Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. “Τεχνο-οικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων”

Διπλωματική Εργασία

«Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO27001:2013 – Υλοποίηση web εφαρμογής για audits»

Διονυσία Λερατάκη

Επιβλέπων: Καθηγητής κ. Χριστόφορος Νταντογιάν

Φεβρουάριος 2016

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα της μεταπτυχιακής διπλωματικής μου εργασίας, Δρ. Χριστόφορο Νταντογιάν για την δυνατότητα που μου προσέφερε να ασχοληθώ με αυτό το ενδιαφέρον για μένα και σύγχρονο θέμα, όπως και για την πολύτιμη βοήθεια που μου παρείχε καθ' όλη την διάρκεια εκπόνησης της διπλωματικής εργασίας.

Θα ήθελα ιδιαίτερα να ευχαριστήσω τον Δρ. Κλεάνθη Δέλιο για την συνεχή καθοδήγηση σε όλη τη διαδικασία της διπλωματικής. Οι συζητήσεις μας, οι ιδέες σας και οι διορθώσεις σας ήταν ανεκτίμητες.

Περίληψη

Η ανάγκη για προστασία της πληροφορίας σήμερα, είναι ένα θέμα που απασχολεί καθημερινά όλες τις επιχειρήσεις, μικρές και μεγάλες. Με εκατομμύρια συναλλαγές να πραγματοποιούνται καθημερινά διαδικτυακά, διακινώντας προσωπικά, επιχειρησιακά και ευαίσθητα δεδομένα οι επιχειρήσεις καλούνται να εξασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα της πληροφορίας αυτής για να εξασφαλίσουν την παραμονή τους στην αγορά. Για το σκοπό αυτό έχουν αναπτυχθεί διάφορα πρότυπα ασφαλείας τα οποία καθοδηγούν έναν οργανισμό ώστε να προστατέψει τη πληροφορία αυτή. Ένα από τα πρότυπα αυτά είναι το ISO27001:2013 με το οποίο θα ασχοληθούμε στα πλαίσια της διπλωματικής αυτής. Θα παρουσιαστεί το πρότυπο και οι απαιτήσεις του, θα αναπτυχθεί μία web εφαρμογή για την καταγραφή των audits με βάση το πρότυπο αυτό και θα εξεταστεί η ασφάλεια της εφαρμογής σε επίπεδο εφαρμογής. Τέλος θα παρουσιαστούν σενάρια χρήσης του εργαλείου σε τρεις εταιρείες που ελέγχτηκαν με βάση το πρότυπο.

Λέξεις κλειδιά: ISO27001:2013, πρότυπο, ασφάλεια, πιστοποίηση, ISMS

Πίνακας Περιεχομένων

Ευχαριστίες 2
Περίληψη 3
Πίνακες 6
1. Εισαγωγή 7
1.1 Αντικείμενο διπλωματικής 7
1.2 Οργάνωση κειμένου 8
1.3 Ορολογία και ακρωνύμια 8
2. Υλοποίηση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) σύμφωνα με το πρότυπο ISO27001:2013 σε μια επιχείρηση 10
2.1 Το πρότυπο ISO27001:2013 10
2.2 Κατανοώντας τις επιχειρηματικές ανάγκες 12
2.3 Συνηθισμένα προβλήματα και κίνδυνοι 13
2.4 Μεθοδολογία 13
Εισαγωγή 13
Φάση 1: Καθιέρωση του ISMS 14
Φάση 2: Υλοποίηση του ISMS 15
Φάση 3: Παρακολούθηση του ISMS 15
Φάση 4: Διατήρηση και Βελτίωση του ISMS 16
3. Σχεδίαση και υλοποίηση μίας web εφαρμογής για υποστήριξη των *ISMS κατά ISO27001:2013* audits 17
3.1 Εισαγωγή 17
3.2 Ανάλυση απαιτήσεων 18
Ανταγωνισμός 19
Χρήστες του συστήματος 19
Λειτουργικές απαιτήσεις 19
Μη λειτουργικές απαιτήσεις 21
3.3 Στήνοντας την εφαρμογή 23
Εργαλεία 23
Διαδικασία Ανάπτυξης 24
4. Μελέτη περίπτωσης 31
4.1 Εισαγωγή 31
4.2 Σενάριο 1: Η επιχείρηση παρουσίασε major non-conformities 32
4.3 Σενάριο 2: Η επιχείρηση παρουσίασε minor non-conformities 35
4.4 Σενάριο 3: Η επιχείρηση πιστοποιείται κατευθείαν κατά ISO27001:2013 37

Penetration testing δραστηριότητες 38
4.5 Εισαγωγή 38
4.6 Μεθοδολογία και εργαλεία 39
4.7 Μετρικές κινδύνου 40
4.8 Κατανομή κινδύνου 40
4.9 Περίληψη ευρημάτων 41
4.10 Ευρήματα και συστάσεις 42
Εύρημα 1: Πολλαπλά προβλήματα αυθεντικοποίησης 42
Εύρημα 2: Μη κρυπτογραφημένο κανάλι επικοινωνίας 45
Εύρημα 3: Προβλήματα στον τερματισμό του session 47
Εύρημα 4: Αποκάλυψη πληροφοριών 48
Εύρημα 5: Clickjacking 49
5. Συμπεράσματα 51
6. Πηγαίος κώδικας εφαρμογής 51
7. Βιβλιογραφία 51

Πίνακες

Πίνακας 1 - Ορολογία και ακρωνύμια 9
Πίνακας 2 - Υποχρεωτικά Έγγραφα κατά το ISO27001:2013 11
Πίνακας 3 - Κατηγορίες των controls 12
Πίνακας 4 - Προβλήματα και Κίνδυνοι κατα την ανάπτυξη ISMS 13
Πίνακας 5 - Επίπεδο αξιολόγησης των non-conformities 32
Πίνακας 6 - Αξιολόγηση κινδύνου 40
Πίνακας 7 - Κατανομή κινδύνου 41
Πίνακας 8 - Περίληψη ευρημάτων 41

1. Εισαγωγή

1.1 Αντικείμενο διπλωματικής

Η ανάγκη για προστασία της πληροφορίας είναι πλέον ορατή και κατανοητή από όλους, πελάτες οργανισμούς και επιχειρήσεις. Τα συστήματα που χρησιμοποιεί μια επιχείρηση για να καλύψει τις ανάγκες της είναι πλέον πολυάριθμα και ποικίλα. Προσωπικοί υπολογιστές υπαλλήλων, εκτυπωτές, βάσεις δεδομένων, active directories,mail servers, web servers, file servers, application servers, εφαρμογές, κινητές συσκευές κ.ά είναι λίγα από τα πολλά διαφορετικά συστήματα που χρησιμοποιούνται καθημερινά. Χρήστες καλούνται να χειριστούν τα συστήματα αυτά, πολλές φόρες αγνοώντας κινδύνους που μπορεί να απειλούν τα δεδομένα μιας επιχείρησης.

Η ανάγκη για ασφαλή διαχείριση της πληροφορίας, των συστημάτων και των χρηστών, οδήγησε στη δημιουργία προτύπων ασφαλείας τα οποία καθοδηγούν μια επιχείρηση να εξασφαλίσει ότι τα δεδομένα της είναι ασφαλή.

Με τη σειρά τους τα πρότυπα αυτά δημιούργησαν την ανάγκη ελέγχου μια επιχείρησης. Οι εκάστοτε ελεγκτές πρέπει να επιβεβαιώνουν ότι οι δραστηριότητες της επιχείρησης συμβαδίζουν με το εκάστοτε πρότυπο, ώστε να πιστοποιούνται και να εξασφαλίζουν τη φήμη τους.

Η διπλωματική αυτή, έχει λοιπόν ως βασικό πυλώνα την δημιουργία μίας δικτυακής εφαρμογής, την οποία θα χρησιμοποιούν οι ελεγκτές των επιχειρήσεων ώστε να αποφανθούν αν η επιχείρηση συμμορφώνεται με τις οδηγίες του προτύπου. Πιο συγκεκριμένα, η εφαρμογή που θα δημιουργηθεί απευθύνεται σε ελεγκτές με βάση το πρότυπο ISO27001:2013

Αναλυτικά, στα πλαίσια της διπλωματικής θα διεξαχθούν τα παρακάτω:

- Ανάλυση του προτύπου ασφάλειας της πληροφορίας ISO 27001:2013
- Δημιουργία εφαρμογής για τους auditors/ελεγκτές των επιχειρήσεων. Η σχεδίαση και ανάπτυξη της εφαρμογής θα γίνει με βάση το κύκλο ζωής του λογισμικού
- Παρουσίαση σεναρίου χρήσης του εργαλείου σε επιχειρήσεις οι οποίες ελέγχτηκαν με βάση το πρότυπο
- Penetration test στην εφαρμογή για να εξασφαλιστεί η ασφάλεια των δεδομένων της, καθώς εταιρικά δεδομένα μπορεί να καταγράφονται.

1.2 Οργάνωση κειμένου

Η παρούσα εργασία αποτελείται από 7 κεφάλαια.

Στο κεφάλαιο 2 παρουσιάζεται το πρότυπο ISO27001:2013 και αναλύονται οι 4 φάσεις ανάπτυξης ενός ISMS.

Στο κεφάλαιο 3 παρουσιάζεται ο κύκλος ανάπτυξης λογισμικού με σκοπό την ανάπτυξη μίας δικτυακής εφαρμογής για την καταχώρηση audits με βάση το πρότυπο ISO27001:2013.

Στο κεφάλαιο 4 παρουσιάζονται 3 διαφορετικά σενάρια χρήσης του εργαλείου που αναπτύχθηκε.

Στο κεφάλαιο 5 καταγράφονται τα αποτελέσματα του penetration test της δικτυακής εφαρμογής και καταγράφεται η μεθοδολογία που ακολουθήθηκε.

Στο κεφάλαιο 6 καταγράφονται τα συμπεράσματα που προκύπτουν και στο κεφάλαιο 7 καταγράφονται οι βιβλιογραφικές πηγές. Ορολογία και ακρωνύμια.

1.3 Ορολογία και ακρωνύμια

Όρος	Αγγλικά	Ελληνικά/ Επεξήγηση
ISMS	Information Security Management System	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
ISO	International Organization for Standardization	Διεθνής Οργανισμός Τυποποίησης
CVSS	Common Vulnerability Scoring System	Σύστημα Βαθμολόγησης ευπαθειών / ανοιχτό πρότυπο για την κατάταξη ευπαθειών ασφάλειας.
CVSSV2 Vector		Περιγράφει τις τιμές των στοιχείων από τα οποία προέκυψε η βαθμολογία
FTP	File Transfer Protocol	Πρωτόκολλο Μεταφοράς Αρχείων
SoA	Statement Of Applicability	
SQL	Structured Query Language	
CMS	Content Management System	Σύστημα διαχείρισης περιεχομένου
PoC	Proof of Concept	Απόδειξη της ιδέας
	Browser	Φυλλομετρητής

	Risk	Κίνδυνος / Συνάρτηση της αξίας ενός αγαθού, της έντασης των απειλών και της σοβαρότητας των αντίστοιχων αδυναμιών.
	Auditor	Επιθεωρητής/ Ελεγκτής
	Audit	Έλεγχος
	Control	Σημείο ελέγχου, δικλείδα ασφαλείας, αντίμετρο
	Conformity	Συμμόρφωση
	Non-Conformity	Μη συμμόρφωση
	Administrator	Διαχειριστής
	Authorization	Εξουσιοδότηση
	Server	Εξυπηρετητής
	Penetration Testing	Δοκιμές παρείσδυσης
	Interface	Διεπαφή
	Impact	Επίπτωση / Η απώλεια που θα προκληθεί από την απώλεια ασφάλειας ενός αγαθού.
	Observation	Παρατήρηση
	Recommendation	Σύσταση

Πίνακας 1 - Ορολογία και ακρωνύμια

2. Υλοποίηση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) σύμφωνα με το πρότυπο ISO27001:2013 σε μια επιχείρηση

2.1 Το πρότυπο ISO27001:2013

Το πρότυπο ISO 27001:2013 καθορίζει τις απαιτήσεις για τον καθορισμό, την εφαρμογή, την διατήρηση και τη συνεχή βελτίωση ενός Συστήματος Διαχείρισης Πληροφοριών με σκοπό την προστασία της πληροφορίας ενός οργανισμού. Το πρότυπο ISO 27002 παρέχει όλες τις βέλτιστες πρακτικές για την υλοποίηση των απαιτήσεων αυτών.

Το ISO27001 περιλαμβάνει επίσης απαιτήσεις για την εκτίμηση και αντιμετώπιση των κινδύνων που αφορούν στην ασφάλεια των πληροφοριών, προσαρμοσμένων στις ανάγκες του οργανισμού. Οι απαιτήσεις που ορίζονται στο πρότυπο είναι γενικές και προορίζονται να εφαρμόζονται σε όλους τους οργανισμούς, ανεξάρτητα από τον τύπο, το μέγεθος ή τη φύση του. Το πρότυπο παρέχει στους οργανισμούς όλων των μεγεθών και τύπων τα μέσα για να εφαρμόσουν ένα αποτελεσματικό σύστημα διαχείρισης ασφάλειας πληροφοριών. Με άλλα λόγια, παρέχει συστάσεις καλών πρακτικών για την διαχείριση της ασφάλειας πληροφοριών, κινδύνων και τα μέτρα ασφαλείας στα πλαίσια του ISMS.

Οι θεμελιώδης αρχές της ασφάλειας των πληροφοριών - τις οποίες επιχειρεί να εξασφαλίσει το πρότυπο - βασίζονται σε τρία βασικά στοιχεία:

Εμπιστευτικότητα (Confidentiality): Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνον από όσους έχουν τα απαραίτητα δικαιώματα.

Ακεραιότητα (Integrity): Διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής.

Διαθεσιμότητα (Availability): Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται.

Το ISMS θα πρέπει να θεωρείται ως ένα framework διαχείρισης και οργάνωσης της ασφάλειας που θα πρέπει να παρακολουθείται συνεχώς και να επανεξετάζεται περιοδικά. Έτσι θα παρέχει αποτελεσματική καθοδήγηση

για την διατήρηση των τριών βασικών αρχών ασφάλειας πληροφοριών του οργανισμού όπως αναφέρθηκαν με σεβασμό στους εκάστοτε εσωτερικούς και εξωτερικούς παράγοντες.

Τα πλεονεκτήματα που απολαμβάνει ένας οργανισμός ακολουθώντας ένα τέτοιο πρότυπο είναι πολυάριθμα:

- Υλοποίηση ξεκάθαρων πολιτικών ασφάλειας για όλα τα μέλη ενός οργανισμού αλλά και τρίτων.
- Ανάλυση απειλών, αδυναμιών και κινδύνων και υλοποίηση των κατάλληλων αντιμέτρων.
- Ύπαρξη Μηχανισμών για τη συνεχή εξέλιξη του οργανισμού
- Αποτελεσματική διαχείριση συμβάντων
- Συμμόρφωση με νομικές και κανονιστικές απαιτήσεις
- Ύπαρξη αποτελεσματικών KPI's (Key Performance Indicators)
- Ανάπτυξη σχέσεων εμπιστοσύνης με πελάτες και συνεργάτες.
- Καλή φήμη

Στο τέλος της υλοποίηση ενός ISMS, ο οργανισμός θα έχει στα χέρια του όλα τα υποχρεωτικά έγγραφα που απαιτεί το πρότυπο.Τα έγγραφα αυτά είναι:

#	Έγγραφο/Καταγραφή
1	Scope of the ISMS
2	Information Security Policy and Objectives
3	Statement of Applicability
4	Risk assessment & treatment methodology
5	Risk assessment & treatment report
6	Risk treatment plan
7	Records of training, skills, experience and qualification
8	Monitoring and measurements results
9	Internal audit program
10	Results of internal audit
11	Results of the management review
12	Results of the corrective actions

Πίνακας 2 - Υποχρεωτικά Έγγραφα κατά το ISO27001:2013

Επιπλέον, το πρότυπο ISO27001:2013 θέτει τις απαιτήσεις και κατηγοριοποιεί τα αντίμετρα στις παρακάτω κατηγορίες:

#	Control
A.5	Information Security Policy
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	User Access Management
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communication security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

Πίνακας 3 - Κατηγορίες των controls

2.2 Κατανοώντας τις επιχειρηματικές ανάγκες

Η προστασία της πληροφορίας είναι σημαντική σε οποιονδήποτε επιχειρησιακό τομέα. Το πρώτο βήμα για επιτυχημένη υλοποίηση ενός ISMS είναι να συνειδητοποιήσει ο εκάστοτε οργανισμός και να αναγνωρίσει την ανάγκη για ασφάλεια της πληροφορίας στο περιβάλλον που λειτουργεί. Το ανώτατο επίπεδο διοίκησης, πρέπει να αναγνωρίσει ότι το πρότυπο ασφάλειας θα αποφέρει οφέλη στον οργανισμό.

