Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

Αυτοματοποιημένο Εργαλείο Αναφορών σε Δοκιμές Παρείσφρησης

Του

Νικόλαου Ε. Ευαγγέλου

Επιβλέπων Καθηγητής

Κωνσταντίνος Λαμπρινουδάκης

Διπλωματική Εργασία υποβλήθηκε στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Ασφάλεια Ψηφιακών Συστημάτων

Πειραιάς, 30 Σεπτεμβρίου 2020

Περιεχόμενα

Εισαγωγή

Μία εταιρεία που παρέχει ψηφιακές υπηρεσίες, θα πρέπει να εξασφαλίσει στους πελάτες της την διαθεσιμότητα της υπηρεσίας όλο το 24ωρο, αλλά και την ασφαλή τους περιήγηση στους πόρους του οργανισμού. Ένας κακόβουλος χρήστης θα προσπαθήσει να διακόψει την ομαλή λειτουργία του πληροφοριακού συστήματος, να υποκλέψει τα προσωπικά δεδομένα των χρηστών ή να αναγκάσει τους χρήστες να εκτελέσουν ένα παραποιημένο request/transaction χωρίς να το αντιληφθούν. Είναι δεδομένο ότι η ασφάλεια ενός πληροφοριακού συστήματος είναι το ίδιο σημαντική όσο και η διαθεσιμότητα της υπηρεσίας.

Vulnerability assessment

Vulnerability assessment είναι η διαδικασία της αναγνώρισης, της ποσοτικοποίησης και της κατηγοριοποίησης των ευπαθειών ενός πληροφοριακού συστήματος (Rouse, 2020). Αξιολογεί εάν το σύστημα είναι ευάλωτο σε κάποια γνωστή ευπάθεια, ορίζει το επίπεδο σοβαρότητας αυτών των ευπαθειών και προτείνει τρόπους αντιμετώπισης ή μετρίασης. Υπάρχουν τεσσάρων ειδών vulnerability assessment:

1. Host assessment: για την αναγνώριση ευπαθειών σε servers, workstations ή άλλα network hosts. Αυτός ο τύπος αξιολόγησης συνήθως εξετάζει για θύρες και services που μπορεί να αποκαλυφθούν σε ένα network-based scan.
2. Network and wireless assessment: για την αναγνώριση πιθανών δικτυακών επιθέσεων, τόσο στο ενσύρματο όσο και στο ασύρματο δίκτυο.
3. Database assessment: για την αναγνώριση των ευαίσθητων σημείων μίας βάσης για να αποφευχθεί μία SQL injection επίθεση.
4. Application assessment: για την αναγνώριση γνωστών ευπαθειών τόσο και λαθών στην παραμετροποίηση του δικτύου ή του web application.

Penetration testing

Το penetration test είναι ένα εγκεκριμένο simulated cyberattack σε ένα πληροφορικό σύστημα, με στόχο την αξιολόγηση της ασφάλειας του συστήματος (Penetration test, 2020). Το penetration test είναι μέρος του vulnerability assessment και έχει ως στόχο την αναγνώριση ευπαθειών στις διαδικασίες ενός οργανισμού, αλλά και στο προσωπικό του μέσω social engineering.

Τα tests μπορούν να γίνουν με 3 τρόπους:

1. Black-box: όπου ο tester έχει καμία ή ελάχιστη πληροφορία για το σύστημα.
2. White-box: όπου έχουν δοθεί στον tester όλες οι πληροφορίες για το σύστημα και επιπλέον του έχει δοθεί πρόσβαση σε αυτό.
3. Grey-box: είναι ένας συνδυασμός των 2 προηγούμενων, ο tester έχει περιορισμένη πληροφορία για το σύστημα και έχει αυξημένα δικαιώματα στο σύστημα.

Πριν ξεκινήσει το penetration testing θα πρέπει να οριστεί ποιους πόρους επιτρέπεται ο tester να εξετάσει. Ένας οργανισμός μπορεί μην θέλει να εκθέσει ευαίσθητες πληροφορίες, οι οποίες μπορεί να υπάρχουν στο σύστημα, οπότε θα πρέπει να οριστεί ένα confidentiality statement μεταξύ των 2 πλευρών.

Penetration testing report

Μια από τις σημαντικότερες διαδικασίες του penetration testing είναι η συγγραφή του report, καθώς είναι το μέσο με το οποίο ο πελάτης θα ενημερωθεί για τις ευπάθειες του πληροφοριακού συστήματός του και για τους τρόπους επίλυσής τους.

Όταν βρεθεί μία ευπάθεια θα πρέπει να καταγραφούν όλες οι ενέργειες, βήμα προς βήμα, που έγιναν για την εκμετάλλευση της, έτσι ώστε οι developers του συστήματος που γίνεται το penetration testing, να μπορούν να επαναλάβουν την επίθεση και να βρουν πιο εύκολα τρόπους αντιμετώπισης. Επίσης, η καταγραφή αυτή είναι χρήσιμη και για τον penetration tester καθώς, αφού διορθωθούν οι ευπάθειες του πληροφοριακού συστήματος, θα πρέπει να επαληθεύσει ότι οι διορθώσεις έχουν υλοποιηθεί σωστά. Τα πειστήρια των ευπαθειών μπορεί να είναι τα input και τα output των testing εργαλείων, οι εντολές ή κομμάτια κώδικα που χρησιμοποιήθηκαν και εικόνες ή βίντεο τα οποία περιγράφουν τις διαδικασίες και τα αποτελέσματα από την εκμετάλλευση των ευπαθειών αυτών (Allen, Heriyanto, & Ali, 2014).

Η Δομή των Reports

Αφού συλλεχτούν όλα τα ευρήματα από το penetration test, πρέπει να γραφτεί ένα report με συστηματικό και δομημένο τρόπο. Το report θα πρέπει να περιγράφει με αναλυτικό τρόπο τις ευπάθειες, πώς μπορεί κάποιος κακόβουλος να τις εκμεταλλευτεί, τι επιπτώσεις θα έχουν στον οργανισμό και με ποιους τρόπους θα αποτραπούν οι κίνδυνοι αυτοί.

Όλα τα παραδοτέα πρέπει να αναφέρουν ποιο είναι το περιεχόμενό τους, ποιες οντότητες/οργανισμοί εμπλέκονται στο παραδοτέο, ποιες ενέργειες έγιναν και ποια ήταν τα αποτελέσματα. Τα κύρια κεφάλαια που πρέπει να περιέχει ένα penetration testing report (Muniz & Lakhani, 2013) είναι:

1. Confidentiality statement
2. Executive summary
3. Μεθοδολογία
4. Σύνοψη των Ευρημάτων
5. Ευπάθειες

Παρακάτω περιγράφονται αναλυτικά τα κεφάλαια αυτά.

Confidentiality statement

Κατά την διάρκεια ενός penetration test συλλέγονται δεδομένα, τα οποία στην πλειοψηφία τους είναι ευαίσθητα. Γι' αυτό το λόγο ο πελάτης θα πρέπει να εξασφαλίσει ότι αυτά τα ευαίσθητα δεδομένα δεν θα καταλήξουν σε άτομα που δεν έχουν εξουσιοδότηση να τα διαθέτουν. Τέτοια δεδομένα μπορεί να είναι: τα προσωπικά δεδομένα των χρηστών, κωδικοί ασφαλείας, η τοπολογία του συστήματος κλπ. Έτσι το confidentiality statement θα πρέπει να περιγράφει το επίπεδο προστασίας των δεδομένων, ποιοι έχουν εξουσιοδοτημένη πρόσβαση στα δεδομένα, τι μπορεί και τι όχι να κρατήσουν στην κατοχή τους οι penetration testers και αν μπορούν να τα μοιραστούν με τρίτους, και άλλα νομικά ζητήματα που μπορούν να εφαρμοστούν. Η παραβίαση των ευαίσθητων δεδομένων μπορεί να οδηγήσει σε οικονομικές και νομικές συνέπειες.

Executive summary

Το Executive summary είναι μία high-level περίληψη των διαδικασιών που πραγματοποιήθηκαν. Το Executive summary πρέπει να περιέχει τις ευπάθειες που βρέθηκαν, να εξηγεί με απλά λόγια τις ενέργειες που μπορεί να πραγματοποιήσει κάποιος κακόβουλος χρήστης και να προτείνει τρόπους αντιμετώπισης. Το Executive summary απευθύνεται στα διοικητικά στελέχη και δεν πρέπει να περιέχει τεχνικές λεπτομέρειες.

Μεθοδολογία

Στην Μεθοδολογία περιέχονται όλες οι τεχνικές και τα εργαλεία που χρησιμοποιήθηκαν κατά την διάρκεια του penetration testing, έτσι ώστε ο πελάτης να είναι ενήμερος για το τρόπο δράσης των penetration testers. Επίσης, οι πιστοποιήσεις μπορούν να εγγυηθούν για την ποιότητα των αποτελεσμάτων. Για παράδειγμα οι πιστοποιήσεις για το penetration testing, όπως το Certified Ethical Hacker (CEH) και το GIAC Penetration Tester (GPEN), μπορούν να επιβεβαιώσουν για τις ικανότητες για τις γνώσεις του penetration tester.

Σύνοψη των Ευρημάτων

Σε αυτό το κεφάλαιο, συγκεντρώνονται όλα τα ευρήματα που βρέθηκαν και αξιολογούνται με βάση την επικινδυνότητά τους και το αντίκτυπο που έχουν στον οργανισμό.

Ευπάθειες

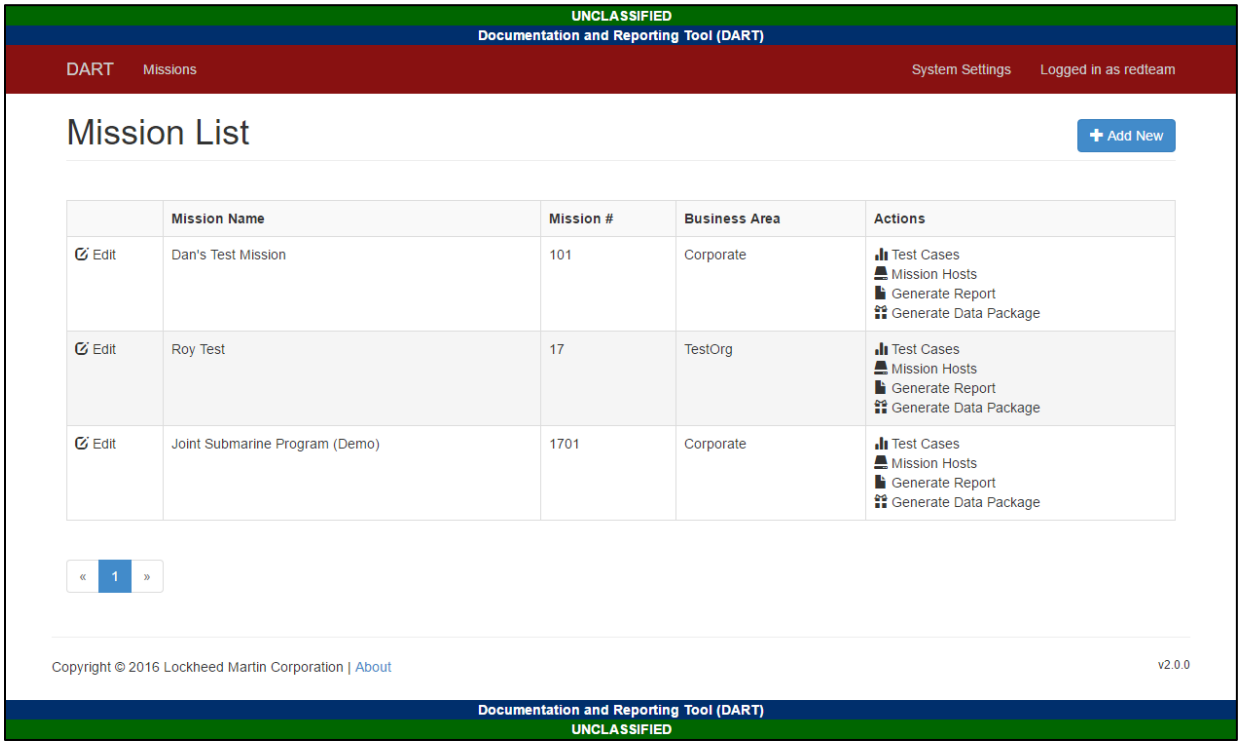
Για κάθε μία ευπάθεια που βρέθηκε προστίθεται η περιγραφή της, το αντίκτυπο που έχει στον οργανισμό και η πιθανότητα κάποιος κακόβουλος χρήστης να την αξιοποιήσει. Επίσης, περιγράφεται και ο τρόπος που βρέθηκε η ευπάθεια (proof of concept) και προτείνονται τρόποι αντιμετώπισης της συγκεκριμένης ευπάθειας.

Εργαλεία

Η διαδικασία συγγραφής ενός penetration testing report είναι χρονοβόρα. Υπάρχουν εργαλεία τα οποία μπορούν να χρησιμοποιηθούν ώστε να εξοικονομηθεί χρόνος και να βοηθήσουν τον penetration tester να οργανώσει τα ευρήματα που βρήκε και τα αποτελέσματα που παρήγαγαν τα εργαλεία που χρησιμοποίησε. Σε αυτό το κεφάλαιο συγκρίνονται μερικά εργαλεία που μπορούν να βοηθήσουν την αυτοματοποίηση της διαδικασίας αυτής.

DART

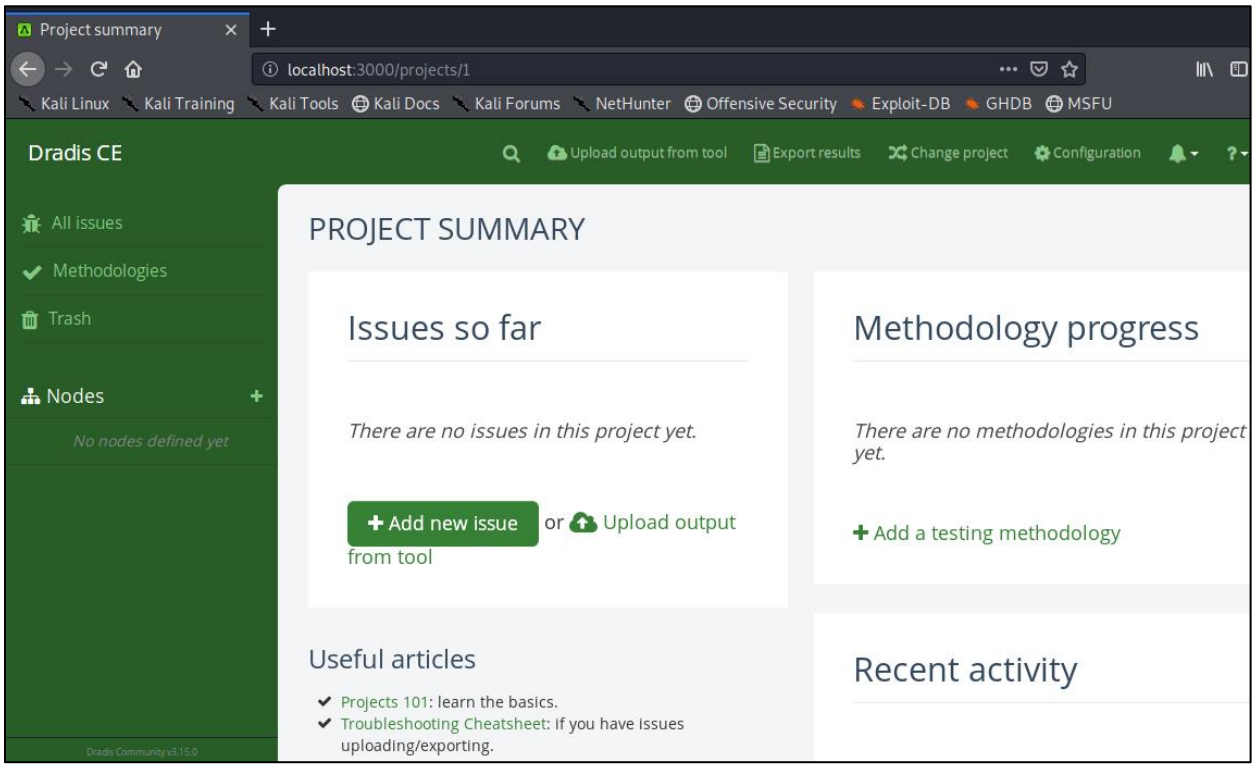
Το DART είναι ένα open source εργαλείο το οποίο στοχεύει στην καλύτερη παρακολούθηση των ενεργειών κατά την διάρκεια του penetration testing και στην καταγραφή των ευπαθειών που βρέθηκαν στη διάρκεια αυτή (DART, 2017).



Εικόνα 1. Αρχική σελίδα DART

Dradis

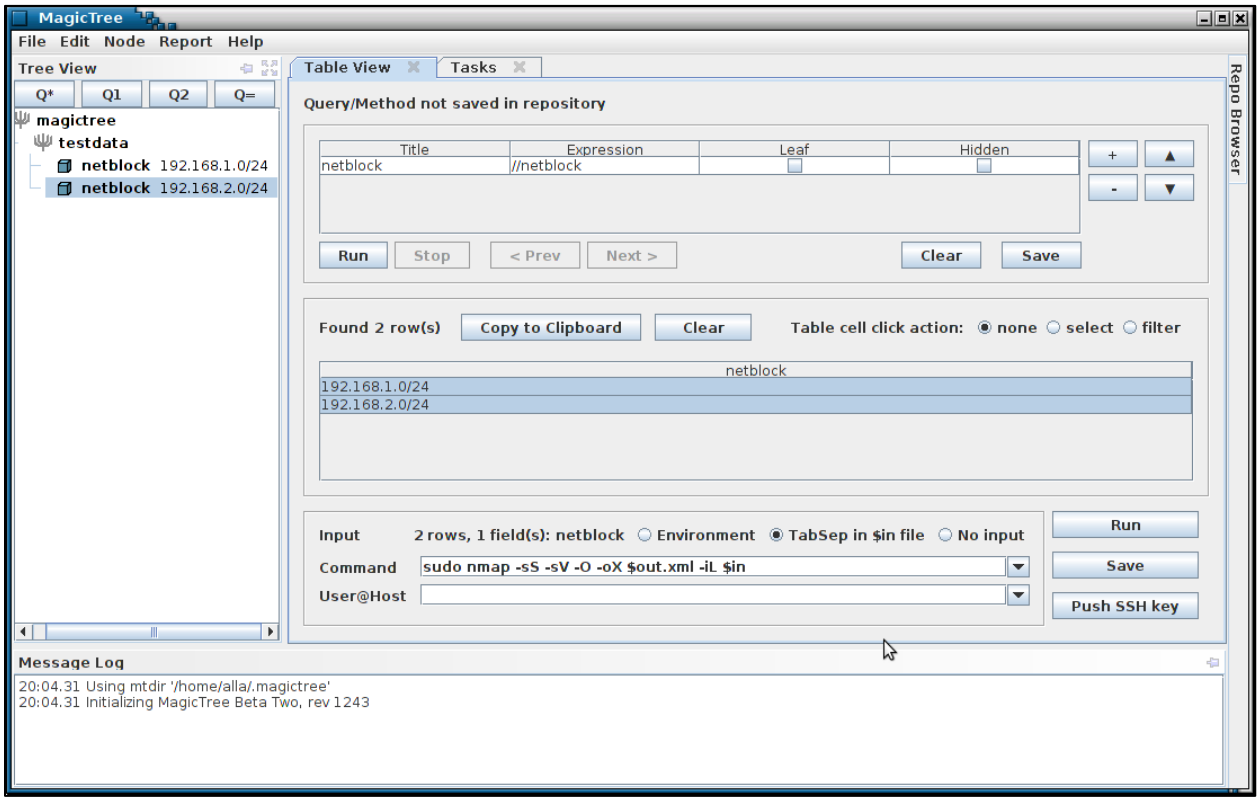
Το Dradis είναι ένα open source framework το οποίο παρέχει ένα σύστημα καταγραφής των όσων έγιναν κατά την διάρκεια του penetration testing. Επίσης, το Dradis δίνει την δυνατότητα να προστεθούν κι άλλοι χρήστες στα tasks και να εισαχθούν τα αποτελέσματα από άλλα εργαλεία όπως το Nessus, το Nmap, το Burp Suite και το ZAP. Τέλος, παράγεται ένα report σε μορφή Word ή HTML (Dradis, 2017).



Εικόνα 2. Αρχική σελίδα Dradis

MagicTree

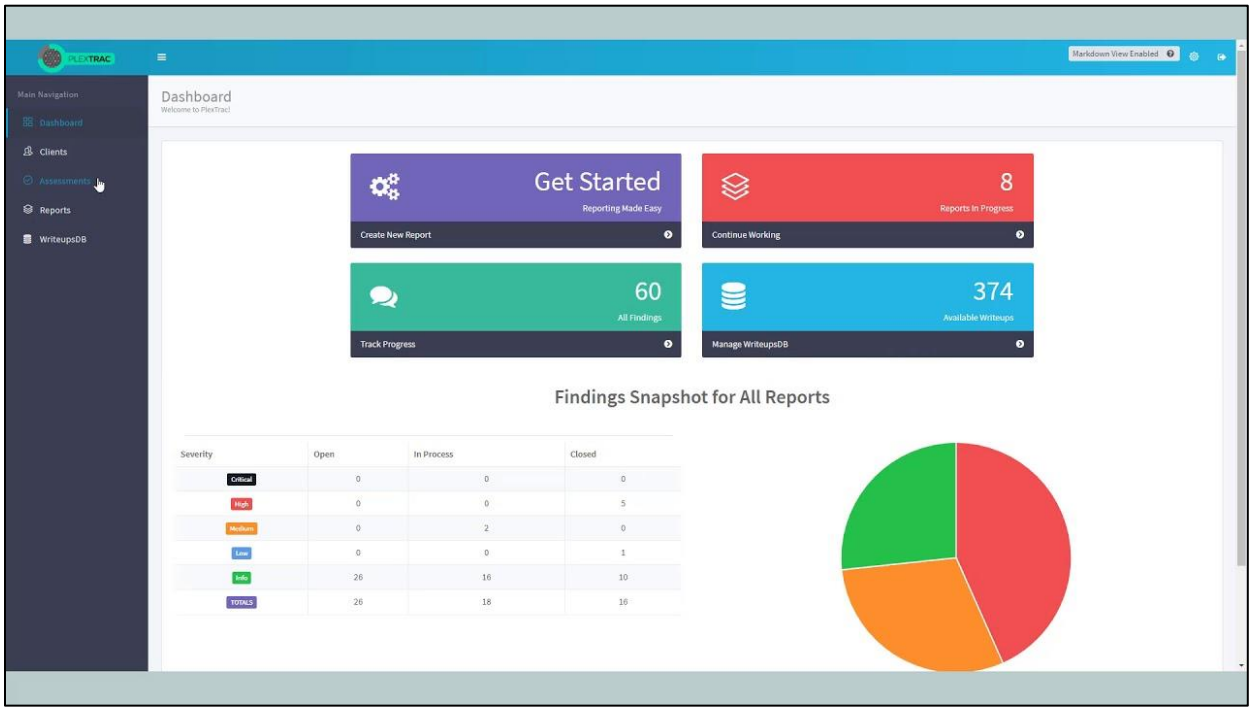
Το MagicTree είναι ένα data-management και reporting tool, όμοιο με το Dradis. Τα δεδομένα αποθηκεύονται σε μια δενδροειδή δομή, με την οποία γίνεται ευκολότερη η οργάνωση των αποτελεσμάτων. Το output που δημιουργεί το εργαλείο είναι σε .doc μορφή (MagicTree, 2020).



Εικόνα 3. Αρχική σελίδα MagicTree

PlexTrac

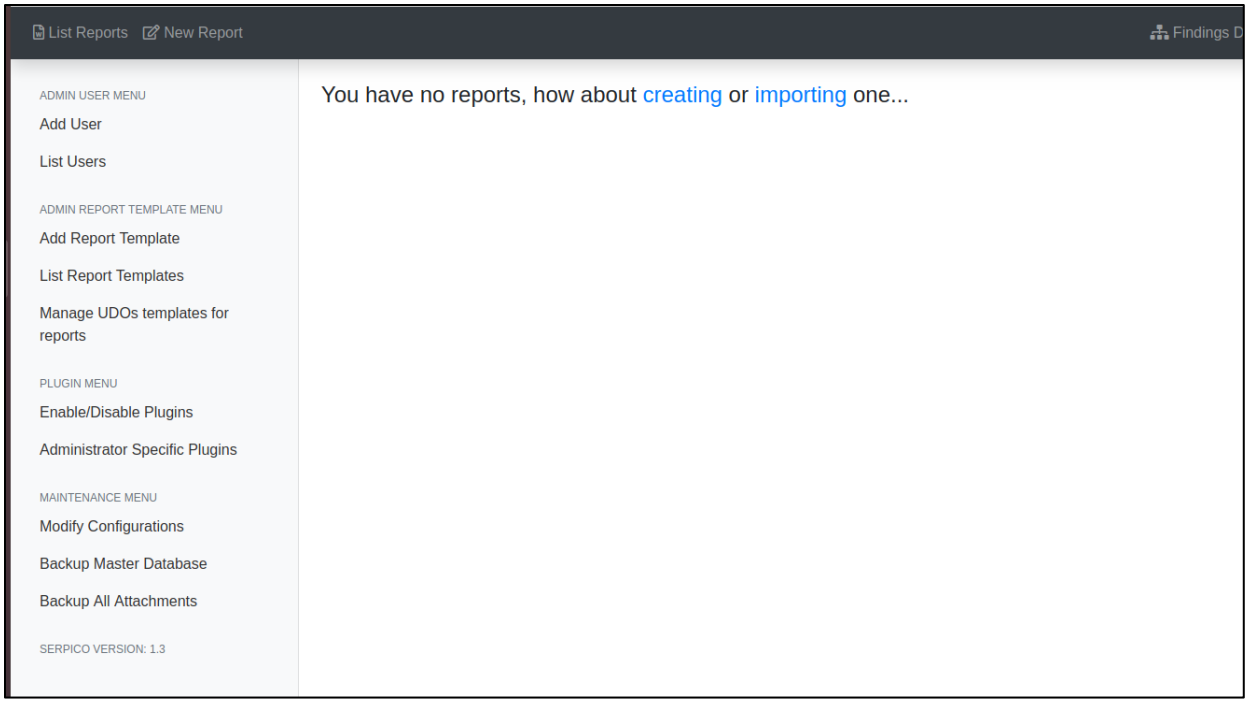
Το PlexTrac είναι ένα commercial εργαλείο στο οποίο μπορείτε να εισάγετε τα αποτελέσματά σας από άλλα εργαλεία, όπως το Nessus, το Burp Suite και το Nexpose. Υπάρχει η δυνατότητα εισαγωγής template, ώστε να προσαρμόσετε το παραγόμενο report στις δικές σας ανάγκες. Επίσης διαθέτει μια βάση με τις περιγραφές των ευπαθειών και τους τρόπους αντιμετώπισής τους. Το output που παράγει το PlexTrac είναι σε μορφή .docx και .pdf (PlexTrac, 2020).



