





**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**  
**Τμήμα Πληροφορικής**



**Εργασία Μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση <<αριθμός άσκησης>>	<b>&lt;&lt;Τελική Εργασία Ασφάλεια Πληροφοριακών Συστημάτων &gt;&gt;</b>
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κωνσταντίνος Κουσουννής ρ14086
Ημερομηνία παράδοσης	30-01-2019



## Εκφόνηση της άσκησης

Να χρησιμοποιήσετε όποια γλώσσα προγραμματισμού επιθυμείτε (ενδεικτικά php, java, .net, python) και να αναπτύξετε μία διαδικτυακή εφαρμογή (με ότι υπηρεσίες θέλετε). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε/τροποποιήσετε κάποια εφαρμογή που έχετε αναπτύξει στο πλαίσιο άλλου μαθήματος. Όλες οι απαιτούμενες τεχνολογίες (web, application, database server) θα είναι επίσης ελεύθερης επιλογής. Η εφαρμογή θα χρησιμοποιηθεί ως περιβάλλον για να υλοποιήσετε τις παρακάτω υπηρεσίες ασφάλειας.

1. Μελέτη ασφάλειας ΠΣ. Σε αυτό το στάδιο θα πραγματοποιήσετε μία σύντομη μελέτη ασφάλειας ΠΣ, η οποία θα περιλαμβάνει: (α) Ανάλυση επικινδυνότητας και (β) Σχέδιο Πολιτικής Ασφάλειας. (Σημείωση: αυτό το βήμα αποτελεί επέκταση της 1ης άσκησης)
2. Να υλοποιήσετε κρυπτογράφηση ssl στον server. Η υπηρεσία σας να λειτουργεί μόνο σε https με τη χρήση πιστοποιητικού στον web server. (Σημείωση: αυτό το βήμα βασίζεται στην 3η άσκηση)
3. Να υλοποιείστε ένα μηχανισμό αυθεντικοποίησης (user authentication), πχ. username,password, one-time password, certificate based κτλ. και ελέγχου πρόσβασης (authorization), π.χ. LDAP-based, identity management, certificate based, group-based, role-based κτλ. (Σημείωση: αυτό το βήμα θα αποτελεί επέκταση της 4ης άσκησης)
4. Για τη λήψη δεδομένων εισόδου από τους χρήστες της εφαρμογής, να χρησιμοποιείσετε συναρτήσεις οι οποίες επιβάλουν input filtering και validation, ανάλογα με το προγραμματιστικό περιβάλλον που επιλέξατε.
5. Να πραγματοποιείσετε αυτοματοποιημένο έλεγχο για την εύρεση επαθειών ασφάλειας (Σημείωση: αυτό το βήμα αποτελεί θα επέκταση της 7ης άσκησης)



**1.Μελέτη ασφάλειας ΠΣ.** Σε αυτό το στάδιο θα πραγματοποιήσετε μία σύντομη μελέτη ασφάλειας ΠΣ, η οποία θα περιλαμβάνει: (α) Ανάλυση επικινδυνότητας και (β) Σχέδιο Πολιτικής Ασφάλειας. (Σημείωση: αυτό το βήμα αποτελεί επέκταση της 1ης άσκησης)

1. Καταγραφή του υπό μελέτη συστήματος. Να πραγματοποιήσετε για το δικό σας ΠΣ μία αρχική καταγραφή των υπηρεσιών και της αρχιτεκτονικής του συστήματος. Να περιγράψετε τουλάχιστον 3 υπηρεσίες του ΠΣ. (1-2 σελίδες με βάση το παραπάνω ενδεικτικό παράδειγμα και ανάλογα με το δικό σας Πληροφοριακό Σύστημα)

#### Ηλεκτρονικό Κατάστημα με Κινητά Τηλέφωνα

**1)Εμφανιση Προιόντων:**Παρέχει την δυνατότητα στούς χρήστες (εγγεγραμένους ή οχι) να βλέπουν τα προϊόντα.

**2)Εγγραφή Χρηστών:**Οι χρήστες εγγράφονται για τις υπηρεσίες του ηλεκτρονικού καταστήματος μεσω web form παρέχοντας στοιχεία Όνομα,Επίθετο,Αριθμός τηλέφωνου,Διεύθυνση Κατοικίας.

**3)Ηλεκτρονική Παραγγελία:** Οι εγγεγραμμένοι χρήστες έχουν την δυνατότητα να πραγματοποιήσουν ηλεκτρονικές παραγγελίες .Ο διαχειριστής θα εγρίνει την παραγγελία του χρήστη με μια ηλεκτρονική σφραγίδα την οποια και θα δείχνει στον διανομέα.