2.3 Συνηθισμένα προβλήματα και κίνδυνοι

Κατά την υλοποίηση ενός ISMS, κίνδυνοι και λειτουργικά προβλήματα μπορεί να προκύψουν, τα οποία θα πρέπει να αντιμετωπιστούν άμεσα και αποτελεσματικά ώστε να ικανοποιηθούν οι στόχοι της υλοποίησης.

Παρακάτω παρουσιάζονται οι ποιο συνηθισμένοι κίνδυνοι και προβλήματα.

Προβλήματα και κίνδυνοι	Αντιμετώπιση
Έλλειψη υποστήριξης από διοίκηση	Η ανώτατη διοίκηση πρέπει να δεσμευτεί από τα πρώτα κιόλας στάδια. Αυτό μπορεί να επιτευχθεί με την οργάνωση ειδικών συναντήσεων της ανώτατης διοίκησης μαζί με τον project manager της εταιρείας, εξηγώντας τους στόχους του έργου, τη ζητούμενη υποστήριξη και την περιγραφή των θετικών αποτελεσμάτων για την επιχείρηση, όταν αυτή υλοποιήσει και πιστοποιήσει το ISMS.
Έλλειψη γνώσης του προτύπου	Η επιχείρηση πρέπει να καταλαβαίνει το πρότυπο και τα πλεονεκτήματα του. Ένα γρήγορο και αποτελεσματικό ερωτηματολόγιο μπορεί να εξασφαλίσει τη ροή της πληροφορίας στην επιχείρηση.
Επιρροή εξωτερικές αλλαγές (περιβάλλον, κανόνες κ.λπ.)	Είναι σημαντικό να αναγνωριστούν όλοι οι εξωτερικοί παράγοντες που μπορούν να επηρεάσουν το έργο.
Εσωτερικά προβλήματα στη διαδικασία ανάθεσης ιδιοκτήτη.(data owner, business owner,κ.λπ.)	Κατά τη διάρκεια της υλοποίησης των controls, είναι πολλές φορές δύσκολο να συγχρονιστούν όλοι οι εμπλεκόμενοι στις συναντήσεις και να συμφωνήσουν στον owner του εκάστοτε αγαθού, ειδικά όταν αυτό σημαίνει επιπλέον ευθύνες. Σε αυτή τη περίπτωση είναι πολύ πιο αποδοτικό να συμφωνήσει ο manager του project με την διοίκηση ότι έχει την αρμοδιότητα να αποφασίζει αυτός τους owners των αγαθών, στα πλαίσια πάντα του project.

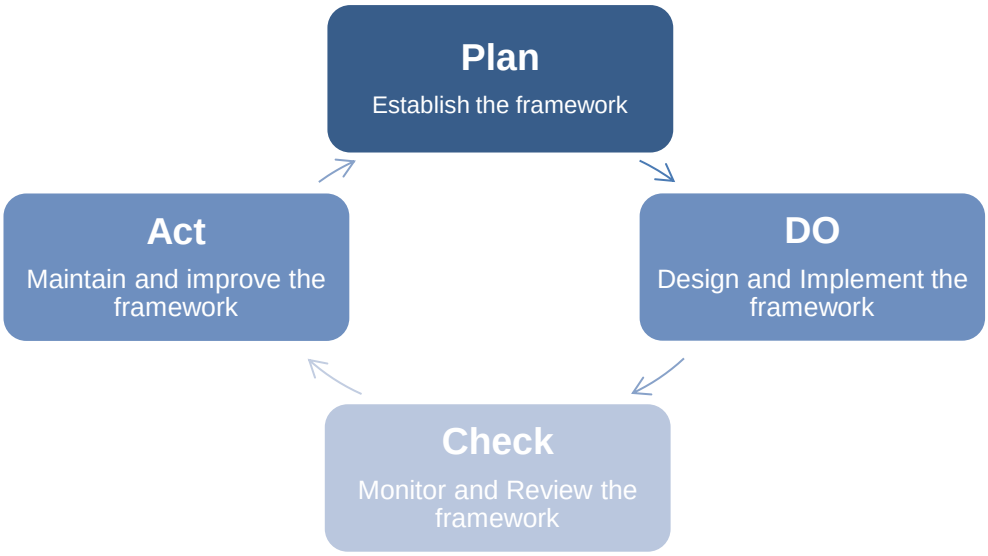
Πίνακας 4 - Προβλήματα και Κίνδυνοι κατα την ανάπτυξη ISMS

2.4 Μεθοδολογία

Εισαγωγή

Το πρότυπο ISO27001 απαιτεί από μία επιχείρηση να καθιερώσει, να υλοποιήσει, να διατηρεί και συνεχώς να βελτιώνει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Όπως και κάθε πρότυπο ISO, έτσι και το ISO 27001 ακολουθεί τον plan-do-check-act (PDCA) κύκλο. Στη συνέχεια αναλύονται η ενέργειες που πρέπει να πραγματοποιήσει ένας οργανισμός σε

κάθε φάση του προτύπου ώστε να συμμορφώνεται με βάση το συγκεκριμένο πρότυπο.



Φάση 1: Καθιέρωση του ISMS

Ο οργανισμός στη φάση αυτή πρέπει να κάνει τα ακόλουθα:

- Να ορίσει το πεδίο εφαρμογής και τα όρια του ISMS ανάλογα με το είδος του οργανισμού, τη τοποθεσία του, τα αγαθά και την τεχνολογία του και να δικαιολογήσει τυχόν εξαιρέσεις.
- Να ορίσει μία πολιτική ασφαλείας
- Να εξασφαλίσει τη δέσμευση της διοίκησης
- Να ορίσει τη προσέγγιση που θα ακολουθεί ο οργανισμός για risk assessment
- Να αναπτύξει κριτήρια για αποδοχή κινδύνου και να ορίσει το αποδεκτό επίπεδο κινδύνου
- Να αναγνωρίσει το ρίσκο
- Να αναγνωρίσει τα αγαθά που ανήκουν στο πεδίο εφαρμογής του ISMS, τους ιδιοκτήτες των αγαθών και τις απειλές για αυτά.
- Να αναγνωρίσει ευπάθειες που μπορεί να εκμεταλλευτούν αυτές οι απειλές
- Να αναγνωρίσει το impact σε περίπτωση απώλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας για κάθε αγαθό.
- Να επιλέξει τα controls που θα υλοποιήσει με βάση το Annex A του προτύπου και τέλος
- Να ετοιμάσει το Statement of Applicability, καταγράφοντας τα επιλεγμένα controls και δικαιολογώντας τυχόν εξαιρέσεις.

Φάση 2: Υλοποίηση του ISMS

Ο οργανισμός στη φάση αυτή πρέπει να κάνει τα ακόλουθα:

- Να διατυπώσει ένα σχέδιο αντιμετώπισης του κινδύνου, το οποίο να αναγνωρίζει τις κατάλληλες ενέργειες από τη μεριά του management, τους πόρους, τις αρμοδιότητες και τις προτεραιότητες για τη διαχείριση των κινδύνων.
- Να υλοποιήσει το σχέδιο αντιμετώπισης του κινδύνου
- Να υλοποιήσει τα επιλεγμένα controls
- Να ορίσει μετρικές για την αποτελεσματικότητα των επιλεγμένων controls
- Να υλοποιήσει trainings και awareness προγράμματα για τα εμπλεκόμενα μέλη
- Να διαχειρίζεται τις λειτουργίες και τους πόρους του ISMS.

Φάση 3: Παρακολούθηση του ISMS

Στη φάση αυτή ο οργανισμός πρέπει:

- Να παρακολουθεί και να ελέγχει τις διαδικασίες και τα controls ώστε να εντοπίζει εγκαίρως πιθανά λάθη.
- Να εντοπίζει πιθανές προσπάθειες ή επιτυχημένες προσπάθειες για περιστατικά ασφαλείας
- Η διοίκηση θα πρέπει να καθορίζει αν οι δραστηριότητες ασφαλείας που έχουν δοθεί σε ανθρώπους ή έχουν υλοποιηθεί με τεχνολογικά μέσα, λειτουργούν όπως είχαν οριστεί.
- Να αποφασίζει αν οι δράσεις που έγιναν για να επιλύσουν ένα κενό ασφαλείας είναι αποτελεσματικές
- Να προβαίνει σε τακτικές αξιολογήσεις της αποτελεσματικότητας του ISMS, λαμβάνοντας υπόψη αποτελέσματα από audit, περιστατικά, μετρήσεις αποτελεσματικότητας και τις προτάσεις από όλα τα ενδιαφερόμενα μέλη.
- Να μετράει την αποτελεσματικότητα των controls για να εξασφαλίζει ότι τηρήθηκαν οι απαιτήσεις ασφαλείας
- Να επανεξετάζει το risk assessment σε τακτά χρονικά διαστήματα και τους εν λόγω κινδύνους, λαμβάνοντας υπόψη τις αλλαγές στον οργανισμό, τη τεχνολογία, τους επιχειρηματικούς στόχους και διαδικασίες, τις εντοπισμένες απειλές και εξωτερικούς παράγοντες όπως αλλαγές στη νομοθεσία και το κοινωνικό κλίμα.
- Να πραγματοποιεί εσωτερικά audit του ISMS σε τακτά χρονικά διαστήματα.
- Να ανανεώνει τα σχέδια ασφαλείας ώστε να συμπεριλαμβάνουν τα ευρήματα της παρακολούθησης και των δραστηριοτήτων επανελέγχου
- Να καταγράφει τις δράσεις και τα γεγονότα που θα μπορούσαν να επηρεάσουν την αποτελεσματικότητα ή την απόδοση του ISMS.

Φάση 4: Διατήρηση και Βελτίωση του ISMS

Ο οργανισμός θα πρέπει να κάνει τακτικά τα ακόλουθα:

- Να επανελέγχει και να μετράει την αποτελεσματικότητα του ISMS
- Να υλοποίει της αναγνωρισμένες βελτιώσεις στα πλαίσια του ISMS
- Να παίρνει τα κατάλληλα μέτρα διορθωτικών ενεργειών
- Να επικοινωνεί τις όποιες ενέργειες και βελτιώσεις σε όλα τα ενδιαφερόμενα μέλη
- Να εξασφαλίζει ότι οι βελτιώσεις επιτυγχάνουν τα σκοπό τους
- Να καταγράφει τις ενέργειες και τα γεγονότα που επηρεάζουν το ISMS.

3. Σχεδίαση και υλοποίηση μίας web εφαρμογής για υποστήριξη των *ISMS κατά ISO27001:2013* audits

3.1 Εισαγωγή

Μια εφαρμογή ακολουθεί ένα κύκλο ζωής που αποτελείται από 5 φάσεις. Τη σύλληψη, την υλοποίηση, τη χρήση και συντήρηση και τέλος την απόσυρση.

Συνήθως η χρήση και η συντήρηση γίνεται συγχρόνως με σκοπό την βελτίωση και διόρθωση λαθών. Μετά την αναγνώριση των αναγκών της επιχείρησης και τη σύλληψη της εφαρμογής, αρχίζει η διαδικασία υλοποίησής του.

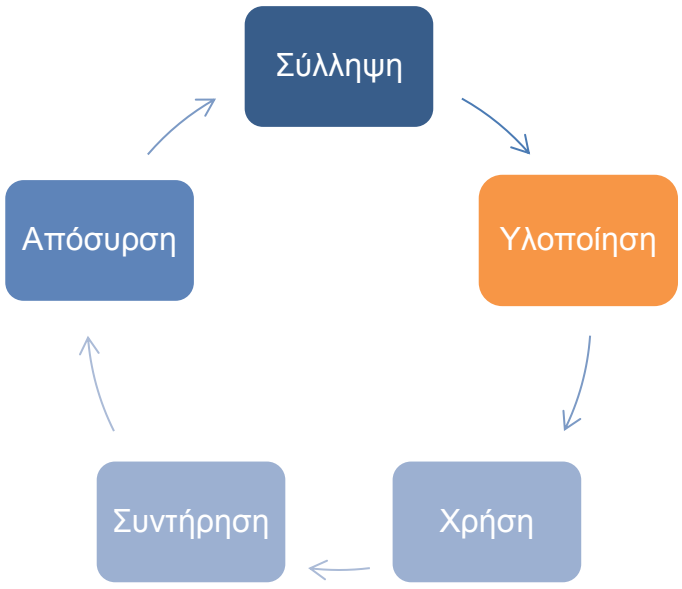
Στη φάση αυτή περιλαμβάνεται

- η ανάλυση των απαιτήσεων
- ο λογικός και φυσικός σχεδιασμός
- η υλοποίηση
- ο έλεγχος και τελικώς
- η εγκατάσταση του συστήματος

Στην συνέχεια ακολουθούν οι φάσεις

- χρήσης
- συντήρησης και
- αξιολόγησης του συστήματος

Μετά από μία χρονική περίοδο όπου το σύστημα έχει ολοκληρώσει τον κύκλο ζωής του και δεν ικανοποιεί πλέον τις ανάγκες της επιχείρησης , αποσύρεται. Στο κεφάλαιο αυτό θα ασχοληθούμε με το κομμάτι του σχεδιασμού του συστήματος. Θα γίνει ανάλυση απαιτήσεων και θα παρουσιαστούν τα εργαλεία που χρησιμοποιήθηκαν με σκοπό την δημιουργία ενός πετυχημένου συστήματος διαχείρισης των audits κατά το πρότυπο ISO27001:2013.



3.2 Ανάλυση απαιτήσεων

Η ανάλυση απαιτήσεων αποτελεί ένα αναπόσπαστο και θεμελιώδες κομμάτι της ανάπτυξης και σχεδίασης ενός λογισμικού. Οργανώνει τη σκέψη των εμπλεκομένων (προγραμματιστών, αναλυτών κλπ) και βοηθά στον επιτυχημένο προγραμματισμό και τη διαχείριση του έργου. Για να στηθεί μία επιτυχημένη web εφαρμογή θα πρέπει να έχει προηγηθεί ορθολογικός σχεδιασμός και ορθή εκτίμηση των αναγκών. Στο κομμάτι αυτό παρουσιάζεται μία λίστα προδιαγραφών που πρέπει να εξασφαλίζει το σύστημα. Για να συμπληρωθεί η λίστα αυτή θα πρέπει να απαντήσουμε σε διάφορα επιχειρηματικά αλλά και τεχνικά ζητήματα.

Για παράδειγμα

Επιχειρηματικά:

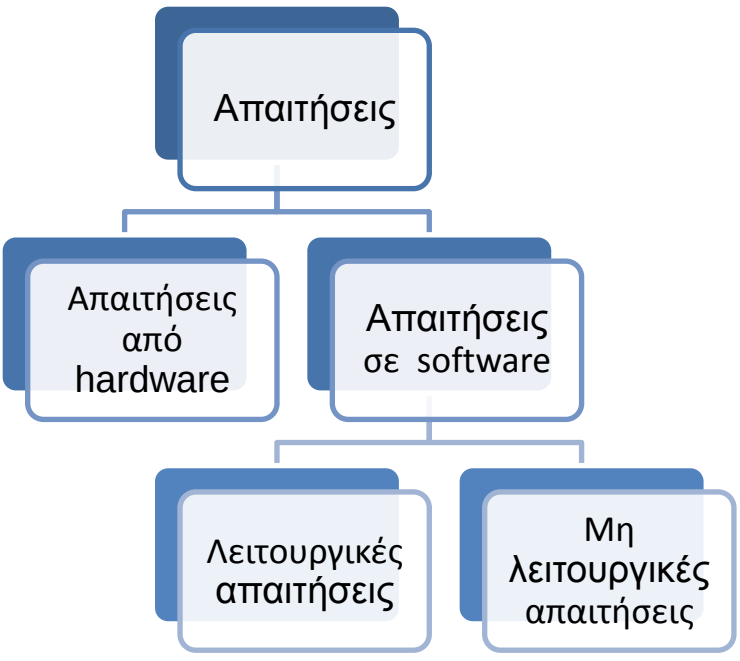
- Πρέπει να γνωρίζουμε τι ακριβώς θέλει να πετύχει η εφαρμογή
- αν υπάρχουν άλλες παρόμοιες
- σε τι κοινό απευθύνεται και
- ποιες οι απαιτήσεις ασφαλείας για τα αποθηκευμένα δεδομένα.

