝΗΘΙΣΜΕΝΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ MYSQL

CVE-2011-2531

Το Prosody 0.8.x, όταν χρησιμοποιείται στη MySQL, αναθέτει ένα λανθασμένο τύπο δεδομένων στην στήλη της αξίας σε συγκεκριμένους πίνακες , πράγμα το οποίο μπορεί να επιτρέψει απομακρυσμένους χρήστες να κάνουν επίθεση για να πραγματοποιήσουν μια άρνηση υπηρεσίας (DoS) (αποκοπή δεδομένων) με την αποστολή μεγάλου αριθμού δεδομένων.

Εκδόθηκε: 22/06/2011

Σοβαρότητα: Μέτρια

CVE-2010-3056

Οι πολλαπλές ευπάθειες cross-site scripting (XSS) στο phpMyAdmin 2.11.x , επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν web script ή HTML αυθαίρετα μέσω παραγόντων .

Εκδόθηκε: 24/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-3064

Μια stack-based υπερχείλιση buffer στη λειτουργία php_mysqlnd_auth_write στην επέκταση Mysqlnd της PHP 5.3, επιτρέπει σε context-dependent επιτιθέμενους να προκαλέσουν μια άρνηση υπηρεσίας (DoS) (κρασάρισμα) και πιθανώς να εκτελέσουν κώδικα αυθαίρετα μέσω ενός μεγάλου όνοματος χρήστη ή ένος γνωρίσματος για όνομα βάσης δεδομένων για το mysql_connect ή τη λειτουργία mysqli_connect.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-3063

Η λειτουργία php_mysqlnd_read_error_from_line στην επέκταση Mysqlnd της PHP 5.3, δεν υπολογίζει σωστά το μήκος του buffer, κάτι το οποίο επιτρέπει σε context-dependent επιτιθέμενους να ενεργοποιήσουν μια heap-based υπερχείλιση buffer μέσω επεξεργασμένων εισόδων και να προκαλέσουν μια αρνητική αξία μήκους.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-3062

Το mysqlnd_wireproforcol.c στην επέκταση Mysqlnd της PHP 5.3, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν ευαίσθητη μνήμη μέσω μιας τροποποιημένης αξίας μήκους , την οποία δεν χειρίζεται κατάλληλα η λειτουργία php_mysqlnd_ok_read ή και για να ενεργοποιήσουν μια heap-based υπερχείλιση buffer μέσω μιας τροποποιημένης αξίας μήκους , την οποία δεν χειρίζεται κατάλληλα η λειτουργία php_mysqlnd_rset_header_read.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-1850

Η υπερχείλιση buffer στην MySQL 5.0, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους επιτιθέμενους να εκτελέσουν αυθαίρετα κώδικα μέσω της εντολής COM_FIELD_LIST με ένα μεγάλο σε μήκος όνομα πίνακα.

Εκδόθηκε: 08/06/2010

Σοβαρότητα: Μέτρια

CVE-2010-1849

Η λειτουργία my_net_skip_rest στην MySQL 5.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση CPU και εύρους ζώνης) με την αποστολή μεγάλου αριθμού πακέτων που υπερβαίνουν το μέγιστο μήκος.

Εκδόθηκε: 08/06/2010

Σοβαρότητα: Μέτρια

CVE-2010-1848

Η ευπάθεια περάσματος καταλόγου στην MySQL 5.0, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να παρακάμψουν τα προοριζόμενα προνόμια του πίνακα για να διαβάσουν τους ορισμούς πεδίων των αυθαίρετων πινάκων και στην έκδοση 5.1 για να διαβάσουν ή να διαγράψουν τα περιεχόμενα των αυθαίρετων πινάκων , μέσω της .. (τελείας τελείας) στο όνομα ενός πίνακα.

Εκδόθηκε: 08/06/2010

Σοβαρότητα: Μέτρια

CVE-2010-2003

Η ευπάθεια του Cross-site scripting (XSS) στην misc/get_admin.php στο Advanced Poll 2.08, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα κώδικα web ή HTML μέσω της παραμέτρου mysql_host.

Εκδόθηκε: 20/05/2010

Σοβαρότητα: Μέτρια

CVE-2010-1621

Η λειτουργία mysql_uninstall_plugin στην MySQL, δεν ελέγχει τα προνόμια πριν απεγκαταστήσει ένα plugin, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να απεγκαταστήσουν αυθαίρετα plugins μέσω της εντολής UNINSTALL PLUGIN .

Εκδόθηκε: 14/05/2010

Σοβαρότητα: Μέτρια

CVE-2009-4833

Το MySQL Connecforr/NET, όταν χρησιμοποιεί κωδικοποίηση δεν ελέγχει τα πιστοποιητικά SSL στη διάρκεια της σύνδεσης , πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν μία επίθεση man-in-the-middle με ένα παραποιημένο πιστοποιητικό SSL.

Εκδόθηκε: 29/04/2010

Σοβαρότητα: Μέτρια

CVE-2010-0336

Η αδιευκρίνιστη ευπάθεια στο kiddog_mysqldumper extension 0.0.3 στο TYPO3, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες μέσω άγνωστων παραγόντων επίθεσης.

Εκδόθηκε: 15/01/2010

Σοβαρότητα: Μέτρια

CVE-2009-4030

Η MySQL 5.1.x, επιτρέπει σε τοπικούς χρήστες να παρακάμψουν συγκεκριμένους ελέγχους για τα προνόμια καλώντας τη δημιουργία πίνακα (create table) στο MyISAM πίνακα με τροποποιημένο κατάλογο δεδομένων ή κατάλογο περιεχομένων , ορίσματα τα οποία αρχικά σχετίζονται με ονόματα μονοπατιών χωρίς symlinks και που μπορούν να δείξουν σε πίνακες σε μέλλοντα χρόνο, όταν το όνομα του μονοπατιού είναι τροποποιημένο για να περιέχει ένα symlink για ένα υποκατάλογο της MySQL του καταλόγου δεδομένων home , που σχετίζεται με λάθος υπολογισμό της αξίας mysql_unpacked_real_data_home.

Εκδόθηκε: 30/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-4028

Η λειτουργία vio_verify_callback στη MySQL 5.0.x, όταν χρησιμοποιείται το OpenSSL, δέχεται τη τιμή του μηδέν για το βάθος του X.509 πιστοποιητικού, το οποίο επιτρέπει σε man-in-the-middle χρήστες να επιτεθούν για να παραποιήσουν αυθαίρετα τους SSL-based MySQL διακομιστές μέσω ενός επεξεργασμένου πιστοποιητικού, όπως καταδεικνύεται από ένα πιστοποιητικό που παρουσιάζεται από έναν διακομιστή που έχει συνδεθεί με τη yaSSL βιβλιοθήκη.

Εκδόθηκε: 30/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-4019

Η mysqld στην MySQL 5.0.x, δεν χειρίζεται σωστά τα λάθη κατά τη διάρκεια της εκτέλεσης συγκεκριμένων select δηλώσεων με υποερωτήματα και δεν διατηρεί συγκεκριμένες σημαίες null_value κατά τη διάρκεια της εκτέλεσης των δηλώσεων που χρησιμοποιούν τη λειτουργία GeomFromWKB, κάτι το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) μέσω μίας επεξεργασμένης δήλωσης.

Εκδόθηκε: 30/11/2009

Σοβαρότητα: Μέτρια

CVE-2008-7247

Το sql/sql_table.cc στην MySQL 5.0.x, όταν ο κατάλογος δεδομένων home περιέχει ένα symlink για ένα διαφορετικό αρχείο συστήματος, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να παρακάμψουν τους συγκεκριμένους περιορισμούς πρόσβασης καλώντας την δημιουργία πίνακα (create table) με το κατάλογο δεδομένων ή το κατάλογο περιεχόμενων, επιχείρημα που αναφέρεται για ένα υποκατάλογο που απαιτεί να ακολουθήσει αυτό το symlink.

Εκδόθηκε: 30/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-3696

Η ευπάθεια του Cross-site scripting (XSS) στον phpMyAdmin 2.11.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web κώδικα ή HTML μέσω ενός επεξεργασμένου ονόματος για έναν MySQL πίνακα.

Εκδόθηκε: 16/10/2009

Σοβαρότητα: Μέτρια

CVE-2008-6655

Οι πολλαπλές ευπάθειες cross-site κρυπτογραφήσεων (XSS) στο GEDCOM_TO _MYSQL 2, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web κώδικα ή HTML μέσω διαφόρων παραμέτρων (nom παράμετροι για php/preno.php, nom_branche για php/index.php , prenom παράμετροι για php/info.php).

Εκδόθηκε: 07/04/2009

Σοβαρότητα: Μέτρια

CVE-2009-0819

Το sql/item_xmlfunc.cc στη MySQL 5.1, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν μία άρνηση υπηρεσίας (DoS) (κρασάρισμα) .

Εκδόθηκε: 05/03/2009

Σοβαρότητα: Μέτρια

CVE-2008-6193

Το Sam Crew MyBlog αποθηκεύει τους κωδικούς πρόσβασης σε καθαρό κείμενο στην βάση δεδομένων της MySQL, το οποίο επιτρέπει σε context-dependent χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες.

Εκδόθηκε: 19/02/2009

Σοβαρότητα: Μέτρια

CVE-2009-0543

Ο διακομιστής ProFTPD 1.3.1, με την NLS υποστήριξη ενεργοποιημένη, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους μηχανισμούς προστασίας από την εισαγωγή ερωτήματος Sql , μέσω κωδικοποίησης χαρακτήρων πολλών byte.

Εκδόθηκε: 12/02/2009

Σοβαρότητα: Μέτρια

CVE-2008-3820

Ο Cisco Security Manager (εκδόσεις 3.1 και 3.2), όταν χρησιμοποιείται ο Cisco IPS Event Viewer (IEV) , εκθέτει TCP πόρτες που χρησιμοποιούνται από το δαίμονα της MySQL και τον διακομιστή IEV , πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν πρόσβαση σε επίπεδο root στο IEV μέσω της χρήσης των TCP συνόδων για αυτές τις πόρτες.

Εκδόθηκε: 22/01/2009

Σοβαρότητα: Μέτρια

CVE-2008-4455

Η ευπάθεια περάσματος καταλόγου στο index.php στη MySQL Quick Admin 1.5.5, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν και να εκτελέσουν αρχεία αυθαίρετα μέσω της .. (τελείας τελείας) στο cookie που αφορά τη γλώσσα.

Εκδόθηκε: 06/10/2008

Σοβαρότητα: Μέτρια

CVE-2008-4454

Η ευπάθεια περάσματος καταλόγου στο EKINdesigns στην MySQL Quick Admin 1.5.5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν και να εκτελέσουν αυθαίρετα αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο lang για το actions.php.

Εκδόθηκε: 06/10/2008

Σοβαρότητα: Μέτρια

CVE-2008-4180

Η αδιευκρίνιστη ευπάθεια στο db.php στο NooMS 1.1, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διευθύνουν επιθέσεις στους κωδικούς πρόσβασης μέσω ενός ονόματος χρήστη στην παράμετρο g_dbuser και ένα κωδικό πρόσβασης στην παράμετρο g_dbpwd , και πιθανώς μια αξία παραμέτρου "localhost" g_dbhost , σχετιζόμενη με την ευπάθεια ωμής βίας.