Εικόνα 4. Αρχική σελίδα PlexTrac

Serpico

Το Serpico (SimplE RePort wrIting and COllaboration tool) είναι ένα open source εργαλείο γραμμένο σε Ruby και έχει ως στόχο να εξοικονομήσει χρόνο στην διαδικασία της δημιουργίας του report. Είναι όμοιο με το PlexTrac, αλλά είναι open source. Διαθέτει μία βάση με τις περιγραφές και τους τρόπους αντιμετώπισης των περισσότερων ευπαθειών, οι οποίες μπορούν να χρησιμοποιηθούν στο report. Το Serpico δίνει την δυνατότητα στους χρήστες να τροποποιήσουν τα templates των reports και να επεκτείνουν τις δυνατότητες του εργαλείου μέσω plugins. Τέλος, το report που παράγεται είναι σε μορφή .docx (Serpico, 2020).



Εικόνα 5. Αρχική σελίδα Serpico

Σύγκριση

Στον παρακάτω πίνακα γίνεται η σύγκριση ανάμεσα στα εργαλεία που περιγράφηκαν παραπάνω. Το DART είναι το πιο απλό σε σχέση με τα υπόλοιπα, έχει λίγες δυνατότητες και δεν υποστηρίζει την εισαγωγή δεδομένων από άλλα εργαλεία. Το Dradis και το MagicTree είναι πιο πλούσια σε λειτουργικότητα. Η εξαγωγή των reports μπορεί να γίνει σε περισσότερες μορφές, υποστηρίζεται η εισαγωγή αποτελεσμάτων από άλλα εργαλεία και επιπλέον το Dradis υποστηρίζει πολλαπλούς χρήστες να επεξεργάζονται ένα report. Το PlexTrac έχει ακόμα περισσότερες δυνατότητες, το γραφικό περιβάλλον είναι πιο user friendly και υπάρχει η δυνατότητα εξατομίκευσης των report templates. Το Serpico είναι όμοιο με το PlexTrac, αλλά είναι open source και παρέχει την δυνατότητα επέκτασης των δυνατοτήτων του εργαλείου, χρησιμοποιώντας plugins.

	DART	Dradis	MagicTree	PlexTrac	Serpico
User friendly UI	YES	NO	NO	YES	YES
Custom Templates	NO	NO	NO	YES	YES
Edit report by multiple users	YES	YES	NO	YES	YES
Export file types	Microsoft Word	Microsoft Word, HTML	Microsoft Word, OpenOffice	Microsoft Word, Markdown, CSV, PDF	Microsoft Word
Import scan results from tools	NONE	Nmap, Nessus, Burp, ZAP	Nmap, Nessus, Burp	Burp, Nessus	Burp, Nessus, Metasploit
License	Open Source	Community & Pro	Open Source	Commercial	Open Source

Με βάση την παραπάνω σύγκριση, επιλέχθηκε το Serpico επειδή έχει τις ίδιες δυνατότητες με το PlexTrac, αλλά είναι open source και επιπλέον υπάρχει η δυνατότητα επέκτασης των λειτουργιών δημιουργώντας plugins.

Οδηγίες Εγκατάστασης

Το Serpico είναι γραμμένο σε Ruby χρησιμοποιώντας τις βιβλιοθήκες Sinatra, Bootstrap και Haml. Η εγκατάσταση γίνεται με τα εξής βήματα:

Εγκατάσταση Ruby

Προετοιμασία

Πρώτα, πρέπει να βεβαιωθείτε ότι τα packages curl gpg είναι εγκατεστημένα στο σύστημα, όπως επίσης και το compiler toolchain. Το curl και το gpg χρειάζονται στα βήματα που ακολουθούν ενώ το compiler toolchain χρειάζεται για την εγκατάσταση των Ruby gems.

Debian, Ubuntu	`$ sudo apt-get update` `$ sudo apt-get install -y curl gnupg build-essential`
CentOS, Fedora, Red Hat	`$ sudo yum install -y curl gpg gcc gcc-c++ make`

Εγκατάσταση RVM

Για να εγκαταστήσετε το RVM, τρέξτε τις παρακάτω εντολές:

```
$ sudo gpg --keyserver hkp://pool.sks-keyservers.net --recv-keys
409B6B1796C275462A1703113804BB82D39DC0E3
7D2BAF1CF37B13E2069D6956105BD0E739499BDB
$ curl -sSL https://get.rvm.io | sudo bash -s stable
$ sudo usermod -a -G rvm $(whoami)
$ source /etc/profile.d/rvm.sh
```

Σημείωση: Σε μερικά συστήματα, ενδέχεται να χρειαστεί να χρησιμοποιήσετε το gpg2 αντί του gpg.

Εγκατάσταση Ruby

Για την εγκατάσταση της Ruby v2.3.3 τρέξτε τις παρακάτω εντολές:

```
$ rvm install ruby-2.3.3
$ rvm --default use ruby-2.3.3
```

Εγκατάσταση Bundler

Το Bundler είναι ένα εργαλείο για την διαχείριση των application gem dependencies. Η εγκατάσταση γίνεται με την παρακάτω εντολή:

```
$ gem install bundler
```

Εγκατάσταση Serpico

Προετοιμασία

Πρώτα, θα πρέπει να βεβαιωθείτε ότι τα παρακάτω dependencies είναι εγκατεστημένα:

Debian, Ubuntu	`$ sudo apt-get install libsqlite3-dev libxslt-dev libxml2-dev zlib1g-dev gcc git`
CentOS, Fedora, Red Hat	`$ sudo yum install -y sqlite-devel libxslt-devel libxml2-devel zlib-devel git`

Εγκατάσταση Serpico

Για να κατεβάσετε το Serpico πρέπει να τρέξετε τις παρακάτω εντολές:

```
$ cd ~
$ git clone https://github.com/nikosev/Serpico.git
$ cd Serpico
$ bundle install
```

Η τελευταία εντολή θα εγκαταστήσει τα dependencies του project.

Σημείωση: Για την διεύθυνση του καταλόγου που θα γίνει η εγκατάσταση θα πρέπει να έχει δικαιώματα ο χρήστης που θα το εκτελέσει.

Στην συνέχεια, αρχικοποιείστε το Serpico με την εντολή:

```
$ ruby scripts/first_time.rb
```

Θα σας ζητηθεί να ορίσετε ένα όνομα χρήστη και στην συνέχεια θα παραχθεί ένα password για το χρήστη. Τέλος πατήστε Y για να προστεθούν τα default templates του Serpico.

Το script αυτό παράγει το certificate του server, έναν admin user και θα αρχικοποιήσει την Βάση Δεδομένων.

Σε περίπτωση που χρειάζεται να αλλάξετε το certificate, απλά αντικαταστήστε το cert.pem αρχείο το οποίο βρίσκεται μέσα στο root directory του Serpico (~/Serpico).

Για να τρέξετε το Serpico χρησιμοποιήστε την εντολή:

```
$ ruby serpico.rb
```

Από προεπιλογή το server τρέχει στην διεύθυνση: https://127.0.0.1:8443/

Αν διακοπεί η εκτέλεση της εντολής, τότε ο server θα πέσει. Για να εκτελέσετε την εντολή στο background μπορείτε να χρησιμοποιήσετε το screen (πληροφορίες στο παράρτημα).

Για να ξεκινήσετε ένα Screen session:

```
$ screen -S serpico
```

Στην συνέχεια ξεκινήστε το Serpico:

```
$ ruby ~/Serpico/serpico.rb
```

Για να κάνετε detach το session χρησιμοποιήστε το shortcut:

```
ctrl+a d
```

Παραμετροποίηση του Serpico

Γενικές Πληροφορίες

Η παραμετροποίηση του Serpico μπορεί να γινεί με δύο τρόπους:

1) Από το UI του Serpico:
   Ανοίξετε ένα browser με την διεύθυνση https://127.0.0.1:8443/admin/config και κάντε login με τον admin user.
2) Τροποποιώντας το config.json:
   ανοίξετε ένα terminal στο server που είναι εγκατεστημένο το Serpico και στην συνέχεια να ανοίξετε το config.json με κάποιο text editor

```
$ nano ~/Serpico/config.json
```

Όταν κάνετε αλλαγές στο configuration του server, πρέπει να κάνετε restart το server για να εφαρμοστούν οι αλλαγές.

Μερικές επιλογές για τροποποίηση είναι:

- Διεύθυνση και θύρα που τρέχει το Serpico
- Τα finding types που θα εμφανίζονται στο server
- Το logo που εμφανίζεται στην ιστοσελίδα
- Το μήνυμα που εμφανίζεται στο footer της ιστοσελίδας
- Τις γλώσσες των reports που θα παράγουμε

Αλλαγές παραμέτρων

Για να ρυθμίσουμε το Serpico να χρησιμοποιεί την Ελληνική γλώσσα και να εισάγουμε τα issue definitions του BurpSuite θα πρέπει να αλλάξουμε τις παραμέτρους του Serpico.

Επιλέξτε ένα από τους 2 τρόπους για να τροποποιήσετε το configuration του Serpico και αλλάξτε τα τις παρακάτω παραμέτρους:

```
finding_types = BurpSuite
languages = English, Greek
```

Στην συνέχεια αποθηκεύστε τις αλλαγές και επανεκκινήστε το Serpico.

Εγκατάσταση Serpico Plugins

Το Serpico παρέχει την δυνατότητα στους developers να δημιουργήσουν τα δικά τους plugins για να επεκτείνουν τις λειτουργίες του εργαλείου ώστε να καλύψει τις ανάγκες τους.

Όλα τα plugins πρέπει να εγκατασταθούν στο plugins directory το οποίο βρίσκεται μέσα στο root directory του Serpico (~/Serpico).

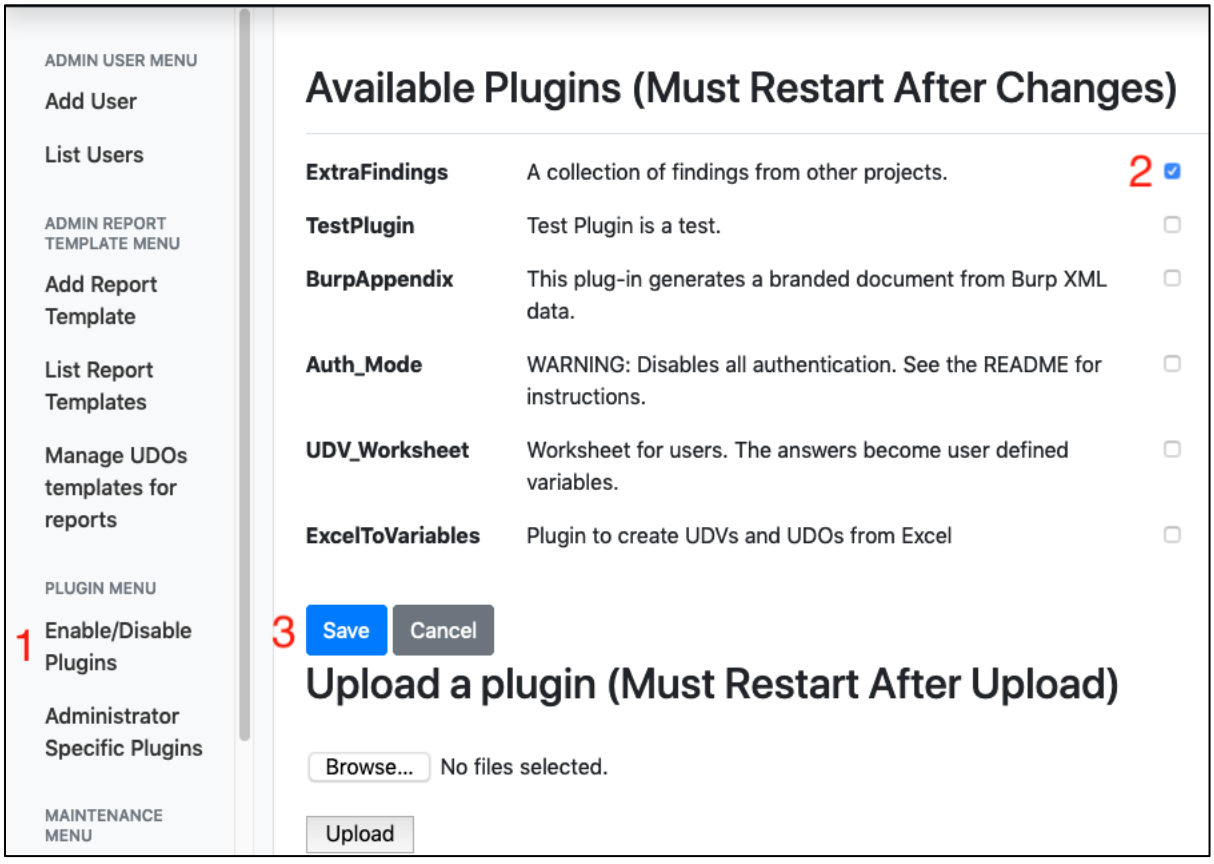
Το Serpico έχει κάποια official plugins τα οποία για να τα εγκαταστήσετε πρέπει να ακολουθήσετε τα εξής βήματα:

```
$ cd ~
$ git clone https://github.com/nikosev/SerpicoPlugins.git -b develop-nikosev
$ ln -s ~/SerpicoPlugins/ ~/Serpico/plugins
```

Στην συνέχεια ανοίξτε στο browser σας την διεύθυνση: https://127.0.0.1:8443/admin/admin_plugins, ενεργοποιείστε τα plugins που επιθυμείτε και τέλος κάντε restart το server.

Ενεργοποίηση του ExtraFindings Plugin

Για να ενεργοποιήσετε το ExtraFindings Plugin, το οποίο περιέχει τα issue definitions από το BurpSuite, επιλέξτε στην αριστερή λίστα **Enable/Disable Plugins** και στην συνέχεια επιλέξτε το **ExtraFindings**:



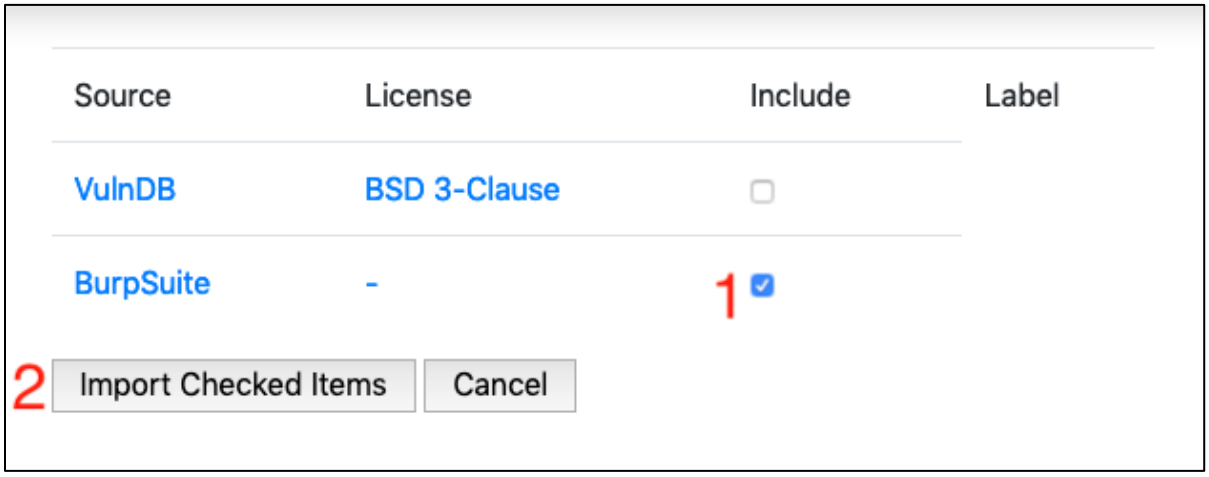
Εικόνα 6. Ενεργοποίηση του ExtraFindings Plugin.

Στην συνέχεια πατήστε **Save** και κάντε επανεκκίνηση το Serpico.

Κάντε ξανά login με τον admin χρήστη σας και από την αριστερή λίστα επιλέξτε το **Administrator Specific Plugins** και πατήστε στο **Extra Findings**.

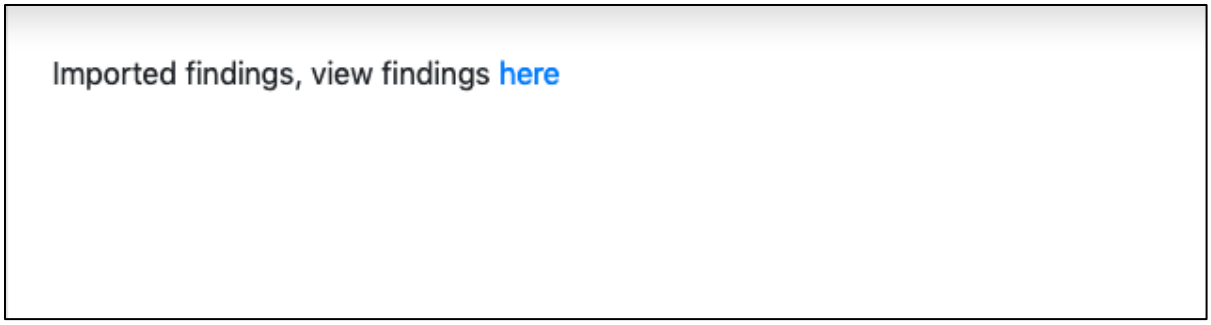
Εικόνα 7. Σελίδα παρουσίασης ενεργοποιημένων Plugins.

Στην συνέχεια επιλέξτε το **BurpSuite** και στην συνέχεια **Import Checked Items**



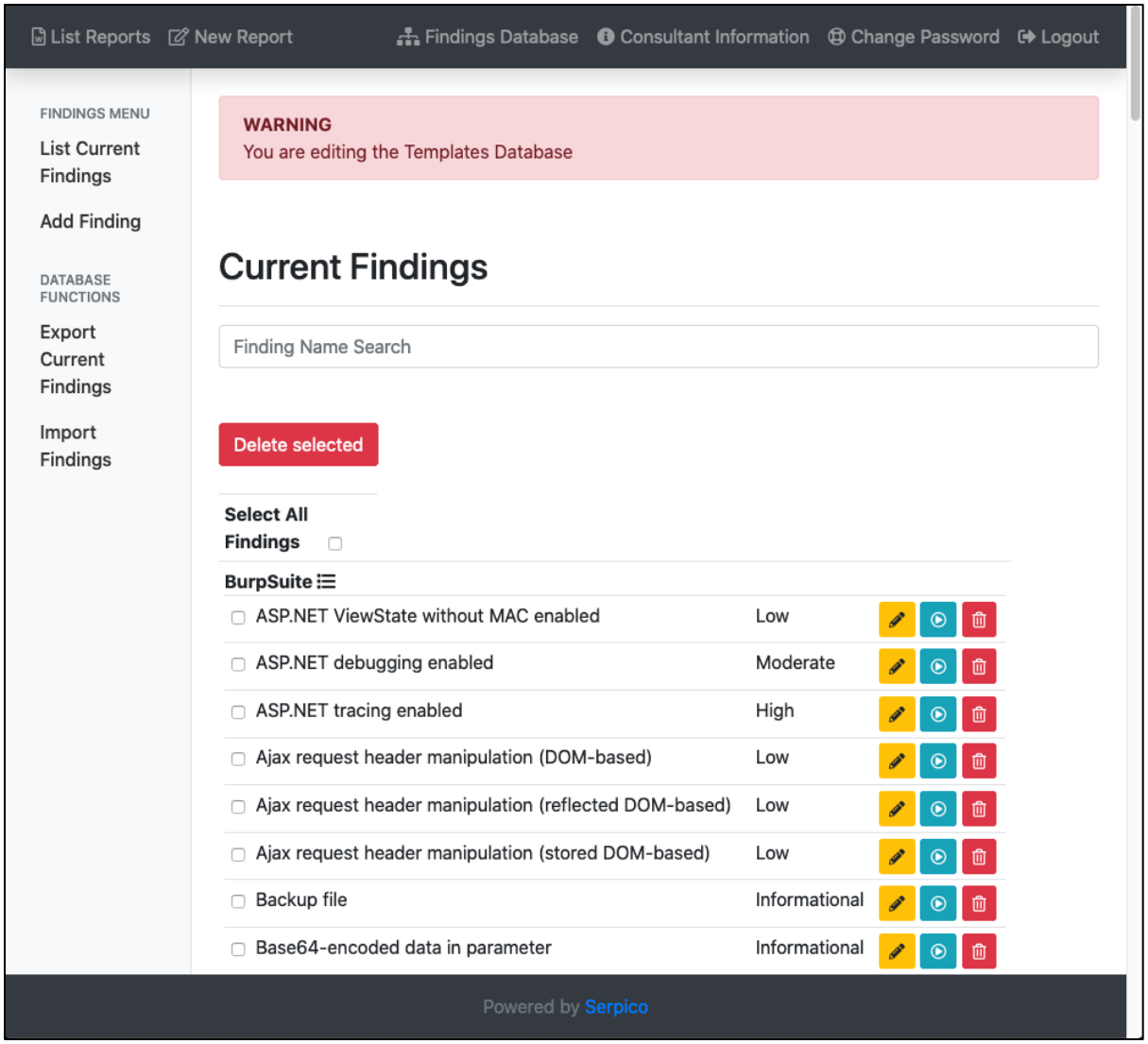
Εικόνα 8. Σελίδα διαχείρισης ExtraFindings Plugin.

Όταν τελειώσει η εισαγωγή των findings του BurpSuite θα δείτε την παρακάτω σελίδα:



Εικόνα 9. Σελίδα στην οποία μεταφέρεται ο administrator μετά από επιτυχή εκτέλεση του ExtraFindings Plugin.

Πατώντας τον σύνδεσμο **here** μπορείτε να δείτε όλα τα findings που εισάχθηκαν στην βάση του Serpico.

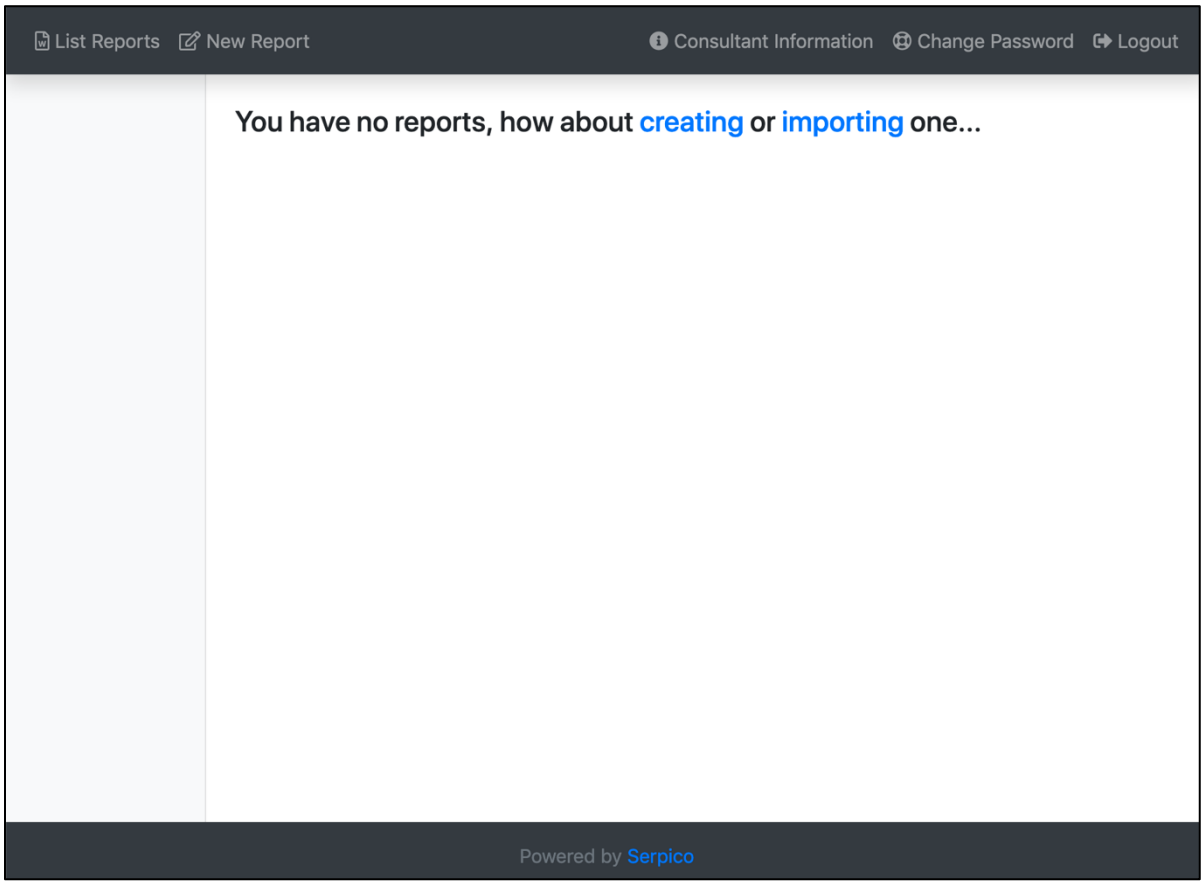


Εικόνα 10. Λίστα με τα διαθέσιμα findings

Εγχειρίδιο Χρήστη

Το Serpico είναι ένα open source reporting tool, και έχει ως στόχο να εξοικονομήσει χρόνο κατά την διάρκεια του reporting phase ενός assessment. Το output που παράγεται είναι εν μέρει συμπληρωμένο, με την περισσότερη δουλειά να είναι ολοκληρωμένη.