Από τεχνική άποψη:

Από τεχνικής απόψεως θα πρέπει να αποφασιστεί

- σε τι πλατφόρμα θα στηθεί η εφαρμογή
- αν θα υπάρχει βάση δεδομένων και ποια
- που θα φιλοξενηθεί
- τι λειτουργίες θα προσφέρονται στον χρήστη
- πως θα είναι εμφανισιακά η εφαρμογή
- από ποιον browser θα είναι καλύτερα προσβάσιμο,
- και πως θα γίνεται η συντήρησή της.

Αυτά είναι λίγα από τα ζητήματα που θα προσπαθήσουμε να διευκρινίσουμε στο κομμάτι αυτό.



Ανταγωνισμός

Με βάση τη γνώση μας αυτή τη στιγμή, υπάρχουν διάφορες web εφαρμογές διαθέσιμες στο internet που παρέχουν παρόμοια υπηρεσία. Οι υπηρεσίες όμως είναι συνδρομητικές και πολλές φορές αρκετά ακριβές. Η εφαρμογή λοιπόν στοχεύει στην ευχρηστία και στην αποτελεσματική παρουσίαση των αποτελεσμάτων ώστε να προτιμάται από τις άλλες και να είναι ιδιαίτερα προσιτό και προτιμητέο.

Χρήστες του συστήματος

Οι τελικοί χρήστες της εφαρμογής είναι:

- Ο διαχειριστής/ administrator
- Ο ελεγκτής/ auditor
- Ο προγραμματιστής

Λειτουργικές απαιτήσεις

Auditor:

- **Σύνδεση (Log in):**

Με όνομα χρήστη και κωδικό, ο ελεγκτής (auditor) θα μπορεί να συνδεθεί στην εφαρμογή

- **Υπενθύμιση κωδικού:**

Σε περίπτωση που ο χρήστης ξεχάσει το κωδικό του, θα συμπληρώνει το e-mail account του και η εφαρμογή θα στέλνει αυτόματα ένα e-mail για αναδημιουργία κωδικού

- **Επεξεργασία profile:**

Ο auditor θα έχει πρόσβαση στην επεξεργασία των στοιχείων του όπως αυτά εμφανίζονται στην εφαρμογή: First name, Last name, Username, e-mail, password και profile picture.

- **Καταχώρηση νέου audit:**

Στη λειτουργία αυτή ο auditor θα καταχωρεί μία νέα φόρμα με τα αντίστοιχα πεδία όπως αυτά εμφανίζονται στην εφαρμογή:

  - Auditor: Το όνομα του auditor που εκτέλεσε το audit.
  - Company: Το όνομα της εταιρείας για την οποία πραγματοποιήθηκε το audit.
  - Το είδος του audit:
    - Initial: Τη πρώτη φορά που η εταιρεία ελέγχεται για το υλοποιημένο ISMS κατά ISO27001:2013
    - 2nd: Σε περίπτωση που η εταιρεία είναι ήδη πιστοποιημένη κατά ISO27001:2013 και πραγματοποιείται επανέλεγχος
    - 3rd: Σε περίπτωση που η εταιρεία είναι ήδη πιστοποιημένη κατά ISO27001:2013 και πραγματοποιείται δεύτερος επανέλεγχος
  - Required documents: Ο auditor θα επιλέγει όλα τα υποχρεωτικά έγγραφα που διατηρεί η εταιρεία και είναι απαραίτητα με βάση το πρότυπο. Σε περίπτωση που ο auditor δεν αναγνωρίσει ένα

έγγραφο (είτε δεν υπάρχει καθόλου είτε είναι ελλιπές), η εφαρμογή το αναγνωρίζει ως non-conformity, και η εταιρεία δεν μπορεί να πιστοποιηθεί.

- Implemented Controls: Ο auditor θα επιλέγει τα controls για το οποία θα ελέγξει την εταιρεία. Συνήθως επιλέγονται κάποια controls, δειγματοληπτικά, με βάση το Statement of Applicability της εταιρείας. Η εφαρμογή θα πρέπει να καθοδηγεί τον auditor για την επιλογή των controls. Για κάθε control, ο auditor θα δηλώνει αν κατά τη διάρκεια του audit το control αναγνωρίστηκε ως conformity ή non/conformity.

- **Προβολή καταχωρημένων audit:**

Ο auditor θα βλέπει όλα τα καταχωρημένα audit ανεξάρτητα από ποιον χρήστη έχουν καταχωρηθεί. Οι πληροφορίες στις οποίες θα έχει πρόσβαση είναι οι ακόλουθες**:**

- Όνομα εταιρείας
- Auditor
- Είδος του audit
- Αναγνωρισμένα Non-Conformities για τα υποχρεωτικά έγγραφα
- Αναγνωρισμένα Non-Conformities για τα επιλεγμένα controls
- Στατιστικά υπαρχόντων εγγράφων και ελεγμένων controls

- **Συμμετοχή σε φόρουμ ερωτήσεων – απαντήσεων:**

Η εφαρμογή θα υποστηρίζει μία λειτουργία τύπου φόρουμ, όπου οι χρήστες/auditors, θα μπορούν να θέτουν άμεσα απορίες σχετικές με την εφαρμογή και θα μπορούν να απαντούν σε ερωτήσεις άλλον χρηστών. Αυτό αποσκοπεί στην άμεση αλληλεπίδραση και συνεργασία χρηστών.

Administrator:

- **Δημιουργία νέων χρηστών/auditors:**

Ο administrator θα μπορεί να δημιουργήσει νέους χρήστες με δικαιώματα χρηστών auditors. Για τη δημιουργία χρήστη χρειάζεται να συμπληρώσει τα παρακάτω πεδία:

- ένα έγκυρο e-mail account
- first name και last name
- username
- password

- **Προβολή όλων των καταχωρημένων audits και επεξεργασία τους:**

Ο administrator θα έχει πρόσβαση σε όλες τις καταχωρήσεις και θα μπορεί να τις επεξεργαστεί/διορθώσει.

- **Διαγραφή καταχωρήσεων:**

Ο administrator μπορεί να διαγράψει τις καταχωρήσεις αν κριθεί απαραίτητο.

- **Εξαγωγή καταχωρήσεων σε “csv” μορφή:**

Ο administrator θα μπορεί να εξάγει τις καταχωρήσεις και τα αποτελέσματα σε csv μορφή για περεταίρω επεξεργασία ή αποστολή των αποτελεσμάτων σε τρίτους.

- **Επεξεργασία υπάρχουσας φόρμας:**

Τέλος, ο administrator μπορεί να αλλάξει τα στοιχεία της φόρμας σε περίπτωση που θέλει να αλλάξει κάποια ερώτηση σχετικά με τα controls ή να προσθέσει κάποιο extra πεδίο.

Μη λειτουργικές απαιτήσεις

- **Σχεδίασης:**
  - Web Server: Apache Server σε Linux περιβάλλον
  - CMS: Wordpress
  - Σύστημα Διαχείρισης Βάσης Δεδομένων: MySql
  - Browser δοκιμής: Google Chrome, Mozilla Firefox,Internet Explorer
  - Σύστημα διαχείρισης της MySql μέσω browser: PhpMyAdmin.

- **Βάσεων δεδομένων**

Θα τηρείται μια Βάση Δεδομένων στην Βάση Δεδομένων του Host με όλους τους απαραίτητους πίνακες όπως αυτοί δημιουργούνται από το CMS και τα διάφορα plugins που θα χρησιμοποιηθούν

- **Χρήσης**

Το πρόγραμμα θα διαθέτει ένα φιλικό περιβάλλον εργασίας.

- **Επιδόσεων**
  - Το λογισμικό θα πρέπει να αποκρίνεται άμεσα και να διαχειρίζεται τα δεδομένα του χρήστη γρήγορα
  - Το σύστημα πρέπει να μπορεί να εξυπηρετεί αποδοτικά πολλούς χρήστες ταυτόχρονα
- **Υλοποίησης**
  - Θα χρησιμοποιούνται Η/Υ οι οποίοι είναι εξοπλισμένοι με φυλλομετρητές. Μας ενδιαφέρουν κυρίως ο Firefox Mozilla και ο Google Chrome καθώς είναι οι πιο διαδεδομένοι στη χώρα μας αλλά και ο Internet Explorer.
  - Οι υπολογιστές που θα συνδέονται στην εφαρμογή, θα πρέπει να ανήκουν σε ένα δίκτυο που τους δίνει πρόσβαση στο WWW.
  - Θα χρησιμοποιηθεί HttpWebServer σε LocalHost εγκατάσταση ώστε σε πρώτη πειραματική φάση, να επιτύχουμε μηδενικό κόστος.
- **Αξιοπιστίας**

Το σύστημα θα πρέπει να είναι διαθέσιμο όποτε το χρειάζεται ο χρήστης του συστήματος . Το σύστημα θα πρέπει να εγγυάται (τις κατά το δυνατόν) λιγότερες αποτυχίες.

- **Συντήρησης**

Το σύστημα θα συντηρείται σε τοπικό επίπεδο για να μην επηρεαστεί η λειτουργικότητα του.

- **Ασφάλειας**

Καθώς στο σύστημα αποθηκεύονται δεδομένα που αποδεικνύουν τη τρέχουσα κατάσταση μίας εταιρείας σχετικά με το ISMS της, θα πρέπει να εξασφαλιστεί ότι το σύστημα είναι όσο το δυνατόν ασφαλές. Αυτό σημαίνει ότι εξασφαλίζει σε ικανοποιητικό βαθμό την εμπιστευτικότητα, την εγκυρότητα και

την διαθεσιμότητα των δεδομένων. Για το σκοπό αυτό θα πραγματοποιηθεί penetration testing στην εφαρμογή σε επίπεδο εφαρμογής και server.

- **Κριτήρια αποδοχής συστήματος**

Για να γίνει δεκτή η εφαρμογή θα πρέπει να πραγματοποιηθεί η υλοποίηση της εντός λογικού χρονικού διαστήματος, να καλύπτει τις ανάγκες για τις οποίες σχεδιάστηκε και να είναι εύκολο στη χρήση.

3.3 Στήνοντας την εφαρμογή

Εργαλεία

Τα παρακάτω εργαλεία χρησιμοποιήθηκαν για να αναπτυχθεί η εφαρμογή:

- Apache Web Server 2.4.17
- MySql Database 5.0.11-dev
- phpMyAdmin 4.5.2
- PHP 5.6.15
- Wordpress 4.4

Σε επίπεδο εφαρμογής χρησιμοποιήθηκαν τα παρακάτω plugins για το Wordpress ώστε να επιτευχθούν οι στόχοι λειτουργίας της εφαρμογής:

- Ninja-form plugin 2.9.33

Με το plugin αυτό, δημιουργήθηκε η κυρίως φόρμα για την καταχώρηση των audits.

- Ninja-form conditional logic 1.3.9

Το plugin αυτό, ήταν απαραίτητο για τη δημιουργία εξαρτημένων ερωτήσεων. Ανάλογα με το control που επιλέγει ο auditor να ελέγξει, εμφανίζετε και η αντίστοιχη ερώτηση που καλείτε να απαντήσει για να κρίνει το control ως conformity ή non-conformity.

- Insert PHP 1.3

Το plugin αυτό, χρειάστηκε ώστε να καταφέρει ο προγραμματιστής να εισάγει προσαρμοσμένο PHP κώδικα με σκοπό να εμφανίσει τα καταχωρημένα audits στους auditor users.

- Login with Ajax 3.1.5

Το plugin αυτό, χρειάστηκε ώστε να μπορούν οι auditors να συνδέονται στην εφαρμογή χωρίς να έχουν πρόσβαση στο back-end της εφαρμογής.

- User Access Manager 2.6.6

Το plugin αυτό, ήταν απαραίτητο για να εξασφαλίσει ότι στη φόρμα καταχώρησης audits έχουν πρόσβαση μόνο συνδεδεμένοι χρήστες

- Jquery-plugin-circliful

Το plugin αυτό, χρησιμοποιήθηκε για τη προβολή των σχεδιαγραμμάτων/στατιστικών αποτελεσμάτων ενός audit.

Διαδικασία Ανάπτυξης

- **Εγκατάσταση λογισμικών:**

Το πρώτο βήμα για τη δημιουργία της εφαρμογής ήταν η εγκατάσταση των παρακάτω λογισμικών

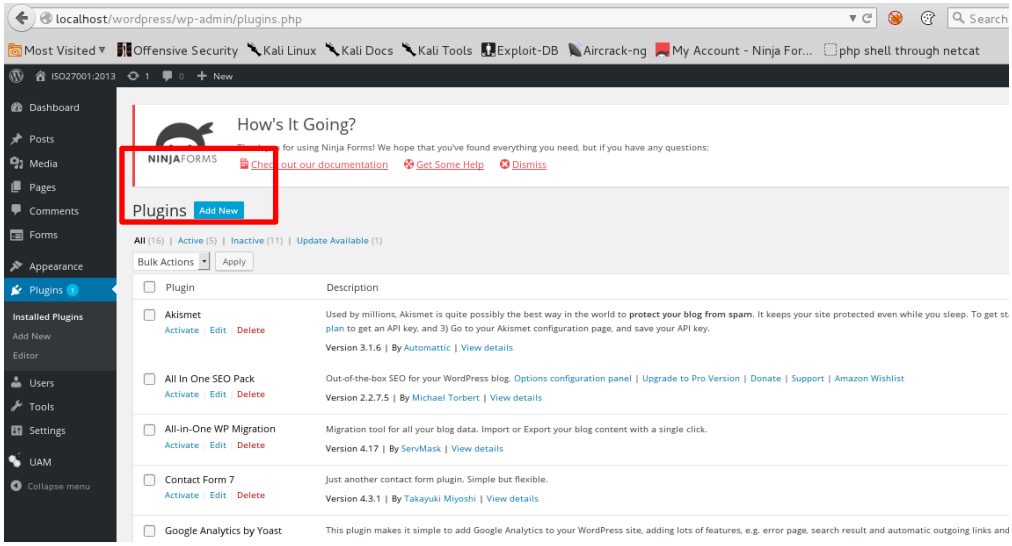
- XAMPP 5.6.15
- Bitnami Wordpress 4.4.00-module

Ακολουθώντας τις εκάστοτε οδηγίες τα εργαλεία αυτά εγκαθιστούν γρήγορα και εύκολα όλα τα απαραίτητα αρχεία και τη βάση δεδομένων. Μετά την εγκατάσταση αυτών των εργαλείων, χρησιμοποιώντας έναν browser και ακολουθώντας των παρακάτω σύνδεσμο μπορούμε να οδηγηθούμε στο default wordpress interface που εγκαταστάθηκε:

- User Interface: http://localhost/wordpress
- Administrator interface: http://localhost/wordpress/wp-admin

- **Εγκατάσταση plugins:**

Χρησιμοποιώντας το interface του administrator, ο συνδεδεμένος χρήστης επιλέγει από το αριστερό μενού “plugins”, και μετά την επιλογή “add new”.



Από εκεί ο administrator μπορεί να κάνει search τα απαραίτητα plugin και το Wordpress θα αναλάβει την εγκατάστασή τους.