**Αρχιτεκτονική Δικτύου δίδεται στο παρακάτω σχήμα.**

**Οι τεχνολογίες πάνω στις οποίες έχει υλοποιηθεί η παραπάνω υπηρεσία είναι ακόλουθες:**

- Λειτουργικό Συστήμα: Windows 10 Version 10.0.17134 Build 17134
- Εξυπηρετητής Ιστού: Apache 2.4.18 με υποστήριξη ssl και Visual C++
- Εξυπηρετητής εφαρμογής: php 5.6
- Εξυπηρετητής βάσης δεδομένων: postgresql-9.2-1002.jdbc4
- Πλαίσιο υλοποίησης (framework): PhpStorm-2018.2.3

2. **Δημιουργία μοντέλου αγαθών (asset model).**). Για κάθε υπολογιστικό σύστημα που αποτελεί μέρος του ΠΣ που έχετε περιγράψει στο προηγούμενο βήμα, να μοντελοποιήσετε αναλυτικά όλα τα αγαθά του υπολογιστικού συστήματος (H/W, S/W, Network, Data). Να καταγράψετε το μοντέλο αγαθών για 3 υπολογιστικά συστήματα. Για την μοντελοποίηση μπορείτε να χρησιμοποιήσετε τον παρακάτω πίνακα για την μοντελοποίηση των αγαθών κάθε Υπολογιστικού Συστήματος.

**Όνομα Υπολογιστικού Συστήματος:**



<b>HW</b>	Server (Μοντέλο,Χαρακτηριστικά)	Apache 2.4.18 με υποστήκαι Visual C++ postgresql-9.2-1002.jdbc4
<b>HW</b>	Τοποθεσία(κτίριο,Δωμάτιο)	Γαλατσι,Χριστιανουπόλεω
<b>SW</b>	Λειτουργικό Σύστημα(Πυρήνας,Έκδοση)	Windows-Version 10.0.17134
<b>SW</b>	Λογισμικό Εφαρμογών	PhpStorm-2018.2.3
<b>Network</b>	Περιοχή Δυκτίου	
<b>Network</b>	Σημείο Σύνδεσης	
<b>Data</b>	Δεδομένα Διαμόρφωσης	Χρήστες,Διαχειριστές
Data	Δεδομένα λειτουργίας Συσκευής	Κινήτα τηλέφωνα

3. Αντιστοίχηση υπηρεσιών και υπολογιστικών συστημάτων. Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αντιστοιχίσετε τα υπολογιστικά συστήματα που χρησιμοποιούνται για την παροχή της υπηρεσίας (από αυτά που περιγράψατε στο βήμα 2). Είναι πιθανό ένα υπολογιστικό σύστημα να χρησιμοποιείται για την παροχή περισσότερων από μία υπηρεσιών.



## Εμφανιση Προιόντων ->SWΛογισμικό Εφαρμογών

**Εγγραφή Χρηστών-> HW Server**

**Ηλεκτρονική Παραγγελία->Network Σημείο Σύνδεσης**

**(4) Αποτίμηση συνέπειών ή επιπτώσεων ασφάλειας (impact assessment).** Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αποτιμήσετε τις πιθανές συνέπειες ασφάλειας (security impact) από την πιθανή παραβίαση της ασφάλειας των αγαθών που συμμετέχουν στην κάθε υπηρεσία, ως εξής:

- Συνέπειες μη διαθεσιμότητας της υπηρεσίας (unavailability / loss of Availability).
- Συνέπειες αποκάλυψης των δεδομένων που διαχειρίζεται η υπηρεσία (disclosure / loss of Confidentiality).
- Συνέπειες τροποποίησης των δεδομένων που διαχειρίζεται η υπηρεσία (modification / loss of Integrity).

Ο Τύπος Συνέπειας θα έχει μία ή περισσότερες από τις παρακάτω επιλογές:

- Άμεσες οικονομικές απώλειες
- Παρεμπόδιση λειτουργιών
- Δυσφήμιση
- Νομικές Κυρώσεις

Ο Βαθμός Συνέπειας θα έχει μία από τις παρακάτω τιμές:

1. Χαμηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος μέχρι €100/περιστατικό.
2. Μέτρια: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος από €101 μέχρι €1.000/περιστατικό.
3. Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €1.001 μέχρι €10.000/περιστατικό.



4. Πολύ Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €10.000/περιστατικό.