Όταν ένας χρήστης μπαίνει στο Serpico θα δει την παρακάτω σελίδα:



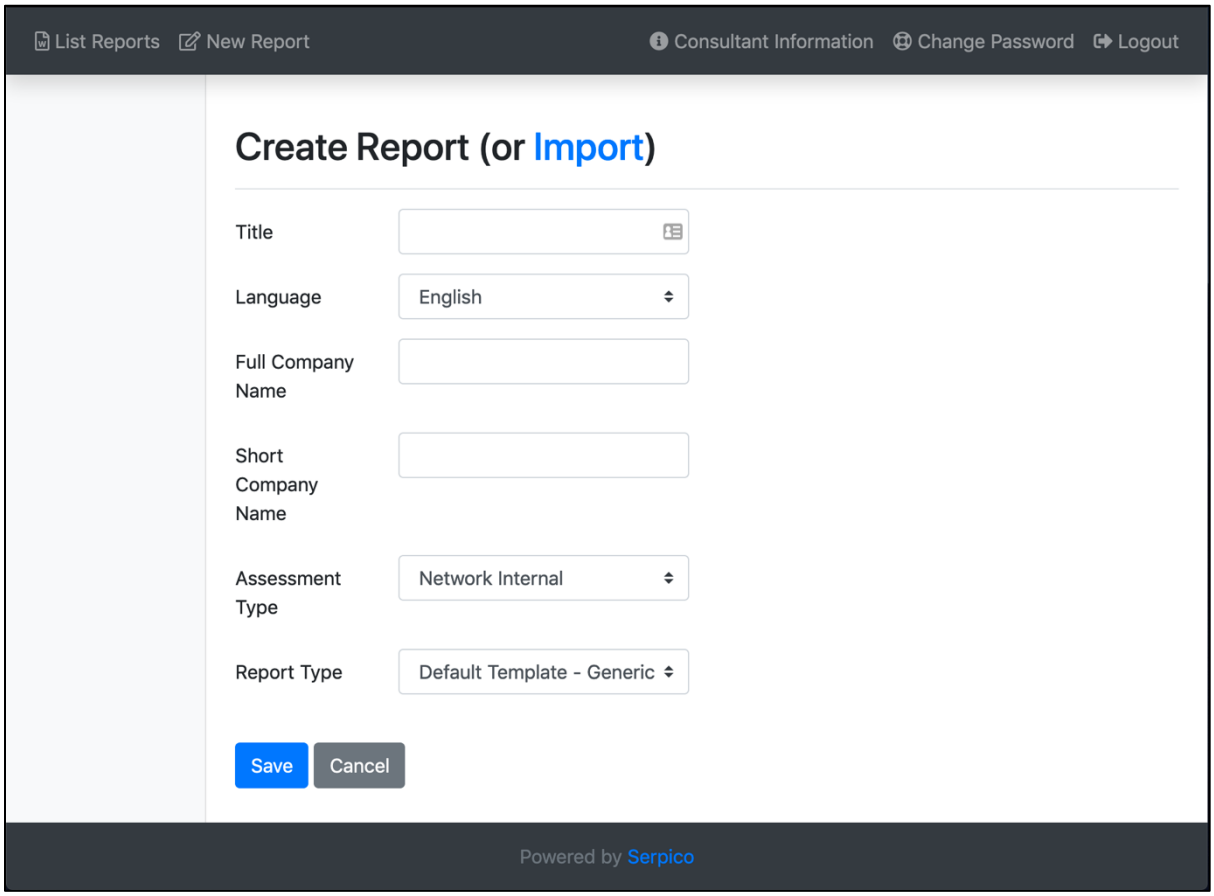
Εικόνα 11. Αρχική σελίδα.

Οι δυνατότητες που έχει ο χρήστης είναι:

1. New Report
   Ο χρήστης μπορεί να δημιουργήσει ένα καινούριο report.
2. List Reports
   Ο χρήστης μπορεί να δει τα διαθέσιμα reports του.
3. Consultant Information
   Ο χρήστης μπορεί να επεξεργαστεί τα στοιχεία του.
4. Change Password
   Ο χρήστης μπορεί να τροποποιήσει το password του.

New report

Για την δημιουργία ενός καινούριου report πατήστε το **New Report** και στην συνέχεια θα πρέπει να συμπληρώσετε στην παρακάτω φόρμα τις βασικές πληροφορίες του report:



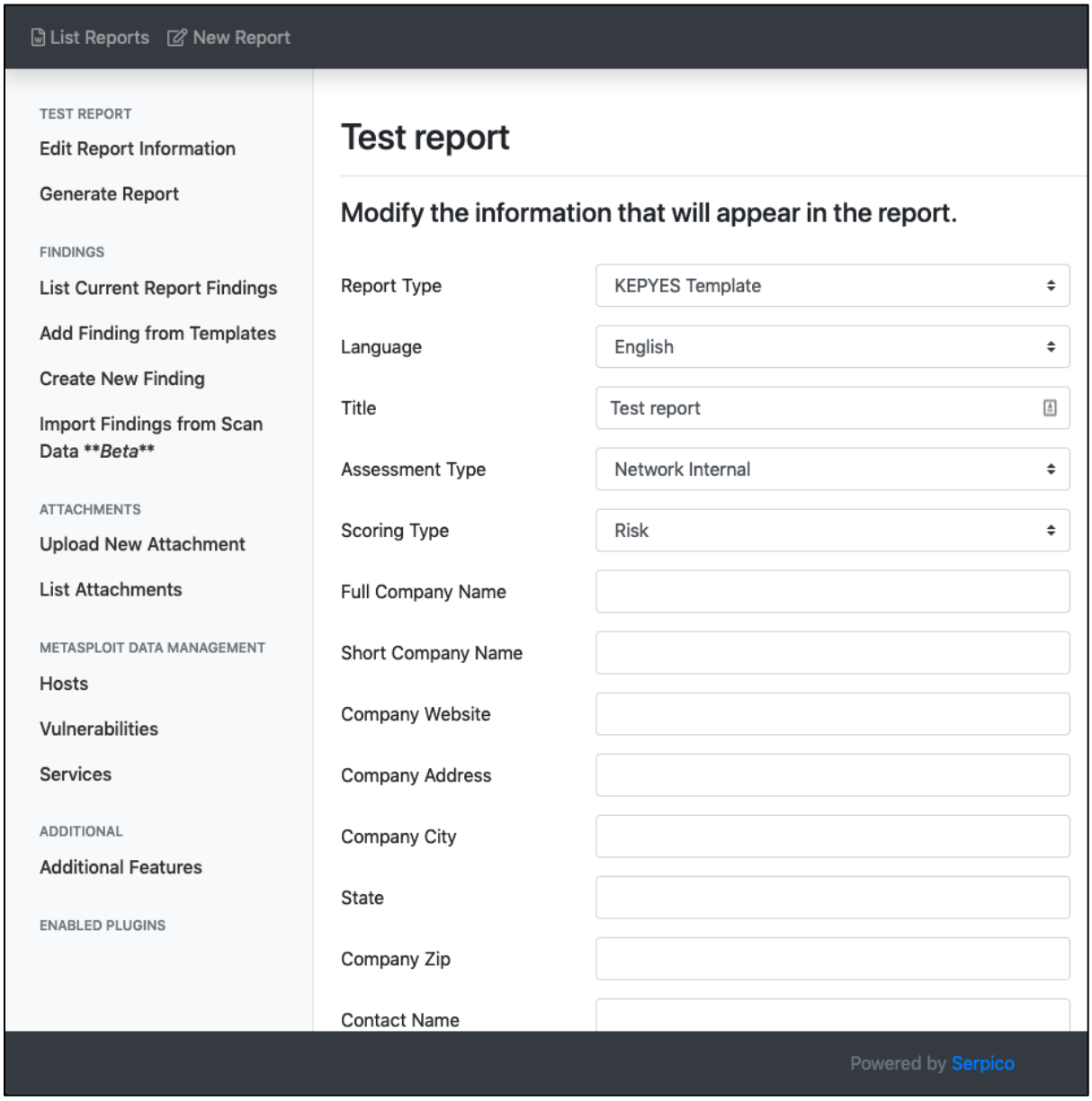
Εικόνα 12. Σελίδα δημιουργίας νέου report.

Η φόρμα αυτή περιέχει τα εξής πεδία:

- Title:
  Ο τίτλος της αναφοράς. Η συμπλήρωση του πεδίου είναι υποχρεωτική.
- Language:
  Η γλώσσα στην οποία θα γραφτεί το report. Η συμπλήρωση του πεδίου είναι υποχρεωτική.
  Επιλογή ανάμεσα σε **English** και **Greek**.
- Full Company Name:
  Το πλήρης όνομα του οργανισμού για τον οποίο αναφέρεται το report. Η συμπλήρωση του πεδίου είναι προαιρετική.
- Short Company Name:
  Το σύντομο όνομα του οργανισμού για τον οποίο αναφέρεται το report. Η συμπλήρωση του πεδίου είναι προαιρετική.
- Assessment Type:
  Ο τύπος του assessment. Η συμπλήρωση του πεδίου είναι υποχρεωτική.
  Επιλογή ανάμεσα σε **Network Internal**, **External**, **Web Application**, **Physical**, **Social engineering** και **Configuration audit**.
- Report Type:
  Το template που θα χρησιμοποιήσετε για την παραγωγή του report. Η συμπλήρωση του πεδίου είναι υποχρεωτική.

Στην συνέχεια πατήστε **Save**.

Στην επόμενη σελίδα θα δείτε μία πιο αναλυτική φόρμα με περισσότερα πεδία, όπως φαίνεται παρακάτω:



Εικόνα 13. Σελίδα τροποποίησης πληροφοριών ενός report.

Τα πεδία αυτά είναι προαιρετικά και μπορούν να χρησιμοποιηθούν στα templates.

Στην αριστερή πλευρά υπάρχουν οι εξής επιλογές για τον χρήστη:

- **TEST REPORT**
  - Edit Report Information
    Ο χρήστης μπορεί να επεξεργαστεί τις πληροφορίες του report. (Εικόνα 3)

- Generate Report
  Παράγεται ένα .docx αρχείο, από το template που επέλεξε ο χρήστης, που περιέχει τα findings που πρόσθεσε ο χρήστης.

- **FINDINGS**
  - List Current Report Findings
    Ο χρήστης μπορεί να δει τα findings που έχει εισάγει στο report.
  - Add Findings from Templates
    Ο χρήστης μπορεί να προσθέσει νέα findings από την βάση του Serpico.
  - Create New Findings
    Ο χρήστης μπορεί να δημιουργήσει καινούρια findings.
  - Import Findings from Scan Data (Beta)
    Ο χρήστης μπορεί να δημιουργήσει αυτόματα καινούρια findings εισάγοντας το scan data XML αρχείο που παράγουν το Nessus, το BurpSuite v1, το Metasploit και το Nmap. Η λειτουργία αυτή είναι σε Beta έκδοση.
- **ATTACHMENTS**
  - Upload Attachments
    Ο χρήστης μπορεί να ανεβάσει εικόνες, οι οποίες μπορούν να εισαχθούν στο report. Υποστηρίζονται μόνο οι .jpg και οι .png εικόνες.
  - List Attachments
    Ο χρήστης μπορεί να δει όλες τις εικόνες που έχουν ανέβει στο Serpico.
- **METASPLOIT DATA MANAGEMENT**
  Δίνεται η δυνατότητα να εισαχθούν οι hosts, τα services και τα vulnerabilities από την βάση δεδομένων του Metasploit στο Serpico. Είναι απαραίτητο να έχει παραμετροποιηθεί το Metasploit RPC Connector.
- **ADDITIONAL**
  Στα additional features υπάρχουν οι παρακάτω λειτουργίες
  - Manage User Defined Variables
    Ο χρήστης μπορεί να ορίσει global variable σε ένα report.
  - Manage User Defined Objects
    Όπως και στο UDV, ο χρήστης μπορεί να ορίσει objects.
  - Export Current Report
    Ο χρήστης μπορεί να κάνει εξαγωγή το report σε .json μορφή.
  - Export Attachments
    Ο χρήστης μπορεί να εξάγει όλα τα screenshots που έχει ανεβάσει στο server σε ένα .zip αρχείο.
  - Restore Attachments
    Ο χρήστης μπορεί να εισάγει ένα .zip αρχείο με screenshots και να τα ανεβάσει στο Serpico.
  - Configure a Metasploit RPC Connection
    Ο χρήστης μπορεί να συνδέσει το Serpico με το Metasploit RPC.
  - Auto Add Vulnerabilities from Metasploit DB
    Εάν υπάρχει Metasploit connection, τότε ο χρήστης μπορεί να εισάγει findings από την βάση δεδομένων του Metasploit.
  - Auto Add Findings from a Nessus XML (Deprecated - Use MSF RPC)
    Ο χρήστης μπορεί να δημιουργήσει αυτόματα καινούρια findings εισάγοντας το scan data XML αρχείο που παράγει το Nessus.
  - Auto Add Findings from a Burp XML scanner report
    Ο χρήστης μπορεί να δημιουργήσει αυτόματα καινούρια findings εισάγοντας το scan data XML αρχείο που παράγει το Burp.
  - Generate Status Report

Ο χρήστης μπορεί να παράγει ένα report σε .docx μορφή, το οποίο περιλαμβάνει μόνο τα findings που βρέθηκαν.

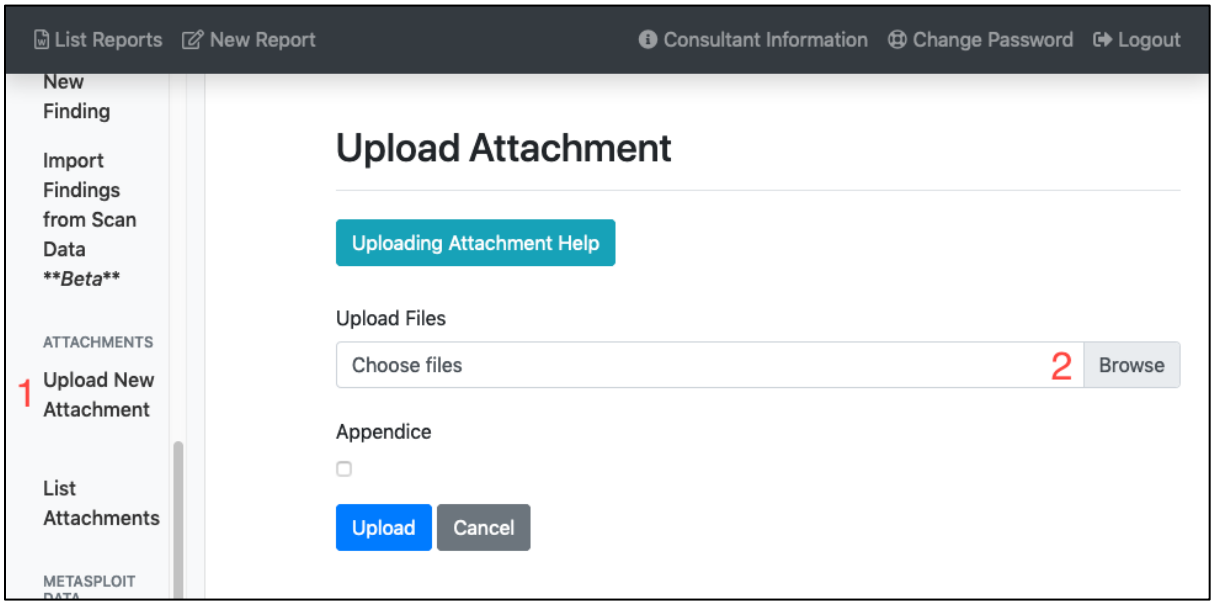
- Generate Text Only Status Report
  Ο χρήστης μπορεί να δει συνοπτικά στην σελίδα την λίστα με τα ονόματα των findings που βρέθηκαν.
- Generate Findings CSV (Pipe Delimited)
  Ο χρήστης μπορεί να εξάγει τα findings που έχει δηλώσει σε CSV μορφή.
- Generate AsciiDoc of Current Findings
  Ο χρήστης μπορεί να εξάγει τα findings που έχει δηλώσει σε AsciiDoc μορφή.
- Generate Presentation from Report
  Ο χρήστης μπορεί να παράγει ένα power point με τα findings που έχουν βρεθεί.
- Generate Presentation to PDF
  Ο χρήστης μπορεί να παράγει ένα power point με τα findings που έχουν βρεθεί. Δίνεται η δυνατότητα να αποθηκευτεί τοπικά κάνοντας print την σελίδα και στην συνέχεια αποθήκευση σε μορφή PDF.
- Export Presentation to HTML
  Ο χρήστης μπορεί να παράγει μία παρουσίαση με τα findings που έχουν βρεθεί σε HTML μορφή. Παράγεται ένα .zip αρχείο το οποίο περιέχει όλα τα HTML αρχεία (css, js, html).

- **ENABLED PLUGINS**
  Εδώ εμφανίζονται τα ενεργοποιημένα plugins, τα οποία μπορούν να χρησιμοποιηθούν στην παραγωγή του report.

Attachments

Upload Attachments

Για να ανεβάσετε screenshots που θα χρησιμοποιηθούν στα findings, επιλέξτε στην αριστερή πλευρά **Upload New Attachments**, κάτω από τα **Attachments** και στην επόμενη σελίδα επιλέξτε **Browse**.

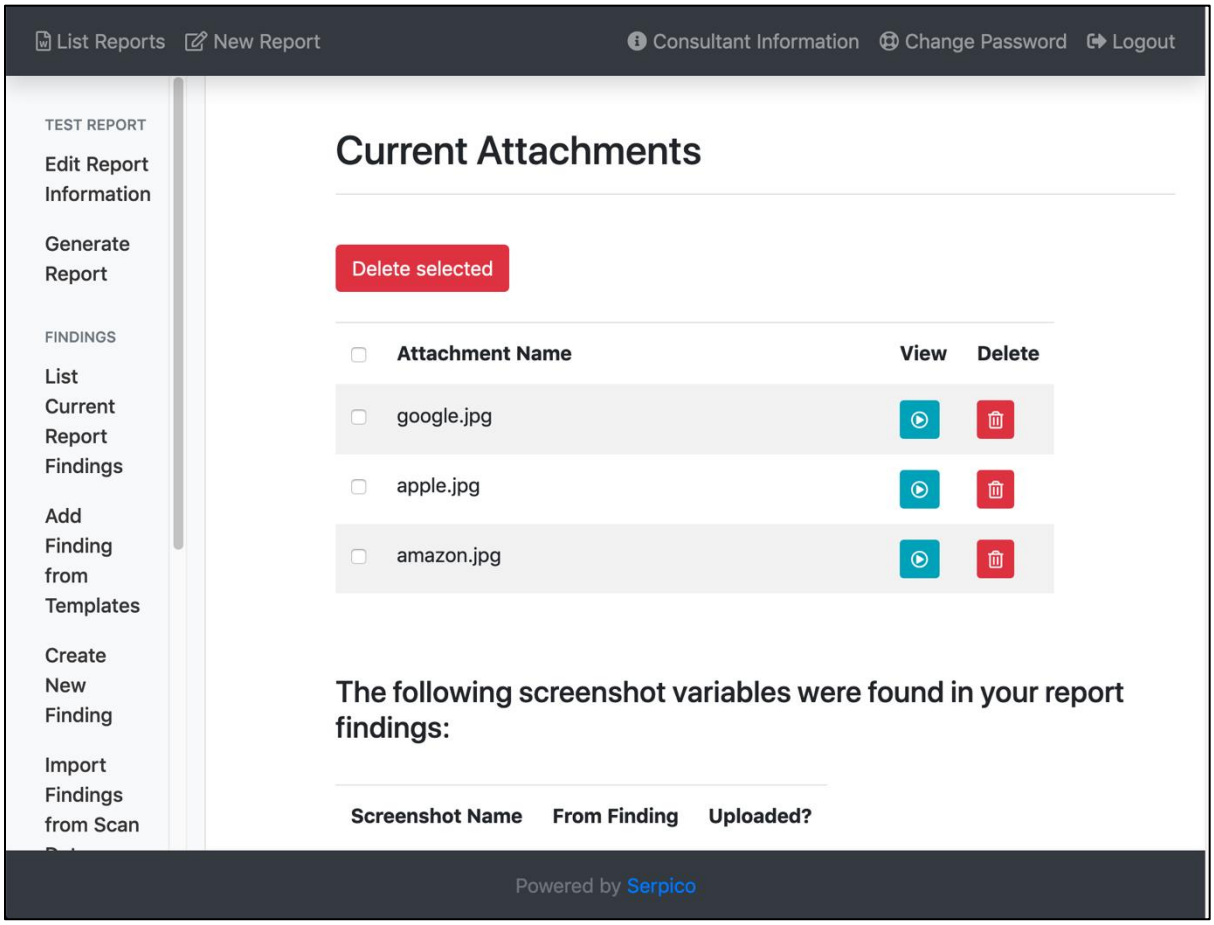


Εικόνα 14. Σελίδα στην οποία γίνονται upload τα attachments.

Επιλέξτε τα screenshots που θέλετε, στο popup παράθυρο που θα σας εμφανιστεί και πατήστε **Upload**.

List Attachments

Για να δείτε τα screenshots που έχετε ανεβάσει, επιλέξτε στην αριστερή πλευρά **List Attachments** κάτω από τα **Attachments**.



Εικόνα 15. Λίστα με τα attachments που έχουν ανέβει.

Για κάθε attachment μπορείτε να κάνετε τα παρακάτω actions:

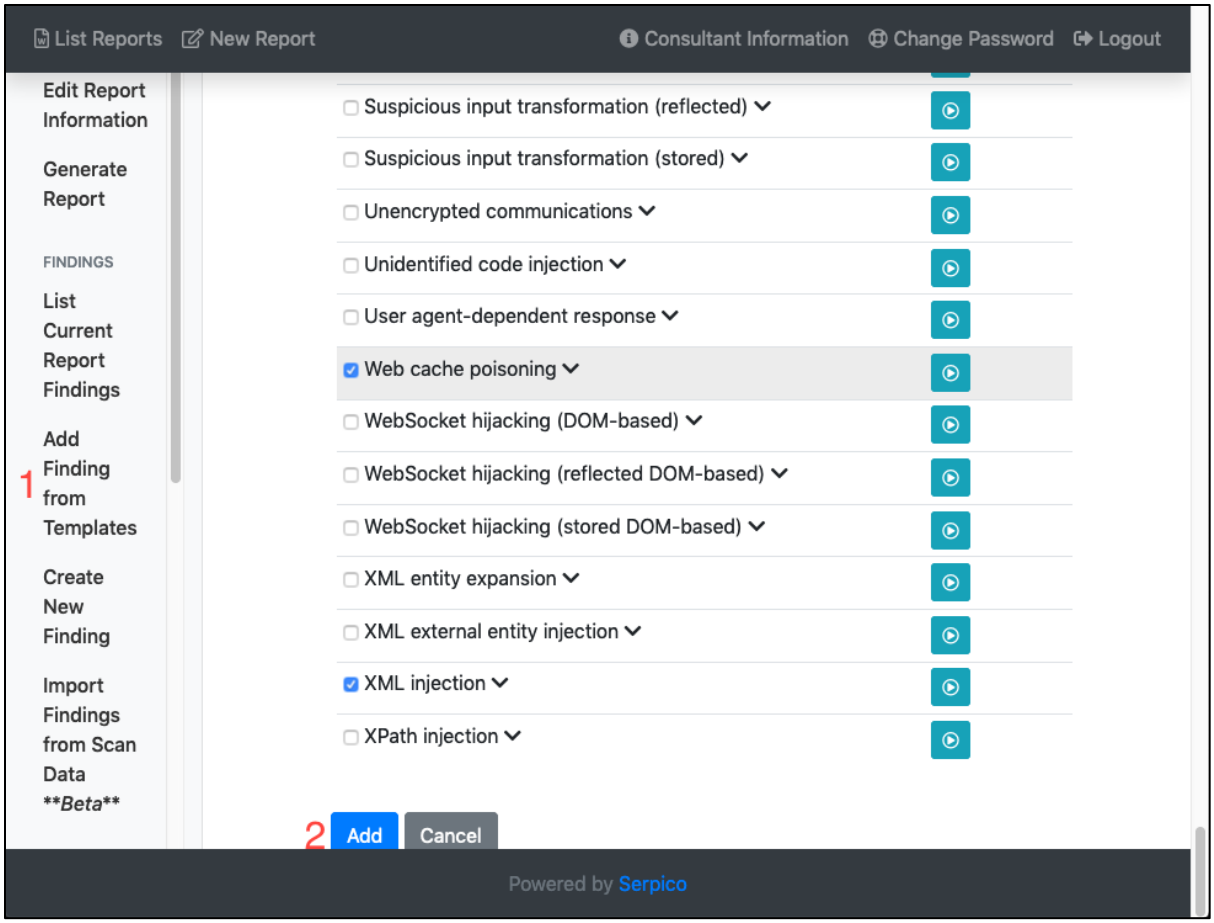
1. View: Πατώντας αυτό το κουμπί θα σας εμφανιστεί ένα popup παράθυρο για να κατεβάσετε το αρχείο και να το δείτε τοπικά στο υπολογιστή σας.
2. Delete: Διαγραφή του αρχείου.