Δουλεύοντας σε localhost περιβάλλον χρειάζεται να προστεθεί η παρακάτω εντολή στο wp-config.php file ώστε να μην απαιτούνται ftp credentials για το host: `define('FS_METHOD','direct');`

- **Δημιουργία φόρμας:**

Επιλέγοντας από το αριστερό μενού την επιλογή “Forms” και στη συνέχεια “add new” και στην καρτέλα “Build your form” ο administrator πρέπει να

δημιουργήσει τη φόρμα που θα συμπληρώνουν οι auditors. Χρειάστηκε να δημιουργηθούν συνολικά 150 πεδία τύπου textbox, checkbox, lists κ.α

Αναλυτικά:

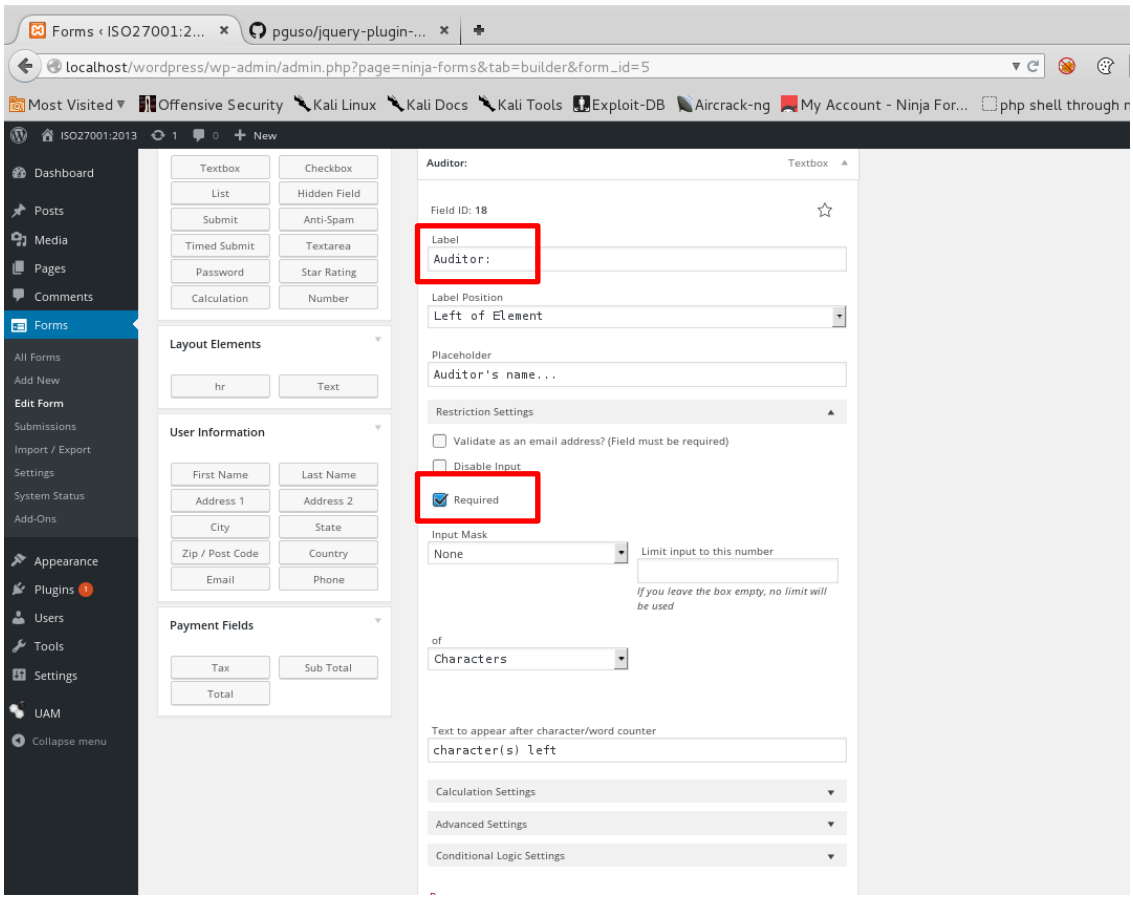
Η φόρμα χωρίζεται σε 3 μέρη:

- Τις αρχικές πληροφορίες
- Τα υποχρεωτικά έγγραφα
- Τα controls και τις ερωτήσεις συμμόρφωσης

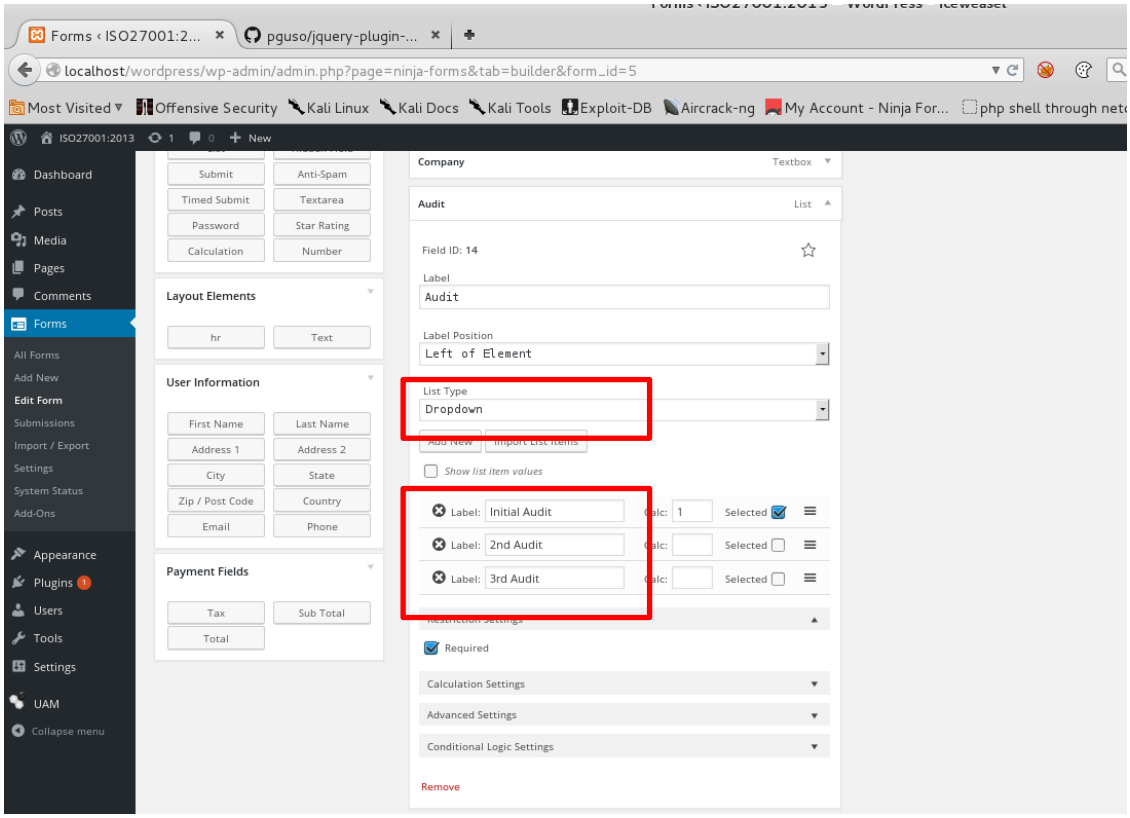
Στις αρχικές πληροφορίες εντάσσονται τα πεδία: Auditor, Company, Audit

όπως αυτά έχουν αναλυθεί στο κεφάλαιο “3.2 Ανάλυση απαιτήσεων ”.

Τα πεδία ορίζονται ως υποχρεωτικά και ο auditor θα πρέπει να τα συμπληρώσει. Στην παρακάτω εικόνα φαίνεται η δομή του πεδίου “auditor”.

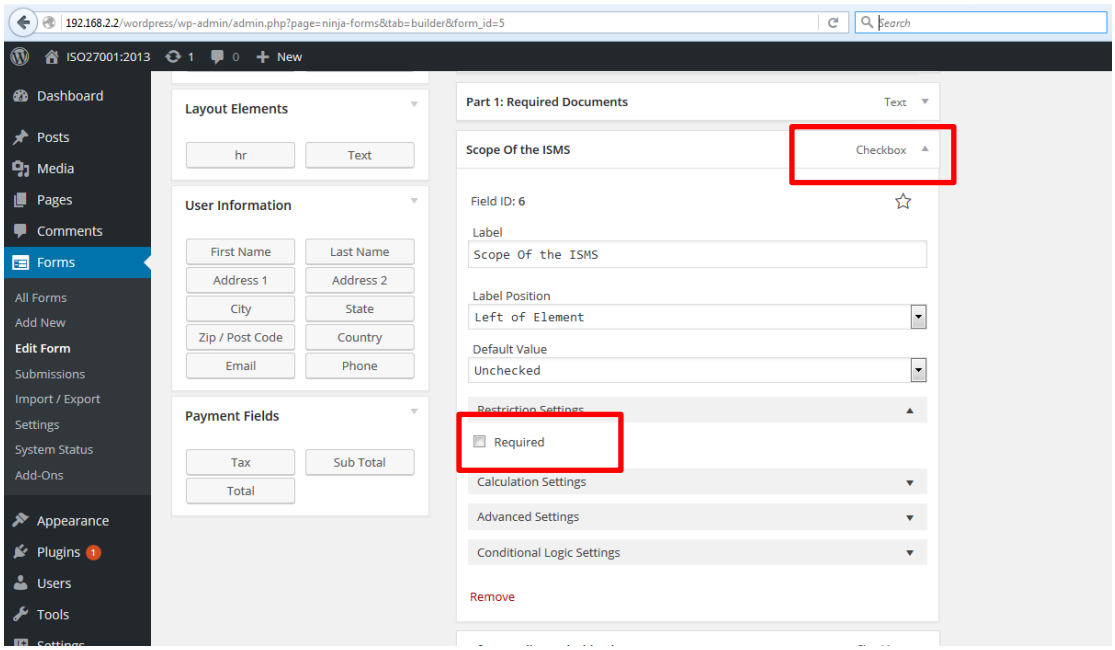


Το πεδίο “audit” έχει 3 προκαθορισμένες τιμές οι οποίες θα εμφανίζονται ως dropdown επιλογές στον χρήστη/auditor.



Στο δεύτερο μέρος, υποχρεωτικά έγγραφα, ο administrator πρέπει να δημιουργήσει μία λίστα από checkbox με όλα τα υποχρεωτικά έγγραφα όπως αυτά ορίζονται από το ISO27001:2013 και παρουσιάζονται στον “Πίνακας 2 - Υποχρεωτικά Έγγραφα κατά το ISO27001:2013”

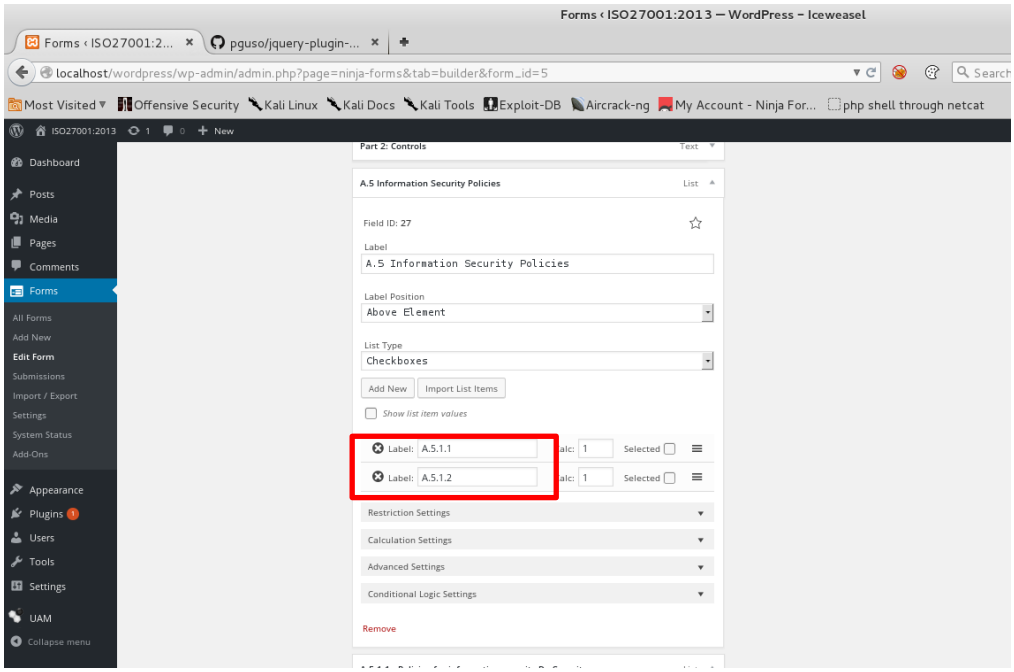
Στη παρακάτω εικόνα βλέπουμε πως ορίζεται το πρώτο έγγραφο “Scope of the ISMS”. Το πεδίο αυτό -όπως και όλη η υπόλοιπη λίστα- δεν είναι υποχρεωτικό, σε περίπτωση όμως που ο auditor δεν το επιλέξει θα οδηγηθεί σε non-conformities αποτελέσματα.



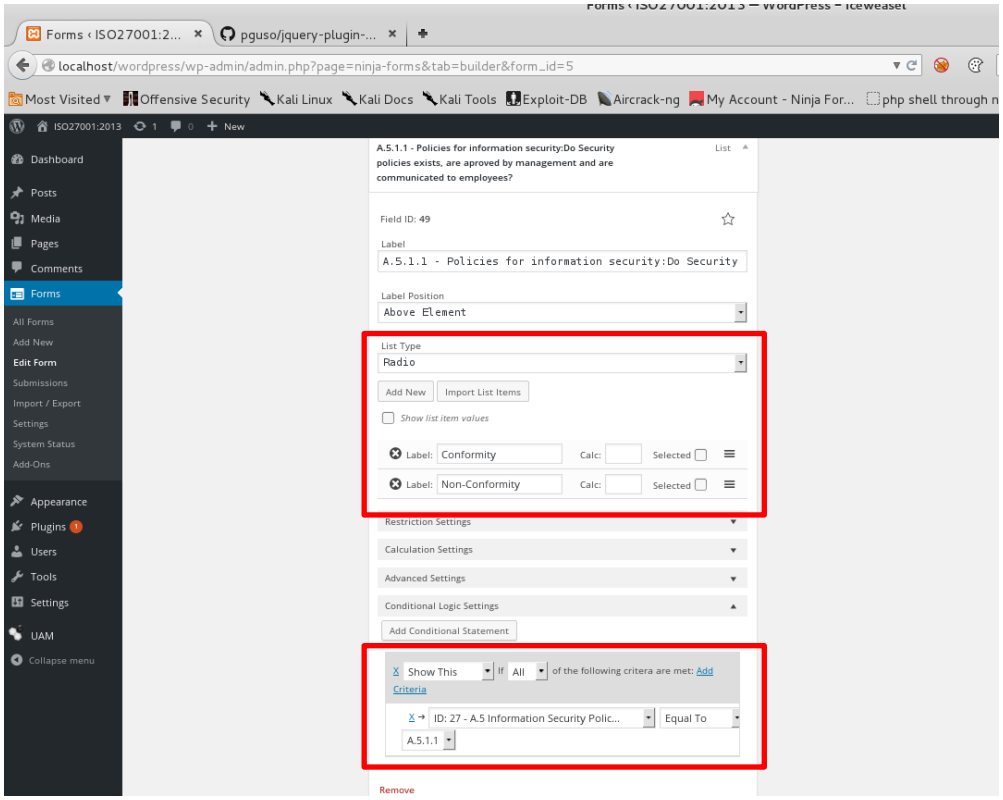
Στο τρίτο μέρος, παρουσιάζονται τα controls που περιλαμβάνονται στο ISO27001:2013. Τα controls χωρίζονται σε 14 κατηγορίες –A.5 έως A.18- και παρουσιάζονται στον “Πίνακας 3 - Κατηγορίες των controls”.

Για κάθε κατηγορία δημιουργήθηκε μία λίστα με checkboxes για όλα τα controls της κατηγορίας. Επιπλέον για κάθε control, δημιουργήθηκε μία ερώτηση με δύο επιλογές τύπου radio, ώστε ο auditor να επιλέγει confromty ή non-conformity αντίστοιχα. Οι ερωτήσεις αυτές έχουν δημιουργηθεί επιλέγοντας τα conditional logic settings, ώστε να εμφανίζονται μόνο εάν ο auditor έχει επιλέξει το αντίστοιχο control για audit. Σε περίπτωση που ο auditor επιλέξει το αντίστοιχο control, πρέπει υποχρεωτικά να απαντήσει στην ερώτηση που θα εμφανιστεί.