Εκδόθηκε: 23/09/2008

Σοβαρότητα: Μέτρια

CVE-2008-4106

Το WordPress δεν χειρίζεται κατάλληλα τις ειδοποιήσεις της MySQL για την εισαγωγή των αλφαριθμητικών ονομάτων χρήστη, τα οποία έχουν υπερβεί το μέγιστο πλάτος της στήλης user_login, και δεν χειρίζεται σωστά τους χαρακτήρες του κενού όταν συγκρίνει τα ονόματα χρήστη, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αλλάξουν αυθαίρετα τον κωδικό πρόσβασης του χρήστη με μία τυχαία τιμή, με την εγγραφή ενός παρόμοιου ονόματος χρήστη και έπειτα να απαιτούν μια αναστοιχειοθέτηση του κωδικού πρόσβασης.

Εκδόθηκε: 18/09/2008

Σοβαρότητα: Μέτρια

CVE-2008-4098

Η MySQL, επιτρέπει σε τοπικούς χρήστες να παρακάμψουν συγκεκριμένους έλεγχους προνομίων με τη δημιουργία πίνακα (create table) στον πίνακα MyISAM με τροποποιημένο το data directory ή το index directory, ορίσματα τα οποία αρχικά σχετιζόντουσαν με ονόματα μονοπατιών χωρίς symlinks, και μπορούν να δείξουν σε πίνακες που θα δημιουργηθούν, στους οποίους το όνομα του μονοπατιού είναι τροποποιημένο να περιέχει ένα symlink για ένα υποκατάλογο του home data καταλόγου της MySQL .

Εκδόθηκε: 18/09/2008

Σοβαρότητα: Μέτρια

CVE-2008-3963

Η MySQL 5.0, δεν χειρίζεται σωστά το token b" , δηλαδή ένα literal κενό αλφαριθμητικό σε bit , το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μια άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) χρησιμοποιώντας αυτό το token σε μία δήλωση της Sql.

Εκδόθηκε: 11/09/2008

Σοβαρότητα: Μέτρια

CVE-2008-3846

Η ευπάθεια Cross-site scripting (XSS) στη mysql-lists 1.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web κώδικα ή HTML μέσω αδιευκρίνιστων παραγόντων.

Εκδόθηκε: 27/08/2008

Σοβαρότητα: Μέτρια

CVE-2008-3840

Το Crafty Syntax Live Help (CSLH) 2.14.6, αποθηκεύει τον κωδικό πρόσβασης σε καθαρό κείμενο σε μια βάση δεδομένων της MySQL, κάτι το οποίο επιτρέπει σε context-dependent χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες .

Εκδόθηκε: 27/08/2008

Σοβαρότητα: Μέτρια

CVE-2008-3582

Η ευπάθεια εισαγωγή ερωτήματος Sql στο login.php στο Keld PHP-MySQL News Script 0.7.1, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα εντολές Sql μέσω της παραμέτρου του ονόματος χρήστη.

Εκδόθηκε: 10/08/2008

Σοβαρότητα: Μέτρια

CVE-2008-2079

Το MySQL 4.1.x, επιτρέπει σε τοπικούς χρήστες να παρακάμψουν συγκεκριμένους ελέγχους προνομίων καλώντας τη δημιουργία πίνακα (create table) στον πίνακα MyISAM με τροποποιημένα το data directory ή το index directory, ορίσματα που είναι ενσωματωμένα στο κατάλογο δεδομένων home της MySQL, τα οποία μπορούν να δείξουν τους πίνακες που θα δημιουργηθούν στο μέλλον.

Εκδόθηκε: 05/05/2008

Σοβαρότητα: Μέτρια

CVE-2008-2029

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο setup_mysql.php και στο setup_options.php στο miniBB 2.2, όταν το register_globals είναι ενεργοποιημένο , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου xtr σε μία δράση userinfo για index.php.

Εκδόθηκε: 30/04/2008

Σοβαρότητα: Μέτρια

CVE-2008-1711

Το Terong PHP Photo Gallery 1.0, αποθηκεύει τους κωδικούς πρόσβασης σε καθαρό κείμενο σε μια βάση δεδομένων της MySQL , κάτι το οποίο επιτρέπει σε context-dependent χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες.

Εκδόθηκε: 09/04/2008

Σοβαρότητα: Μέτρια

CVE-2008-1486

Η ευπάθεια εισαγωγής ερωτήματος Sql στο Phorum, όταν το mysql_use_ft είναι απενεργοποιημένο, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω μιας non-fulltext αναζήτησης.

Εκδόθηκε: 24/03/2008

Σοβαρότητα: Μέτρια

CVE-2008-0249

Το PHP Webquest 2.6, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να ανακτήσουν πιστοποιητικά της βάσης δεδομένων μέσω ενός άμεσου αιτήματος για το admin/backup_phpwebquest.php, το οποίο θα διαρρέει τα πιστοποιητικά σε ένα μήνυμα λάθους αν μια κλήση στο /usr/bin/mysqldump αποτύχει.

Εκδόθηκε: 12/01/2008

Σοβαρότητα: Μέτρια

7. ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PHP

7.1. ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PHP

CVE-2011-2181

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο A Really Simple Chat (ARSC) 3.3-rc2, επιτρέπουν στους απομακρυσμένους χρήστες να εκτελέσουν αυθαίρετα Sql εντολές μέσω των παραμέτρων arsc_user στο base/admin/edit_user.php, arsc_layout_id στο base/admin/edit_layout.php, arsc_room στο base/admin/edit_room.php.

Εκδόθηκε: 29/06/2011

Σοβαρότητα: Υψηλή

CVE-2011-1480

Η ευπάθεια εισαγωγής ερωτήματος Sql στο admin.php στο Francisco Burzi PHP-Nuke 8.0, επιτρέπει σε απομακρυσμένους χρήστες την εκτέλεση αυθαίρετα Sql εντολών μέσω της παραμέτρου chng_uid.

Εκδόθηκε: 21/06/2011

Σοβαρότητα: Υψηλή

CVE-2010-3077

Η ευπάθεια Cross-site scripting (XSS) στο util/icon_browser.php στο Horde Application Framework, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου subdir.

Εκδόθηκε: 09/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-1523

Πολλαπλές heap-based υπερχειλίσεις buffer στο Winamp, μπορούν να επιτρέψούν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου VP6 αρχείου video ή video stream.

Εκδόθηκε: 06/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-4185

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Energine, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετες Sql εντολές μέσω του NRGNSID cookie.

Εκδόθηκε: 05/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-2941

Το ipp.c στο CUPS 1.4.4, δεν κατανέμει σωστά την μνήμη για τις τιμές των παραμέτρων με λανθασμένους τύπους αλφαριθμητικών δεδομένων, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μία άρνηση υπηρεσίας (DoS) (use-after-free και κρασάρισμα εφαρμογής) ή πιθανόν να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου IPP αιτήματος.

Εκδόθηκε: 05/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-4006

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο search.php στο WSN Links 5.0.x, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου namecondition ή της παραμέτρου namesearch.

Εκδόθηκε: 03/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-4147

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο Pentasoft Avactis Shopping Cart 1.9.1, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της επικεφαλίδας User-Agent για το index.php και για το product-list.php .

Εκδόθηκε: 02/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-4025

Η αδιευκρίνιστη ευπάθεια στο Doc Viewer στο HP Palm webOS 1.4.1, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου εγγράφου.

Εκδόθηκε: 28/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3714

Το jumpUrl της εφαρμογής στο TYPO3 4.2.x, δεν συγκρίνει σωστά συγκεκριμένες hash αξίες κατά τη διάρκεια αποφάσεων πρόσβασης - ελέγχου, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχεία μέσω αδιευκρίνιστων παραγόντων.

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3076

Η λειτουργία φίλτρου στο php/src/include.php στο Simple Management, δεν παρέχει μια συγκεκριμένη κανονική έκφραση , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν επιθέσεις εισαγωγής ερωτήματος Sql και να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου username για την σελίδα εισόδου του admin.

Εκδόθηκε: 14/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-2797

Η ευπάθεια περάσματος καταλόγου στο lib/translation.functions.php στο CMS Made Simple, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να συμπεριλάβουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω της .. (τελείας τελείας) στην προεπιλεγμένη παράμετρο _cms_lang για ένα script του admin, όπως παρουσιάζεται από το admin/addbookmark.php.

Εκδόθηκε: 08/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3742

Οι πολλαπλές ευπάθειες συνυπολογισμού σε απομακρυσμένα αρχεία στο themes/default/index.php στο Free Simple CMS 1.0, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στη παράμετρο meta ή στη παράμετρο phpincdir.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3307

Οι πολλαπλές ευπάθειες συνυπολογισμού σε απομακρυσμένα αρχεία στο themes/ default /index.php στο Free Simple CMS 1.0, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στη παράμετρο body, στη παράμετρο footer, στη παράμετρο header, στη παράμετρο menu_left, στη παράμετρο menu_right .

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3688

Η ευπάθεια περάσματος καταλόγου στο ADMIN/login.php στο NetArtMEDIA WebSiteAdmin, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να συμπεριλάβουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω των διασταυρωμένων ακολουθιών καταλόγου στην παράμετρο lng.

Εκδόθηκε: 29/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3608

Πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο wpQuiz 2.7, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id και της παραμέτρου κωδικού πρόσβασης (pw) για το admin.php ή το user.php.

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3601

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο ibPhotohost 1.1.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου img .

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3485

Η ευπάθεια εισαγωγής ερωτήματος Sql στο common.php στο LightNEasy 3.2.1, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω του userhandle cookie για το LightNEasy.php.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3484

Η ευπάθεια εισαγωγής ερωτήματος Sql στο common.php στο LightNEasy 3.2.1, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου handle για το LightNEasy.php .

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3483

Το cms_write.php στο Primitive CMS 1.0.9, δεν περιορίζει σωστά τη πρόσβαση, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν προνόμια διαχειριστή μέσω ενός άμεσου αιτήματος. Αυτή η ευπάθεια μπορεί να μοχλευτεί για να διευθύνει επιθέσεις cross-site scripting, χρησιμοποιώντας τις παραμέτρους title, content και menutitle.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3479

Η ευπάθεια εισαγωγής ερωτήματος Sql στο list.php στο BoutikOne 1.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου page.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2009-5003

Η ευπάθεια εισαγωγής ερωτήματος Sql στο click.php στο e-soft24 Banner Exchange Script 1.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου targeted.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3313

Το phpgwapi/js/ fckeditor/editor/dialog/fck_spellerpages/spellerpages/ serverscripts/ spellchecker.php στο EGroupware, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα εντολές μέσω shell metacharacters στις παραμέτρους aspell_path ή spellchecker_lang.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3461

Η ευπάθεια εισαγωγής ερωτήματος Sql στη μονάδα Publisher στο eNdonesia 8.4, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου artid στην ενέργεια printarticle στο mod.php.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3458

Η ευπάθεια εισαγωγής ερωτήματος Sql στο lib/γιαολkit/events/event.section.php στο Symphony CMS (εκδόσεις 2.0.7 και 2.1.1), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου send-email[recipient] στο about/ .

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3428

Η ευπάθεια εισαγωγής ερωτήματος Sql στο modules/notes/json.php στο Intermesh Group-Office 3.5.9, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου category_id σε μια ενέργεια.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3426

Η ευπάθεια περάσματος καταλόγου στο στοιχείο JPhone 1.0 Alpha 3 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να συμπεριλάβουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο controller για το index.php.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3422

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο JGen 0.9.33 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id σε μια ενέργεια view για το index.php.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3419

Οι πολλαπλές ευπάθειες συνυπολογισμού στο Haudenschilt Family Connections CMS (FCMS) 2.2.3, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL, που είναι στην παράμετρο current_user_id, στο familynews.php και στο settings.php.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3212

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Seagull 0.6.7, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου frmQuestion σε μία ενέργεια retrieve , σε συνδυασμό με ένα user/ κωδικό πρόσβασης PATH_INFO.