Επίσης, μπορείτε να κάνετε διαγραφή πολλαπλών αρχείων επιλέγοντας τα αρχεία που θέλετε και στην συνέχεια πατώντας **Delete selected**.

Findings

Add Findings from Templates

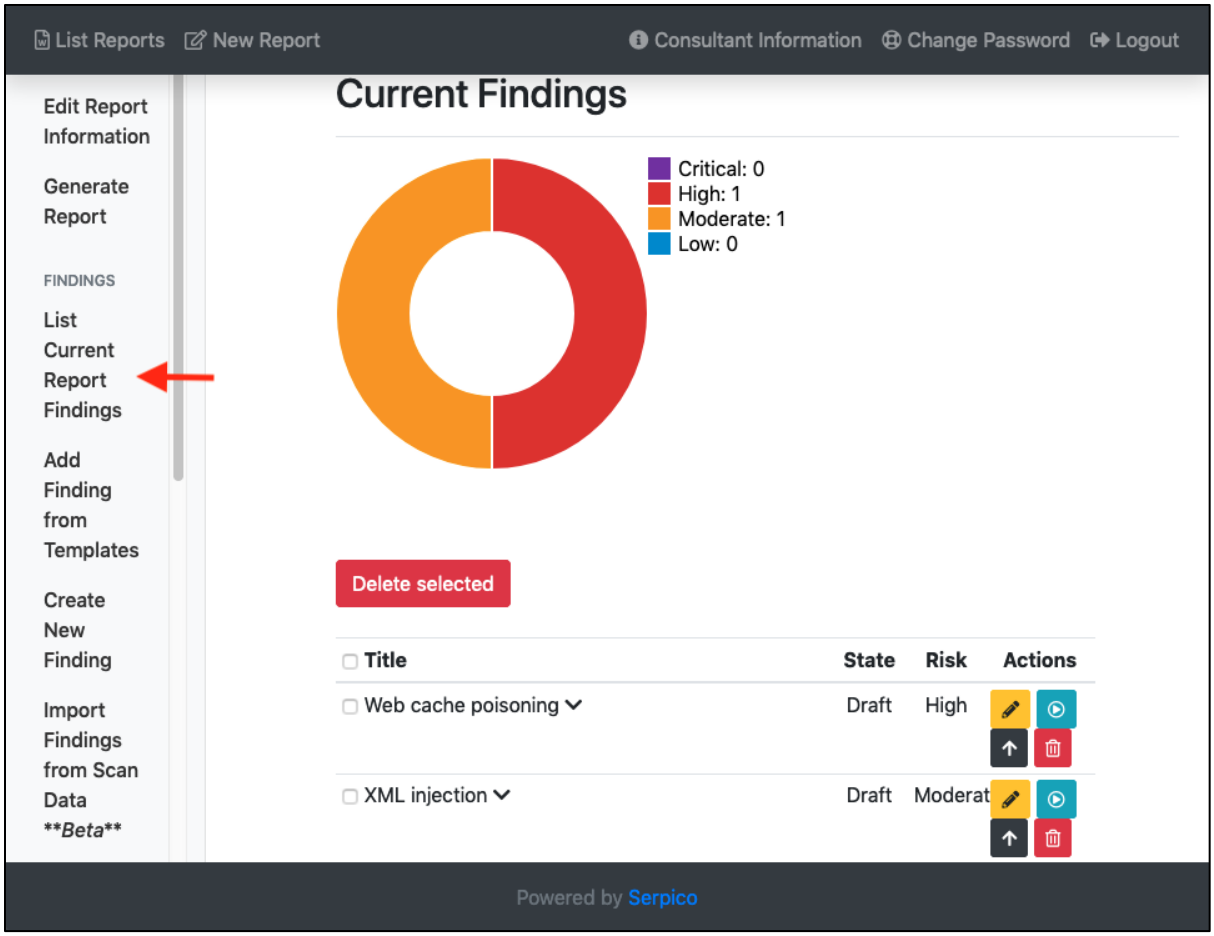
Για να προσθέσετε findings στο report σας, επιλέξτε από την αριστερή πλευρά **Add Findings from Templates** κάτω από τα **Findings**. Στην συνέχεια επιλέξτε τα findings που σας ενδιαφέρουν και πατήστε κάτω στο τέλος της λίστας **Add**.



Εικόνα 16. Λίστα με τα διαθέσιμα findings

List Current Report Findings

Για να δείτε τα findings που έχετε προσθέσει στο report σας, επιλέξτε από την αριστερή πλευρά **List Current Report Findings** κάτω από τα **Findings**.



Εικόνα 17. Λίστα με τα findings που έχουν προστεθεί στο report.

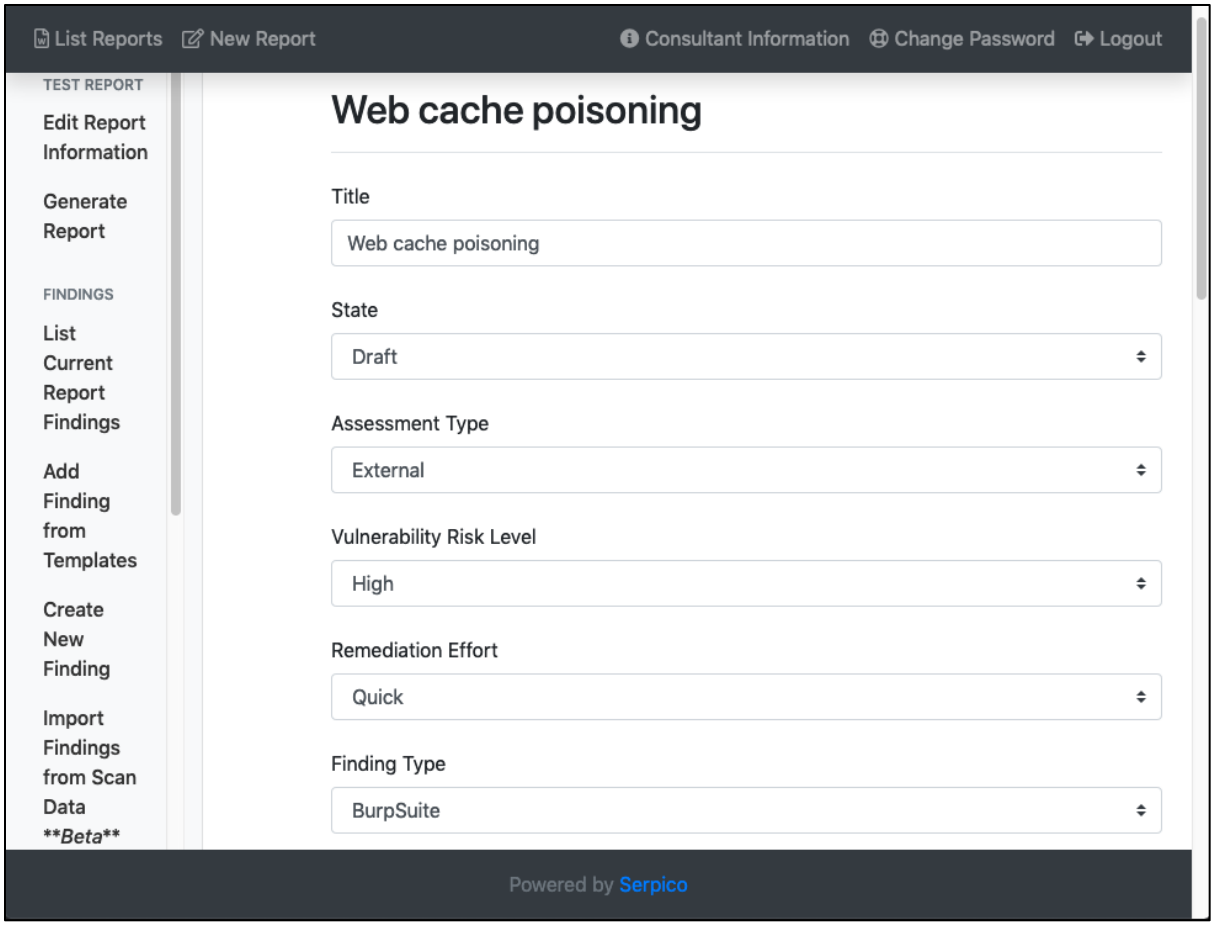
Για κάθε finding μπορείτε να κάνετε τα παρακάτω actions:

1. Edit: Επεξεργασία του finding (Description, Proof of Concept, Remediation, κτλ.).
2. Preview: Πατώντας αυτό το κουμπί θα σας εμφανιστεί ένα popup παράθυρο για να κατεβάσετε ένα .docx αρχείο, ώστε να δείτε το finding τοπικά στο υπολογιστή σας.
3. Upload: Για να κάνετε το finding upload στην τοπική database.
4. Delete: Διαγράφη του finding.

Επίσης, μπορείτε να κάνετε διαγραφή πολλαπλών findings επιλέγοντας τα findings που θέλετε και στην συνέχεια πατώντας **Delete selected**.

Edit Finding

Πατώντας **Edit** σε ένα finding θα δείτε την παρακάτω φόρμα:



Εικόνα 18. Σελίδα επεξεργασίας ενός finding.

Τα πεδία που είναι διαθέσιμα προς επεξεργασία είναι:

- Title
  Ο τίτλος του finding.
- State
  Το στάδιο στο οποίο βρίσκετε η συγγραφή του finding (**Draft**, **Under Preview**, **Completed**)
- Assessment Type
  Ο τύπος του assessment (**External**, **Internal**, **Internal/External**, **Wireless**, **Web Application**, **DoS**)
- Vulnerability Risk Level
  Το επίπεδο της επικινδυνότητας του finding (**Informational**, **Low**, **Moderate**, **High**, **Critical**)
- Remediation Effort
  Η προσπάθεια που πρέπει να γίνει για να επιλυθεί η ευπάθεια (**Quick**, **Planned**, **Involved**)
- Finding Type
  Η κατηγορία που ανήκει το finding.
- Description
  Η περιγραφή του finding.
- Proof of Concept
  Η απόδειξη, πως βρέθηκε η ευπάθεια.
- Affected Hosts/URLs
  Οι διευθύνσεις και τα URL που επηρεάζονται από την ευπάθεια.

- Remediation
  Ενέργειες που πρέπει να γίνουν για να επιλυθεί η ευπάθεια.
- References
  Αναφορές που σχετίζονται με το finding.
- Notes Data
  Σημειώσεις που προστίθενται στο template της παρουσίασης.
- Presentation Data
  Παράγραφος που προστίθεται στο template της παρουσίασης.

Αφού κάνετε τις αλλαγές σας, πατήστε **Save** στο τέλος της φόρμας.

Meta Markup Χαρακτήρες

Στα παραπάνω πεδία μπορούν να χρησιμοποιηθούν τα meta markup characters του Serpico. Ορίζοντας ένα markup χαρακτήρα σε μια παράγραφο, θα εμφανιστεί με διαφορετικό τρόπο στο report που θα παραχθεί.

Αυτά τα meta markup characters είναι:

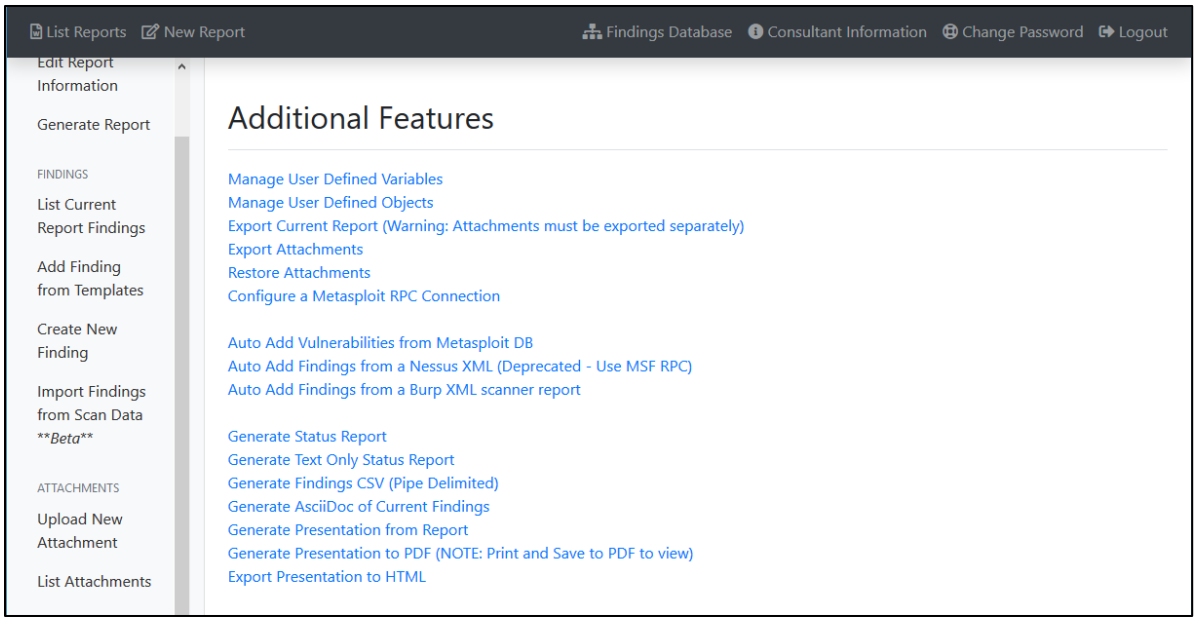
1. URL
   Για να εμφανιστεί ένα link σε μορφή hyperlink στο Word, τότε πρέπει να βάλετε το URL ανάμεσα σε "{{" και "}}".
   Παράδειγμα:
   {{https://www.example.org}}
2. Variables
   Για να εισάγετε την τιμή μίας μεταβλητής στο report, τότε πρέπει να δηλώσετε το όνομα της μεταβλητής ανάμεσα σε "<<" και ">>".
   Παράδειγμα:
   <<full_company_name>>
3. Bullets
   Για να εμφανιστεί μία παράγραφος σε μια λίστα με bullets, τότε πρέπει να βάλετε το κείμενο ανάμεσα σε "*-" και "-*".
   Παράδειγμα:
   -Bulleted text goes here-
4. Heading
   Για να εμφανιστεί μία πρόταση σε μορφή επικεφαλίδας, τότε πρέπει να την δηλώσετε ανάμεσα σε "[==" και "==]".
   Παράδειγμα:
   [==Heading text goes here==]
5. Italics
   Για να εμφανιστεί μία πρόταση σε italics μορφή, τότε πρέπει να την δηλώσετε ανάμεσα σε "[~~" και "~~]".
   Παράδειγμα:
   [~~Italics~~]
6. Code
   Για να εμφανιστεί μία πρόταση σε μορφή κώδικα, τότε πρέπει να την δηλώσετε ανάμεσα σε "[[[" και "]]]". Σημείωση: Ο κώδικας πρέπει να είναι σε μία γραμμή.
   Παράδειγμα:
   [[[code]]]
7. Screenshot
   Για να προσθέσετε ένα screenshot στο report, τότε θα πρέπει να γράψετε το όνομα του αρχείου ανάμεσα σε "[!!" και "!!]".

Παράδειγμα:
[!!screenshot_name.png!!]

User Defined Variables (UDV)

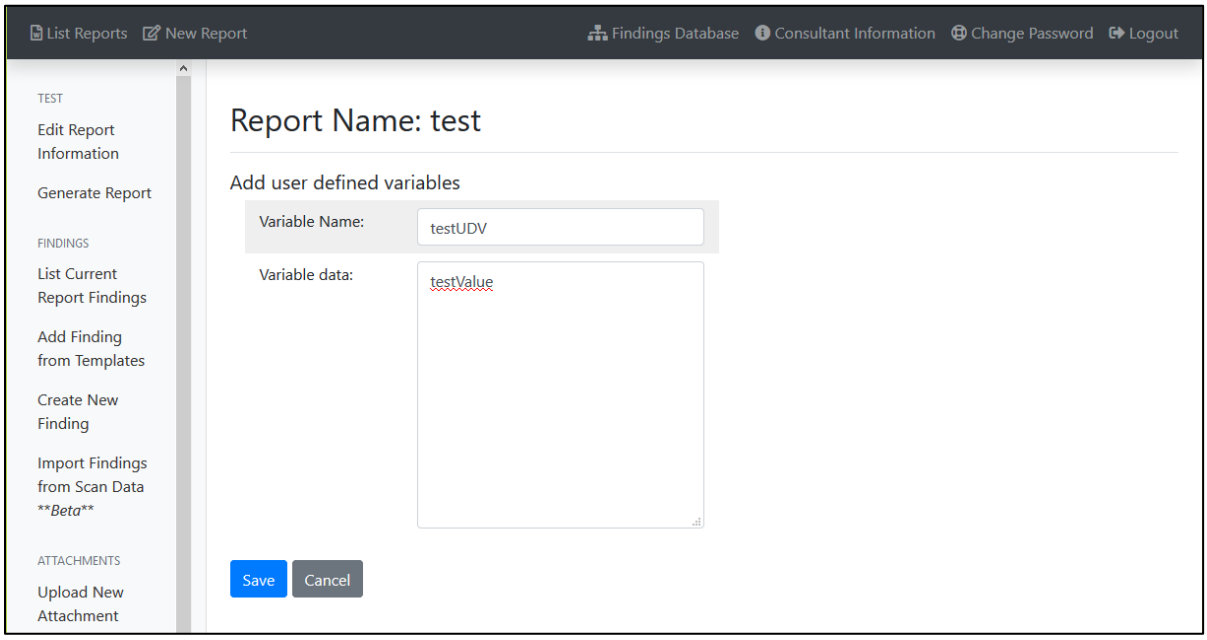
Τα User Defined Variables δίνουν την δυνατότητα στους χρήστες να ορίζουν global μεταβλητές σε ένα report.

Για να φτιάξετε ένα UDV, επιλέξτε από την αριστερή πλευρά **Additional Features** και στην συνέχεια **Manage User Defined Variables**.



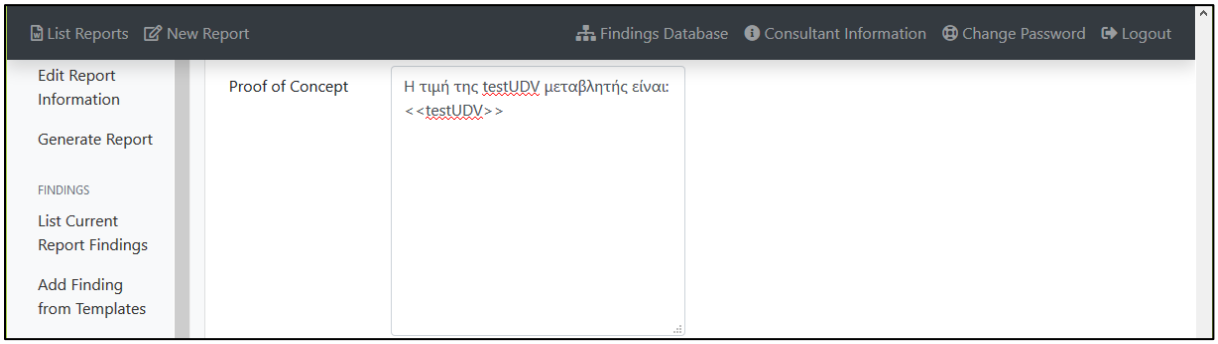
Εικόνα 19. Επιλογές μενού Additional Features

Στην συνέχεια ορίστε το όνομα της μεταβλητής και την τιμή της και πατήστε **Save**.



Εικόνα 20. Σελίδα αρχικοποίησης ενός UDV

Τώρα για να εισάγετε το UDV στο report, ανοίξτε ένα finding που έχετε εισάγει στο report σας και προσθέστε την μεταβλητή στο πεδίο που θέλετε, μέσα σε εισαγωγικά.



Εικόνα 21. Κλήση ενός UDV

Το παραπάνω πεδίο θα εμφανιστεί στο παραγόμενο report, όπως φαίνεται στο παρακάτω screenshot:

Η τιμή της testUDV μεταβλητής είναι: testValue

Εικόνα 22. Η τιμή του UDV στο παραγόμενο report

Reserved UDVs

Κατά την παραγωγή του report, το Serpico δημιουργεί αυτόματα 6 μεταβλητές, οι οποίες δηλώνουν το συνολικό αριθμό των findings που έχουν δηλωθεί στο report, βάσει της σοβαρότητας της ευπάθειας. Οι μεταβλητές αυτές είναι:

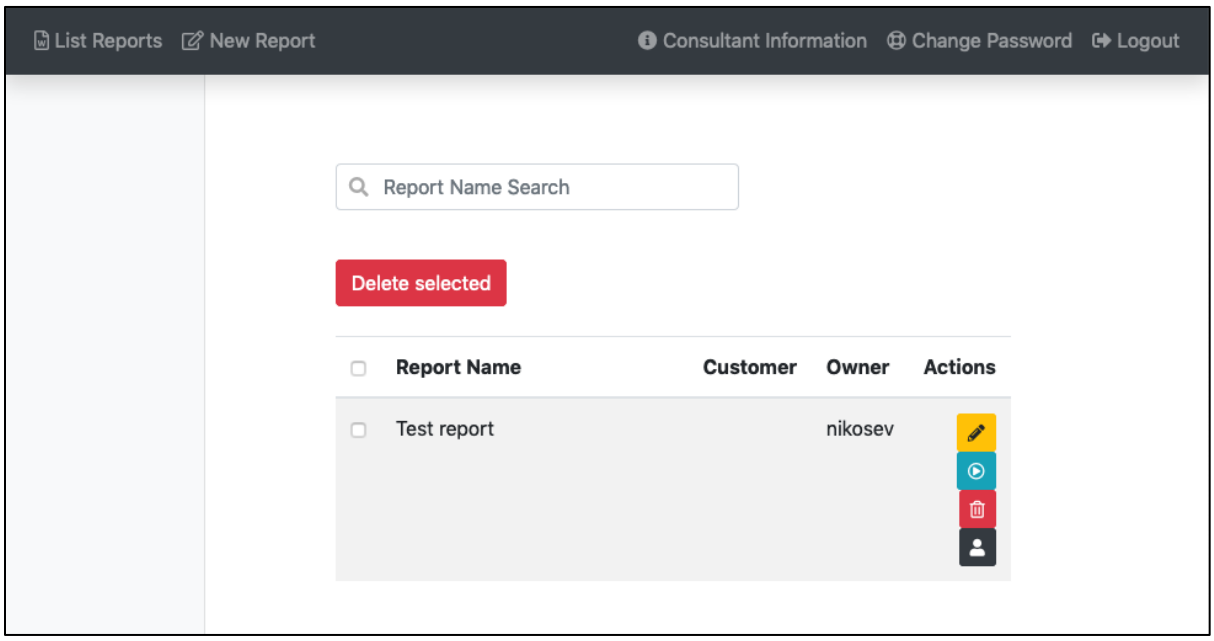
- total_tally: Συνολικός αριθμός των ευπαθειών
- critical_tally: Συνολικός αριθμός των κρίσιμων ευπαθειών

- high_tally: Συνολικός αριθμός των υψηλών ευπαθειών
- moderate_tally: Συνολικός αριθμός των μέτριων ευπαθειών
- low_tally: Συνολικός αριθμός των χαμηλών ευπαθειών
- informational_tally: Συνολικός αριθμός των ενημερωτικών ευπαθειών

Αυτές οι μεταβλητές είναι χρήσιμες επειδή μπορούν να χρησιμοποιηθούν σε διάφορες ενότητες (π.χ. σύνοψη) χωρίς να χρειάζεται να υπολογίζονται κάθε φορά.

List Reports

Επιλέγοντας **List Reports** στην μπάρα περιήγησης, ο χρήστης μπορεί να δει όλα τα reports που έχει δημιουργήσει, όπως φαίνεται στο παρακάτω screenshot:



Εικόνα 23. Λίστα με τα reports που έχει δημιουργήσει ο χρήστης.

Για κάθε report μπορείτε να κάνετε τα παρακάτω actions:

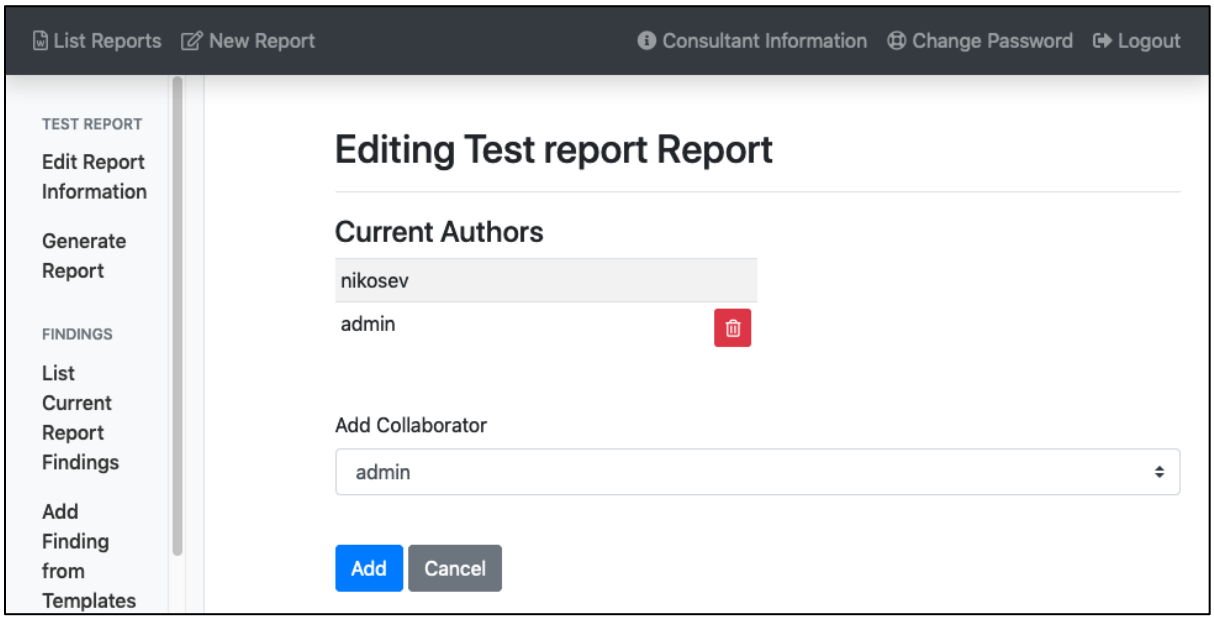
1. Edit: Επεξεργασία του report (όπως περιγράφεται στο κεφάλαιο New report).
2. Preview: Πατώντας αυτό το κουμπί θα σας εμφανιστεί ένα popup παράθυρο για να κατεβάσετε το report σε .docx μορφή, ώστε να δείτε το report τοπικά στο υπολογιστή σας.
3. Delete: Διαγράφη του finding.
4. Add Author: Προσθήκη άλλων χρηστών που θα μπορούν να επεξεργαστούν το report.