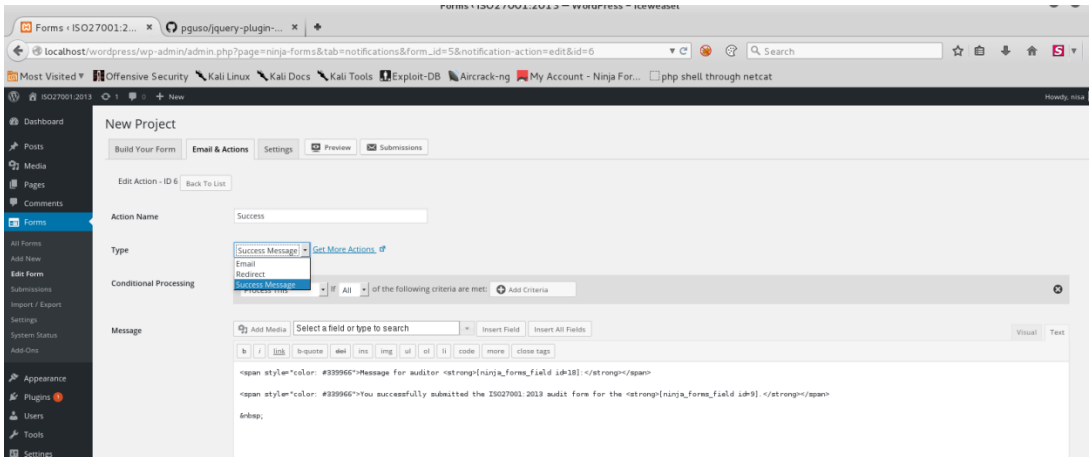
Στην εικόνα παρακάτω φαίνεται η δημιουργία της κατηγορίας A.5 με τα αντίστοιχα controls.



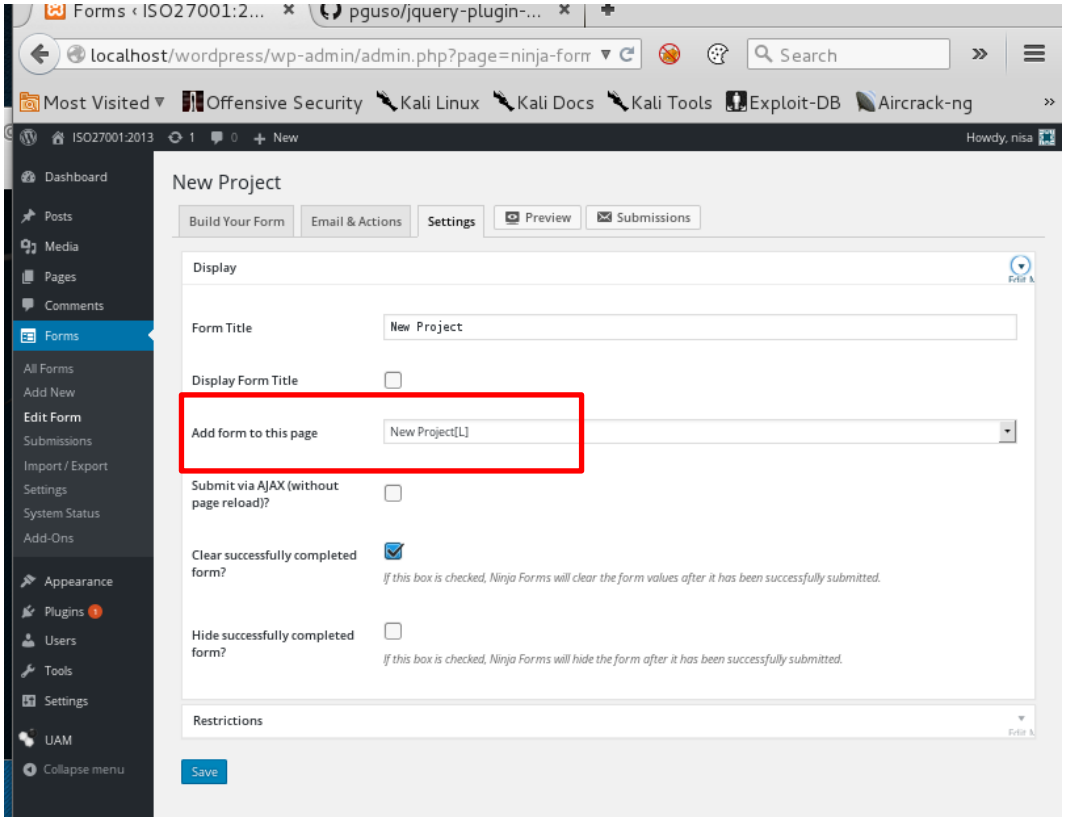
Στην εικόνα παρακάτω φαίνεται η δημιουργία της ερώτησης που αφορά το control A.5.1.1 και εμφανίζεται μόνο αν ο auditor το επιλέξει.



Επιπλέον, επιλέγοντας την καρτέλα “Email & Actions” , ο administrator μπορεί να δημιουργήσει ένα “success message” να εμφανίζεται κάθε φορά που ο auditor καταχωρεί τη φόρμα.



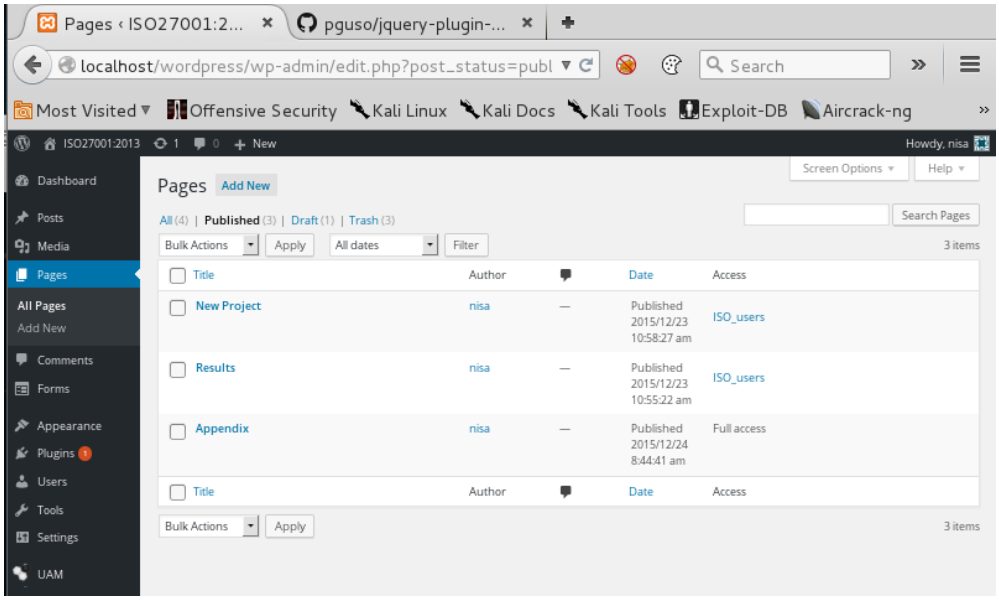
Τέλος, επιλέγοντας την καρτέλα “Settings”, ο administrator επιλέγει να εμφανίσει τη φόρμα στη σελίδα με όνομα “New Project”



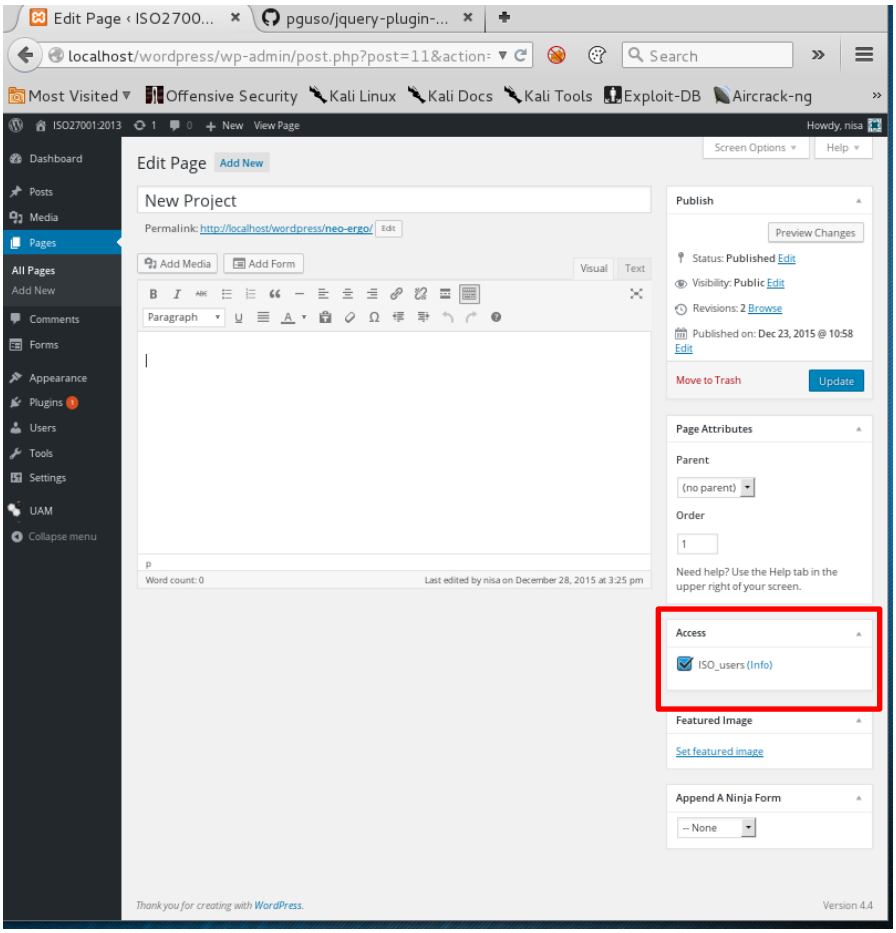
- **Δημιουργία σελίδων (Pages)**

Επιλέγοντας “Pages” από το αριστερό μενού του administrator, ο χρήστης επιλέγει τις σελίδες που θα δημιουργηθούν για να υποστηρίξουν την εφαρμογή. Τρεις σελίδες κρίθηκαν απαραίτητο ότι πρέπει να δημιουργηθούν:

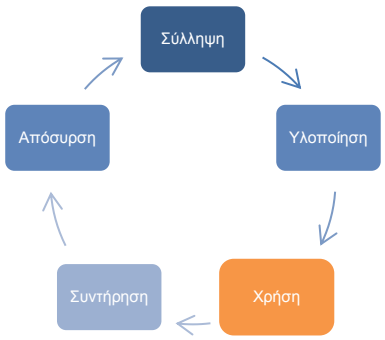
- New project: εδώ εμφανίζεται η φόρμα καταχώρησης νέου audit
- Results: εδώ εμφανίζονται πληροφορίες για όλα τα audits που έχουν καταχωρηθεί.
- Appendix: εδώ εμφανίζονται συμπληρωματικές πληροφορίες για τους auditors



Οι δύο πρώτες σελίδες είναι προσβάσιμες μόνο από συνδεδεμένους χρήστες/auditors. Αυτό το ρυθμίζει ο administrator με τη βοήθεια του “User Access Manager” plugin, όπως φαίνεται παρακάτω.



4. Μελέτη περίπτωσης



4.1 Εισαγωγή

Στην συνέχεια του κεφαλαίου παρουσιάζονται 3 διαφορετικές περιπτώσεις επιχειρήσεων οι οποίες πέρασαν έλεγχο με βάση το πρότυπο ISO27001:2013. Κάθε εύρημα που αναγνωρίστηκε κατά τη διάρκεια του ελέγχου ως non-conformity βαθμολογείται με βάση τον παρακάτω πίνακα:

Επίπεδο αξιολόγησης ευρημάτων	Περιγραφή
Major	Ευρήματα του audit που χαρακτηρίζονται ως major, είναι σημαντικά non-conformities και πρέπει να δρομολογηθούν για επίλυση εντός 2 εβδομάδων. Επιπλέον ένα follow-up audit πρέπει να προγραμματιστεί στο τέλος αυτού του διαστήματος. Η επιχείρηση δεν πιστοποιείται.
Minor	Ευρήματα του audit που χαρακτηρίζονται ως minor, είναι μικρής σημασίας non-conformities και πρέπει να δρομολογηθούν για επίλυση εντός 2 μηνών. Επιπλέον ένα follow-up audit πρέπει να προγραμματιστεί στο τέλος αυτού του διαστήματος. Η επιχείρηση πιστοποιείται αλλά σε περίπτωση αδυναμίας συμμόρφωσης, το πιστοποιητικό ανακαλείται.
Observation	Ευρήματα του audit που χαρακτηρίζονται ως observation πρέπει να δρομολογηθούν για επίλυση εντός 6 μηνών και η εξέλιξη τους πρέπει να παρακολουθείτε τακτικά μέχρι την οριστική επίλυση τους.
Recommendation	Ευρήματα του audit που χαρακτηρίζονται ως recommendations δεν είναι απαραίτητο να επιλυθούν. Μπορούν να προγραμματιστούν εντός 8 μηνών και η παρακολούθηση τους μπορεί και να μην προγραμματιστεί.

Πίνακας 5 - Επίπεδο αξιολόγησης των non-conformities

4.2 Σενάριο 1: Η επιχείρηση παρουσίασε major non-conformities

Η εταιρεία “CompanyA S.A”, η οποία δραστηριοποιείται στο τομέα των τηλεπικοινωνιών, υπόκειται σε έλεγχο και επιθυμεί να πιστοποιηθεί για πρώτη φορά με βάση το ISO 27001:2013. Για το σκοπό αυτό, το τμήμα πληροφορικής της εταιρείας ανέλαβε σε συνεργασία με τους διευθυντές των υπολοίπων τμημάτων, την προετοιμασία και υλοποίηση των απαραίτητων πολιτικών, διαδικασιών και δικλείδων ασφαλείας (controls) ώστε η επιχείρηση να πιστοποιηθεί.

Παρόλα αυτά, κατά τη διάρκεια του πρωταρχικού (initial) audit, αναγνωρίστηκαν διάφορα non-conformities όπως αυτά θα αναλυθούν παρακάτω. Ανάλογα με το επίπεδο αξιολόγησης η επιχείρηση έχει 2 εβδομάδες ή 3 μήνες για να συμμορφωθεί αλλιώς το πιστοποιητικό θα ακυρωθεί.

Αναλυτικά, η εταιρεία βρέθηκε να τηρεί όλα τα υποχρεωτικά έγγραφα όπως αυτά ορίζονται από το πρότυπο. Επιπλέον επιλέχτηκαν 15 controls από το SoA για έλεγχο με βάση τη μεθοδολογία επιλογής controls για audit που παρουσιάζεται εντός του εργαλείου. Τα ακόλουθα 3 controls αναγνωρίστηκαν ως non-conformity.

- 7.3.1 Termination or change of employment responsibilities
- 11.1.1 Physical security perimeter
- 17.1.2 Implementing information security continuity

Control	7.3.1 - Termination or change of employment responsibilities
Level	Major

Εντοπίσαμε 5 εργαζομένους οι οποίοι έχουν αποχωρήσει από την εταιρεία και ο εταιρικός τους λογαριασμός δεν έχει απενεργοποιηθεί στο active directory και στις εφαρμογές που είχαν πρόσβαση.

Επιπλέον, εντοπίσαμε 2 λογαριασμούς χρηστών οι οποίοι είχαν αποχωρήσει από τον Μάρτιο του ‘15 και ο λογαριασμός τους απενεργοποιήθηκε τον Ιανουάριο του 2016.

Καθυστερημένη ανάκληση των δικαιωμάτων πρόσβασης των χρηστών μπορεί να αυξήσει τον κίνδυνο οι πρώην εργαζόμενοι και /ή άλλοι εξωτερικοί συνεργάτες, να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα και εφαρμογές της Εταιρείας.

Επιπλέον, περιττοί λογαριασμοί χρηστών μπορεί να χρησιμοποιηθούν καταχρηστικά από τους υπάρχοντες εργαζομένους της εταιρείας για την εκτέλεση μη εξουσιοδοτημένων συναλλαγών.

Control	11.1.1 Physical security perimeter
Level	Major

Με βάση την επίσκεψή μας στο computer room της εταιρείας, το οποίο φιλοξενείται τοπικά στις εγκαταστάσεις της εντοπίστηκαν τα ακόλουθα:

- Σημειώθηκε ότι η θερμοκρασία στο δωμάτιο παρακολουθείται κατά τη διάρκεια των καθημερινές επισκέψεις του φύλακα με τη χρήση ενός κοινού θερμομέτρου.
- Ένα χειροκίνητο σύστημα πυρόσβεσης ήταν στη θέση του (οι συνήθεις κόκκινοι φορητοί πυροσβεστήρες). Ωστόσο, δεν υπήρχε ανιχνευτής πυρκαγιάς στο δωμάτιο.
- Δεν υπήρχαν αισθητήρες υγρασίας και πλημμύρας
- Η αίθουσα υπολογιστών είναι ένας κοινός χώρος γραφείων που δεν είναι επαρκώς προστατευμένος από περιστατικά πυρκαγιάς. Επιπλέον, η μία πλευρά καλύπτεται από ένα κοινό παράθυρο εκθέτοντας το δωμάτιο σε περιβαλλοντικούς κινδύνους (πλημμύρα, άνεμος, κ.λπ.).
- Δεν υπήρχαν κάμερες παρακολούθησης του χώρου.
- Το δωμάτιο βρέθηκε να είναι διαταραγμένο και ανοργάνωτο (καλώδια στο πάτωμα, τα αγαθά ήταν τοποθετημένα χωρίς τάξη, κλπ)
- Παρατηρήσαμε τέλος, ότι υπήρχε έλλειψη διαθέσιμου χώρου.