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3210

Οι πολλαπλές ευπάθειες συνυπολογισμού στο Multi-lingual E-Commerce System 0.2, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο include_path .

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3209

Οι πολλαπλές ευπάθειες συνυπολογισμού στο Seagull 0.6.7, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο includeFile.

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3206

Οι πολλαπλές ευπάθειες συνυπολογισμού στο DiY-CMS 1.0, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στις παραμέτρους lang, main_unit και getFile .

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3205

Οι πολλαπλές ευπάθειες συνυπολογισμού στο index.php στο Textpattern CMS 4.2.0, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο inc .

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3204

Οι πολλαπλές ευπάθειες συνυπολογισμού στο Pecio CMS 2.0.5, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο template για το post.php, το article.php, το blog.php ή το home.php στο pec_templates/nova-blue/ .

Εκδόθηκε:03/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-1818

Η λειτουργία IPersistPropertyBag2::Read στο QTPlugin.ocx στο Apple QuickTime 6.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω της ιδιότητας the _Marshaled_pUnk , η οποία ενεργοποιεί το unmarshaling (είναι η διαδικασία της μετατροπής του byte-stream beack στα αρχικά δεδομένα ή αντικείμενα) του αναξιόπιστου pointer.

Εκδόθηκε: 31/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-2875

Το λάθος του signedness (ιδιότητα των μεταβλητών που αντιπροσωπεύει νούμερα σε προγράμματα των υπολογιστών) ακεραίου στον Adobe Shockwave Player (πριν την έκδοση 11.5.8.612), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μία άρνηση υπηρεσίας (DoS) (καταστροφή μνήμης) ή και να εκτελέσουν κώδικα αυθαίρετα μέσω μίας αξίας μήκους που σχετίζεται με το tSAC chunk στον κατάλογο της ταινίας.

Εκδόθηκε: 26/08/2010

Σοβαρότητα: Υψηλή

CVE-2009-4993

Η ευπάθεια συνυπολογισμού σε απομακρυσμένα αρχεία στο home.php στο LM Starmail Paidmail 2.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο page.

Εκδόθηκε: 25/08/2010

Σοβαρότητα: Υψηλή

CVE-2009-4992

Η ευπάθεια εισαγωγής ερωτήματος Sql στο paidbanner.php στο LM Starmail Paidmail 2.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id.

Εκδόθηκε: 25/08/2010

Σοβαρότητα: Υψηλή

CVE-2009-4987

Το admin/header.php στο Scripteen Free Image Hosting Script 2.3, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την αυθεντικοποίηση και να κερδίσουν πρόσβαση, ορίζοντας την αξία cookie cookgid για 1.

Εκδόθηκε: 25/08/2010

Σοβαρότητα: Υψηλή

CVE-2009-4985

Η ευπάθεια εισαγωγής ερωτήματος Sql στο browse.php στο Accessories Me PHP Affiliate Script 1.4, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου go.

Εκδόθηκε: 25/08/2010

Σοβαρότητα: Υψηλή

CVE-2009-4979

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο search.php στο Photokorn Gallery 1.81, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω των παραμέτρων where, sort, order, και match.

Εκδόθηκε: 25/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3055

Το script για την εγκατάσταση διαμόρφωσης στο phpMyAdmin 2.11.x, δεν περιορίζει σωστά τα ονοματα των κλειδιών στο αρχείο εξόδου, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός επεξεργασμένου POST αιτήματος.

Εκδόθηκε: 24/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3103

Η ευπάθεια περάσματος καταλόγου στο FTPGetter Team FTPGetter 3.51.0.05, επιτρέπει σε απομακρυσμένους FTP διακομιστές να γράψουν αυθαίρετα αρχεία μέσω της ..\ (τελείας τελείας backslash) σε ένα όνομα αρχείου.

Εκδόθηκε: 21/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3099

Η ευπάθεια περάσματος καταλόγου στο SmartSoft Ltd SmartFTP Client 4.0.1124.0, επιτρέπει σε απομακρυσμένους FTP διακομιστές να «υπερεγγράψουν» αυθαίρετα αρχεία μέσω της ..\ (τελείας τελείας backslash) σε ένα όνομα αρχείου.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3097

Η ευπάθεια περάσματος καταλόγου στο WinFrigate Frigate 3 FTP client 3.36, επιτρέπει σε απομακρυσμένους FTP διακομιστές να «υπερεγγράψουν» αυθαίρετα αρχεία μέσω της ..\ (τελείας τελείας backslash) σε ένα όνομα αρχείου.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3029

Η ευπάθεια εισαγωγής ερωτήματος Sql στο statistics.php στο PHPKick 0.8, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου gameday σε μια ενέργεια overview.

Εκδόθηκε: 16/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3027

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Tycoon Baseball Script 1.0.9, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου game_id σε μια ενέργεια game_player.

Εκδόθηκε: 16/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-3013

Η ευπάθεια εισαγωγής ερωτήματος Sql στο groupadmin.php στο Pligg, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου role.

Εκδόθηκε: 16/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-2577

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο Pligg, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου title για το storyrss.php για το story.php.

Εκδόθηκε: 16/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-2933

Η ευπάθεια εισαγωγής ερωτήματος Sql στο AV Scripts του AV Arcade 3, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω του cookie ava_code για τη κεντρική σελίδα που σχετίζεται με την index.php και το login task.

Εκδόθηκε: 05/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-2926

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο sNews 1.7, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου category.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2925

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Freeway CMS 1.4.3.210, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου ecPath .

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2924

Η ευπάθεια εισαγωγής ερωτήματος Sql στο myLDlinker.php στο myLinksDump Plugin 1.2 for WordPress, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου url.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2923

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο YouTube 1.5 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id_cate για το index.php.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2921

Η ευπάθεια εισαγωγής ερωτήματος Sql στο Golf Course Guide για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id σε μια ενέργεια golfcourses για το index.php.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2919

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο StaticXT για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id για το index.php.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2918

Η ευπάθεια συνυπολογισμού στο στοιχείο core/include/myMailer.class.php στο Visites για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα PHP κώδικα μέσω ενός URL στην παράμετρο mosConfig_absolute_path.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2916

Η ευπάθεια εισαγωγής ερωτήματος Sql στο news.php στο AJ Square AJ HYIP MERIDIAN, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2915

Η ευπάθεια εισαγωγής ερωτήματος Sql στο welcome.php στο AJ Square AJ HYIP PRIME, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id.

Εκδόθηκε: 30/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2912

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Kayako eSupport 3.70.02, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου _a στην ενέργεια downloads.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2911

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο Kayako eSupport 3.70.02, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου newsid στην ενέργεια viewnews .

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2910

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο Ozio Gallery για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου Itemid για το index.php.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2909

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο ttvideo.php στο TTVideo 1.0 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου cid στην ενέργεια video για το index.php.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2908

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο Joomdle 0.24 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου course_id στην ενέργεια detail για το index.php.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2907

Η ευπάθεια εισαγωγής ερωτήματος Sql στο στοιχείο Huru Helpdesk για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου cid[0] στην ενέργεια detail για το index.php.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2906

Η ευπάθεια εισαγωγής ερωτήματος Sql στο articlesdetails.php στο ScriptsFeed και στο BrotherScripts (BS) , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-2905

Η ευπάθεια εισαγωγής ερωτήματος Sql στο info.php στο ScriptsFeed και στο BrotherScripts (BS), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2009-4974

Η ευπάθεια περάσματος καταλόγου στο box_display.php για το TotalCalendar 2.4 , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχεία και πιθανόν να προκαλέσουν άλλες ακαθόριστες ζημιές μέσω της .. (τελείας τελείας) στην παράμετρο box .

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2009-4973

Η ευπάθεια εισαγωγής ερωτήματος Sql στο rss.php στο TOtalCalendar 2.4, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου selectedCal στην ενέργεια witchCal .

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2009-4958

Η ευπάθεια εισαγωγής ερωτήματος Sql στο video.php στο EMO Breeder Manager, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου idd .

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

CVE-2010-0833

Η βιβλιοθήκη pam_lsass στο Likewise Open 5.4 και στο CIFS 5.4, χρησιμοποιεί το "SetPassword logic" όταν τρέχει σαν μέρος της υπηρεσίας root, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την αυθεντικοποίηση για το λογαριασμό Likewise Security Authority (lsassd), του οποίου ο κωδικός πρόσβασης έχει χαρακτηριστεί σαν να έχει λήξει.

Εκδόθηκε: 28/07/2010

Σοβαρότητα: Υψηλή

7.2 ΣΥΝΗΘΙΣΜΕΝΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PHP

CVE-2011-2470

Η ευπάθεια Cross-site scripting (XSS) στο chat/base/admin/login.php στο A Really Simple Chat (ARSC) 3.3-rc2, επιτρέπει σε απομακρυσμένους χρήστες να πραγματοποιήσουν επίθεση με την εισαγωγή αυθαίρετα web script ή HTML μέσω της παραμέτρου arsc_message.

Εκδόθηκε: 29/06/2011

Σοβαρότητα: Μέτρια

CVE-2011-1482

Οι πολλαπλές ευπάθειες παραποίησης cross-site αιτημάτων (CSRF) στο mainfile.php στο Francisco Burzi PHP-Nuke 8.0, επιτρέπουν σε απομακρυσμένους χρήστες να υποκλέψουν την αυθεντικοποίηση των διαχειριστών για να πραγματοποιήσουν αιτήματα που προσθέτουν λογαριασμούς χρηστών και χορηγούν τα προνόμια του διαχειριστή σε ένα απλό λογαριασμό χρήστη.

Εκδόθηκε: 21/06/2011

Σοβαρότητα: Μέτρια

CVE-2010-3709

Η λειτουργία ZipArchive::getArchiveComment στην PHP 5.2.x, επιτρέπει σε context-dependent χρήστες να επιτεθούν για προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποίηση δείκτη διεύθυνσης dereference και κρασάρισμα εφαρμογής) μέσω ενός επεξεργασμένου συμπιεσμένου αρχείου.

Εκδόθηκε: 09/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-3436

Η fopen_wrappers.c στην PHP 5.3.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους περιορισμούς για το open_basedir μέσω παραγόντων που σχετίζονται με το μήκος ενός ονόματος αρχείου.

Εκδόθηκε: 09/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-4208

Η Cross-site scripting (XSS) ευπάθεια στο Flash στοιχείο στο YUI 2.5.0, όπως χρησιμοποιείται στον Bugzilla, στο Moodle, και σε άλλα προϊόντα, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα κώδικα web ή HTML μέσω παραγόντων που σχετίζονται με το uploader/assets/uploader.swf.

Εκδόθηκε: 07/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-4207

Η Cross-site scripting (XSS) ευπάθεια στο Flash στοιχείο στο YUI 2.4.0, όπως χρησιμοποιείται στον Bugzilla, στο Moodle, και σε άλλα προϊόντα, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα κώδικα web ή HTML μέσω vectors που σχετίζονται με το charts/assets/charts.swf.

Εκδόθηκε: 07/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-4155

Οι πολλαπλές ευπάθειες Cross-site scripting (XSS) στο eXV2 CMS 2.10, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα κώδικα web ή HTML μέσω της παραμέτρου rssfeedURL για το manual/caferss/example.php και της sumb παραμέτρου για το modules/news/archive.php, το modules/news/topics.php και το modules/contact/index.php .

Εκδόθηκε: 03/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-4151

Η ευπάθεια εισαγωγής ερωτήματος Sql στο misc.php στο DeluxeBB 1.3, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου xthedateformat σε μια ενέργεια εγγραφής.