Επίσης, μπορείτε να κάνετε διαγραφή πολλαπλών reports επιλέγοντας τα reports που θέλετε και στην συνέχεια πατώντας **Delete selected**.

Add Author

Ο χρήστης έχει την δυνατότητα να δει την λίστα με τους **authors** που έχει προσθέσει, και να προσθέσει καινούριους, επιλέγοντας έναν χρήστη από μία λίστα και στην συνέχεια πατώντας **Add**. Επίσης μπορεί να διαγράψει από την λίστα κάποιον άλλον χρήστη πατώντας το εικονίδιο της διαγραφής δίπλα από το username του.

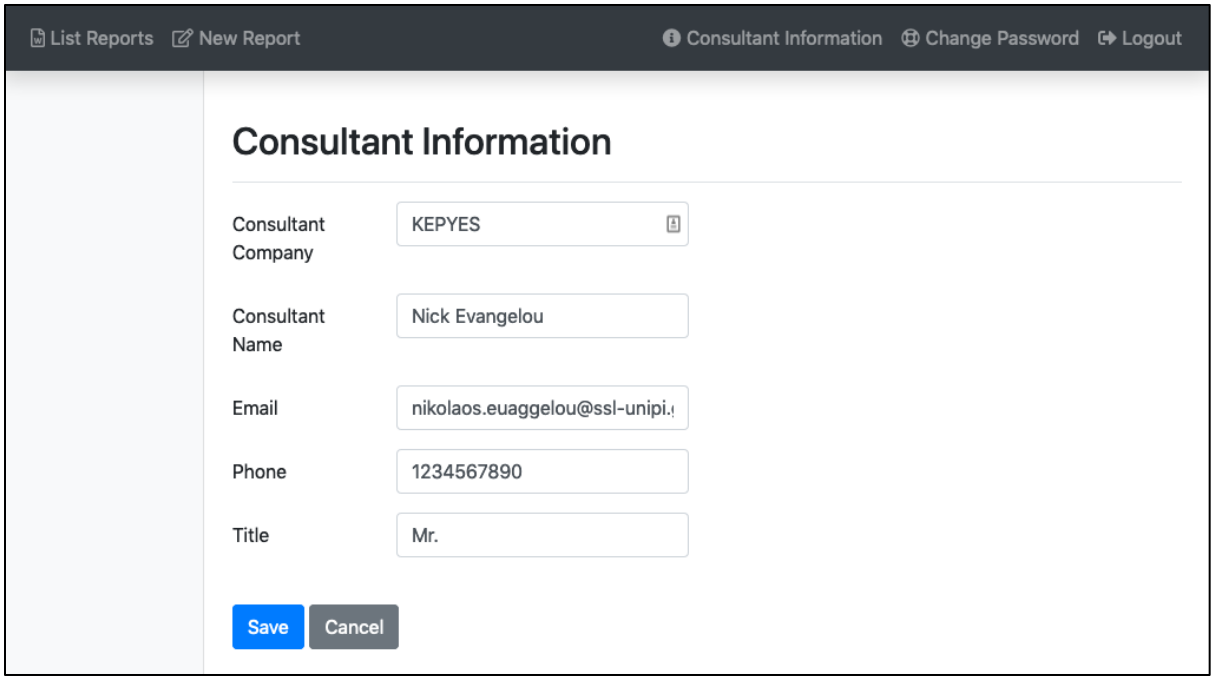
Στο παρακάτω screenshot φαίνεται η σελίδα επεξεργασίας των authors:



Εικόνα 24. Προσθήκη συνεργάτη σε ένα report.

Consultant Information

Ο χρήστης έχει την δυνατότητα να προσθέσει πληροφορίες για το λογαριασμό του, όπως φαίνεται στο παρακάτω screenshot:



Εικόνα 25. Σελίδα επεξεργασίας στοιχείων χρήστη.

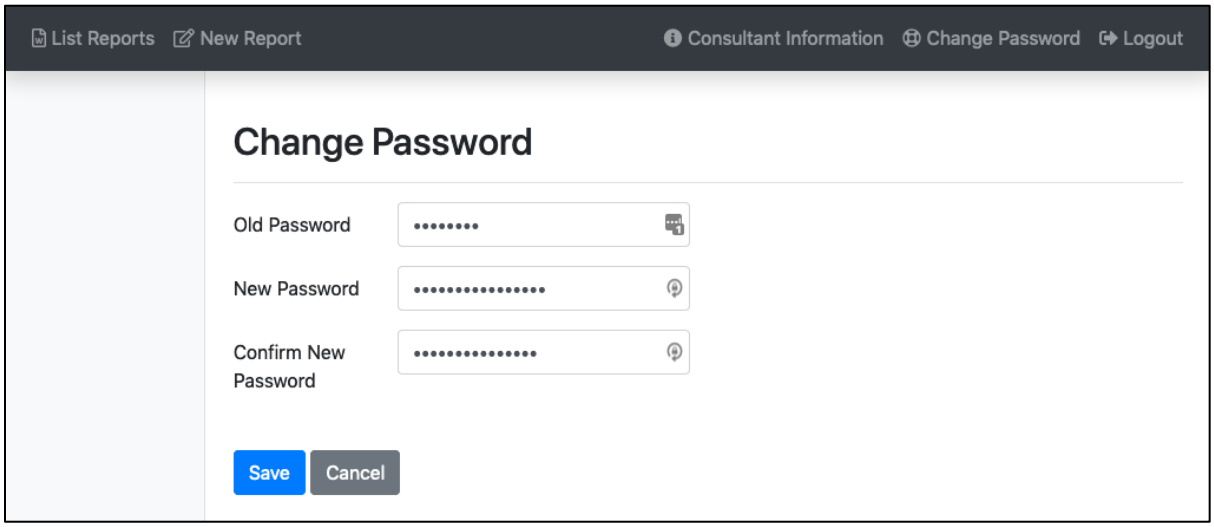
Τα πεδία που μπορεί να προσθέσει ο χρήστης είναι:

1. Consultant Company
   Το όνομα της εταιρίας/οργανισμού για τον οποίον ο χρήστης εργάζεται.
2. Consultant Name
   Το ονοματεπώνυμο του χρήστη.
3. Email
   Η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη.
4. Phone
   Τον αριθμό τηλεφώνου του χρήστη.
5. Title
   Ο τίτλος του χρήστη (π.χ. Mr, Mrs, Dr, Maj, MSgt κλπ.)

Για να αποθηκευτούν οι αλλαγές πατήστε **Save.**

Change Password

Ο χρήστης έχει την δυνατότητα να τροποποιήσει το password του, όπως φαίνεται στο παρακάτω screenshot:

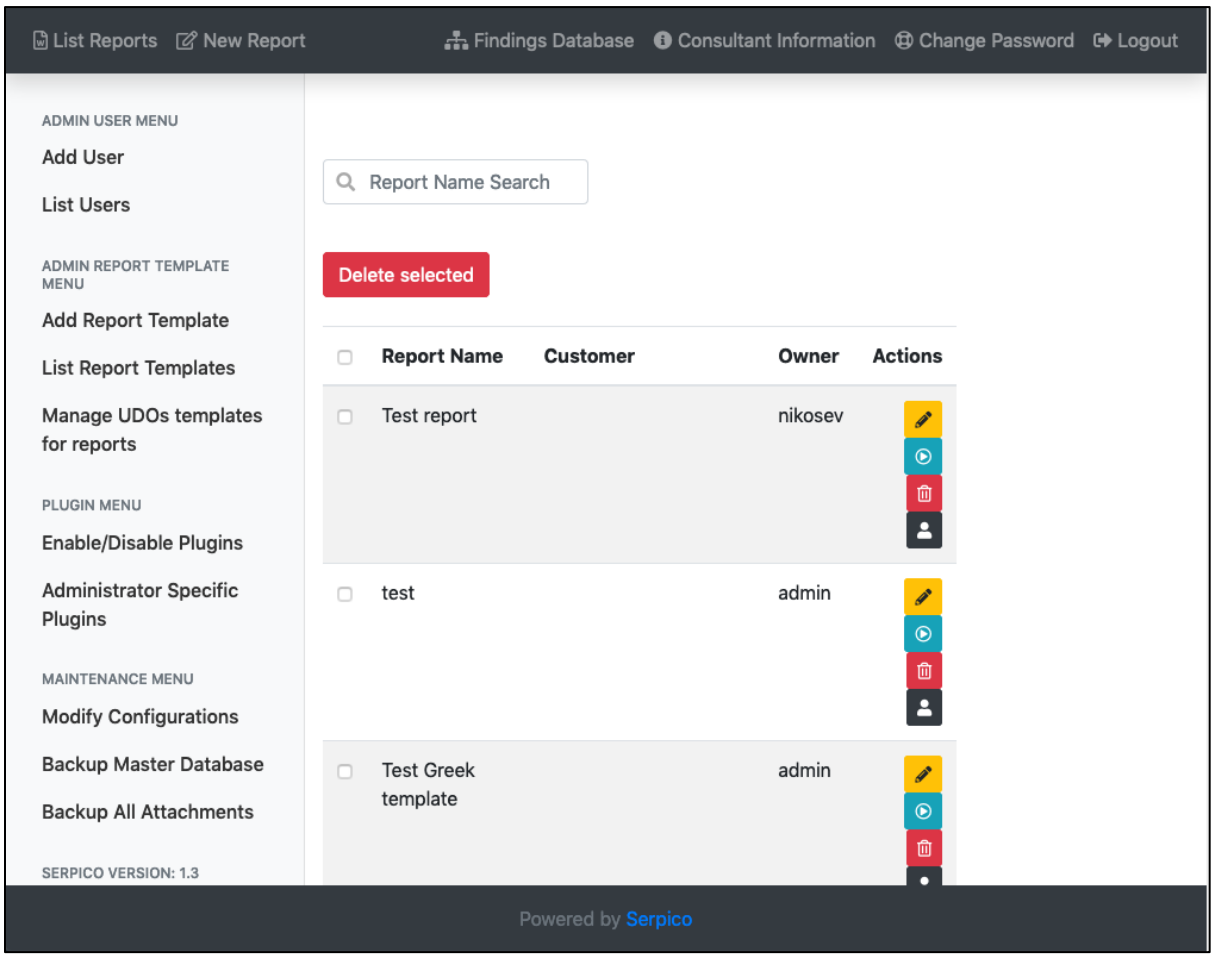


Εικόνα 26. Σελίδα αλλαγής password.

Ο χρήστης πρέπει να εισάγει το παρόν password του και στην συνέχεια να πληκτρολογήσει το καινούριο δύο φορές, για να επικυρωθεί το νέο password.

Εγχειρίδιο Διαχειριστή

Οι διαχειριστές, πέρα από τις δυνατότητες που έχουν οι απλοί χρήστες, έχουν την δυνατότητα να πραγματοποιήσουν κάποιες επιπλέον ενέργειες, όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 27. Αρχική σελίδα

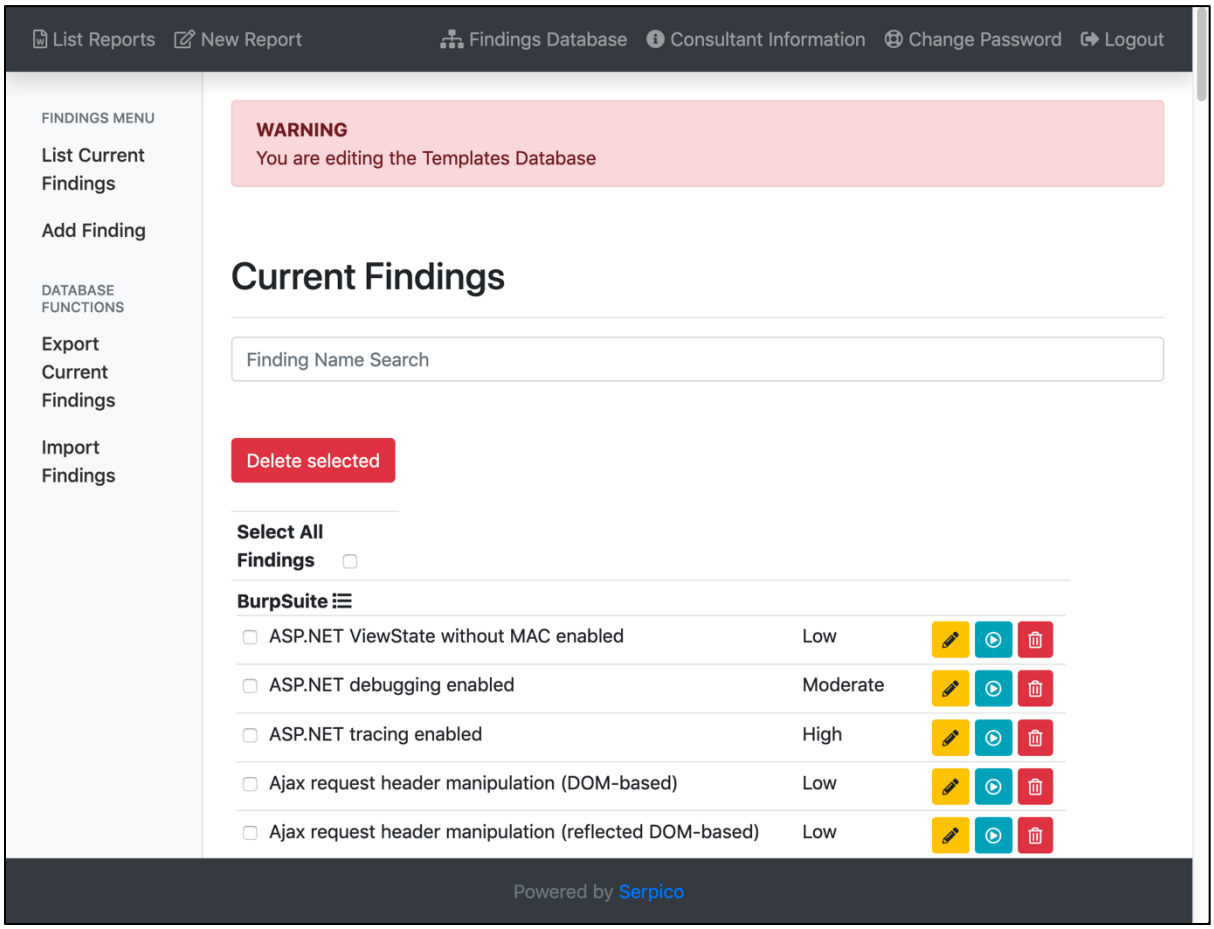
Οι δυνατότητες των διαχειριστών είναι:

1. List Reports
   Ο διαχειριστής μπορεί να δει τα διαθέσιμα reports του.
2. New Report
   Ο διαχειριστής μπορεί να δημιουργήσει ένα καινούριο report.
3. Findings Database
   Ο διαχειριστής μπορεί να επεξεργαστεί τα findings που βρίσκονται στην Βάση Δεδομένων του Serpico.
4. Consultant Information
   Ο διαχειριστής μπορεί να επεξεργαστεί τα στοιχεία του.
5. Change Password
   Ο διαχειριστής μπορεί να τροποποιήσει το password του.
6. Admin User Menu
   Ο διαχειριστής μπορεί να επεξεργαστεί τους χρήστες του συστήματος.

7. Admin Report Template Menu
   Ο διαχειριστής μπορεί να επεξεργαστεί τα templates των reports.
8. Plugin Menu
   Ο διαχειριστής μπορεί να επεξεργαστεί τα plugins του συστήματος.
9. Maintenance Menu
   Ο διαχειριστής μπορεί να επεξεργαστεί το configuration του server.

Findings Database

Σε αυτήν την σελίδα ο διαχειριστής μπορεί να δει όλα τα διαθέσιμα findings που υπάρχουν στην Βάση Δεδομένων του Serpico, να προσθέσει καινούρια και να τα κάνει export/import.



Εικόνα 28. Λίστα με τα διαθέσιμα findings

Στην αριστερή πλευρά υπάρχουν οι εξής επιλογές για τον διαχειριστή:

- **FINDINGS MENU**
  - List Current Findings
    Ο διαχειριστής μπορεί να δει όλα τα findings που υπάρχουν στην Βάση Δεδομένων του Serpico.
  - Add Findings
    Ο διαχειριστής μπορεί να προσθέσει καινούρια findings.
- **DATABASE FUNTIONS**
  - Export Current Findings

Ο διαχειριστής μπορεί να εξάγει τα findings που υπάρχουν στην Βάση Δεδομένων του Serpico σε ένα αρχείο με .json μορφή.

- Import Findings
  Ο διαχειριστής μπορεί να εισάγει ένα .json αρχείο το οποίο έχει παραχθεί από το Serpico.

Findings Menu

List Current Findings

Σε αυτήν την σελίδα (Εικόνα 28. Λίστα με τα διαθέσιμα findings) εμφανίζονται όλα τα findings του Serpico, ανά finding_type. Τα findings που έχουν ανέβει από απλούς χρήστες, εμφανίζονται στον πίνακα με κόκκινο background.

Για κάθε finding μπορείτε να κάνετε τα παρακάτω actions:

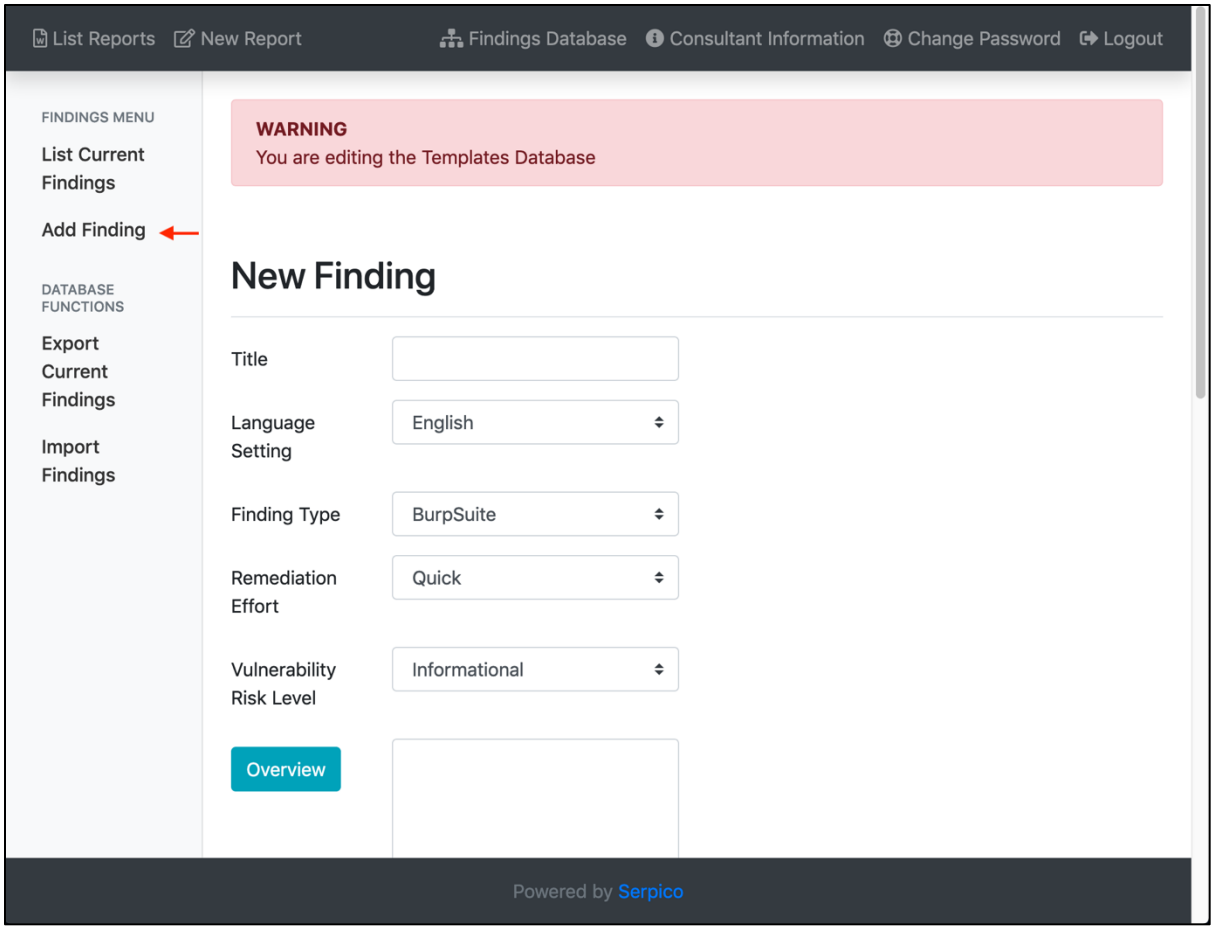
1. Edit: Επεξεργασία του finding (Title, Description, Remediation, κτλ.)
2. Preview: Πατώντας αυτό το κουμπί θα σας εμφανιστεί ένα popup παράθυρο για να κατεβάσετε ένα .docx αρχείο, ώστε να δείτε το finding τοπικά στο υπολογιστή σας.
3. Delete: Διαγράφη του finding.

Για να κάνετε διαγραφή πολλαπλών findings, επιλέξτε τα findings που θέλετε και στην συνέχεια πατήστε **Delete selected**.

Επίσης, μπορείτε να κάνετε αναζήτηση για κάποιο finding με βάση τον τίτλο. Πληκτρολογήστε το τίτλο στην μπάρα αναζήτησης και πατήστε **Enter** στο πληκτρολόγιο.

Add Findings

Για να δημιουργήσετε ένα finding, επιλέξτε στην αριστερή πλευρά **Add Finding** κάτω από το **Findings Menu** και θα εμφανιστεί η παρακάτω σελίδα:



Εικόνα 29. Σελίδα δημιουργίας finding

Τα πεδία που είναι διαθέσιμα προς επεξεργασία είναι:

- Title
  Ο τίτλος του finding.
- Language Setting
  Ορίζεται η γλώσσα στην οποία είναι γραμμένο το finding (**English**, **Greek**).
- Finding Type
  Η κατηγορία στην οποία ανήκει το finding.
- Remediation Effort
  Η προσπάθεια που πρέπει να γίνει για να επιλυθεί η ευπάθεια (**Quick**, **Planned**, **Involved**)
- Vulnerability Risk Level
  Το επίπεδο της επικινδυνότητας του finding (**Informational**, **Low**, **Moderate**, **High**, **Critical**)
- Description
  Η περιγραφή του finding.
- Proof of Concept
  Η απόδειξη, πως βρέθηκε η ευπάθεια (αφήστε το κενό, το POC ορίζεται στο report).

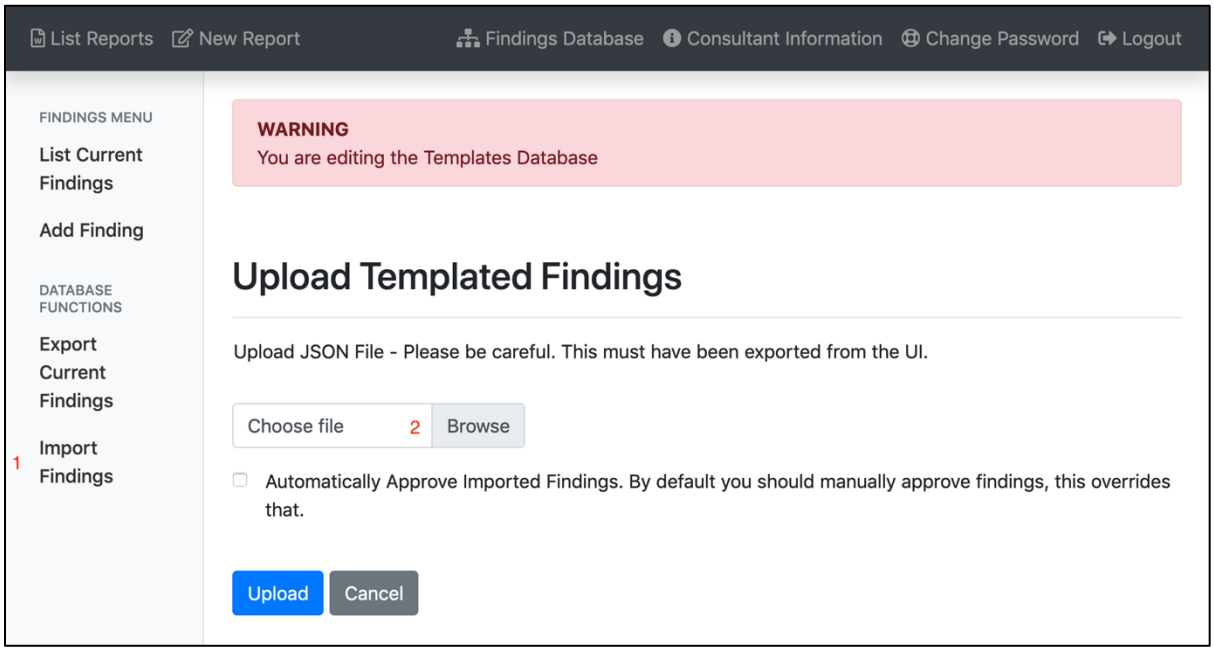
- Remediation
  Ενέργειες που πρέπει να γίνουν για να επιλυθεί η ευπάθεια.
- References
  Αναφορές που σχετίζονται με το finding.