Η αποτίμηση συνεπειών θα γίνει, για κάθε υπηρεσία με τη βοήθεια του παρακάτω πίνακα:

‘Όνομα Υπηρεσίας	Τύπος Συνέπειας	Βαθμός Συνέπειας	Συντομη Αιτιολόγηση
<b>Συνεπειες για:</b>			
<b>(1)Μη Διαθεσιμοτητα</b>	Δυσφήμιση	Μετρια	Η ζημια θα προκυψει για μερικές ώρες
<b>(2)Αποκάλυψη Δεδομένων</b>	Καμία	Κανένας	Τα στοιχεία είναι δημόσια
<b>(3)Τροποποίηση Δεδομένων</b>	Αμεσες Οικονομικές Απώλειες	Υψηλή	Αλαγή στο ποσό αγοράς προιόντος

‘Όνομα Υπηρεσίας	Εγγραφή Χρηστών
------------------	-----------------

	Τύπος Συνέπειας	Βαθμός Συνέπειας	Συντομη Αιτιολόγηση
<b>Συνεπειες για:</b>			
<b>(1)Μη Διαθεσιμοτητα</b>	Αμεσες Οικονομικές Απώλειες	Υψηλή	Οι χρηστες δεν θα είναι σε θέση να αγοράζουν προϊόντα
<b>(2)Αποκάλυψη Δεδομένων</b>	Νομικές Κυρώσεις	Πολύ Υψηλή	Πρόστιμο απο όλους τους χρήστες
<b>(3)Τροποποίηση Δεδομένων</b>	Παρεμπόδιση Λειτουργιών	Υψηλή	Δεν πραγματοποιούνται παραγγελιές προιόντων



Όνομα Υπηρεσίας	Ηλεκτρονική Παραγγελία
-----------------	------------------------

	Τύπος Συνέπειας	Βαθμός Συνέπειας	Συντομη Αιτιολόγηση
<b>Συνεπειες για:</b>			
<b>(1)Μη Διαθεσιμοτητα</b>	Δυσφήμιση	Υψηλή	Δεν πραγματοποιείται Πώληση προϊόντων
<b>(2)Αποκάλυψη Δεδομένων</b>	Νομικές Κυρώσεις	Πολύ Υψηλή	Προστιμο απο τους χρήστες που πραγματοποιησαν παραγγελίες
<b>(3)Τροποποίηση Δεδομένων</b>	Αμεσες Οικονομικές Απώλιες	Υψηλή	Δεν παραδίδονται τα προιόντα στους χρήστες

**(5)Αποτίμηση απειλών(threat assessment).** Να αξιολογήσετε τις παρακάτω απειλές για κάθε ένα από τα 3 υπολογιστικά συστήματα που καταγράψατε στο βήμα 2:

- Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (**Unauthorized Access**).
- Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (**Ransomware**).
- Παραποίηση ιστοσελίδας (**Web Defacement**).
- Μη εξουσιοδοτημένη εκτέλεση κώδικα (**Code Injection**).
- Άρνηση υπηρεσίες (**Denial of Service**).

Η αποτίμηση κάθε απειλής για κάθε ένα από τα 3 υπολογιστικά συστήματα που μελετάτε, θα γίνει με βάση την κλίμακα:

**0. Δεν εφαρμόζεται (not applicable):** Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.



- 1. Χαμηλή πιθανότητα (Low likelihood):** Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%. 3
- 2. Μέτρια πιθανότητα (Medium likelihood):** Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 30%.
- 3. Υψηλή πιθανότητα (High likelihood):** Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.
- 4. Πολύ υψηλή πιθανότητα (Very High likelihood):** Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

1)Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access).

Χαμηλή πιθανότητα (Low likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%. 3

2)Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware).

Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

3)Παραποίηση ιστοσελίδας (Web Defacement).

Υψηλή πιθανότητα (High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.

4)Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection).

0. Δεν εφαρμόζεται (not applicable): Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.

5) • Άρνηση υπηρεσίες (Denial of Service).

4. Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.



**(6)Αποτίμηση αδυναμιών (vul).nerabil).ity assessment).** Να γίνει αποτίμηση αδυναμιών για όλα τα αγαθά λογισμικού των τριών υπό μελέτη υπολογιστικών συστημάτων (Λειτουργικό Σύστημα, λογισμικό εφαρμογών). Να χρησιμοποιήσετε διαθέσιμες βάσεις αδυναμιών π.χ. τη βάση αδυναμιών ασφάλειας του NIST (<http://nvd.nist.gov/>). Στην έρευνά σας θα πρέπει να συγκεντρώσετε και να περιγράψετε τις βασικότερες αδυναμίες ασφάλειας που υπάρχουν για τις συγκεκριμένες εκδόσεις λογισμικού που περιλαμβάνονται στα υπό μελέτη υπολογιστικά συστήματα.