Η προστασία του υλικού πληροφορικής και των δεδομένων είναι κρίσιμη για τη διατήρηση παροχής υπηρεσιών στην επιχείρηση.

Control	17.1.2 Implementing information security continuity
Level	Minor

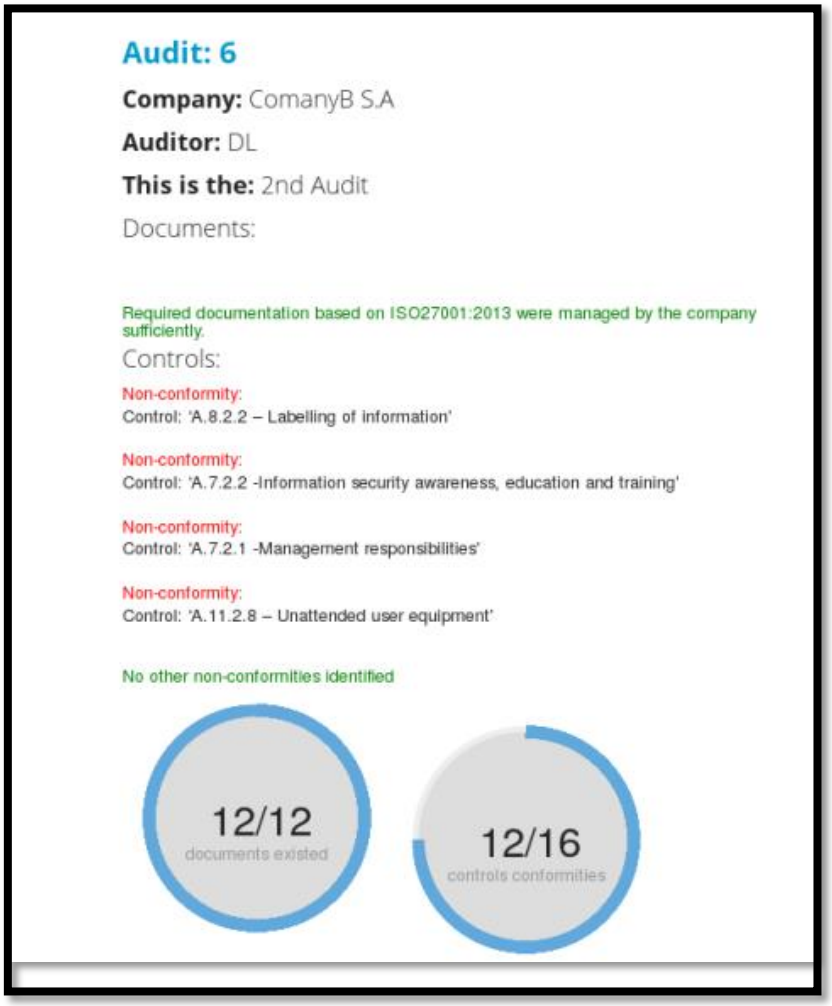
Η επισκόπησή μας εντόπισε ότι αν και έχουν αναπτυχθεί διαδικασίες επαναφοράς συστήματος για επιλεγμένα κρίσιμα συστήματα, δεν υπάρχει επίσημο και καταγεγραμμένο Business Continuity Plan (BCP) και Πλάνο Αποκατάστασης Καταστροφών (DRP) το οποίο να είναι σε θέση να εξασφαλίσει τη συνέχεια των κρίσιμων επιχειρηματικών διαδικασιών και υποδομών σε περίπτωση διακοπής.

Η απουσία των σχεδίων αποκατάστασης καταστροφών μπορεί να οδηγήσει σε αδυναμία έγκαιρης ανάκτησης κρίσιμων υπηρεσιών μετά από απρόβλεπτη διακοπή. Δεδομένου ότι υπάρχουν ήδη οι διαδικασίες, θα πρέπει να καταγραφούν και εγκριθούν από τη διοίκηση.


Audit: 5
Company: CompanyA S.A
Auditor: DL
This is the: Initial Audit
Documents:
Required documentation based on ISO27001:2013 were managed by the company sufficiently.
Controls:
Non-conformity:
Control: 'A.7.3.1 – Termination or change of employment responsibilities'
Non-conformity:
Control: 'A.11.1.1 – Physical security perimeter'
Non-conformity:
Control: 'A.17.1.2 – Implementing information security continuity'
No other non-conformities identified
12/12
documents existed
12/15
controls conformities

4.3 Σενάριο 2: Η επιχείρηση παρουσίασε minor non-conformities

Η επιχείρηση “CompanyB S.A” ελέγχεται για 2η φορά με βάση το πρότυπο ISO27001:2013. Ακολουθούν τα αποτελέσματα του audit.



Control	7.2.1 - Management responsibilities 7.2.2 - Information security awareness, education and training 8.2.2 - Labelling of information
Level	Minor

Παρατηρήθηκε ότι πολλοί νέοι υπάλληλοι δεν γνώριζαν τη πολιτική της επιχείρησης σχετικά με την ασφάλεια της πληροφορίας και ειδικότερα δεν γνώριζαν για τη διαδικασία «καταστροφής εμπιστευτικών εγγράφων». Έγγραφο με την ένδειξη “CONFIDENTIAL” βρέθηκε στον κάδο χωρίς να έχει καταστραφεί όπως ορίζει η πολιτική. Ένα πρόγραμμα ενημέρωσης των νέων υπαλλήλων για τη πολιτική της εταιρείας θα πρέπει να διεξάγεται σε τακτά χρονικά διαστήματα.

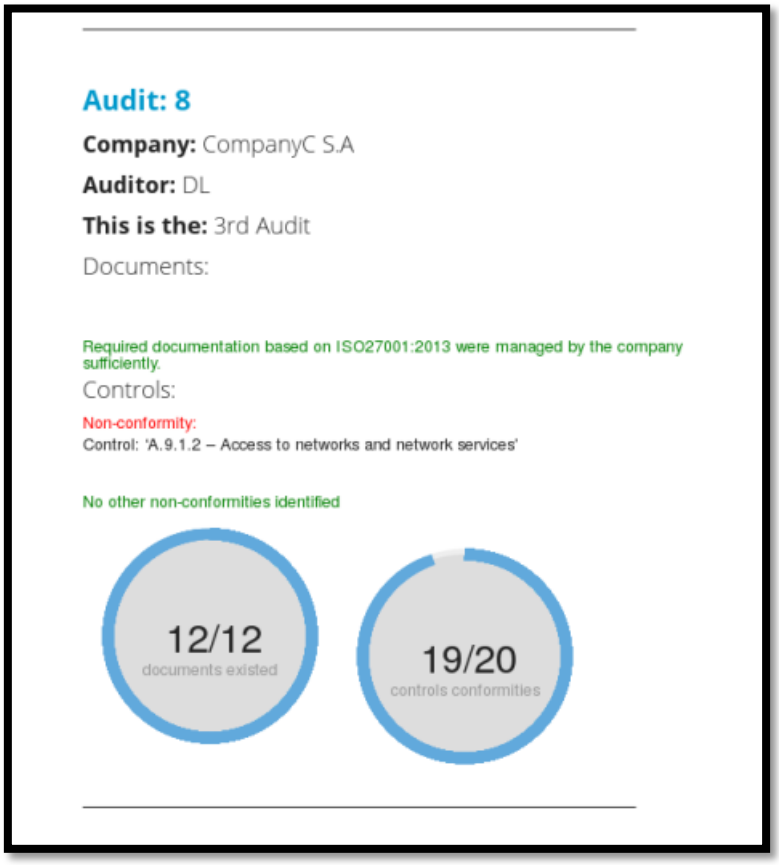
Control	11.2.8 Unattended user equipment 8.2.2 - Labelling of information
Level	Minor

Κατά τη διάρκεια του audit, ένα εταιρικό laptop βρέθηκε ξεκλείδωτο χωρίς την παρουσία του χρήστη που του ανήκε. Ένα πρόγραμμα ενημέρωσης των υπαλλήλων για τη πολιτική της εταιρείας θα πρέπει να διεξάγεται, ώστε να αποφεύγονται τέτοια περιστατικά.

4.4 Σενάριο 3: Η επιχείρηση πιστοποιείται κατευθείαν κατά ISO27001:2013

Η επιχείρηση "CompanyC S.A", πέρασε τον 3ο έλεγχο αξιολόγησης του ISMS της με βάση το πρότυπο ISO27001:2013. Η επιχείρηση ελέγχθηκε για άλλη μια φορά με επιτυχία και κρατάει τη πιστοποίηση της για 3η συνεχόμενη χρονιά. Πρόκειται για μια επιχείρηση παροχής συμβουλευτικών υπηρεσιών η οποία συστεγάζεται σε κεντρικό κτήριο μαζί με άλλες επιχειρήσεις.

Το αποτέλεσμα του audit παρουσιάζεται με τη βοήθεια του εργαλείου που δημιουργήθηκε.



Ο auditor κατέγραψε μόνο τη παρακάτω παρατήρηση (observation) χωρίς όμως αυτή να προκαλεί πρόβλημα συμμόρφωσης για την εταιρεία.

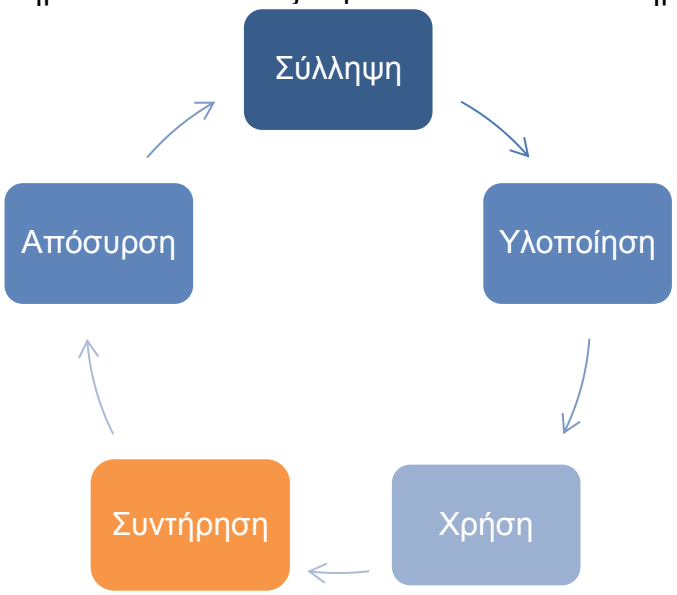
Control	9.1.2 - Access to networks and network services
Level	Observation

Παρατηρήθηκε ότι παρόλο που έχει εγκατασταθεί μηχανισμός για Access Control εντός του ανελκυστήρα, δεν έχει ενεργοποιηθεί και επομένως δεν χρησιμοποιείτε από τους υπαλλήλους. Στη περίπτωση αυτή, οποιοσδήποτε με πρόσβαση στο κτήριο μπορεί να εισέλθει στις εγκαταστάσεις της εταιρείας «CompanyC» και ως εκ τούτου στο data και computer room. Ο μηχανισμός θα πρέπει να ενεργοποιηθεί και μόνο εξουσιοδοτημένα άτομα να έχουν πρόσβαση.

Penetration testing δραστηριότητες

4.5 Εισαγωγή

Μία νέα τεχνολογία όπως μία web εφαρμογή, εφαρμογή κινητών κ.λ.π είναι σημαντικό να εξασφαλιστεί ότι η εφαρμογή είναι ασφαλής πριν αρχίσει η φάση χρήση της. Πραγματοποιώντας ένα penetration test σε μία νέα εφαρμογή μπορεί πολλές φορές να γλυτώσει χρόνο, χρήμα και μπελάδες. Επιπλέον, κατά τη διάρκεια ζωής της εφαρμογής θα πρέπει αυτή να ελέγχεται σε τακτά χρονικά διαστήματα ώστε να εξασφαλιστεί ότι το σύστημα είναι ασφαλές.



Για το λόγο αυτό, πραγματοποιήθηκε ένα penetration test με white-box προσέγγιση ώστε να αναγνωριστούν πιθανές ευπάθειες, οι οποίες μπορούν να διακινδυνέψουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα της εφαρμογής.

4.6 Μεθοδολογία και εργαλεία

Η προσέγγιση που ακολουθείτε συνδυάζει αυτόματες αλλά και manual τεχνικές για την διεξαγωγή του white box - security test της εφαρμογής και της υποδομής.

Έχοντας πλήρη γνώση των λειτουργιών της εφαρμογής και της υποστηρικτικής της υποδομής, χρησιμοποιήθηκαν διάφορα εργαλεία και manual τεχνικές για να αναγνωριστούν συνήθεις ευπάθειες και προβλήματα ασφάλειας.

Phase 1: Application mapping – Η πρώτη φάση σε κάθε penetration test είναι να χαρτογραφηθεί η εφαρμογή. Κάθε σελίδα με φόρμα, σημειώνεται για περεταίρω έλεγχο στις επόμενες φάσεις. Το Burp Suite Pro είναι το κύριο εργαλείο που χρησιμοποιήθηκε στη φάση αυτή μαζί με χειροκίνητο έλεγχο.

Phase 2: Vulnerability scanning – στη φάση αυτή χρησιμοποιήθηκε κυρίως το Burp Suite Pro και το Nikto. Άλλα εργαλεία όπως το Dirbuster και το SSLScan θα μπορούσαν να χρησιμοποιηθούν αλλά δεν χρειάστηκε καθώς ακολουθήθηκε white-box η προσέγγιση. Κάθε εύρημα επιβεβαιώθηκε με χειροκίνητους ελέγχους.

Phase 3: Εκμετάλλευση αδυναμιών manually - The results obtained in previous phases, were used in the manual exploitation of application vulnerabilities phase. Προσπαθείς έγιναν για:

- Προσπέραση αυθεντικοποίησης
- Εκμετάλλευση Bypass validations or manipulate application business logic
- Μη εξουσιοδοτημένη πρόσβαση στην εφαρμογή

Ο έλεγχος συμπεριελάμβανε τις ακόλουθες δραστηριότητες:

- Αυθεντικοποίηση
  - Αξιολόγηση της λειτουργίας αυθεντικοποίησης
  - Αξιολόγηση των lock-out ρυθμίσεων για τους χρήστες
- Authorization και διαχείριση των session
  - Έλεγχος εντροπίας του Session ID
  - Αδυναμίες στον μοντέλο σχεδίασης authorization
- Προσπάθειες για horizontal και vertical privilege escalation
- Input validation
  - Έλεγχος όλων των παραμέτρων που επηρεάζονται από το input του χρήστη για πιθανές ευπάθειες.
- Business logic
  - Προσπάθειες για κακόβουλη συμπεριφορά της εφαρμογής παραβιάζοντας τις προκαθορισμένες λειτουργίες.
- Ρυθμίσεις του server
  - Ανάλυση των HTTP μεθόδων κ.α.
- Error handling
  - Αξιολόγηση της διαδικασίας διαχείρισης σφαλμάτων όταν αυτά προκαλούνται στην εφαρμογή. Προσπάθεια συλλογής πληροφοριών για το σύστημα μέσω μη αναμενόμενων σφαλμάτων.
- Ανάλυση μετάδοσης πακέτων
  - Αξιολόγηση χρήση του SSL
- Αξιολόγηση της επίπτωσης των αναγνωρισμένων ευπαθειών.

4.7 Μετρικές κινδύνου

Η μετρική που χρησιμοποιήθηκε για την αξιολόγηση κινδύνου βασίζεται στην επίπτωση, στην ευκολία εκμετάλλευσης και σε κάποιες περιπτώσεις την αυθεντικοποίηση και την δικτυακή τοποθεσία.

Για κάθε ευπάθεια που βρέθηκε, αξιολογήθηκε ο κίνδυνος με τα παραπάνω κριτήρια χρησιμοποιώντας την παρακάτω συνάρτηση:

Risk = Impact * Exploitability * (Authentication + Location)

- Παράδειγμα 1: Risk = (Critical impact * Difficult exploitability * (Anonymous + distant) = High.
- Παράδειγμα 2: Risk = (High impact * Standard exploitability * (Authenticated + Local) =Medium.