Αφού ορίσετε τα πεδία, πατήστε **Save** στο τέλος της φόρμας.

Database Function

Import Findings

Για να εισάγετε τα findings στην βάση, επιλέξτε στην αριστερή πλευρά **Import Findings** κάτω από το **Database Functions** και στην επόμενη σελίδα επιλέξτε **Browse**.



Εικόνα 30. Σελίδα Upload Templated Findings

Επιλέξτε το αρχείο που θέλετε, στο popup παράθυρο που θα σας εμφανιστεί, και πατήστε **Upload**.

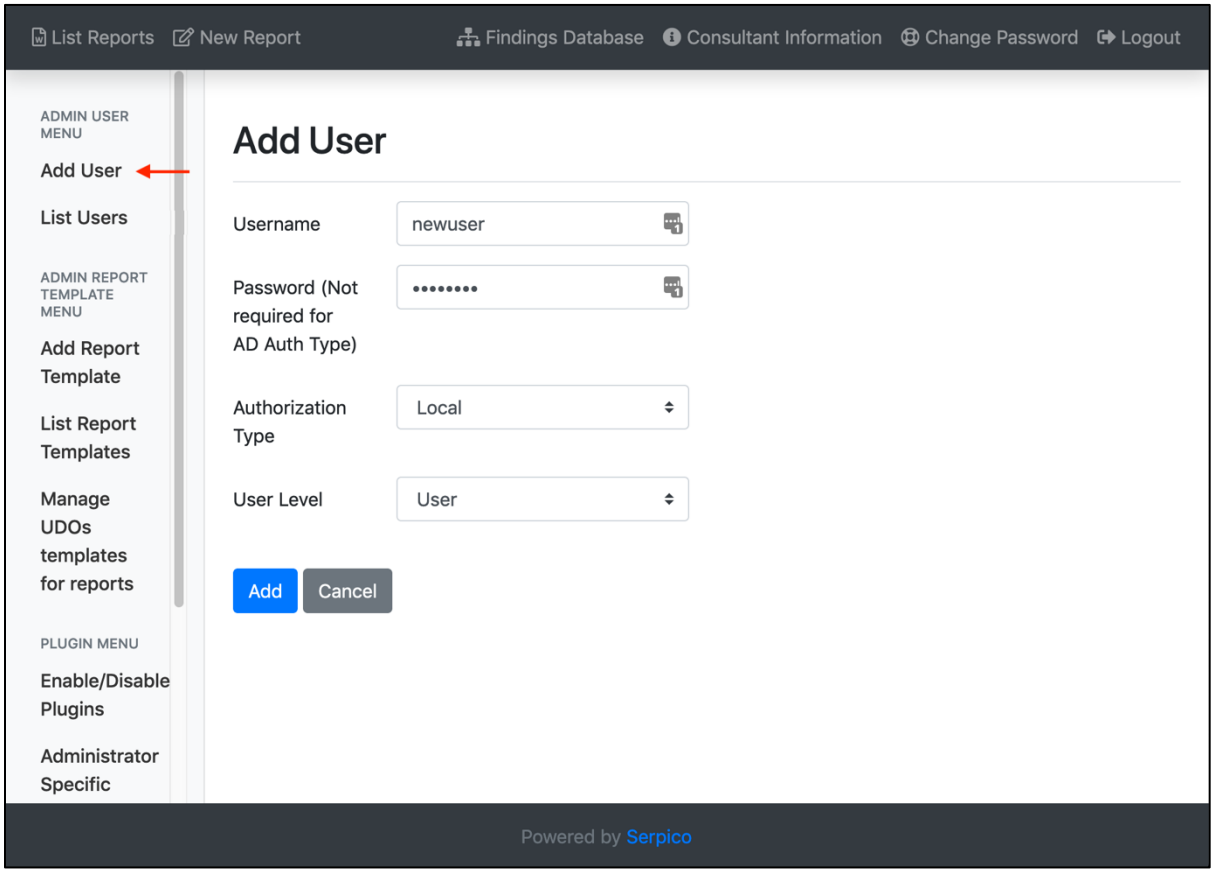
Admin User Menu

Σε αυτήν την κατηγορία ο διαχειριστής έχει τις εξής δυνατότητες:

- Add User
  Ο διαχειριστής μπορεί να δημιουργήσει καινούριο λογαριασμό.
- List User
  Ο διαχειριστής μπορεί να δει τους λογαριασμούς που υπάρχουν στο server.

Add User

Για να δημιουργήσετε ένα καινούριο λογαριασμό, επιλέξετε **Add User** κάτω από το **Admin User Menu** και θα δείτε την παρακάτω φόρμα:



Εικόνα 31. Σελίδα δημιουργίας νέου χρήστη

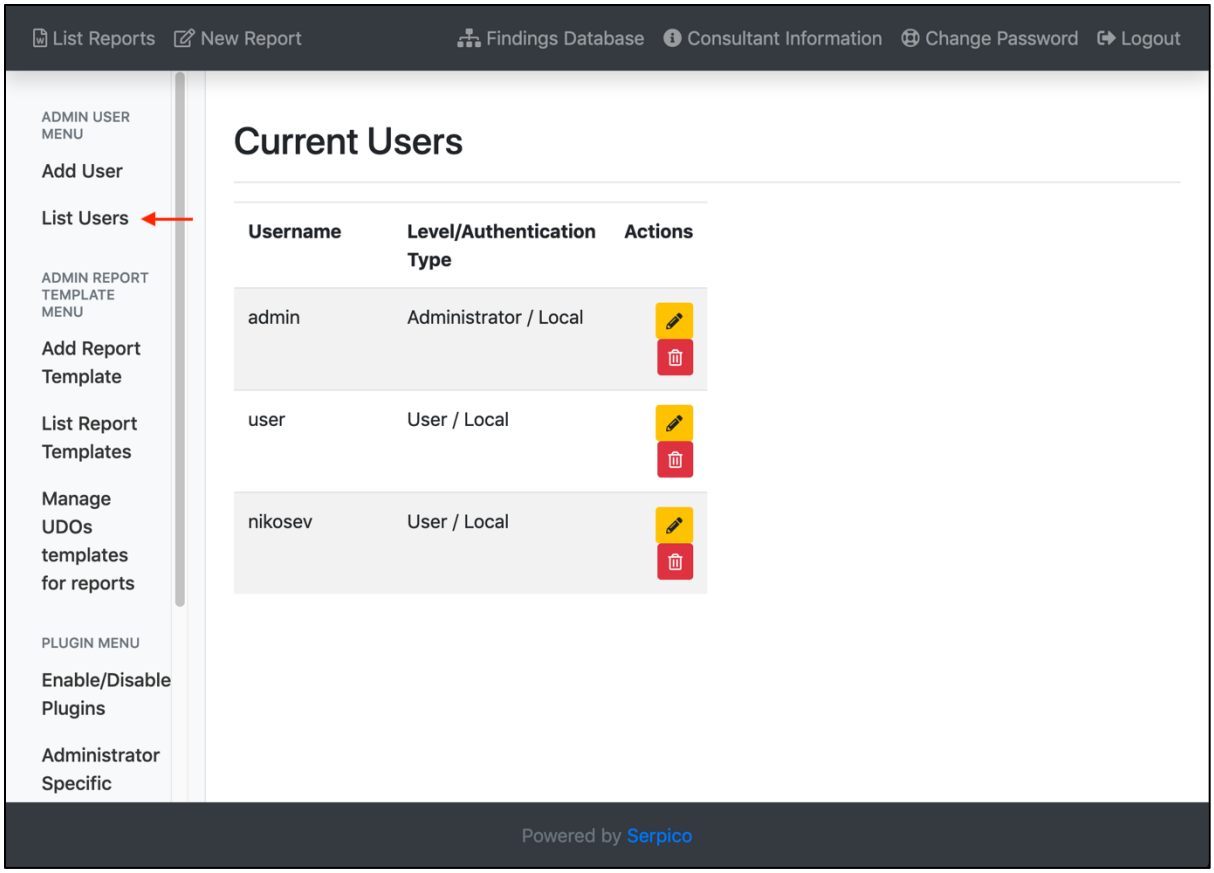
Τα πεδία που είναι διαθέσιμα προς επεξεργασία είναι:

- Username
  Ορίζεται το username του λογαριασμού.
- Password
  Ορίζεται το password του λογαριασμού.
- Authorization Type
  Επιλέξτε “Local” για να μπορεί να κάνει login στο Serpico.
- User Level
  Ορίζεται ο τύπος του λογαριασμού (**User**, **Administrator**).

Στην συνέχεια πατήστε **Add**.

List User

Για να δείτε όλους τους λογαριασμούς που υπάρχουν στο server, επιλέξετε **List User** κάτω από το **Admin User Menu** και θα δείτε τον παρακάτω πίνακα:



Εικόνα 32. Λίστα με τους διαθέσιμους χρήστες

Για κάθε χρήστη μπορείτε να κάνετε τα παρακάτω actions:

5. Edit: Επεξεργασία του report (όπως περιγράφεται στην ενότητα Add User).
6. Delete: Διαγράφη του λογαριασμού.

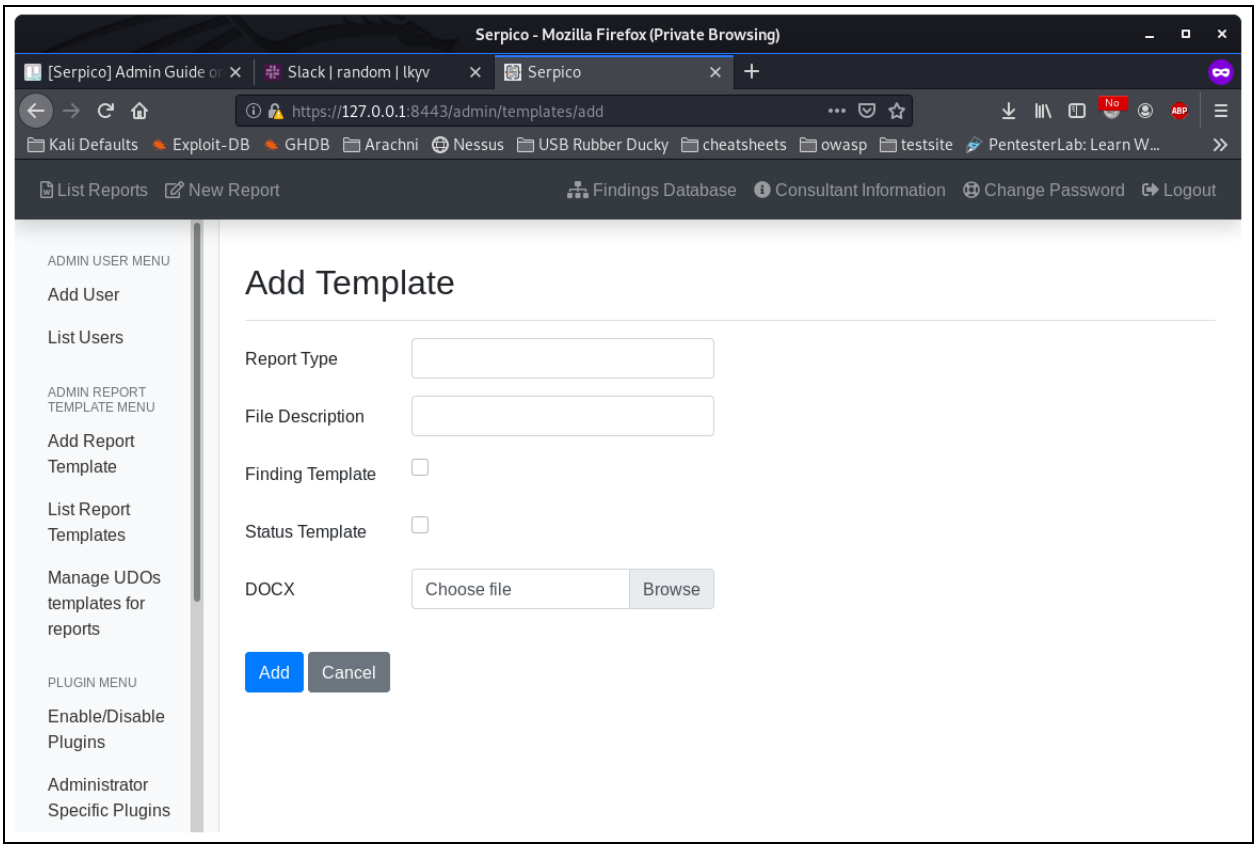
Admin Report Template Menu

Σε αυτήν την κατηγορία ο διαχειριστής έχει τις εξής δυνατότητες:

- Add Report Template
  Ο διαχειριστής έχει την δυνατότητα να προσθέσει νέα templates για reports.
- List Report Templates
  Ο διαχειριστής έχει την δυνατότητα να δει την λίστα με τα templates που έχουν ανέβει στο server.
- Manage UDOs templates for reports
  Ο διαχειριστής έχει την δυνατότητα να επεξεργαστεί τα UDOs (User Defined Objects).

Add Report Template

Για να προσθέσετε νέα report template, επιλέξτε **Add Report Template** κάτω από το **Admin Report Template Menu** και θα δείτε την παρακάτω σελίδα:



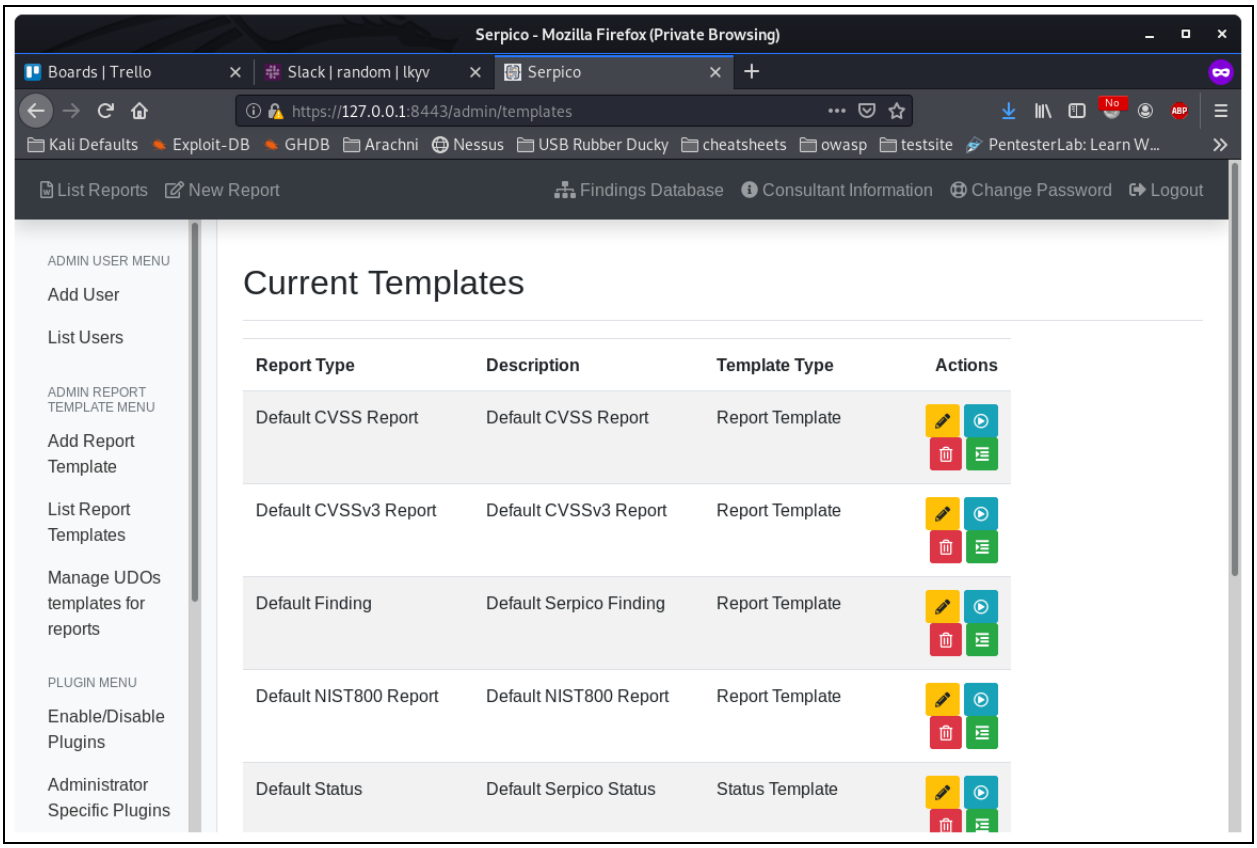
Εικόνα 33. Σελίδα προσθήκης νέου template

Η φόρμα αυτή περιέχει τα εξής πεδία:

- Report Type
  Ουσιαστικά, είναι το όνομα του template.
- File Description
  Η περιγραφή του αρχείου.
- Finding Template
  Επιλέξτε το checkbox εάν είναι template για findings.
- Status Template
  Επιλέξτε το checkbox εάν είναι template για αναφορά status.
- DOCX
  Επιλέξτε **Browse** και στην συνέχεια στο popup παράθυρο που θα σας εμφανιστεί, βρείτε το το template που θέλετε να ανεβάσετε και πατήστε **Add**.

List Report Template

Για να δείτε τα διαθέσιμα templates που υπάρχουν στο σύστημα, επιλέξτε στην αριστερή πλευρά **List Report Templates** κάτω από το **Admin Report Template Menu**.



Εικόνα 34. Λίστα με τα διαθέσιμα templates

Για κάθε template μπορείτε να κάνετε τα παρακάτω actions:

1. Edit: Επεξεργασία του template (Όνομα, Περιγραφή, κτλ.).
2. Preview: Πατώντας αυτό το κουμπί θα σας εμφανιστεί ένα popup παράθυρο για να κατεβάσετε ένα .docx αρχείο ώστε να δείτε το finding τοπικά στον υπολογιστή σας.
3. Delete: Διαγραφή του finding.

Serpico Meta Language

Για να εμπλουτίσουμε τα reports με την πληροφορία που θέλουμε από το Serpico, χρησιμοποιούμε το Meta Language του Serpico. Η γλώσσα αυτή μας βοηθάει να προσθέσουμε μεταβλητές, να δημιουργήσουμε βρόγχους, να κάνουμε ελέγχους και συγκρίσεις και σε σπάνιες περιπτώσεις να γράψουμε κώδικα σε XSLT.

Meta Characters

Ακολουθεί η λίστα με τα Meta Characters:

- Ω - Χρησιμοποιείται για την εισαγωγή των system variables του Serpico. Οι μεταβλητές αυτές είναι:
  - consultant_name
  - consultant_company
  - consultant_phone
  - consultant_email

- contact_name
- contact_phone
- contact_email
- contact_city
- contact_address
- contact_zip
- full_company_name
- short_company_name
- company_website
- assessment_end_date
- assessment_start_date

Οι τιμές των παραπάνω μεταβλητών, ορίζονται από τις τιμές που συμπληρώνουμε στην φόρμα του **Report Information** (Εικόνα 13. Σελίδα τροποποίησης πληροφοριών ενός report.).

Παράδειγμα:

```
ΩFULL_COMPANY_NAMEΩ
```

- § - Χρησιμοποιείται για την εισαγωγή custom μεταβλητών που δημιουργήθηκαν από τους χρήστες.
  Παράδειγμα:
  ```
  §custom_variable§
  ```
- ¬ - Χρησιμοποιείται για την δημιουργία ενός for each βρόγχου.
  Η συνθήκη μπαίνει ανάμεσα σε "¬". Στις επόμενες γραμμές γράψτε τις εντολές που θέλετε και τέλος κλείστε τον βρόγχο με το σύμβολο "Δ".
  Παράδειγμα:
  ```
  ¬finding¬
  ...code...
  Δ
  ```
- Δ - Χρησιμοποιείται για να δηλώσει τον τερματισμό του βρόγχου.
- Ɣ - Χρησιμοποιείται για την εισαγωγή των system variables του Serpico μέσα σε ένα βρόγχο. Ουσιαστικά αντικαθιστά το "Ω".
  Παράδειγμα:
  ```
  ¬report/findings_list/findings¬
  ƔtitleƔ
  Δ
  ```

For each inside tables

- æ - Χρησιμοποιείται για την δημιουργία ενός for each βρόγχου, το οποίο σε κάθε επανάληψη θα δημιουργεί μία γραμμή πίνακα.
  Παράδειγμα:
  ```
  æreport/findings_list/findingsæ
  ```
- ::: - Χρησιμοποιείται για την δήλωση if statements σε έναν βρόγχο.
  Παράδειγμα:
  ```
  ¬report/findings_list/findings:::cvss_total>=9¬
  ```
  Ή με πολλαπλές συνθήκες

```
¬report/findings_list/findings:::cvss_total>=7:::cvss_total<9¬
```

- ∞ - Χρησιμοποιείται για την εισαγωγή των system variables του Serpico μέσα σε έναν βρόγχο, το οποίο σε κάθε επανάληψη θα δημιουργεί μία γραμμή πίνακα. Ουσιαστικά αντικαθιστά το "Ω" και το "𝘟".
  Παράδειγμα:

```
æreport/findings_list/findings:::DREAD_TOTAL>35æ ∞title∞
```

If statement

- † - Χρησιμοποιείται για την δήλωση if conditions.
  Η συνθήκη μπαίνει ανάμεσα σε "†". Στις επόμενες γραμμές γράψτε τις εντολές που θέλετε και τέλος κλείστε το statement με το σύμβολο "¥".
  Παράδειγμα:

```
† DREAD_SCORE > 1 †
HELLO WORLD
¥
```

- ¥ - Χρησιμοποιείται για να δηλώσει τον τερματισμό του if statement.

choose/when structure

Για να κάνετε πολλαπλούς ελέγχους μπορείτε να χρησιμοποιήσετε το choose/when structure, το οποίο είναι παρόμοια με το switch statement στον προγραμματισμό.

Παράδειγμα:

```
¬overview/paragraph¬
µCONDITIONALµ 𝘟.𝘟
ƒcodeƒ 𝘟.𝘟
ƒitalicsƒ 𝘟.𝘟
÷ 𝘟.𝘟 ≠
```

Στο παραπάνω παράδειγμα εάν η γραμμή είναι μέσα σε code tag ([[[...code...]]]) τότε η γραμμή θα κληρονομήσει το styling του 𝘟.𝘟. Αντίστοιχα τα italics. Εάν δεν είναι τίποτα από τα παραπάνω, τότε θα κληρονομήσει το default styling που είναι στην τελευταία γραμμή (÷ 𝘟.𝘟 ≠).

- µ - Χρησιμοποιείται για την αρχικοποίηση μιας choose/when structure.
- *ƒ* - Χρησιμοποιείται για να οριστεί η τιμή του when attribute. Οι τιμές που μπορεί να πάρει είναι:
  - bullet: Πρώτο επίπεδο bullet
  - bullet1: Εμφωλευμένο (nested) bullet
  - h4: Επικεφαλίδα
  - indented: Ένα τα πιο μέσα στην στοίχιση
  - italics: Εμφάνιση γραμμάτων σε italics format.
- ÷ - Χρησιμοποιείται για να δηλώσει την προεπιλεγμένη (default) συνθήκη του choose/when structure.
- å - Χρησιμοποιείται για να δηλώσει τον τερματισμό του choose/when structure, όταν είναι έξω από βρόγχο.
- ≠ - Χρησιμοποιείται για να δηλώσει τον τερματισμό του choose/when structure, όταν είναι μέσα σε βρόγχο.

String Comparison

- √ - Χρησιμοποιείται για σύγκριση συμβολοσειρών.

Παραδείγματα:

Classic String Comparison

```
¬report/findings_list/findings:::risk>3¬
†
translate(assessment_type,$up,$low)=translate('External',$up,$low)
†
FINDINGS
¥
Δ
```

Στο παραπάνω παράδειγμα εάν το ‘assessment_type’ είναι ίσο με ‘'External'’ τότε θα εμφανίσει το ‘FINDINGS’.

Για να εκτελέσετε το παραπάνω μέσα σε ένα πίνακα, χρησιμοποιείστε το παρακάτω:

```
æreport/findings_list/findings:::risk<5:::translate(assessment_typ
e,$up,$low)=translate('external',$up,$low)æ ∞title∞
```

String Comparison on Global Variable

```
† √ short_company_name:::acme inc √ †
The company name is acme.
¥
```

Στο παραπάνω παράδειγμα συγκρίνουμε το ‘short_company_name’ με την τιμή ‘acme inc’. Εάν η συνθήκη είναι αληθής, τότε θα εμφανιστεί το μήνυμα ‘The company name is acme.’

String Comparison on UDV

Εάν θέλετε να συγκρίνετε ένα UDV τότε προσθέστε το σύμβολο ‘:’ μπροστά από το όνομα της μεταβλητής.
Παράδειγμα:

```
† √ :my_udv_name:::udv value √ †
This test’s for a udv
¥
```

Στο παραπάνω παράδειγμα γίνεται σύγκριση της μεταβλητής ‘my_udv_name’ με το string ‘udv value’. Εάν η συνθήκη είναι αληθής, τότε θα εκτυπωθεί στο report το μήνυμα “This test’s for a udv”.

String Comparison for Finding Variable

Για να συγκρίνετε μία μεταβλητή ενός finding τότε πρέπει να προσθέσετε το σύμβολο ‘+’ μπροστά από το όνομα της μεταβλητής.

Παράδειγμα:

```
† √ +title:::cross site scripting √ †
The title is cross site scripting.
¥
```

Στο παραπάνω παράδειγμα γίνεται σύγκριση της μεταβλητής ‘title’ με το string ‘cross site scripting’. Εάν η συνθήκη είναι αληθής τότε θα εκτυπωθεί στο report το μήνυμα “The title is cross site scripting”.

Inserting Screenshots

- Ʊ - Χρησιμοποιείται για την εισαγωγή εικόνων στο report template.