Εκδόθηκε: 03/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-3977

Οι πολλαπλές ευπάθειες Cross-site scripting (XSS) στο wp-content/plugins/cforms/ lib_ajax.php στο cforms WordPress plugin 11.5, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web κώδικα ή HTML μέσω των παραμέτρων rs και rsargs[].

Εκδόθηκε: 03/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-4143

Η ευπάθεια εισαγωγής ερωτήματος Sql στο chart.php στο phpCheckZ 1.1.0, όταν απενεργοποιείται το magic_quotes_gpc , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου id .

Εκδόθηκε: 02/11/2010

Σοβαρότητα: Μέτρια

CVE-2010-3713

Το rss.php στο UseBB, δεν χειρίζεται σωστά τις διαμορφώσεις στο φόρουμ στο οποίο ένας χρήστης έχει την άδεια view αλλά όχι την άδεια read , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης με την ανάγνωση του feed του φόρουμ σε συνδυασμό με το feed forpic.

Εκδόθηκε: 28/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4097

Οι πολλαπλές ευπάθειες Cross-site scripting (XSS) στο index.php στο Aardvark Topsites PHP (εκδόσεις 5.2.0 και 5.2.1), επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web κώδικα ή HTML μέσω των παραμέτρων mail, title, u και url.

Εκδόθηκε: 27/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3717

Η λειτουργία t3lib_div::validEmail στο TYPO3 4.2.x, δεν περιορίζει σωστά την εισαγωγή για τις διαδικασίες filter_var FILTER_VALIDATE_EMAIL στην PHP, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και κρασάρισμα εφαρμογής) , μέσω ενός μεγάλου αλφαριθμητικού για την διεύθυνση e-mail.

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3710

Η ευπάθεια κατανάλωσης stack στη λειτουργία filter_var στην PHP 5.2.x, όταν το FILTER_VALIDATE_EMAIL mode χρησιμοποιείται , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και κρασάρισμα εφαρμογής) μέσω ενός μεγάλου αλφαριθμητικού για την διεύθυνση e-mail.

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3900

Το Midori , δεν ελέγχει τα πιστοποιητικά X.509 , κάτι το οποίο επιτρέπει σε man-in-the-middle χρήστες να επιτεθούν για να παραποιήσουν αυθαίρετα https ιστότοπους μέσω ενός επεξεργασμένου πιστοποιητικού διακομιστή.

Εκδόθηκε: 14/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3692

Η ευπάθεια περάσματος καταλόγου στην λειτουργία callback στο client.php στο phpCAS,όταν το proxy mode είναι ενεργοποιημένο, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να δημιουργήσουν ή να «υπερεγγράψουν» αυθαίρετα αρχεία μέσω των διασταυρωμένων ακολουθιών καταλόγου στην παράμετρο Proxy Granting Ticket IOU (PGTiou).

Εκδόθηκε: 07/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3690

Οι πολλαπλές ευπάθειες Cross-site scripting (XSS) στο phpCAS, όταν το proxy mode είναι ενεργοποιημένο, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML είτε μέσω μίας επεξεργασμένης Proxy Granting Ticket IOU (PGTiou) παραμέτρου για την λειτουργία callback στο client.php, είτε παράγοντες που αφορούν λειτουργίες που κάνουν κλήσεις getCallbackURL, είτε παράγοντες που αφορούν λειτουργίες που κάνουν κλήσεις getURL.

Εκδόθηκε: 07/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3763

Η ευπάθεια Cross-site scripting (XSS) στο core/summary_api.php στο MantisBT, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για εισάγουν αυθαίρετα web script ή HTML μέσω του πεδίου σύνοψης.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-2453

Οι πολλαπλές ευπάθειες Cross-site scripting (XSS) στο Synology Disk Station 2.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML συνδέοντας τον διακομιστή FTP και παρέχοντας μία εντολή για ένα επεξεργασμένο όνομα χρήστη ή για ένα επεξεργασμένο κωδικό πρόσβασης , η οποία είναι γραμμένη από την FTP logging μονάδα για ένα παράθυρο ιστορικού διαδικτυακής διεπαφής.

Εκδόθηκε: 29/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3490

Η ευπάθεια περάσματος καταλόγου στο page.recordings.php στο System Recordings στοιχείο στην διεπαφή διαμόρφωσης FreePBX 2.8.0, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους διαχειριστές να δημιουργήσουν αυθαίρετα αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο usersnum για το admin/config.php, όπως γίνεται όταν δημιουργούμε ένα .php αρχείο κάτω από το web root.

Εκδόθηκε: 28/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3070

Η ευπάθεια Cross-site scripting (XSS) στο NuSOAP 0.9.5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω του PATH_INFO για ένα αυθαίρετο PHP script το οποίο χρησιμοποιεί κλάσεις NuSOAP.

Εκδόθηκε: 28/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2950

Η ευπάθεια format αλφαριθμητικού στο stream.c στην επέκταση phar στηνPHP 5.3.x, επιτρέπει σε context-dependent χρήστες να επιτεθούν για να λάβουν ευαίσθητες πληροφορίες (περιεχόμενα μνήμης) και πιθανόν να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου phar:// URI που δεν χειρίζεται σωστά από την λειτουργία phar_stream_flush, οδηγώντας την σε λάθη στην λειτουργία php_stream_wrapper_log _error.

Εκδόθηκε: 28/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3606

Οι πολλαπλές ευπάθειες περάσματος καταλόγου στο AGENTS/index.php στο NetArt MEDIA Real Estate Portal 2.0, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να συμπεριλάβουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω διασταυρωμένων ακολουθιών καταλόγου στις παραμέτρους folder και action.

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3306

Η ευπάθεια περάσματος καταλόγου στην λειτουργία modURL στο Weborf, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχείος μέσω ..%2f ακολουθίες σε ένα URI.

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3294

Η ευπάθεια Cross-site scripting (XSS) στο apc.php στην επέκταση Alternative PHP Cache (APC), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω ακαθόριστων παραγόντων .

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2491

Η ευπάθεια Cross-site scripting (XSS) στο cgi/client.py στο Roundup, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω του γνωρίσματος template για το πρόγραμμα /issue.

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3489

Η ευπάθεια Cross-site scripting (XSS) στο netautor/napro4/home/login2.php στο CMS Digital Workroom 5.5.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου goback.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Μέτρια

CV-2010-3482

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο cms_write.php στο Primitive CMS 1.0.9, επιτρέπουν σε απομακρυσμένους αυθεντικοποιημένους διαχειριστές να εκτελέσουν αυθαίρετα Sql εντολές μέσω των παραμέτρων title και menutitle .

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3481

Οι πολλαπλές ευπάθειες εισαγωγής ερωτήματος Sql στο login.php στο ApPHP PHP MicroCMS 1.0.1, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω των μεταβλητών ονόματος χρήστη και κωδικού πρόσβασης, που πιθανόν σχετίζεται με το include/classes/Login.php.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3480

Η ευπάθεια περάσματος καταλόγου στο index.php στο ApPHP PHP MicroCMS 1.0.1, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν και να εκτελέσουν αυθαίρετα τοπικά αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο page.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3314

Η ευπάθεια Cross-site scripting (XSS) στο login.php στο EGroupware, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου lang.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3467

Η ευπάθεια εισαγωγής ερωτήματος Sql στο modules/sections/index.php στο E-Xoopport Samsara 3.1, όταν ενεργοποιείται η μονάδα Tutorial, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου secid στην δράση listarticles.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3466

Η ευπάθεια Cross-site scripting (XSS) στο index.php στη μονάδα hosted_signup στο NetArt Media iBoutique.MALL 1.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου tmpl.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3464

Η ευπάθεια παραποίησης Cross-site αιτημάτων (CSRF) στο admin/manager_ users.class.php στο SantaFox 2.02, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να χακάρουν την αυθεντικοποίηση των διαχειριστών για τα αιτήματα, όπως αποδεικνύεται με την εισαγωγή χρηστών με προνόμια διαχειριστή μέσω της ενέργειας save_admin για admin/index.php.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3463

Η ευπάθεια Cross-site scripting (XSS) στο modules/search/search.class.php στο SantaFox 2.02, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου search για το search.html.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3462

Η ευπάθεια Cross-site scripting (XSS) στο backend/plugin/Registration/index.php στο Mollify 1.6, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου confirm.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3456

Η ευπάθεια περάσματος καταλόγου στο download.php στο EnergyScripts Simple Download 1.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο file.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3455

Η ευπάθεια Cross-site scripting (XSS) στο index.php στο AChecker 1.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου uri.

Εκδόθηκε: 17/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3427

Οι πολλαπλές ευπάθειες cross-site scripting (XSS) στο Open Classifieds 1.7.0.2, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω των παραμέτρων desc, price, title και place για το index.php και της παραμέτρου subject για το contact.htm .

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3424

Η ευπάθεια Cross-site scripting (XSS) στο admin/sources/classes/bbκώδικα/custom/ defaults.php στο Invision Power Board 3.1.2, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3421

Η ευπάθεια Cross-site scripting (XSS) στο AffiliateLogin.asp στο ProductCart, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου redirectUrl .

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3420

Η ευπάθεια Cross-site scripting (XSS) στο Products_Results.php στο PowerStore 3.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου FortalRows_WADAProducts.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3418

Η ευπάθεια cross-site scripting (XSS) στο NetArt Media Car Portal 2.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω των παραμέτρων car_id για το index.php και y για το include/images.php.

Εκδόθηκε: 16/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2953

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού σε ένα συγκεκριμένο Debian GNU/Linux patch για το couchdb script στο CouchDB 0.8.0, επιτρέπει σε τοπικούς χρήστες να αποκτήσουν δικαιώματα μέσω μίας επεξεργασμένης shared βιβλιοθήκης στον τρέχων κατάλογο.

Εκδόθηκε: 14/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-0154

Η ευπάθεια περάσματος καταλόγου στο sla/index.php στο Local Management Interface, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να διαβάσουν αυθαίρετα αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο l .

Εκδόθηκε: 14/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-0152

Η ευπάθεια cross-site scripting (XSS) στο Local Management Interface, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω των παραμέτρων date1 για το pvm_messagestore.php, userfilter για το pvm_user_management.php, ping για το sys_tools.php σε μία ενέργεια sys_ping.php, action για το pvm_cert_commaction.php, action για το pvm_cert_serveraction.php, action για το pvm_smtpstore.php, l για το sla/index.php, ή ακαθόριστων αποθηκευμένων δεδομένων και επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να εισάγουν αυθαίρετα web script ή HTML μέσω αποθηκευμένων φίλτρων αναζήτησης.

Εκδόθηκε: 14/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3263

Η ευπάθεια Cross-site scripting (XSS) στο setup/frames/index.inc.php στο script εγκατάστασης στο phpMyAdmin 3.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω ενός ονόματος server .

Εκδόθηκε: 10/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2949

Το bgpd στο Quagga, δεν αναλύει σωστά τα AS μονοπάτια, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποίηση δείκτη διεύθυνσης dereference και κρασάρισμα δαιμόνων) μέσω ενός άγνωστου AS τύπου στο AS χαρακτηριστικό του μονοπατιού σε ένα μήνυμα BGP UPDATE .

Εκδόθηκε: 10/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2948

Μια stack-based υπερχείλιση buffer στην λειτουργία bgp_route_refresh_receive στο Quagga, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαιμόνων) ή πιθανόν να εκτελέσουν αυθαίρετα κώδικα μέσω μιας κακοφτιαγμένης εγγραφής Outbound Route Filtering (HF) στο μήνυμα BGP ROUTE-REFRESH (RR).