Risk	Περιγραφή
Critical	Ο κίνδυνος που συσχετίζεται με την ευπάθεια επιτρέπει το πλήρη έλεγχο του συστήματος ή της εφαρμογής, πέραν του ότι έχει σημαντικές παράπλευρες απώλειες.
High	Ο κίνδυνος που σχετίζεται με την ευπάθεια επιτρέπει μερικό έλεγχο του συστήματος ή της εφαρμογής
Medium	Ο κίνδυνος που σχετίζεται με την ευπάθεια επιτρέπει την αποκάλυψη πληροφοριών που θα μπορούσαν να διευκολύνουν περίπλοκες και στοχευμένες επιθέσεις.
Low	Ο κίνδυνος που σχετίζεται με την ευπάθεια είναι πολύ περιορισμένος. Συνήθως αντιπροσωπεύει μια έλλειψη καλών πρακτικών παρακολούθησης, αλλά δεν έχει άμεσες επιπτώσεις στον οργανισμό.

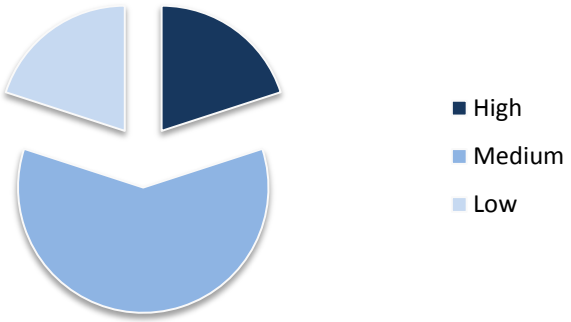
Πίνακας 6 - Αξιολόγηση κινδύνου

4.8 Κατανομή κινδύνου

Κατά τη διάρκεια του penetration test της ISO27001:2013 web εφαρμογής, 5 ευπάθειες αναγνωρίστηκαν. Αυτές οι ευπάθειες κατανέμονται όπως απεικονίζεται παρακάτω:

- 1 ευπάθεια χαρακτηριζόμενη ως high risk
- 3 ευπάθειες χαρακτηριζόμενες ως medium risk
- 1 ευπάθεια χαρακτηριζόμενη ως low risk

Πίνακας 7 - Κατανομή κινδύνου



4.9 Περίληψη ευρημάτων

ID	Εύρημα	CVSS2 RISK
1	Πολλαπλά προβλήματα αυθεντικοποίησης	8
2	Μη κρυπτογραφημένο κανάλι επικοινωνίας	6.1
3	Προβλήματα στον τερματισμό του session	5.8
4	Αποκάλυψη πληροφοριών	5
5	Clickjacking	2.6

Πίνακας 8 - Περίληψη ευρημάτων

4.10 Ευρήματα και συστάσεις

Εύρημα 1: Πολλαπλά προβλήματα αυθεντικοποίησης

Impact	Likelihood	CVSS2 Risk
HIGH	HIGH	HIGH (8)
Επηρεασμένο σύστημα	ISO27001:2013 Web Application System	
CVSS2 Vector	AV:N/AC:L/Au:S/C:C/I:P/A:P	

Περιγραφή

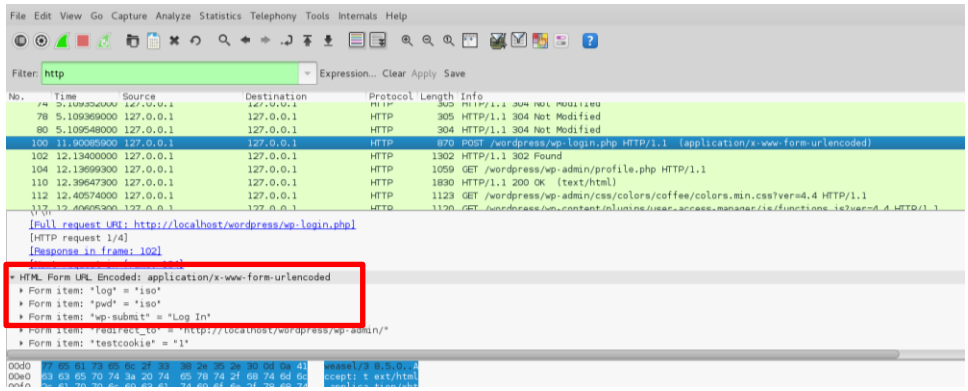
Αναγνωρίστηκαν πολλαπλά προβλήματα αυθεντικοποίησης. Συγκεκριμένα:

- **Έλλειψη πολιτικής για τα passwords:** Τα Passwords αποτελούν μια σημαντική πτυχή της ασφάλειας των συστημάτων. Συνήθως είναι η πρώτη γραμμή προστασίας για έναν λογαριασμό χρήστη. Η επιλογή ενός αδύναμου password μπορεί να οδηγήσει σε σοβαρά προβλήματα:
  - Απώλεια ή έκθεση ευαίσθητων δεδομένων
  - Μη εξουσιοδοτημένες ενέργειες.
- **User enumeration:** Η εφαρμογή επέστρεφε μήνυμα λάθους κατά την αυθεντικοποίηση, υποδηλώνοντας αν ο χρήστης υπάρχει ή όχι στο σύστημα. Αυτή την ευπάθεια μπορεί να την εκμεταλλευτεί ένας κακόβουλος χρήστης ώστε να αναγνωρίσει έγκυρα ονόματα χρηστών. Αυτό μπορεί να χρησιμοποιηθεί αργότερα για επιθέσεις όπως brute force στα password σε περίπτωση που δεν έχει υλοποιηθεί lock out μηχανισμός. Διαφορετικά, ο επιτιθέμενος μπορεί να προκαλέσει Denial of Service κλειδώνοντας τους λογαριασμούς αυτούς.
- **Έλλειψη lock out μηχανισμού:** Κατά τη διάρκεια του ελέγχου παρατηρήθηκε ότι η εφαρμογή δεν κλειδώνει έναν χρήστη μετά από επανειλημμένες προσπάθειας σύνδεσης με λάθος password. Σε περίπτωση brute force επιθέσεων, αυτό μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στην εφαρμογή.
- **Ταυτόχρονες συνδέσεις:** Ήταν πιθανό να δημιουργηθούν δυο αυθεντικοποιημένες συνδέσεις στην εφαρμογή με τον ίδιο χρήστη συγχρόνως. Αυτό επιτεύχθηκε κάνοντας login στην εφαρμογή από δύο διαφορετικούς browsers την ίδια χρονική στιγμή. Αυτό επιτρέπει το διαμοιρασμό των ίδιων στοιχείων εισόδου μεταξύ των χρηστών και μειώνει το accountability..

Proof of Concept

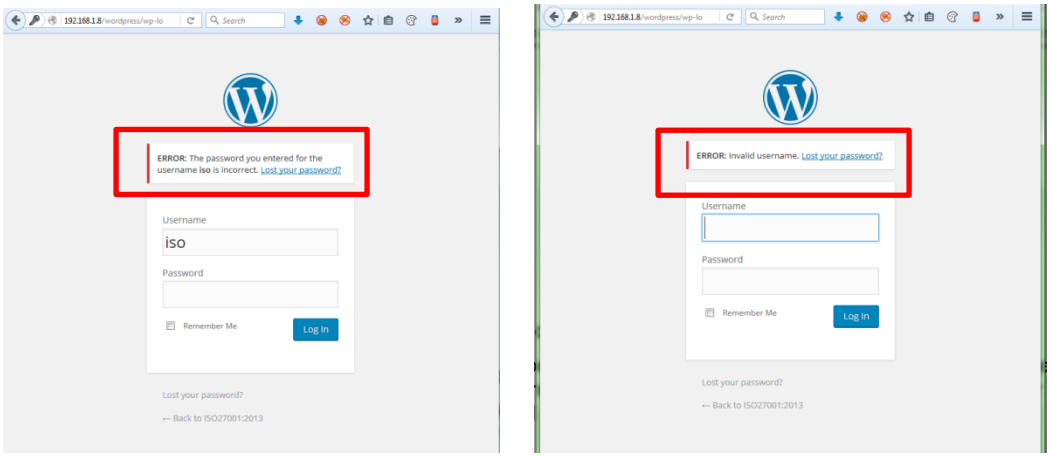
- Έλλειψη πολιτικής για τα passwords

  Στην παρακάτω εικόνα βλέπουμε τον χρήστη “iso” να κάνει login με password=”iso”



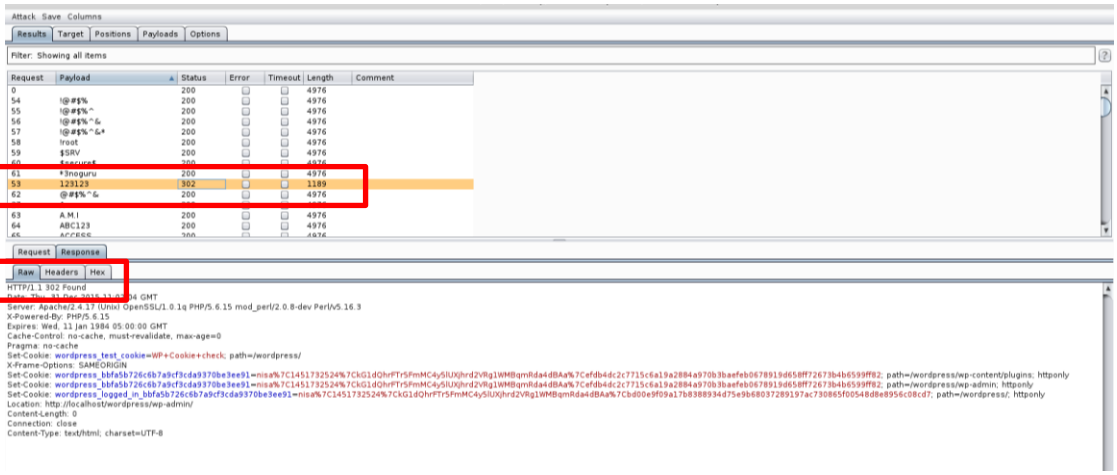
- User enumeration

Στην παρακάτω εικόνα φαίνεται το σφάλμα που δημιουργεί η εφαρμογή. Στην πρώτη περίπτωση ο χρήστης υπάρχει ενώ στην δεύτερη όχι.



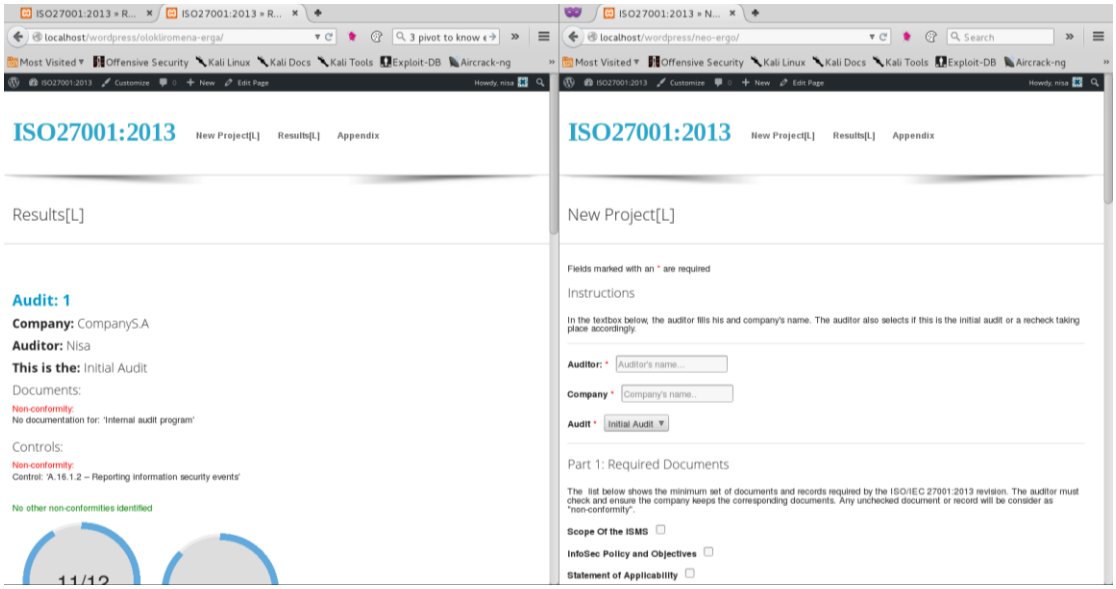
- Έλλειψη lock out μηχανισμού

Πραγματοποιήθηκε brute force επίθεση για τον χρήστη “nisa”. Όπως φαίνεται παρακάτω, το 53^{ο} request ήταν έγκυρο. Ο λογαριασμός του χρήστη δεν κλειδώθηκε ή απενεργοποιήθηκε.



- Ταυτόχρονες συνδέσεις

Στη παρακάτω εικόνα φαίνεται ο ίδιος χρήστης συνδεδεμένος από δύο διαφορετικούς browsers συγχρόνως.



Σύσταση

- Προτείνεται να υλοποιηθεί μία πολιτική για τα passwords με βάση τα best practices.
- Προτείνεται να αλλαχθούν τα μηνύματα λάθους έτσι ώστε να μην αναγνωρίζεται αν ο χρήστης υπάρχει ή όχι.
- Προτείνεται μετά από 5 λάθος προσπάθειες σύνδεσης ο λογαριασμός χρήστη να κλειδώνεται. Ο χρήστης θα πρέπει να έρθει σε επικοινωνία με τον administrator της εφαρμογής ώστε να τον ενεργοποιήσει.
- Προτείνεται να μην επιτρέπεται στον χρήστη να συνδέεται στην εφαρμογή συγχρόνως παραπάνω από μία φορά. Όταν ο χρήστης προσπαθεί να συνδεθεί, θα πρέπει να ελέγχεται αν υπάρχει ήδη κάποιο session ανοιχτό για αυτόν. Αν υπάρχει θα πρέπει ο χρήστης να ενημερώνεται κατάλληλα και να αποσυνδέεται από το προηγούμενο session.

Εύρημα 2: Μη κρυπτογραφημένο κανάλι επικοινωνίας

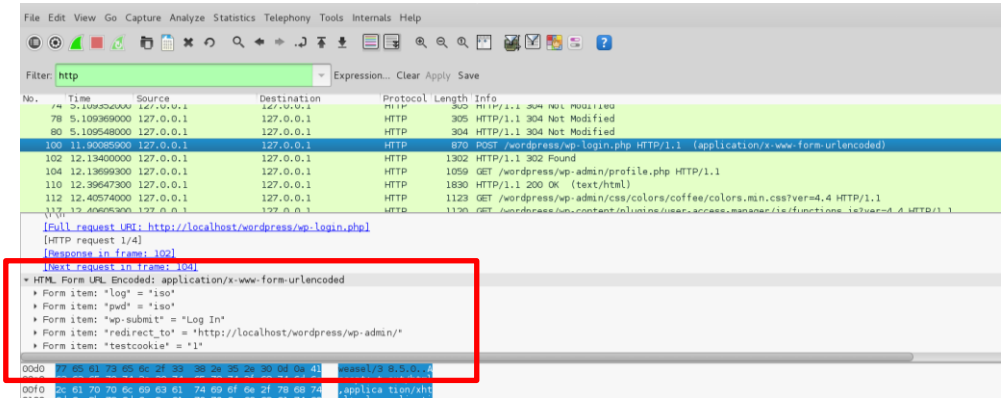
IMPACT	LIKELIHOOD	CVSS2 RISK
MEDIUM	LOW	MEDIUM (6.1)
Affected Systems	ISO27001:2013 Web Application System	
CVSS2 Vector	(AV:A/AC:L/Au:N/C:C/I:N/A:N)	

Περιγραφή

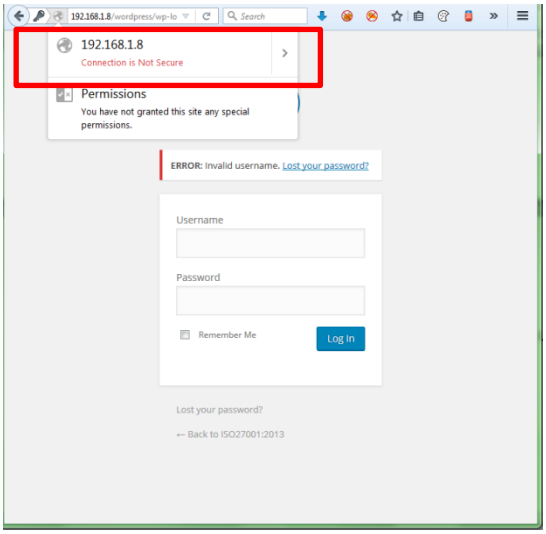
Η κίνηση των δεδομένων από και προς την ISO27001:2013 web εφαρμογή στέλνεται μη κρυπτογραφημένη. Αυτό σημαίνει ότι δεδομένα, όπως τα στοιχεία σύνδεσης, είναι ευάλωτα σε Man-in-The-Middle επιθέσεις. Ένας επιτιθέμενος μπορεί να παρεισφρήσει στην επικοινωνία, παραποιώντας τα δεδομένα. Επιπλέον, proxy servers μεταξύ τον χρήστης και τον server μπορούν να διατηρήσουν logs και ευαίσθητη πληροφορία σε cleartext μορφή.