Παράδειγμα:

```
Ʉlogo.pngɄ
```

XSLT code block symbol

Σε σπάνιες περιπτώσεις στις οποίες τα παραπάνω tags δεν σας επιτρέπουν να κάνετε αυτό που επιθυμείτε, τότε μπορείτε να εισάγετε το δικό σας κώδικα χρησιμοποιώντας το σύμβολο “ϕ”.

Η γλώσσα η οποία υποστηρίζει το Serpico είναι η XSLT.

Παράδειγμα:

```
ϕ
<xsl:variable name="totalCrit"
select="report/udv/critical_tally"/>
<xsl:variable name="totalHigh" select="report/udv/high_tally"/>
<xsl:value-of select="$totalCrit + $totalHigh"/>
ϕ
```

Στο παραπάνω παράδειγμα δημιουργούμε τις μεταβλητές ”totalCrit” και “highCrit” οι οποίες παίρνουν τις τιμές των UDV critical_tally και high_tally αντίστοιχα, και στην συνέχεια υπολογίζετε το άθροισμά τους.

Variables in Headers/Footers of a document

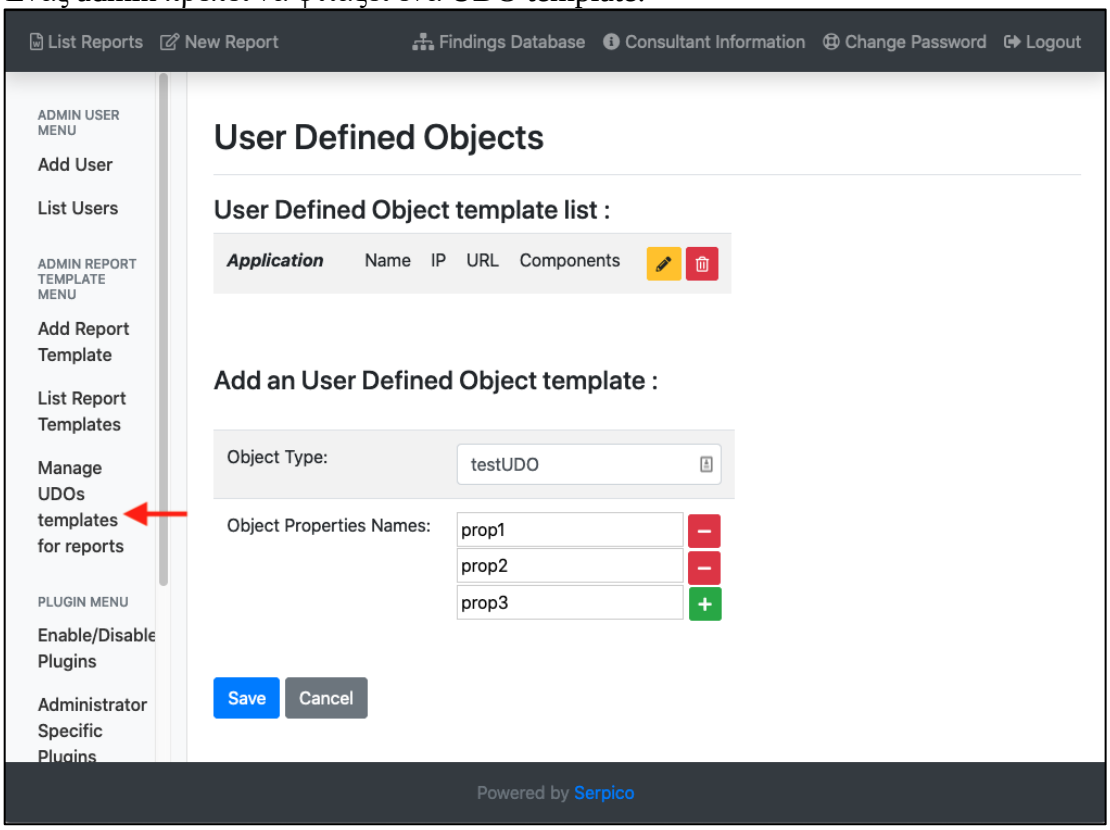
Τα παρακάτω Meta Characters επιτρέπονται στο Header και στο Footer του report:

- Ω - Χρησιμοποιείται για την εισαγωγή των system variables του Serpico
- § - Χρησιμοποιείται για την εισαγωγή custom μεταβλητών που δημιουργήθηκαν από τους χρήστες.

Manage UDOs templates for reports

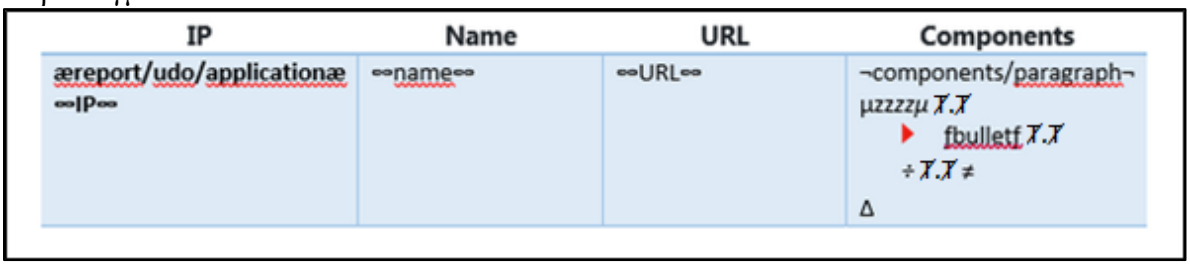
Τα User Defined Objects βασίζονται στη λογική των User Defined Variables. Τα UDOs είναι object, τα οποία περιέχουν παραπάνω από property, και χρησιμοποιούνται κατά κύριο λόγο για την δημιουργία πινάκων.
Η διαδικασία για την δημιουργία ενός UDO είναι:

1. Ένας admin πρέπει να φτιάξει ένα UDO template:



Εικόνα 35. Σελίδα αρχικοποίησης UDO

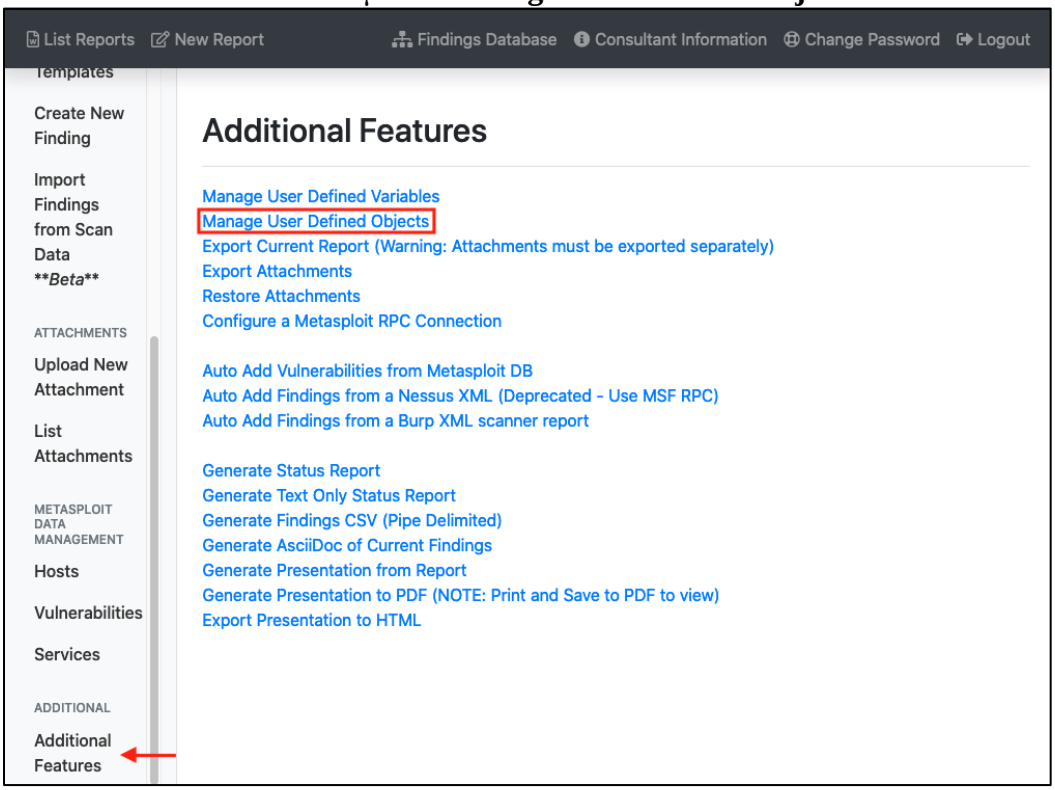
2. Στην συνέχεια ο admin επεξεργάζεται το report template και φτιάχνει ένα βρόγχο μέσα σε έναν πίνακα 1x n και καλεί τα properties.
Παράδειγμα:



Εικόνα 36. Προσθήκη UDO στο template

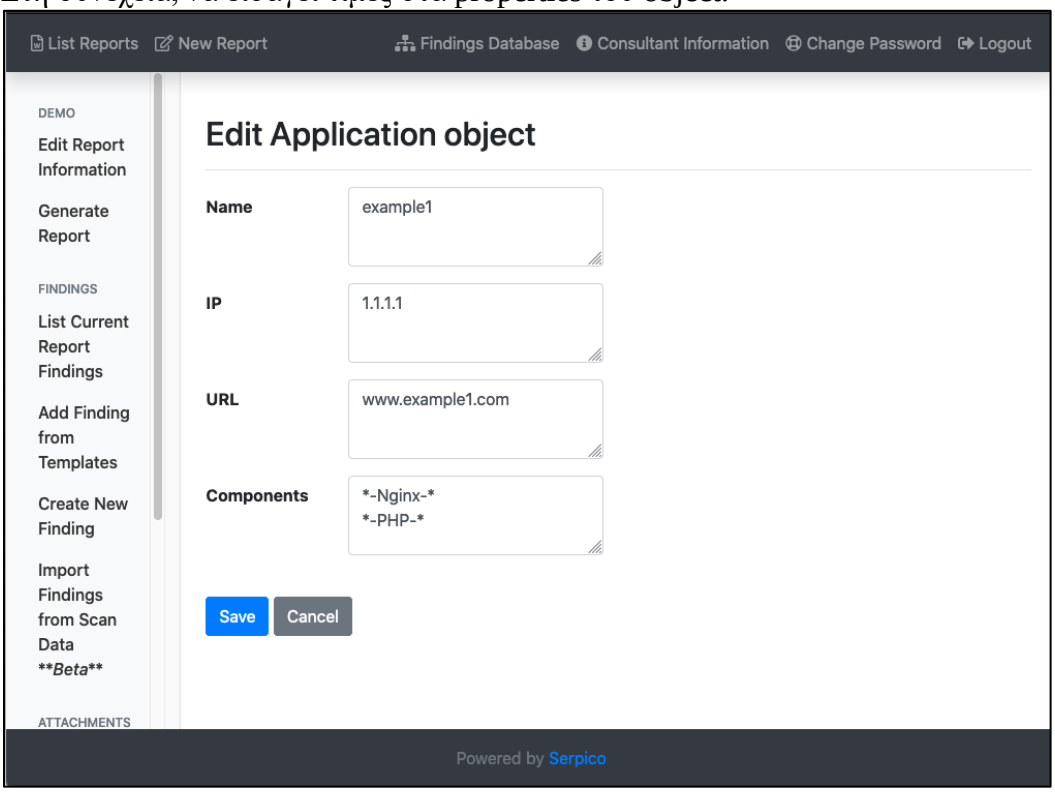
3. Ένας user/admin μπορεί να δημιουργήσει objects από το UDO template:

i. Πηγαίνοντας στο report που θέλει να εισάγει τα objects και να επιλέξει «**Additional Features**» και μετά «**Manage User Defined Objects**».

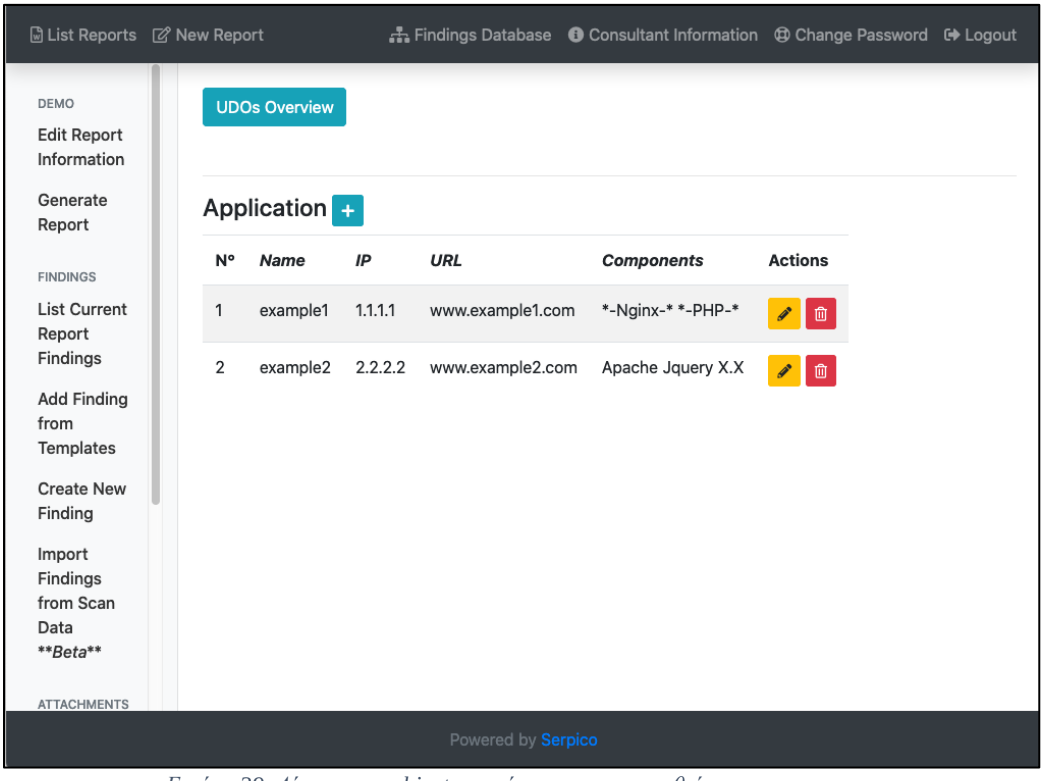


Εικόνα 37. Επιλογές μενού Additional Features

ii. Στη συνέχεια, να εισάγει τιμές στα properties του object.



Εικόνα 38. Αρχικοποίηση των properties ενός object



Εικόνα 39. Λίστα με τα objects που έχουν αρχικοποιηθεί

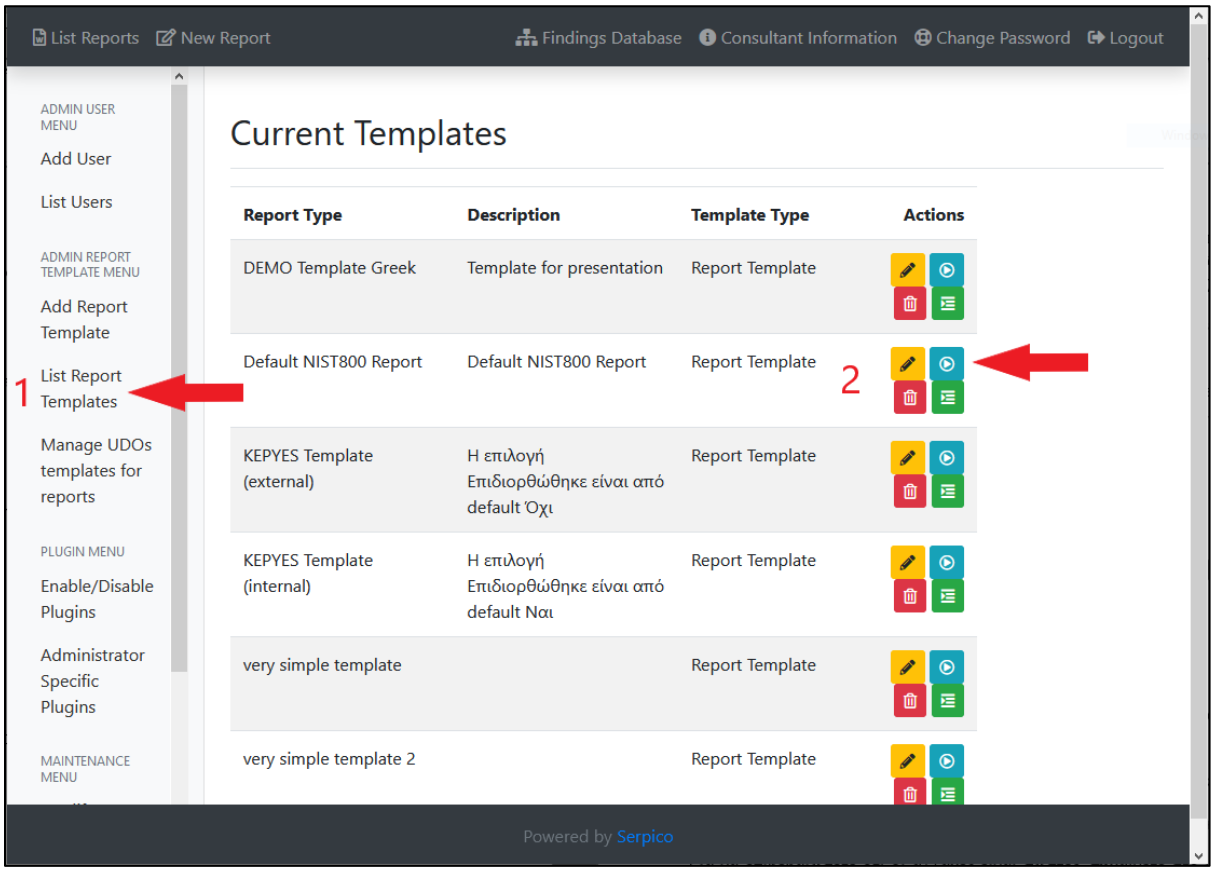
4. Τέλος, όταν δημιουργηθεί το τελικό report ο πίνακας θα φαίνεται όπως στην παρακάτω εικόνα:

IP	Name	URL	Components
1.1.1.1	exemple1	www.exemple1.com	Nginx PHP
2.2.2.2	ëxemple2	www.exemple2.com	Apache Jquery X.X

Εικόνα 40. Οι τιμές των objects στο παραγόμενο report

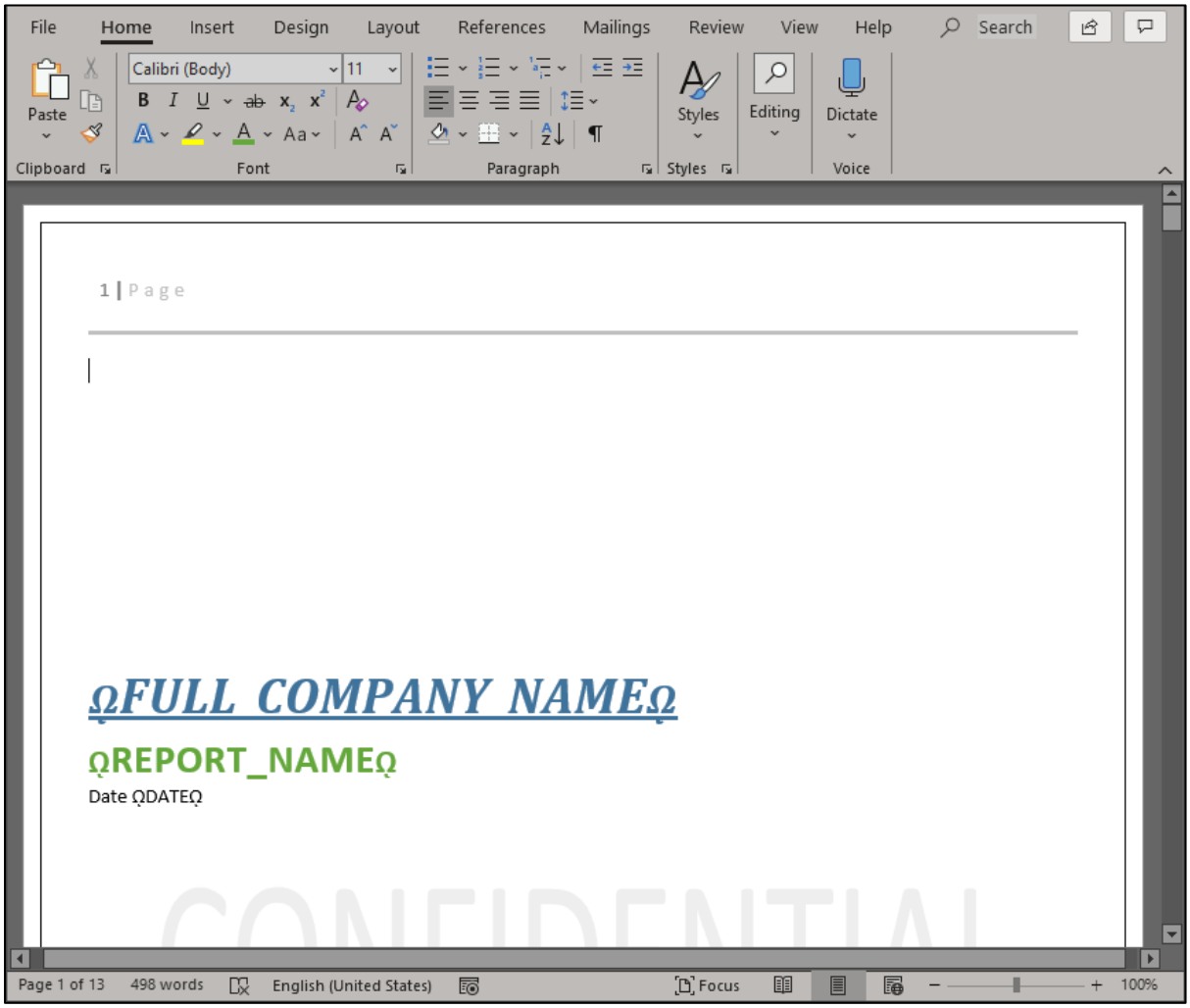
Επεξεργασία report template

Για να κάνετε αλλαγές σε κάποιο report template, επιλέξτε **List Report Templates** κάτω από το **Admin Report Template Menu**. Στην συνέχεια πατήστε το κουμπί **Preview** στο template που σας ενδιαφέρει και θα εμφανιστεί ένα pop παράθυρο για να κατεβάσετε το .docx αρχείο.



Εικόνα 41. Επισκόπηση του template

Ανοίξτε το .docx αρχείο που κατεβάσατε και κάντε τις αλλαγές που επιθυμείτε.

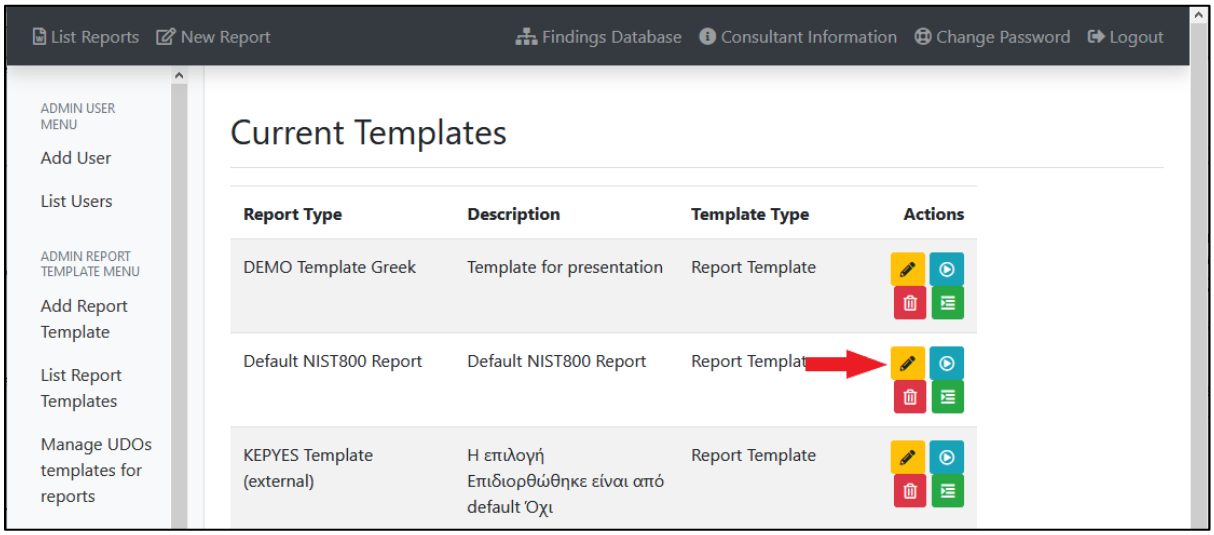


Εικόνα 42. Επεξεργασία του .docx αρχείου

Σε αυτό το παράδειγμα, γίνεται αλλαγή του χρώματος του τίτλου (μεταβλητή REPORT_NAME) σε πράσινο.