Εκδόθηκε: 10/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3208

Η ευπάθεια Cross-site scripting (XSS) στο ajax.php στο Wiccle Web Builder (WWB) (εκδόσεις 1.00 και 1.0.1), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εισάγουν αυθαίρετα web script ή HTML μέσω της παραμέτρου post_text σε μια ενέργεια custom_search στον ιστότοπο για το index.php.

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3207

Η ευπάθεια εισαγωγής ερωτήματος Sql στο index.php στο GaleriaSHQIP 1.0, όταν απενεργοποιείται το magic_quotes_gpc, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου album_id.

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3203

Η ευπάθεια περάσματος καταλόγου στο στοιχείο PicSell 1.0 για το Joomla! , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχεία μέσω της .. (τελείας τελείας) στην παράμετρο dflink στην ενέργεια prevsell dwnfree για το index.php.

Εκδόθηκε: 03/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-2575

Η heap-based υπερχείλιση buffer στην RLE λειτουργικότητα αποσυμπίεσης στην λειτουργία TranscribePalmImageTOJPEG στο KDE SC , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) ή πιθανόν να εκτελέσουν αυθαίρετα κώδικα μέσω μιας επεξεργασμένης εικόνας σε ένα PDB αρχείο.

Εκδόθηκε: 30/08/2010

Σοβαρότητα: Μέτρια

CVE-2010-2363

Η εφαρμογή του IPv6 Unicast Reverse Path Forwarding (RPF) στους δρομολογητές SEIL/X1, SEIL/X2, και SEIL/B1, όταν χρησιμοποιείται το strict mode, δεν ρίχνει σωστά τα πακέτα, κάτι το οποίο μπορεί να επιτρέψει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης μέσω μίας πλαστογραφημένης διεύθυνσης IP.

Εκδόθηκε: 30/08/2010

Σοβαρότητα: Μέτρια

8. ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PERL

8.1 ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PERL

CVE-2011-2628

Ο Opera (πριν την έκδοση 11.11), δεν χειρίζεται σωστά τα στοιχεία frameset , το οποίο επιτρέπει σε απομακρυσμένους χρήστες να εκτελέσουν αυθαίρετα κώδικα ή να πραγματοποιήσουν επίθεση και να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης) μέσω παραγόντων που σχετίζονται με το unload της σελίδας.

Εκδόθηκε: 01/07/2011

Σοβαρότητα: Υψηλή

CVE-2010-4216

Ο διακομιστής IBM Tivoli Directory 6.0.0.x, δεν χειρίζεται σωστά τις λανθασμένες αναφορές του buffer στα αιτήματα LDAP BER , πράγμα το οποίο μπορεί να επιτρέψει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) μέσω παραγόντων που αφορούν έναν buffer ο οποίος έχει διεύθυνση μνήμης κοντά στην μεγαλύτερη δυνατή διεύθυνση .

Εκδόθηκε: 09/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-0786

Το στοιχείο του Web Services Security στην εφαρμογή IBM WebSphere Application Server, δεν εφαρμόζει σωστά την Java API για το XML Web Services, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (αλλοίωση δεδομένων) μέσω ενός επεξεργασμένου αιτήματος JAX-WS το οποίο οδηγεί σε λανθασμένα κρυπτογραφημένα δεδομένα.

Εκδόθηκε: 09/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-3636

Ο Adobe Flash Player, δεν χειρίζεται σωστά τις ακαθόριστες κρυπτογραφήσεις κατά τη διάρκεια μίας ανάλυσης ενός cross-domain policy αρχείου, κάτι το οποίο επιτρέπει σε απομακρυσμένους διαδικτυακούς διακομιστές να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης μέσω άγνωστων παραγόντων.

Εκδόθηκε: 07/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-2941

Το ipp.c στο cupsd στο CUPS, δεν κατανέμει σωστά την μνήμη για τις τιμές των γνωρισμάτων, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (use-after-free και κρασάρισμα εφαρμογής) ή πιθανόν να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου IPP αιτήματος.

Εκδόθηκε: 05/11/2010

Σοβαρότητα: Υψηλή

CVE-2010-3491

Τα στοιχεία ActiveMatrix Runtime και ActiveMatrix Administrator στοTIBCO ActiveMatrix Service Grid, δεν χειρίζονται σωστά τις συνδέσεις JMX , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα, να αποκτήσουν ευαίσθητες πληροφορίες ή και να προκαλέσουν άρνηση υπηρεσίας (DoS) μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 26/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3714

Η εφαρμογή jumpUrl στο TYPO3 4.2.x, δεν συγκρίνει σωστά συγκεκριμένες hash αξίες κατά τη διάρκεια αποφάσεων πρόσβασης – ελέγχου , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να διαβάσουν αυθαίρετα αρχεία μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-4045

Το Opera 10.63, δεν περιορίζει σωστά τα web script , σε ακαθόριστες συνθήκες, που αφορούν επαναφορτώσεις και επανακατευθύνσεις, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να πλαστογραφήσουν την μπάρα διεύθυνσης, να διεξάγουν cross-site scripting (XSS) επιθέσεις και πιθανόν να εκτελέσουν αυθαίρετα κώδικα με την μόχλευση της ικανότητας ενός script για την αλληλεπίδραση με μία ιστοσελίδα από ένα διαφορετικό τομέα ή ένα διαφορετικό περιεχόμενο ασφαλείας .

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3183

Η λειτουργία LookupGetterORSetter στον Mozilla Firefox 3.6.x, δεν υποστηρίζει σωστά τις κλήσεις λειτουργίας window.__lookupGetter__ που στερούνται ορισμάτων, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα ή να προκαλέσουν άρνηση υπηρεσίας (DoS) (λανθασμένο dereference δείκτη διεύθυνσης και κρασάρισμα εφαρμογής) μέσω ενός επεξεργασμένου HTML εγγράφου.

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3173

Η SSL υλοποίηση στον Mozilla Firefox 3.6.x , δεν θέτει σωστά το ελάχιστο μήκος κλειδιού για το Diffie-Hellman Ephemeral (DHE) τρόπο λειτουργίας, το οποίο διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να νικήσουν τους κρυπτογραφημένους μηχανισμούς προστασίας μέσω μίας επίθεσης ωμής βίας .

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3749

Η υλοποίηση browser-plugin στο RealNetworks RealPlayer 11.0, δεν χειρίζεται σωστά έναν ακαθόριστο χαρακτήρα με ορίσματα για τη μέθοδο RecordClip, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να κατεβάσουν αυθαίρετα ένα πρόγραμμα στην μηχανή του πελάτη, και να εκτελέσουν αυτό το πρόγραμμα μέσω μίας επεξεργασμένης μεθόδου κλήσης.

Εκδόθηκε:19/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3747

Το ActiveX control στο RealNetworks RealPlayer 11.0, δεν αρχικοποιεί σωστά ένα ακαθόριστο στοιχείο αντικειμένου κατά τη διάρκεια συντακτικής ανάλυσης του CDDA URI, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα ή να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποιημένος δείκτης διεύθυνσης dereference και κρασάρισμα εφαρμογής) μέσω ενός μεγάλου μήκους URI.

Εκδόθηκε:19/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3110

Οι πολλαπλές υπερχειλίσεις buffer στη μονάδα Novell Client novfs για το Linux kernel στο SUSE Linux Enterprise 11 SP1 και στο openSUSE 11.3, επιτρέπουν σε τοπικούς χρήστες να κερδίσουν προνόμια μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 12/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3760

Το FastBackMount.exe στην υπηρεσία Mount στο IBM Tivoli Storage Manager, δεν χειρίζεται σωστά μια συγκεκριμένη βλάβη στη κατανομή μνήμης , πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποιημένος δείκτης διεύθυνσης dereference, κρασάρισμα δαίμονα και αποτυχία ανάκτησης) καθορίζοντας μια αξία μεγάλου μεγέθους μέσα σε πακέτο δεδομένων TCP.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3731

Η υπερχείλιση buffer στη λειτουργία com.ibm.db2.das.core.DasSysCmd στο στοιχείο db2dasrrm του DB2 Administration Server, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) ή πιθανόν και να εκτελέσουν αυθαίρετα κώδικα μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Υψηλή

CVE-2010-3081

Οι λειτουργίες compat_alloc_user_space στα αρχεία include/asm/compat.h στο Linux kernel, δεν κατανέμουν σωστά την μνήμη userspace που χρειάζεται για το επίπεδο συμβατότητας των 32-bit, κάτι το οποίο επιτρέπει σε τοπικούς χρήστες να κερδίσουν προνόμια με τη μόχλευση της ικανότητας της λειτουργίας compat_mc_getsockopt για να ελέγξουν μία συγκεκριμένη τιμή μήκους.

Εκδόθηκε: 24/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-2836

Η διαρροή μνήμης στο χαρακτηριστικό SSL VPN στο Cisco IOS 12.4, όταν ενεργοποιείται η ανακατεύθυνση θύρας HTTP , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης) με την εσφαλμένη αποσύνδεση SSL συνόδων, κάτι που οδηγεί σε συνδέσεις που παραμένουν στη κατάσταση CLOSE-WAIT.

Εκδόθηκε: 23/09/2010

Σοβαρότητα: Υψηλή

CVE-2010-3483

Το cms_write.php στο Primitive CMS 1.0.9, δεν περιορίζει σωστά την πρόσβαση , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να κερδίσουν προνόμια παρόμοια με του διαχειριστή μέσω ενός άμεσου αιτήματος. Αυτή η ευπάθεια μπορεί να μοχλευτεί ώστε να πραγματοποιηθούν cross-site scripting επιθέσεις (XSS) χρησιμοποιώντας τον τίτλο, το περιεχόμενο και τις παραμέτρους του menutitle.

Εκδόθηκε: 22/09/2010

Σοβαρότητα: Υψηλή

8.2 ΣΥΝΗΘΙΣΜΕΝΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PERL

CVE-2011-2639

Ο Opera (πριν την έκδοση 11.10), δεν χειρίζεται σωστά τις κρυμμένες κινούμενες GIF εικόνες, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να πραγματοποιήσουν επίθεση για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση CPU) μέσω ενός αρχείου εικόνας που πραγματοποιεί επαναλαμβανόμενα βαψίματα.

Εκδόθηκε: 01/07/2011

Σοβαρότητα: Μέτρια

CVE-2010-3933

Το Ruby on Rails (εκδόσεις 2.3.9 και 3.0.0), δεν χειρίζεται σωστά τα φωλιασμένα γνωρίσματα, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να τροποποιήσουν αυθαίρετα εγγραφές με την αλλαγή των ονομάτων των παραμέτρων για την εισαγωγή σε φόρμες.

Εκδόθηκε: 28/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3713

Το rss.php στο UseBB 1.0.11, δεν χειρίζεται σωστά τις διαμορφώσεις του forum στο οποίο ένας χρήστης έχει την άδεια view αλλά όχι την άδεια read, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης με την ανάγνωση του ιστορικού του forum σε συνδυασμό με το ιστορικό ενός θέματος.

Εκδόθηκε: 28/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3711

Το libpurple στο Pidgin 2.7.4, δεν επικυρώνει σωστά την επιστροφή της τιμής της λειτουργίας purple_base64_decode , κάτι το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποίηση δείκτη διεύθυνσης dereference και κρασάρισμα εφαρμογής) μέσω ενός επεξεργασμένου μηνύματος που σχετίζεται με τα plugins για MSN, MySpaceIM, XMPP, και Yahoo! και την υποστήριξη αυθεντικοποίησης NTLM .