Proof of Concept

Με τη χρήση του Wireshark, μπορούμε να δούμε τα στοιχεία αυθεντικοποίησης μη κρυπτογραφημένα.



Ο browser επίσης ενημερώνει τον χρήστη ότι η σύνδεση δεν είναι ασφαλής.



Σύσταση

Προτείνεται να χρησιμοποιείται το HTTPS πρωτόκολλο για τη μεταφορά της πληροφορίας. Κάθε request στο HTTP κανάλι θα πρέπει να δρομολογείται στο HTTPS. Επιπλέον, το HTTP κανάλι συστήνεται να απενεργοποιηθεί τελείως.

Εύρημα 3: Προβλήματα στον τερματισμό του session

IMPACT	LIKELIHOOD	CVSS2 RISK
MEDIUM	MEDIUM	MEDIUM (5.8)
Affected Systems	ISO27001:2013 Web Application System	
CVSS2 Vector	AV:A/AC:M/Au:S/C:C/I:P/A:N	

Περιγραφή

Όταν ένας χρήστης στέλνει αίτημα αποσύνδεσης, θα πρέπει το sessions του να τερματίζει από τη πλευρά του server. Παρόλα αυτά παρατηρήθηκε ότι ένα αναγνωριστικό session μπορούσε να χρησιμοποιηθεί για έγκυρα request παρόλο πού ο χρήστης είχε αποσυνδεθεί. Η έλλειψη τερματισμού του session από τη πλευρά του server, επιτρέπει το ενδεχόμενο επαναχρησιμοποίησης του σε περίπτωση που το αποκτήσει ένας επιτιθέμενος. Επιπλέον, αν ο υπολογιστής χρησιμοποιείται από περισσότερους από έναν χρήστη, η αδυναμία αυτή μπορεί να προκαλέσει session hijacking και replay attacks.

Proof of Concept

Αφού συνδεθούμε στην εφαρμογή, πιάνουμε ένα request για αυθεντικοποιημένους χρήστες χρησιμοποιώντας έναν ενδιάμεσο proxy (Burp-Suite).

Στέλνουμε το request στον repeater του Burp-Suite.

Αποσυνδεόμαστε από την εφαρμογή.

Στέλνουμε το request μέσω του repeater στον server και παρατηρούμε ότι το session έχει γίνει δεκτό και έχουμε πλήρη πρόσβαση στην εφαρμογή.

Σύσταση

Όταν ένας χρήστης επιλέγει να αποσυνδεθεί θα πρέπει το session να τερματίζεται από τη πλευρά του server, και ένα νέο, άδειο να ορίζεται για τον συγκεκριμένο χρήστη.

Εύρημα 4: Αποκάλυψη πληροφοριών

IMPACT	LIKELIHOOD	CVSS2 RISK
LOW	HIGH	MEDIUM (5)
Affected Systems	ISO27001:2013 Web Application System	
CVSS2 Vector	AV:N/AC:L/Au:N/C:P/I:N/A:N	

Description

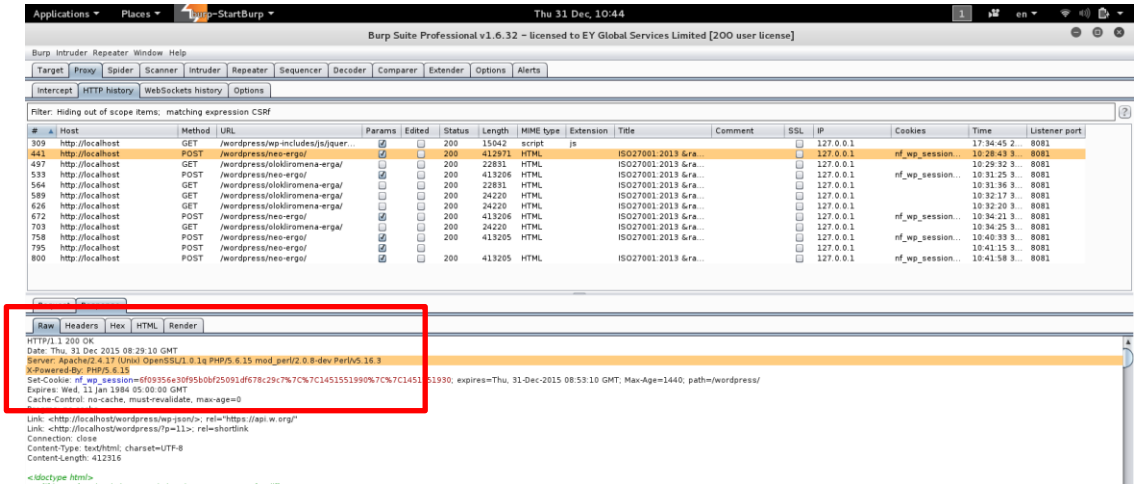
The version information associated with the server is disclosed in the 'Server' header in responses returned from the HTTP server. It was determined that Server Apache/2.4.17was in use. Also the following information was retrieved:

- OpenSSL/1.0.1q
- PHP/ 5.6.15
- Perl 5.16.3

A skilled attacker will attempt to gain as much knowledge about a target application as possible. Such information can be used to enable further attack strategies in order to attempt to launch more sophisticated attacks on the application. Technical information is rarely of use to the standard application user.

Proof of Concept

Στην παρακάτω εικόνα φαίνεται η απάντηση του server, η οποία περιλαμβάνει επιπλέον πληροφορία στους headers.



Σύσταση

Προτείνεται να ρυθμιστεί ο server κατάλληλα ώστε να μην στέλνει επιπλέον πληροφορίες για την έκδοση του λογισμικού.

Εύρημα 5: Clickjacking

IMPACT	LIKELIHOOD	CVSS2 RISK
LOW	LOW	LOW (2.6)
Affected Systems	ISO27001:2013 Web Application System	
CVSS2 Vector	AV:N/AC:H/Au:N/C:P/I:N/A:N	

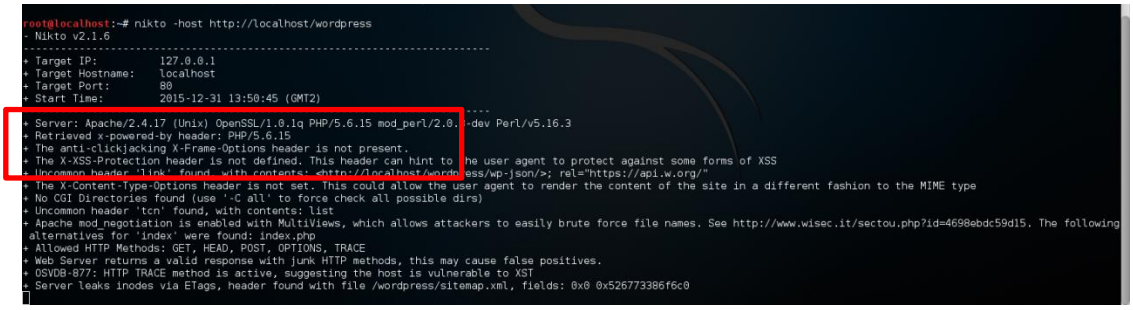
Περιγραφή

Η εφαρμογή είναι ευάλωτη σε επιθέσεις Clickjacking: Ο 'X-Frame-Options' header λείπει από τις απαντήσεις του server.

Με την επίθεση αυτή ένας επιτιθέμενος μπορεί να δημιουργήσει μία κακόβουλη σελίδα η οποία φορτώνει μέσω του iframe το έμπιστο site. Το θύμα πιστεύοντας ότι είναι στο έμπιστο site, περιπλανείται και εκτελεί ενέργειες χωρίς τη θέληση του. Αξίζει να σημειωθεί ότι η επίθεση αυτή προσπερνάει αντίμετρα για CSRF επιθέσεις.

Proof of Concept

Χρησιμοποιώντας έναν intercepting proxy για να δούμε τα request προς τον server, παρατηρήθηκε ότι λείπει ο X-Frame header από το response. Επιπλέον, χρησιμοποιώντας το εργαλείο Nikto, επιβεβαιώνεται η έλλειψη αυτή.

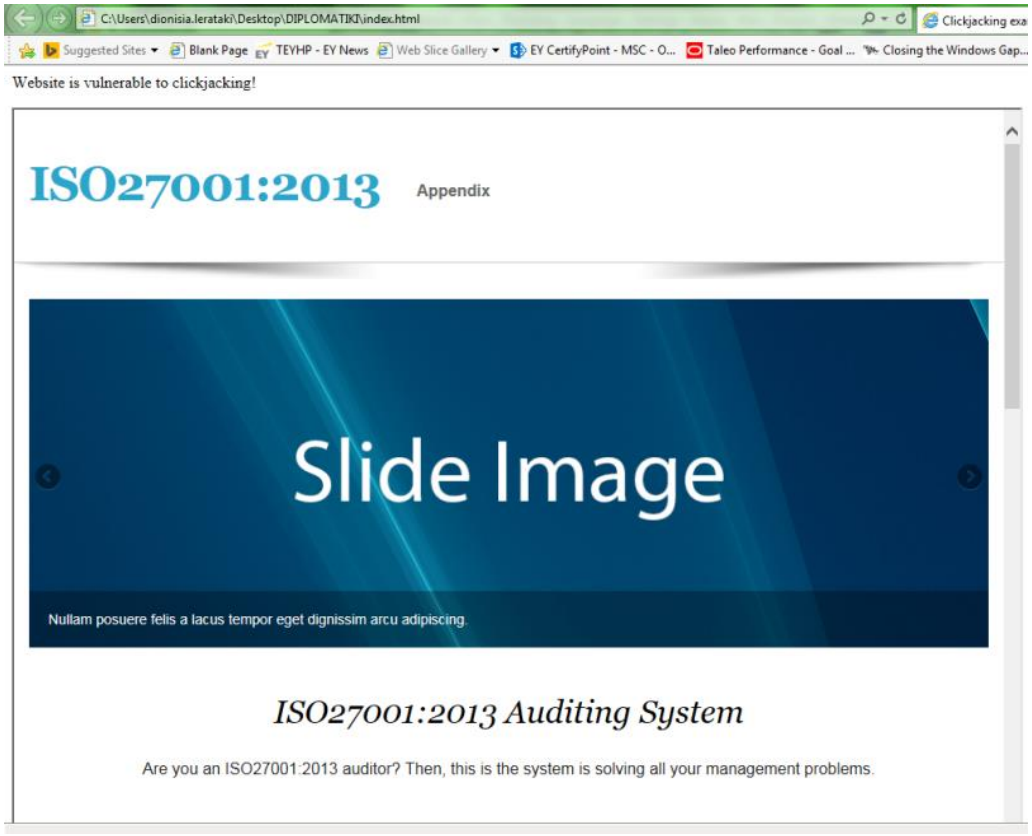


Για την εκμετάλλευση αυτής της αδυναμίας, δημιουργήθηκε ένα αρχείο index.html με τον παρακάτω κώδικα.

```
<html>
<head><title> Clickjacking example</title></head>
<body>
<p> Website is vulnerable to clickjacking!</p>
<iframe src="http://192.168.1.8/wordpress" width="1000" height="1000"></iframe>
</body>
```

```
</html>
```

Στην παρακάτω εικόνα φαίνεται η εφαρμογή μέσω ένος iframe.



Σύσταση

Για να προστατευτεί μία εφαρμογή από επιθέσεις Clickjacking, προτείνεται να τεθεί ο X-Frame-Options HTTP header στην τιμή SAMEORIGIN ή DENY.

5. Συμπεράσματα

Η διπλωματική αυτή κάλυψε αρκετές ενότητες της επιστήμης της «ασφάλειας της πληροφορίας».

Ασχολήθηκε με ένα διεθνές επιχειρηματικό πρότυπο πιστοποίησης, την ανάπτυξη δικτυακής εφαρμογής και τον έλεγχο της ασφάλειας της εφαρμογής αυτής.

Συμπερασματικά μπορούμε να πούμε πως:

- Οι επιχειρήσεις αναγνωρίζουν την ανάγκη για ασφάλεια της πληροφορίας
- Η αναγνώριση αυτή βοήθησε για τη δημιουργία προτύπων ασφαλείας
- Το ISO27001:2013 αποτελεί ένα διεθνές πρότυπο το οποίο καθοδηγεί τις επιχειρήσεις να προστατεύουν τις υποδομές και τα δεδομένα τους.
- Ένας οργανισμός μπορεί να αντιμετωπίσει πολλαπλά προβλήματα κατά τη διάρκεια ανάπτυξης ενός ISMS
- Ένας οργανισμός για να πιστοποιηθεί με βάση το ISO27001:2013 πρέπει να καταλάβει τη σημαντικότητα και τα πλεονεκτήματα του προτύπου πριν δεσμευτεί. Η διαδικασία ανάπτυξης ενός ISMS μπορεί να είναι χρονοβόρα και ακριβή διαδικασία.
- Ένα εργαλείου που να διαχειρίζεται τα audits και να είναι υπεύθυνο για τη κεντρικοποιημένη αποθήκευση τους είναι απαραίτητο για την αποτελεσματική εργασία των auditors.

Η εφαρμογή που δημιουργήθηκε για να καλύψει την ανάγκη αυτή θα μπορούσε να βελτιωθεί περεταίρω με βάση τις παρακάτω λειτουργίες.

- Προσωρινή αποθήκευση της φόρμας των audits πριν την οριστική καταχώρηση της.
- Χωρισμός της φόρμας των audits σε περισσότερες σελίδες για την καλύτερη δομή και συνοχή της εφαρμογής.

Περαιτέρω έρευνα στις ανάγκες των auditor θεωρείται απαραίτητο με σκοπό τη βελτίωση των λειτουργιών της εφαρμογής. Για το σκοπό αυτό θα μπορούσε να πραγματοποιηθεί μια σειρά συνεντεύξεων με τους auditors για να διευκρινιστούν οι ανάγκες τους και να βελτιωθεί η εφαρμογή.

6. Πηγαίος κώδικας εφαρμογής


wordpress.zip


bitnami_wordpress.sql

7. Βιβλιογραφία

C., M. J. (9/2008). *Μάθετε PHP, MySQL και Apache.* Αθήνα: Γκιούρδας Μ.

Implementing ISO 27001:2013. (2016, February). Ανάκτηση από NetGrowth: http://www.netgrowthltd.co.uk/ISO27001.aspx

ISO/IEC 27001:2013. (2013, 10 01). Ανάκτηση February 2016, από iso.org: http://www.iso.org/iso/catalogue_detail?csnumber=54534

ISO/IEC 27001:2013: Information technology - Security techniques – Information security management systems – Requirements. (2013). Geneva, Switzerland: International Organization for Standardization.

Joseph Muniz, Aamir Lakhani. (2013). *Web Penetration Testing with Kali Linux .* PACKT.

Pfleeger, S. L. (n.d.). *Τεχνολογία λογισμικού - Θεωρία και πράξη .* Κλειδάριθμος.

Planning for and Implementing ISO 27001 . (n.d.). Ανάκτηση January 2016, από isaca.org: http://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

The ISO27001 Certification Process. (n.d.). Ανάκτηση February 2016, από 27000.org: http://www.27000.org/ismsprocess.htm

Κάτσικας, Σ. (2004). *Ασφάλεια Πληροφοριακών Συστημάτων .* Εκδόσεις Νέων Τεχνολογιών.

Κάτσικας, Σ. (2014). *Διαχείριση της ασφάλειας πληροφοριών.* Αθήνα: ΠΕΔΙΟ.