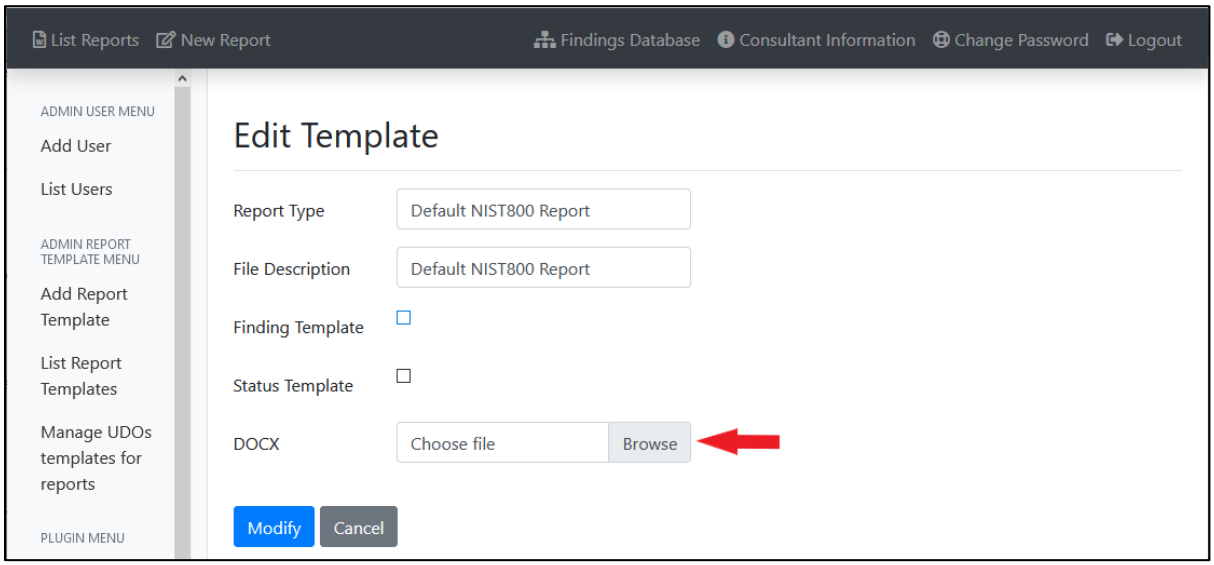
Γενικά, οι μεταβλητές κληρονομούν το styling της σειράς στην οποία τοποθετούνται.

Όταν τελειώσετε με τις αλλαγές σας, πηγαίνετε πίσω στο browser και πατήστε το κουμπί **Edit**



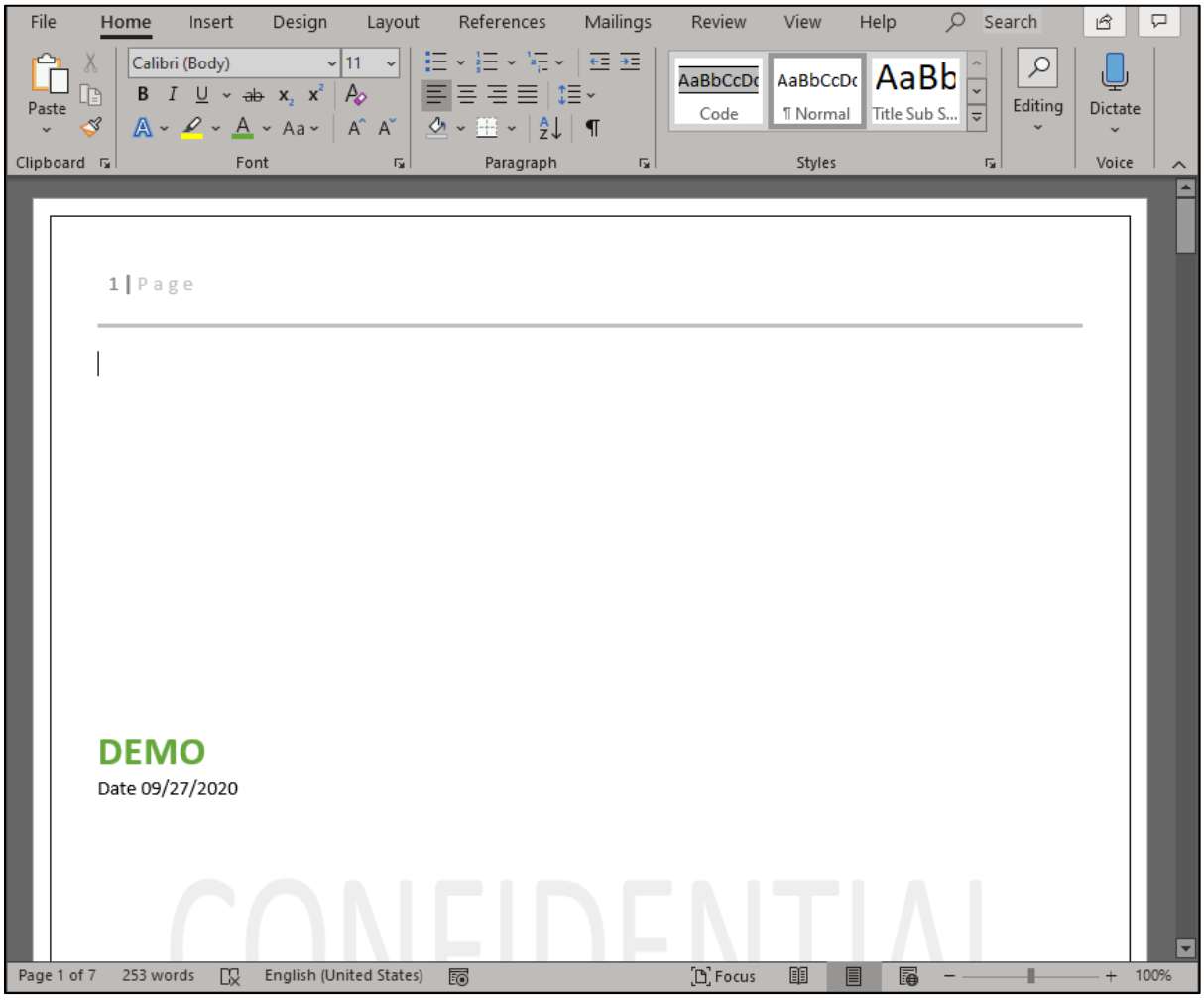
Εικόνα 43. Επεξεργασία του template

Ανεβάστε το καινούριο template σας και στην συνέχεια πατήστε το κουμπί **Modify**.



Εικόνα 44. Upload του .docx αρχείου

Για να επιβεβαιώσετε ότι οι αλλαγές είναι σωστές, πηγαίνετε στο report σας και πατήστε **Generate Report**.



Εικόνα 45. Δημιουργία report

Μπορείτε να δείτε περισσότερες χρήσεις των meta characters στην ενότητα «Serpico Meta Language».

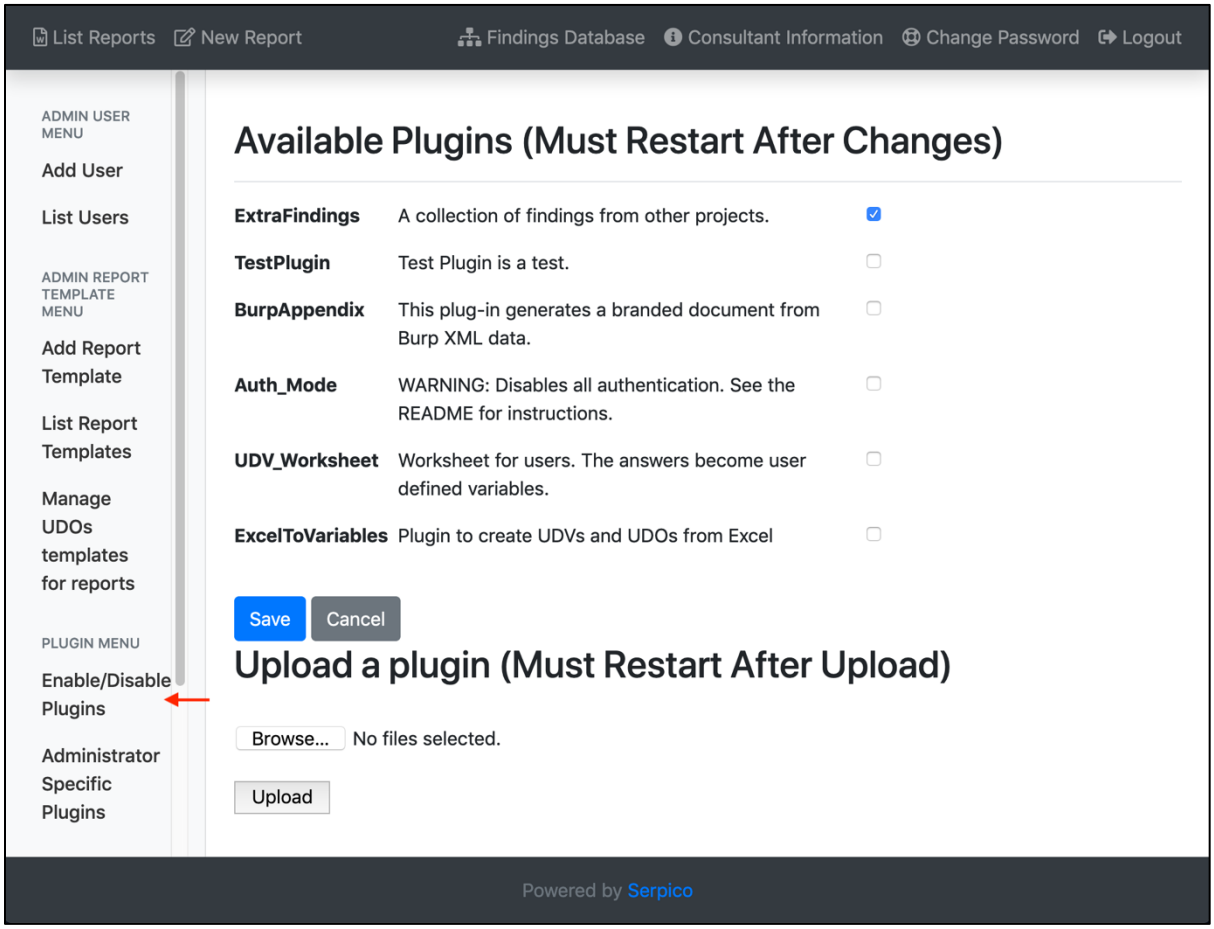
Plugin Menu

Σε αυτήν την κατηγορία ο διαχειριστής έχει τις εξής δυνατότητες:

- Enable/Disable Plugins
  Ο διαχειριστής μπορεί να ενεργοποιήσει και να απενεργοποιήσει τα εγκατεστημένα plugins του Serpico.
- Administrator Specific Plugins
  Η σελίδα αυτή περιέχει όλα τα ενεργοποιημένα plugins που προορίζονται για χρήση μόνο από τους διαχειριστές.

Enable/Disable Plugins

Για να ενεργοποιήσετε και να απενεργοποιήσετε τα εγκατεστημένα plugins, επιλέξτε **Enable/Disable Plugins** κάτω από το **Plugin Menu** και θα δείτε την παρακάτω σελίδα:



Εικόνα 46. Λίστα με τα διαθέσιμα plugins

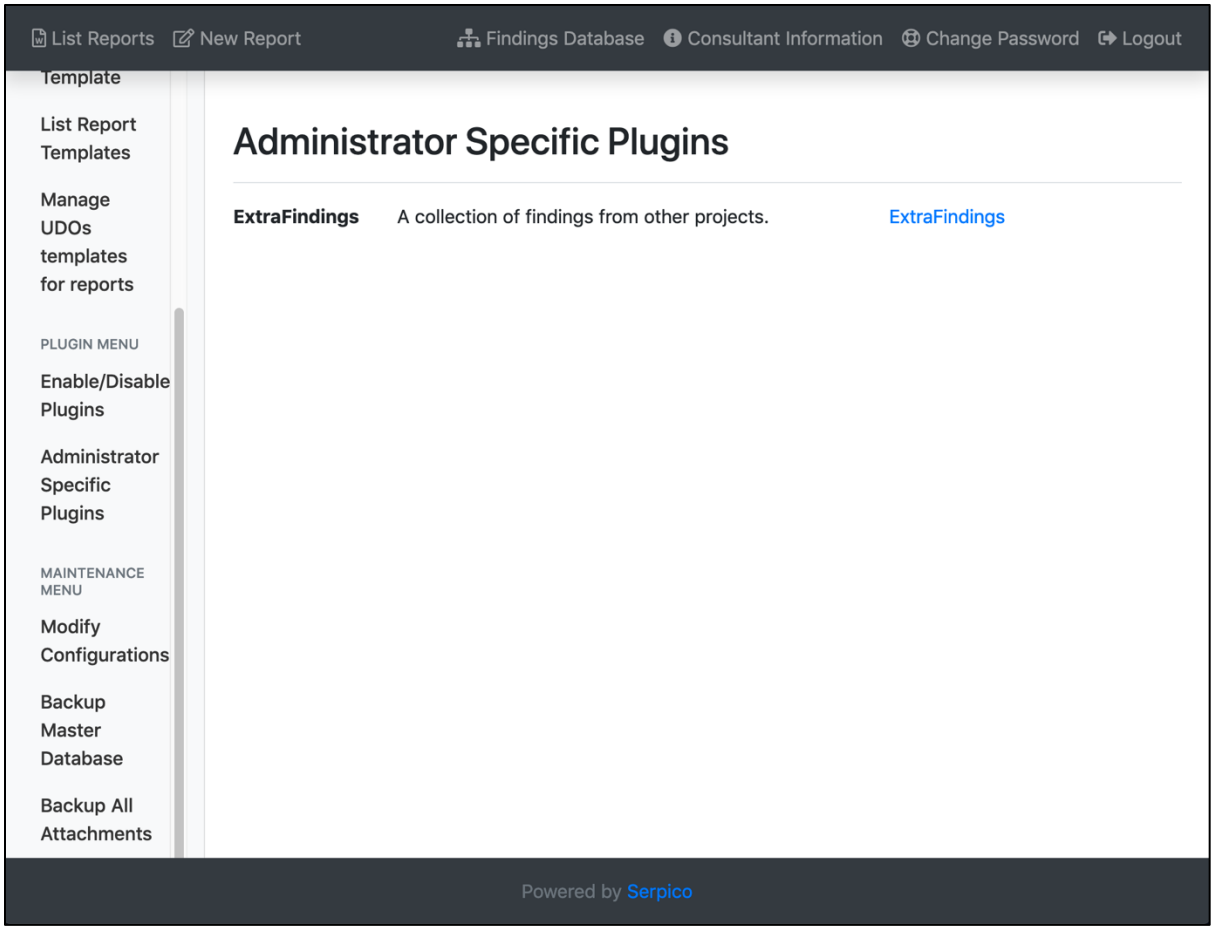
Επιλέξτε τα plugins που θέλετε να είναι ενεργοποιημένα και πατήστε **Save**. Μετά θα χρειαστεί να κάνετε restart το server για να φορτωθούν τα plugins.

Για να κάνετε restart το server, τρέξτε τις παρακάτω εντολές:

```
$ screen -r serpico
ctrl+c
$ ruby ~/Serpico/serpico.rb
ctrl+a d
```

Administrator Specific Plugins

Για να ανοίξετε τα plugin για τους admins που έχετε ενεργοποιήσει, επιλέξτε **Administrator Specific Plugins** κάτω από το **Plugin Menu** και θα δείτε την παρακάτω σελίδα:



Εικόνα 47. Σελίδα διαχείρισης plugin

Επιλέγοντας κάποιο plugin, θα μεταφερθείτε στη σελίδα διαχείρισης του plugin, και από εκεί μπορείτε να τρέξετε τις ενέργειες που μπορεί να κάνει το plugin.

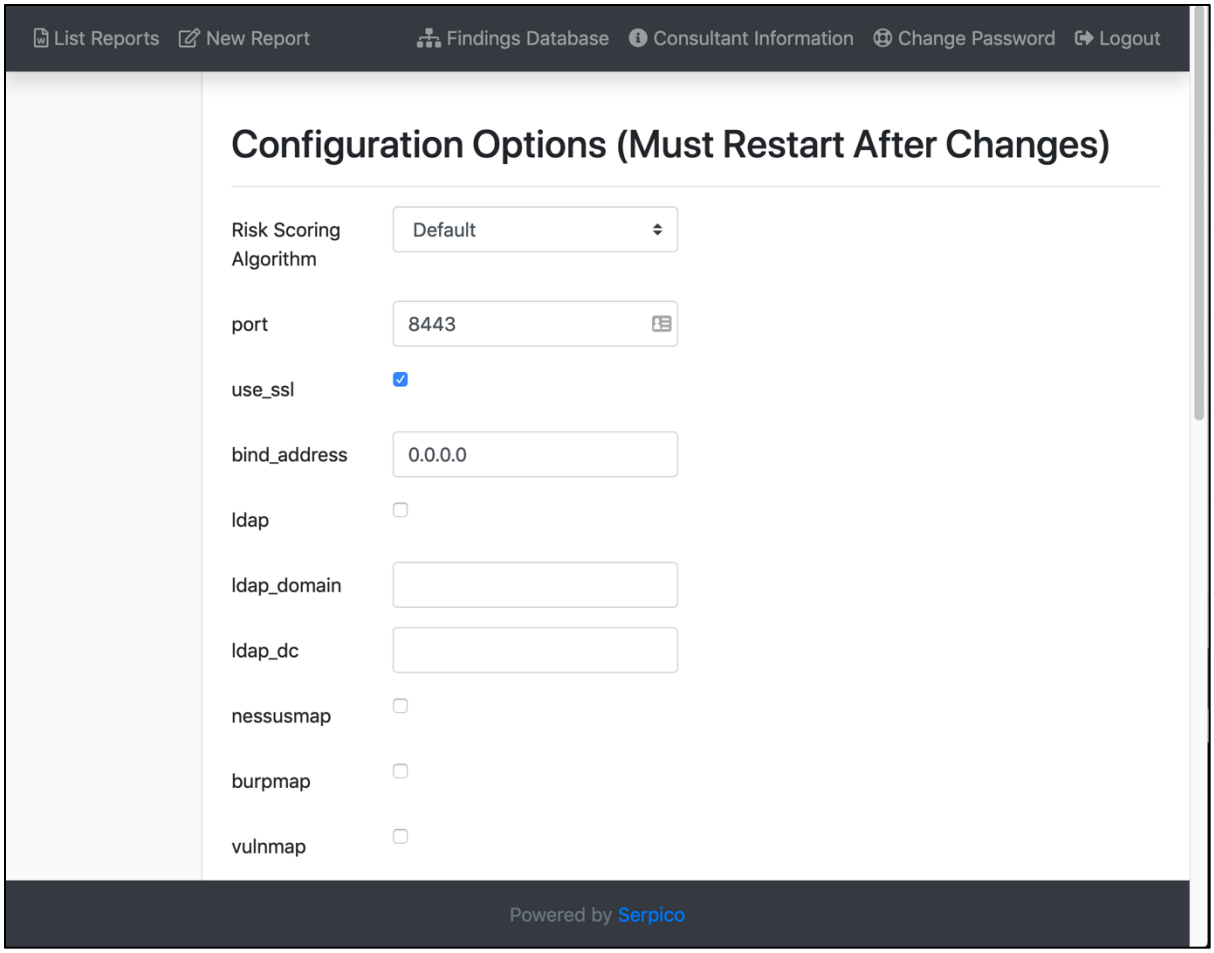
Maintenance Menu

Σε αυτήν την κατηγορία ο διαχειριστής έχει τις εξής δυνατότητες:

- Modify Configuration
  Ο διαχειριστής μπορεί να τροποποιήσει τις παραμέτρους του server μέσω του UI. Απαιτείται επανεκκίνηση του server για να εφαρμοστούν οι αλλαγές.
- Backup Master Database
  Ο διαχειριστής μπορεί να κατεβάσει ένα dump της βάσης σε μορφή .bak.
- Backup All Attachments
  Ο διαχειριστής μπορεί να κατεβάσει ένα .zip αρχείο με όλα τα attachments που έχουν ανεβάσει όλοι οι χρήστες.

Modify Configuration

Για να τροποποιήσετε τις παραμέτρους του Serpico, επιλέξτε **Modify Configuration** κάτω από το **Maintenance Menu** και θα δείτε την παρακάτω σελίδα:



Εικόνα 48. Επεξεργασία των ρυθμίσεων του Serpico

Οι παράμετροι που είναι διαθέσιμοι για παραμετροποίηση είναι:

- Risk Scoring Algorithm: Ο αλγόριθμος που χρησιμοποιείτε για την αξιολόγηση του κινδύνου των ευπαθειών.
- port: Η θύρα στην οποία τρέχει το Serpico.
- use_ssl: Αν θα χρησιμοποιηθεί το HTTPS.
- bind_address: Η δυεύθυνση στην οποία τρέχει το Serpico.
- ldap: Αν θα χρησιμοποιηθεί LDAP server για την αυθεντικοποίηση.
- ldap_domain: Η διεύθυνση του LDAP server.
- ldap_dc: Το Domain Component του LDAP server.
- nessusmap: Αν τα ευρήματα του Nessus θα αντιστοιχίζονται στα ευρήματα του Serpico.
- burpmap: Αν τα ευρήματα του Burp Suite θα αντιστοιχίζονται στα ευρήματα του Serpico.
- vulnmap: Αν τα ευρήματα του VulnDB θα αντιστοιχίζονται στα ευρήματα του Serpico.
- finding_types: Οι κατηγορίες των findings.
- finding_states: Τα status των findings.
- logo: Path ή URL για το logo στην login σελίδα.
- footer_message: Μήνυμα στο footer.
- footer_href_url: Το URL του link στο footer.
- footer_href_message: Το μήνυμα του link στο footer.
- auto_import: Αυτόματο import των ευρημάτων όταν εισάγονται από άλλα εργαλεία.

- chart: Ενεργοποίηση του support.
- user_defined_variables: Ονόματα μεταβλητών UDV.
- report_assessment_types: Κατηγορίες report.
- findings_assessment_types: Κατηγορίες ευρημάτων.
- threshold: Η ελάχιστη τιμή του severity που μπορεί να έχει ένα finding.
- show_exceptions: Εμφάνιση των debug μηνυμάτων.
- cvssv2_scoring_override: Παράκαμψη του CVSSv2 scoring algorithm.
- ssl_ciphers: Αλγόριθμοι SSL που υποστηρίζονται.
- languages: Γλώσσες που υποστηρίζονται.

Backup Master Database

Για να κατεβάσετε ένα dump της βάσης, επιλέξτε **Backup Master Database** κάτω από το **Maintenance Menu** και θα εμφανιστεί ένα pop παράθυρο για να κατεβάσετε το dump.

Backup All Attachments

Για να κατεβάσετε ένα backup των attachments που έχουν ανέβει στο server, επιλέξτε **Backup All Attachments** κάτω από το **Maintenance Menu** και θα εμφανιστεί ένα pop παράθυρο για να κατεβάσετε το .zip αρχείο.

User Defined Variables (UDV)

Τα User Defined Variables δίνουν την δυνατότητα στους χρήστες να ορίζουν global μεταβλητές σε ένα report.(βλ. User Defined Variables (UDV))

Reserved UDVs

Κατά την παραγωγή του report, το Serpico δημιουργεί αυτόματα 6 μεταβλητές, οι οποίες δηλώνουν το συνολικό αριθμό των findings που έχουν δηλωθεί στο report, βάσει της σοβαρότητας της ευπάθειας. Οι μεταβλητές αυτές είναι:

- total_tally: Συνολικός αριθμός των ευπαθειών
- critical_tally: Συνολικός αριθμός των κρίσιμων ευπαθειών
- high_tally: Συνολικός αριθμός των υψηλών ευπαθειών
- moderate_tally: Συνολικός αριθμός των μέτριων ευπαθειών
- low_tally: Συνολικός αριθμός των χαμηλών ευπαθειών
- informational_tally: Συνολικός αριθμός των ενημερωτικών ευπαθειών

Αυτές οι μεταβλητές είναι χρήσιμες, επειδή μπορούν να χρησιμοποιηθούν σε διάφορες ενότητες (π.χ. σύνοψη) χωρίς να χρειάζεται να υπολογίζονται κάθε φορά.

Προσθήκη global UDV στο config.json

Υπάρχει η δυνατότητα να προσθέσετε UDVs στο config.json ώστε να μην χρειάζεται να δηλώνετε την μεταβλητή ξεχωριστά για κάθε ένα report.

Για να δηλώσετε στο config.json προσθέστε το όνομα της μεταβλητής στο πεδίο user_defined_variables.

π.χ. "user_defined_variables":["testUDV"]

Στην συνέχεια για να δηλώσετε την τιμή της μεταβλητής, ακολουθείτε τα βήματα της ενότητας «User Defined Variables (UDV)»

Βιβλιογραφία

Allen, L., Heriyanto, T., & Ali, S. (2014). *Kali Linux - Assuring Security by Penetration Testing.* Packt.

DART. (2017). Ανάκτηση από GitHub: https://github.com/lmco/dart

Dradis. (2017). Ανάκτηση από GitHub: https://github.com/dradis/dradis-ce

MagicTree. (2020). Ανάκτηση από gremwell: https://www.gremwell.com/what_is_magictree

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux.* Packt.

Penetration test. (2020, August 18). Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Penetration_test

PlexTrac. (2020). Ανάκτηση από PlexTrac: https://plextrac.com/

Rouse, M. (2020, July). *vulnerability assessment (vulnerability analysis)*. Ανάκτηση από Search Security: https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis

Serpico. (2020). Ανάκτηση από Github: https://github.com/SerpicoProject/Serpico

Serpico Fork. (2020). Ανάκτηση από GitHub: https://github.com/nikosev/Serpico

Serpico Plugins Fork. (2020). Ανάκτηση από GitHub: https://github.com/nikosev/SerpicoPlugins

Παράρτημα

Linux Screen

Εγκατάσταση

Για την εγκατάσταση του screen χρησιμοποιείστε την εντολή:

Debian, Ubuntu	`$ sudo apt-get install screen`
CentOS, Fedora, Red Hat	`$ sudo yum install screen`

Χρήσιμες εντολές για το screen

Για να ξεκινήσετε ένα Screen session:

```
$ screen -S <NAME>
```

Όπου <NAME> είναι το όνομα του session.

Για να κάνετε reattach το session:

```
$ screen -r <NAME>
```

Για να δείτε την λίστα με όλα τα session:

```
$ screen -ls
```

Για να κάνετε detach το session:

```
$ screen -d <SCREENID>
```

Όπου <SCREENID> είναι το ID (5ψήφιος αριθμός) του session.

Για να διαγράψετε κάποιο session:

```
$ screen -X -S <SCREENID> quit
```

Χρήσιμα shortcut για το screen:

1. Για να κάνετε detach το session χρησιμοποιήστε το shortcut
   ```
   Ctrl+a d
   ```
2. Για να κάνετε kill το session χρησιμοποιήστε το shortcut
   ```
   Ctrl+a k
   ```