Εκδόθηκε: 28/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4068

Αδιευκρίνιστη ευπάθεια στο Extension Manager στο TYPO3 4.2.x, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους διαχειριστές να διαβάσουν και πιθανόν να τροποποιήσουν αυθαίρετα αρχεία μέσω μίας επεξεργασμένης παραμέτρου.

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3717

Η λειτουργία t3lib_div::validEmail στο TYPO3 4.2.x, δεν περιορίζει σωστά την είσοδο για το filter_var FILTER_VALIDATE_EMAIL για τις λειτουργίες στην PHP, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και κρασάρισμα εφαρμογής) μέσω ενός μεγάλου σε μήκους αλφαριθμητικού διεύθυνσης e-mail .

Εκδόθηκε: 25/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4057 , CVE-2010-4056

Το solid.exe στο IBM solidDB 6.5.0.3, δεν εκτελεί σωστά μία επαναλαμβανόμενη κλήση για μία συγκεκριμένη λειτουργία μετά τη λήψη πακέτου δεδομένων που περιέχει πολλά πεδία ακεραίων με δύο διαφορετικές τιμές, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη έγκυρη πρόσβαση μνήμης και κρασάρισμα δαίμονα) μέσω μίας συνόδου TCP στην θύρα 1315.

Εκδόθηκε: 23/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4049

Ο Opera 10.62, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) μέσω μίας Flash ταινίας με ένα διάφανο Window Mode , το οποίο δεν λειτουργεί σωστά κατά τη διάρκεια πλοήγησης του μακριά από το εμπεριεχόμενο HTML έγγραφο.

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4047

Ο Opera 10.62, δεν επιλέγει σωστά το περιεχόμενο ασφαλείας του JavaScript κώδικα που συνδέεται με μία σελίδα error, το οποίο επιτρέπει σε user-assisted απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν cross-site scripting (XSS) επιθέσεις μέσω μίας επεξεργασμένης ιστοσελίδας.

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-4046

Ο Opera 10.62, δεν επαληθεύει σωστά την προέλευση του περιεχομένου των βίντεο, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να αποκτήσουν ευαίσθητες πληροφορίες .

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3178

Ο Mozilla Firefox 3.6.x, δεν χειρίζεται σωστά συγκεκριμένες τυπικές κλήσεις δημιουργημένες από javascript με αποτέλεσμα τα URLs να σχετίζονται με το άνοιγμα ενός νέου παραθύρου και να εκτελούν cross-domain πλοήγηση, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την Same Origin Policy μέσω ενός επεξεργασμένου HTML εγγράφου.

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3170

Ο Mozilla Firefox 3.6.x, αναγνωρίζει μία wildcard διεύθυνση IP στο πεδίο Common Name του υποκειμένου ενός X.509 πιστοποιητικού, πράγμα το οποίο μπορεί να επιτρέψει σε man-in-the-middle χρήστες να επιτεθούν για να πλαστογραφήσουν αυθαίρετα SSL διακομιστές μέσω ενός επεξεργασμένου πιστοποιητικού που έχει εκδοθεί από μία θεμιτή Αρχή Πιστοποίησης .

Εκδόθηκε: 21/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3369

Τα mdb και mdb-symbolreader scripts στον mono-debugger 2.4.3, τοποθετούν ένα όνομα καταλόγου με μηδενικό μήκος στο LD_LIBRARY_PATH, το οποίο επιτρέπει σε τοπικούς χρήστες να κερδίσουν προνόμια μέσω ενός Trojan horse με βιβλιοθήκη κοινής χρήσης στον τρέχων κατάλογο.

Εκδόθηκε: 20/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3353

Το Cowbell 0.2.7.1, τοποθετεί ένα όνομα καταλόγου με μηδενικό μήκος στο LD_LIBRARY_PATH, το οποίο επιτρέπει σε τοπικούς χρήστες να κερδίσουν προνόμια μέσω ενός Trojan horse με βιβλιοθήκη κοινής χρήσης στον τρέχων κατάλογο.

Εκδόθηκε: 20/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3574

Αδιευκρίνιστη ευπάθεια στο στοιχείο Networking στο Oracle Java SE και στο Java for Business 6 Update 21, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα μέσω αγνώστων παραγόντων.

Εκδόθηκε: 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3934

Ο περιηγητής στο Research In Motion (RIM) BlackBerry Device Software 5.0.0.593, δεν περιορίζει σωστά την cross-domain εκτέλεση του JavaScript, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την Same Origin Policy μέσω παραγόντων που σχετίζονται με την κλήση του window.open και το στοιχείο IFRAME.

Εκδόθηκε: 14/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3564

Αδιευκρίνιστη ευπάθεια στο στοιχείο Oracle Communications Messaging Server, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να επηρεάσουν την εμπιστευτικότητα και ακεραιότητα μέσω άγνωστων παραγόντων που σχετίζονται με το Webmail.

Εκδόθηκε: 14/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3901

Το OpenConnect 2.24, δεν επικυρώνει σωστά τα πιστοποιητικά X.509, πράγμα το οποίο επιτρέπει σε man-in-the-middle χρήστες να επιτεθούν για να πλαστογραφήσουν αυθαίρετα AnyConnect SSL VPN διακομιστές μέσω ενός επεξεργασμένου πιστοποιητικού που δεν ανταποκρίνεται στο όνομα εξυπηρετητή του διακομιστή ή παρουσιάζεται στις περιστάσεις όταν λείπει η επιλογή διαμόρφωσης για το -- cafile .

Εκδόθηκε: 14/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3781

Το PL/php add-on 1.4, δεν προστατεύει σωστά την εκτέλεση των script από ένα χρήστη με διαφορετική ταυτότητα Sql εντός της ίδιας συνόδου, πράγμα το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να κερδίσουν προνόμια μέσω ενός επεξεργασμένου script κώδικα σε μια security definer λειτουργία.

Εκδόθηκε: 06/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3433

Οι υλοποιήσεις PL/perl και PL/Tcl στο PostgreSQL 7.4, δεν προστατεύουν σωστά την εκτέλεση των script από ένα χρήστη με διαφορετική ταυτότητα Sql εντός της ίδιας συνόδου, κάτι το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να κερδίσουν προνόμια μέσω ενός επεξεργασμένου script κώδικα σε μια security definer λειτουργία, όπως παρουσιάζεται από τον επαναπροσδιορισμό πρότυπων λειτουργιών ή τον επαναπροσδιορισμό των χειριστών.

Εκδόθηκε: 06/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3762

Το ISC BIND 9.7.1, όταν η DNSSEC επικύρωση ενεργοποιείται, δεν χειρίζεται σωστά συγκεκριμένες κακές υπογραφές εάν υπάρχουν πολλαπλές άγκυρες εμπιστοσύνης (trust anchors) για μια ενιαία ζώνη, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) μέσω ενός ερωτήματος DNS.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3756

Η λειτουργία _CalcHashValueWithLength στο FastBackserver.exe στο IBM Tivoli Storage Manager FastBack 5.5.0.0, δεν επικυρώνει σωστά μια τιμή με ακαθόριστο μήκος , κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα δαίμονα) με την αποστολή δεδομένων μέσω TCP.

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3740

Η Net Search Extender υλοποίηση στο στοιχείο Text Search στο IBM DB2 UDB 9.5, δεν χειρίζεται σωστά μια αλφαριθμητική Fuzzy αναζήτηση, κάτι το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και κρέμασμα συστήματος) μέσω της λειτουργίας db2ext.textSearch .

Εκδόθηκε: 05/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3315

Το authz.c στην μονάδα mod_dav_svn για τον Apache HTTP διακομιστή, όταν ενεργοποιείται το SVNPathAuthz short_circuit , δεν χειρίζεται σωστά ένα καθορισμένο χώρο αποθήκευσης σαν (rule scope), κάτι το οποίο επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης μέσω svn εντολών.

Εκδόθηκε: 04/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-1623

Η διαρροή μνήμης στην λειτουργία apr_brigade_split_line στο buckets/apr_brigade.c στην Apache Portable Runtime Utility βιβλιοθήκη, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης) μέσω ακαθόριστων παραγόντων που σχετίζονται με την καταστροφή ενός APR bucket.

Εκδόθηκε: 04/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3429

Το flicvideo.c στο libavcodec 0.6, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω ενός επεξεργασμένου flic αρχείου.

Εκδόθηκε: 30/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3298

Η λειτουργία hso_get_count στους drivers/net/usb/hso.c στο Linux kernel 2.6.35, δεν αρχικοποιεί σωστά ένα συγκεκριμένο structure μέλος, πράγμα το οποίο επιτρέπει σε τοπικούς χρήστες να αποκτήσουν ενδεχομένως ευαίσθητες πληροφορίες από τη kernel stack μνήμη μέσω μίας κλήσης TIOCGICOUNT ioctl .

Εκδόθηκε: 30/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3297

Η λειτουργία eql_g_master_cfg στους drivers/net/eql.c στο Linux kernel 2.6.35, δεν αρχικοποιεί σωστά ένα συγκεκριμένο μέλος δομής, κάτι το οποίο επιτρέπει σε τοπικούς χρήστες να αποκτήσουν ενδεχομένως ευαίσθητες πληροφορίες από τη kernel stack μνήμη μέσω μίας κλήσης EQL_GETMASTRCFG ioctl .

Εκδόθηκε: 30/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3296

Η λειτουργία cxgb_extension_ioctl στους drivers/net/cxgb3/cxgb3_main.c στο Linux kernel 2.6.35, δεν αρχικοποιεί σωστά ένα συγκεκριμένο structure μέλος, το οποίο επιτρέπει σε τοπικούς χρήστες να αποκτήσουν ενδεχομένως ευαίσθητες πληροφορίες από τη kernel stack μνήμη μέσω μίας κλήσης CHELSIO_GET_QSET_NUM ioctl .

Εκδόθηκε: 30/09/2010

Σοβαρότητα: Μέτρια

CVE-2010-3079

Το kernel/trace/ftrace.c στο Linux kernel 2.6.35.4, όταν ενεργοποιείται το debugfs, δεν χειρίζεται σωστά την αλληλεπίδραση μεταξύ της mutex κατοχής και των llseek πράξεων , πράγμα το οποίο επιτρέπει σε τοπικούς χρήστες να προκαλέσουν άρνηση υπηρεσίας (DoS) (μη αρχικοποίηση δείκτη διεύθυνσης dereference και διακοπή όλων των λειτουργιών εντοπισμού αρχείων) μέσω μίας κλήσης lseek .

Εκδόθηκε: 30/09/2010

Σοβαρότητα: Μέτρια

9. ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PYTHON

9.1 ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PYTHON

CVE-2010-2944

Η λειτουργία authenticate στο LDAPUserFolder/LDAPUserFolder.py στο zope-ldapuserfolder 2.9-1, δεν επικυρώνει τον κωδικό πρόσβασης για το λογαριασμό emergency, κάτι το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να κερδίσουν προνόμια.

Εκδόθηκε: 20/08/2010

Σοβαρότητα: Υψηλή

CVE-2010-1450

Οι πολλαπλές υπερχειλίσεις buffer στον αποκωδικοποιητή RLE στην μονάδα rgbimg στον Python 2.5, επιτρέπουν σε απομακρυσμένους χρήστες να επιτεθούν για να έχουν μία ακαθόριστη επίδραση, μέσω ενός αρχείου εικόνας που περιέχει επεξεργασμένα δεδομένα τα οποία ενεργοποιούν την λανθασμένη επεξεργασία στην λειτουργία longimagedata ή και στην λειτουργία expandrow.

Εκδόθηκε: 27/05/2010

Σοβαρότητα: Υψηλή

CVE-2010-1449

Η υπερχείλιση ακεραίου στο rgbimgunit.c στην μονάδα rgbimg στον Python 2.5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να έχουν μια ακαθόριστη επίπτωση μέσω μίας μεγάλης εικόνας που ενεργοποιεί μια υπερχείλιση buffer.

Εκδόθηκε: 27/05/2010

Σοβαρότητα: Υψηλή

CVE-2010-1338

Η ευπάθεια εισαγωγής Sql ερωτήματος στο ts_other.php στο Teamsite Hack plugin 3.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Sql εντολές μέσω της παραμέτρου userid στην ενέργεια modboard.

Εκδόθηκε: 09/04/2010

Σοβαρότητα: Υψηλή

CVE-2009-3578

Το Autodesk Maya 8.0, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα κώδικα μέσω των αρχείων .ma και .mb που χρησιμοποιούν την Maya Embedded Language (MEL) python εντολή ή ακαθόριστες άλλες MEL εντολές, σχετιζόμενες με το "Script Nodes."

Εκδόθηκε: 24/11/2009

Σοβαρότητα: Υψηλή

CVE-2009-2940

Η μονάδα pygresql (εκδόσεις 3.8.1 και 4.0) για την Python, δεν υποστηρίζει σωστά την λειτουργία PQescapeStringConn, πράγμα το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να μοχλεύσουν διαφυγόντα θέματα που σχετίζονται με κωδικοποίηση χαρακτήρων πολλών bytes.

Εκδόθηκε: 22/10/2009

Σοβαρότητα: Υψηλή

CVE-2008-6954

Η διαδικτυακή διεπαφή (CobblerWeb) στο Cobbler, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να εκτελέσουν αυθαίρετα Python κώδικα στο cobblerd με την επεξεργασία μίας Cheetah kickstart template για να εισάγουν αυθαίρετα Python modules.

Εκδόθηκε: 12/08/2009

Σοβαρότητα: Υψηλή

CVE-2009-0669

Η βάση δεδομένων Zope Object Database (ZODB) 3.8.1, όταν ενεργοποιείται στο Zope Enterprise Objects η κοινή χρήση της βάσης δεδομένων , επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν την αυθεντικοποίηση μέσω παραγόντων που αφορούν το πρωτόκολλο δικτύου ZEO.

Εκδόθηκε: 07/08/2009

Σοβαρότητα: Υψηλή

CVE-2008-6547

Το schema.py στον FormEncode για την Python (python-formencode) 1.0, δεν εφαρμόζει το γνώρισμα chained_validators, το οποίο επιτρέπει σε χρήστες να επιτεθούν για να παρακάμψουν τους προοριζόμενους περιορισμούς πρόσβασης μέσω ακαθόριστων παραγόντων.

Εκδόθηκε: 30/03/2009

Σοβαρότητα: Υψηλή

CVE-2009-0367

Η μονάδα Python AI στο Wesnoth 1.4.x, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να παρακάμψουν το sandbox και να εκτελέσουν αυθαίρετα κώδικα χρησιμοποιώντας την μονάδα whitelisted που εισάγει μια μη ασφαλή μονάδα και έπειτα χρησιμοποιεί το όνομα μίας ιεραρχικής μονάδας για να έχει πρόσβαση στην μη ασφαλή μονάδα μέσω της whitelisted μονάδας.

Εκδόθηκε : 03/05/2009

Σοβαρότητα : Υψηλή

9.2 ΣΥΝΗΘΙΣΜΕΝΑ ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ PYTHON

CVE-2011-1521

Οι μονάδες urllib και urllib2 στην Python 2.x,επεξεργάζονται επικεφαλίδες θέσης (Location headers) που καθορίζουν την ανακατεύθυνση στο αρχείο : URL, το οποίο διευκολύνει τους απομακρυσμένους χρήστες να αποκτήσουν ευαίσθητες πληροφορίες ή να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση πόρων) μέσω ενός επεξεργασμένου URL.

Εκδόθηκε : 24/05/2011

Σοβαρότητα: Μέτρια

CVE-2011-1158

Η ευπάθεια Cross-site scripting (XSS) στο feedparser.py στο Universal Feed Parser 5.x, επιτρέπει σε απομακρυσμένους χρήστες να εισάγουν αυθαίρετα web script ή HTML μέσω ενός απρόσμενου σχήματος URI.

Εκδόθηκε : 11/04/2011

Σοβαρότητα: Μέτρια

CVE-2010-3495

Η κατάσταση Race στο ZEO/StorageServer.py στην Zope Object Database (ZODB), επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν μια άρνηση υπηρεσίας (DoS) (outage δαίμονα) με την εδραίωση και έπειτα το άμεσο τερματισμό μίας σύνδεσης TCP , που οδηγεί την accept λειτουργία να κάνει την απρόσμενη επιστροφή μηδενικής τιμής (None) για τη διεύθυνση ή για ένα ECONNABHTED, EAGAIN, ή EWOULDBLOCK σφάλμα.

Εκδόθηκε : 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3494

Η κατάσταση Race στην κλάση FTPHandler στο ftpserver.py, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (outage δαίμονα) με την εδραίωση και έπειτα το άμεσο τερματισμό μίας σύνδεσης TCP, που οδηγεί την accept λειτουργία να κάνει την απρόσμενη επιστροφή μηδενικής τιμής (None) για τη διεύθυνση ή ένα ECONNABHTED, EAGAIN, ή EWOULDBLOCK σφάλμα.

Εκδόθηκε: 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3493

Οι πολλαπλές καταστάσεις race στο smtpd.py στην smtpd μονάδα στον Python 2.6, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (outage δαίμονα) με την εδραίωση και έπειτα το άμεσο τερματισμό μίας σύνδεσης TCP, που οδηγεί την accept λειτουργία να κάνει την απρόσμενη επιστροφή μηδενικής τιμής (None) για τη διεύθυνση ή ένα ECONNABHTED, EAGAIN, ή EWOULDBLOCK σφάλμα.

Εκδόθηκε: 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2010-3492

Η μονάδα asyncore στον Python 3.1, δεν χειρίζεται σωστά τις ανεπιτυχείς κλήσεις για τη λειτουργία accept και δεν έχει συνοδευτικά έγγραφα που περιγράφουν πως οι εφαρμογές δαιμόνων θα πρέπει να χειρίζονται τις ανεπιτυχείς κλήσεις για τη λειτουργία accept, πράγμα το οποίο διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν επιθέσεις άρνησης υπηρεσίας (DoS) που τερματίζουν αυτές τις εφαρμογές μέσω δικτυακών συνδέσεων.

Εκδόθηκε: 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2009-5010

Η κατάσταση Race στη κλάση FTPHandler στο ftpserver.py, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (outage δαίμονα) με την εδραίωση και τον άμεσο τερματισμό μιας σύνδεσης TCP, που οδηγεί την λειτουργία accept να έχει μία απρόσμενη επιστροφή μηδενικής τιμής (None).

Εκδόθηκε: 19/10/2010

Σοβαρότητα: Μέτρια

CVE-2009-4924

Το Dan Pascu python-cjson 1.0.5, δεν χειρίζεται σωστά το χαρακτηριστικό ['/'] για το cjson.encode, πράγμα το οποίο διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν συγκεκριμένες cross-site scripting (XSS) επιθέσεις που συμπεριλαμβάνουν τον Firefox και το τελικό tag ενός SCRIPT στοιχείου.

Εκδόθηκε: 02/07/2010

Σοβαρότητα: Μέτρια

CVE-2010-2480

Το Mako 0.3.3 βασίζεται στην cgi.escape λειτουργία στην Python standard βιβλιοθήκη για cross-site scripting (XSS) προστασία, πράγμα το οποίο διευκολύνει τους απομακρυσμένους χρήστες να επιτεθούν για να πραγματοποιήσουν XSS επιθέσεις μέσω παραγόντων που συμπεριλαμβάνουν single-quote χαρακτήρες και ένα JavaScript onLoad χειριστή γεγονότων για το στοιχείο BODY.

Εκδόθηκε: 02/07/2010

Σοβαρότητα: Μέτρια

CVE-2010-1666

Η υπερχείλιση buffer στο Dan Pascu python-cjson 1.0.5, όταν ενεργοποιείται η κωδικοποίηση UCS-4, επιτρέπει σε context-dependent χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) ή πιθανόν να επιδρούν διαφορετικά μέσω παραγόντων που αφορούν την επεξεργασμένη είσοδο Unicode για τη cjson.encode λειτουργία.

Εκδόθηκε: 02/07/2010

Σοβαρότητα: Μέτρια

CVE-2010-2089

Η μονάδα audioop στο Python (εκδόσεις 2.7 και 3.2) , δεν πιστοποιεί τις σχέσεις μεταξύ χαρακτηριστικών μεγέθους και μήκη αλφαριθμητικών σε byte, το οποίο επιτρέπει σε context-dependent χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κατανάλωση μνήμης και κρασάρισμα εφαρμογής) μέσω επεξεργασμένων χαρακτηριστικών, όπως παρουσιάζεται από μία κλήση στην audioop.reverse με αλφαριθμητικό με ένα byte.

Εκδόθηκε: 27/05/2010

Σοβαρότητα: Μέτρια

CVE-2010-1634

Οι πολλαπλές υπερχειλίσεις ακεραίων στο audioop.c στην μονάδα audioop στον Python (εκδόσεις 2.6, 2.7, 3.1, και 3.2), επιτρέπουν σε context-dependent χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) μέσω ενός μεγάλου fragment, όπως παρουσιάζεται από μία κλήση για το audioop.lin2lin με ένα μεγάλο αλφαριθμητικό στο πρώτο χαρακτηριστικό, που οδηγεί σε υπερχείλιση buffer .

Εκδόθηκε: 27/05/2010

Σοβαρότητα: Μέτρια

CVE-2009-4134

Η υποχείλιση buffer στην μονάδα rgbimg στον Python 2.5, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) μέσω μίας μεγάλης zsize τιμής σε μία ασπρόμαυρη rgb εικόνας που ενεργοποιεί ένα λανθασμένο dereference δείκτη διεύθυνσης.

Εκδόθηκε: 27/05/2010

Σοβαρότητα: Μέτρια

CVE-2009-3560

Η λειτουργία big2_γιαUtf8 στην libexpat στο Expat 2.0.1, επιτρέπει σε context-dependent χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) μέσω ενός εγγράφου XML με παραποιημένες UTF-8 ακολουθίες που ενεργοποιούν την «υπερανάγνωση» του buffer, και σχετίζονται με τη λειτουργία doProlog στην lib/xmlparse.c .

Εκδόθηκε: 04/12/2009

Σοβαρότητα: Μέτρια

CVE-2009-4081

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στο dstat, επιτρέπει σε τοπικούς χρήστες να αποκτήσουν προνόμια μέσω ενός Trojan horse Python module στο τρέχων working directory.

Εκδόθηκε: 29/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-3894

Οι πολλαπλές ευπάθειες μη έμπιστης αναζήτησης μονοπατιού στο dstat, επιτρέπει σε τοπικούς χρήστες να κερδίσουν προνόμια μέσω ενός Trojan horse Python module στο τρέχων working directory ή σε ένα συγκεκριμένο υποκατάλογο του working directory.

Εκδόθηκε: 29/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-3720

Η λειτουργία updatePosition στο lib/xmltok_impl.c στην libexpat στο Expat 2.0.1, επιτρέπει σε context-dependent χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (κρασάρισμα εφαρμογής) μέσω ενός εγγράφου XML με τροποποιημένες UTF-8 ακολουθίες που ενεργοποιούν μια «υπερανάγνωση» buffer.

Εκδόθηκε: 03/11/2009

Σοβαρότητα: Μέτρια

CVE-2009-2701

Η αδιευκρίνιστη ευπάθεια στην λειτουργικότητα του Zope Enterprise Objects (ZEO) storage-server στην Zope Object Database (ZODB) 3.8, όταν η κοινή χρήση της ZEO βάσης δεδομένων και η blob υποστήριξη ενεργοποιούνται, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να διαβάσουν ή και να διαγράψουν αυθαίρετα αρχεία μέσω άγνωστων παραγόντων.

Εκδόθηκε: 08/09/2009

Σοβαρότητα: Μέτρια

CVE-2009-0668

Η αδιευκρίνιστη ευπάθεια στην Zope Object Database (ZODB) 3.8.1, όταν ενεργοποιείται η κοινή χρήση της βάσης δεδομένων, επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να εκτελέσουν αυθαίρετα Python κώδικα μέσω παραγόντων που αφορούν το πρωτόκολλο δικτύου ZEO.

Εκδόθηκε: 07/08/2009

Σοβαρότητα: Μέτρια

CVE-2008-6549

Η λειτουργία password_checker στο MoinMoin 1.6.1, χρησιμοποιεί τα χαρακτηριστικά cracklib και python-crack ακόμα και αν δεν είναι ασφαλή για τα νήματα, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να επιτεθούν για να προκαλέσουν άρνηση υπηρεσίας (DoS) (σφάλμα κατάτμησης και κρασάρισμα) μέσω άγνωστων παραγόντων.

Εκδόθηκε: 30/03/2009

Σοβαρότητα: Μέτρια

CVE-2008-6539

Η ευπάθεια εισαγωγής στατικού κώδικα στο user/settings/ στο DeStar 0.2.2-5, επιτρέπει σε απομακρυσμένους αυθεντικοποιημένους χρήστες να εισάγουν αυθαίρετα διαχειριστές και να εισάγουν αυθαίρετα Python κώδικα στο destar_cfg.py μέσω μιας επεξεργασμένης pin παραμέτρου.

Εκδόθηκε: 30/03/2009

Σοβαρότητα: Μέτρια

CVE-2009-0318

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στον μεταφραστή wrapper GObject Python στο Gnumeric, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2009-0317

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στα Python language bindings για το Nautilus , επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2009-0316

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στο src/if_python.c στη διεπαφή Python στο Vim, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2009-0315

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στην μονάδα Python στο xchat, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2009-0314

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στην μονάδα Python στο gedit, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2008-5987

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στην διεπαφή Python στο Eye of GNOME (eog) 2.22.3, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python module στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

CVE-2008-5986

Η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού στο "VST plugin with Python scripting" και στο "VST plugin for writing score generators in Python" στο Csound 5.08.2, επιτρέπει σε τοπικούς χρήστες να εκτελέσουν αυθαίρετα κώδικα μέσω ενός Trojan Horse Python αρχείου στο τρέχων working directory.

Εκδόθηκε: 28/01/2009

Σοβαρότητα: Μέτρια

10. ΣΥΜΠΕΡΑΣΜΑΤΑ

Λαμβάνοντας υπόψιν τις ευπάθειες σε κάθε στοιχείο του συστήματος LAMP διαπιστώνουμε τα εξής :

Στον Apache η ευπάθεια άρνησης υπηρεσίας ήταν η δημοφιλέστερη. Ακολουθεί η ευπάθεια παραποίησης cross-site αιτημάτων, η ευπάθεια cross-site scripting, οι υπερχειλίσεις buffer και ακεραίων, η εισαγωγή ερωτήματος Sql , η επίθεση man-in-the-middle , η ευπάθεια περάσματος καταλόγου και τελευταία αλλά καθόλου ασήμαντη η ευπάθεια του προεπιλεγμένου κωδικού πρόσβασης.

Στην MySql η ευπάθεια εισαγωγής ερωτήματος Sql ήταν η δημοφιλέστερη. Ακολουθεί η άρνηση υπηρεσίας, η υπερχείλιση buffer, η ευπάθεια cross-site scripting, η ευπάθεια περάσματος καταλόγου, η επίθεση man-in-the-middle, η ευπάθεια συνυπολογισμού, η επίθεση ωμής βίας τελευταία αλλά καθόλου ασήμαντη η ευπάθεια του προεπιλεγμένου κωδικού πρόσβασης.

Στην Php η ευπάθεια εισαγωγής ερωτήματος Sql ήταν η δημοφιλέστερη. Ακολουθεί η ευπάθεια cross-site scripting, η ευπάθεια περάσματος καταλόγου, η ευπάθεια συνυπολογισμού, η άρνηση υπηρεσίας, η υπερχείλιση buffer , η ευπάθεια παραποίησης cross-site αιτημάτων, η επίθεση man-in-the-middle και η μη έμπιστη αναζήτηση μονοπατιού.

Στην Perl η ευπάθεια άρνησης υπηρεσίας ήταν η δημοφιλέστερη. Ακολουθεί η ευπάθεια cross-site scripting, η υπερχείλιση buffer, η επίθεση man-in-the-middle και η επίθεση ωμής βίας.

Στην Python η ευπάθεια άρνησης υπηρεσίας ήταν η δημοφιλέστερη. Ακολουθεί η ευπάθεια μη έμπιστης αναζήτησης μονοπατιού, η υπερχείλιση buffer , η ευπάθεια cross-site scripting, η υπερχείλιση ακεραίων και η ευπάθεια εισαγωγής ερωτήματος Sql.

Με βάση τα παραπάνω αποτελέσματα βλέπουμε ότι οι συχνότερες επιθέσεις είναι η άρνηση υπηρεσίας και η εισαγωγή ερωτήματος Sql, χωρίς αυτό να σημαίνει ότι οι υπόλοιπες ευπάθειες δεν δημιουργούν εξίσου πρόβλημα.

Ένα σημαντικό θέμα είναι και οι ευπάθειες που αφορούν τους κωδικούς πρόσβασης. Χωρίς να συμπεριλάβουμε τις περιπτώσεις όπου ο επιτιθέμενος ενεργά προσπαθεί να «σπάσει» τους κωδικούς πρόσβασης (ωμή βία), υπάρχουν και αρκετές περιπτώσεις όπου προγράμματα όριζαν προεπιλεγμένους κωδικούς πρόσβασης ή είχαν πολύ χαμηλή ασφάλεια.

Ένα ακόμα θέμα είναι ότι αρκετές από τις ευπάθειες είναι αποτελέσματα λανθασμένων διορθώσεων σε προηγούμενες ευπάθειες.

Εν κατά κλείδι, με προσεκτικά και σωστα θωρακισμένες διαδικτυακές εφαρμογές, με την χρήση ασφαλών κωδικών πρόσβασης και με τη σωστή διόρθωση των υπάρχοντων προβλημάτων, είναι δυνατό ο αριθμός των ευπαθειών να μειωθεί σημαντικά.

11. ΟΡΙΣΜΟΙ ΚΑΙ ΕΠΕΞΗΓΗΣΕΙΣ

Backend σύνδεση : η σύνδεση σε μια βάση δεδομένων που είναι δεν είναι απευθείας προσβάσιμη από χρήστες αλλά μέσω μιας εξωτερικής εφαρμογής

Buffer : περιοχή προσωρινής αποθήκευσης δεδομένων

Feed :ένα διαδικτυακό έγγραφο που είναι η σύντομη μορφή μιας ιστοσελίδας

Stack : τύπος δομής δεδομένων , στην οποία τα αντικείμενα αφαιρούνται με την ανάποδη σειρά από την οποία μπήκαν (LIFO)

Use after free : όταν ένας δείκτης είναι free γίνεται αναξιόπιοστος καθώς δείχνει σε μία περιοχή μνήμης με απροσδιόριστο περιεχόμενο. Εάν γίνει χρήση του δείκτη αφού έχει γίνει free , τότε υπάρχει περίπτωση αλλοίωσης ή υπερεγγραφής των δεδομένων σε κάποια τυχαία περιοχή μνήμης

Αληθινή τιμή (literal) : μια τιμή η οποία γράφεται ακριβώς όπως ερμηνεύεται , π.χ. στην έκφραση x=3 , το x είναι η μεταβλητή και το 3 είναι το literal

Αξία hash : ένας αριθμός που έχει παραχθεί από ένα αλφαριθμητικό ή ένα κείμενο , ώστε έπειτα να κρυπτογραφηθεί και να σταλεί με ασφάλεια

Δαίμονας : μία διαδικασία που τρέχει στο παρασκήνιο και εκτελεί μια συγκεκριμένη λειτουργία σε προκαθορισμένες περιόδους ή ως απάντηση σε ορισμένα γεγονότα

Δείκτης διεύθυνσης dereference : ο δείκτης που «δείχνει» σε μία τιμή που αποθηκεύεται στο αντικείμενο , στο οποίο ο δείκτης έχει αναφερθεί και όχι στην αξία της μεταβλητης του δείκτη

Διαδικασία παιδί : είναι η διαδικασία που έχει δημιουργηθεί από μία άλλη διαδικασία (γονιός)

Έκφραση : στον προγραμματισμό είναι ο οποιοσδήποτε νόμιμος συνδυασμός από σύμβολα που αντιπροσωπεύει μια αξία

Κρασάρισμα (crash) : μια σοβαρή βλάβη του υπολογιστή, όπου ο υπολογιστής σταματάει να δουλεύει ή ένα πρόγραμμα τερματίζεται απρόσμενα

Κρέμασμα (hang) : όταν ο υπολογιστής δεν ανταποκρίνεται στις εντολές ή στις εισόδους

Κώδικας αυθεντικοποίησης μηνύματος (Message Authentication Code - MAC) : ένα μικρό κομμάτι πληροφορίας που χρησιμοποιείται για να γίνει αυθεντικοποίηση σε ένα μήνυμα

Υπερανάγνωση (over-read) : η ανάγνωση των δεδομένων περισσότερο από όσο θα έπρεπε

Υπερεγγραφή (over-write) : η εγγραφή καινούργιων δεδομένων πάνω σε ήδη υπάρχοντα δεδομένα

Χακάρισμα (hack) : η τροποποίηση ενός προγράμματος συχνά με μη εξουσιοδοτημένο τρόπο , με την αλλαγή του ίδιου του κώδικα

12. ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλίο (πρώτη έκδοση)	Κάτσικας , Σ. , Γκριτζάλης , Δ. , Γκριτζάλης , Σ. (2004) , 'Ασφάλεια Πληροφοριακών Συστημάτων' , Εκδόσεις Νέων Τεχνολογιών
Βιβλίο (πρώτη έκδοση)	Γκριτζάλης , Σ. , Κάτσικας , Σ. , Γκριτζάλης , Δ. (2003) , 'Ασφάλεια Δικτύων Υπολογιστών' , Εκδόσεις Παπασωτηρίου
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://nvd.nist.gov/home.cfm
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://cve.mitre.org/index.html
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.apache.org/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.mysql.com/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.php.net/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.perl.org/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.python.org/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://en.wikipedia.org/wiki/Main_Page
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.webopedia.com/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.serverwatch.com/news/article.php/3869321/Multiple-Apache--Web-Server-Flaws-Patched.htm

Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://osvdb.org/search?search[vuln_title]=mysql&search[text_type]=alltext
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://security.nknu.edu.tw/psnl/publications/2009/08_HUANG,PENG-YU/2009CISP_ResearchAndIntegrationOfHeterogeneousVulnerabilityDatabase.pdf
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://www.apacheweek.com/
Βιβλιογραφική Αναφορά : κείμενο σε ιστοσελίδα	http://dev.mysql.com/tech-resources/articles/guide-to-php-security-ch3.pdf