**Λειτουργικό Σύστημα:** Windows 10 Version 10.0.17134 Build 17134

<https://nvd.nist.gov/vuln/detail/CVE-2018-8406>



## Εξυπηρετητής Ιστου APACHE 2.4.18

Ο Apache HTTP 2.4.17 μεχρι και την εκδοση 2.4.18,όταν mod\_http2 είναι ενεργοποιημένο,δεν περιορίζει τον οριθμό των ταυτόχρονων steam worker για εναν HTTP/2 σύνδεση,όπου επιτρέπει σε άτομα που κάνουν απομακρυσμένες επιθέσεις να προκαλέσουν μια αρνηση υπηρεσιών (μετάδοση-processing outage)διαμεσου τροποποιημένων ελεγχου ροης των windows

<https://nvd.nist.gov/vuln/detail/cve-2016-1546>

Ο Apache HTTP 2.4.18 μεχρι και την εκδοση 2.4.20, όταν το mod\_http2 και mod\_ssl ειναι ενεργοποιημένα,δεν αναγνωρίζει κατάλληλα το SSLVerifyClient require καθοδηγητικό για HTTP/2 απαίτησης αξουσιοδότησεις,όπου επιτρέπει σε άτομα που κάνουν απομακρυσμένες επιθέσεις να προσπεράσουν προβλεπόμενους περιορισμούς πρόσβασης με το να υποκινούν την ικανότητα να στέλνουν πολλαπλά αιτήματα για μια συνδεση καταργόντας την επαναδιαπραγμάτευση

<https://nvd.nist.gov/vuln/detail/cve-2016-4979>

Εξηπηρετητης Εφαρμογής:php 5.6

Στην php πριν την εκδοση 5.6.31,7x πριν την έκδοση 7.0.21, and 7.1.x πριν 7.1.7,μια στοίβα βασισμένη σε εναν ρυθμιστή υπερχειλισης στο zend\_ini\_do\_op()  
συναρτηση στο zend/Zend\_ini\_parser.c θα μπορουσε να προκαλέσει μια αρνηση υπηρεσιών ή υπαρχει πιθανοτητα να επιτρπει να εκτελεστεί εκτελέσιμος κώδικας .Σημείωση αυτό συσχετίζεται μόνο με php εφαρμογές που επιτρέπουν μη εμπιστες εισαγωγές(αντι για τα συστήματα php.ini αρχεία)για το parse\_ini\_string ή parse\_ini\_file συνάρτηση,e.g, μια ιστοσελίδα για συντακτική επικυρωση php.ini καθοδηγητικα

<https://nvd.nist.gov/vuln/detail/CVE-2017-11628>



**Να υλοποιείσετε κρυπτογράφηση ssl στον server. Η υπηρεσία σας να λειτουργεί μόνο σε https με τη χρήση πιστοποιητικού στον web server. (Σημείωση: αυτό το βήμα βασίζεται στην 3η άσκηση)**

1) Δημιουργία ΑΠ: Δημιουργήστε μία δοκιμαστική ΑΠ. Η ΑΠ θα έχει αυτο-υπογεγραμμένο πιστοποιητικό (όπως στο εργαστηριακό παράδειγμα)

```
Windows Command Prompt
D:\openssl-1.0.2j-fips-x86_64\OpenSSL\bin>dir
Directory of D:\openssl-1.0.2j-fips-x86_64\OpenSSL\bin

11/16/2017  12:59 PM    <DIR>          .
11/16/2017  12:59 PM    <DIR>          ..
11/16/2017  12:59 AM           1,024 .rnd
11/16/2017  12:45 PM           5,688 CA.pl
11/16/2017  12:45 PM           5,175 CA.sh
11/16/2017  10:22 AM           3,949 CAcnf.txt
11/01/2006  10:52 AM    <DIR>          certs
11/01/2006  10:52 AM    <DIR>          crt
11/16/2017  12:45 PM           119 c_hash
11/16/2017  12:45 PM           152 c_info
11/16/2017  12:45 PM           112 c_issuer
11/16/2017  12:45 PM           110 c_name
11/16/2017  12:45 PM           5,092 c_rehash
11/16/2017  12:46 PM           6,668 fipstd
09/27/2016  12:24 PM           64,866 fips_standalone_sha1.exe
11/16/2017  10:22 AM           0 index.txt
11/01/2006  10:52 AM    <DIR>          newcerts
11/16/2017  12:46 PM           10,835 openssl.cnf
09/27/2016  05:54 PM           4,058,465 openssl.exe
11/16/2017  01:00 PM    <DIR>          private
11/16/2017  10:22 AM           4 serial
11/16/2017  12:46 PM           6,419 tsget
11/16/2017  10:22 AM           4,498 usercnf.txt
17 File(s)      4,173,168 bytes
6 Dir(s)   837,616,594,944 bytes free

D:\openssl-1.0.2j-fips-x86_64\OpenSSL\bin>
```



```
Command Prompt - openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
C:\OpenSSL-Win32\bin\lab>openssl req -new -x509 -keyout private/CAkey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
Generating a 2048 bit RSA private key
...+ ++
.....+ ++
writing new private key to 'private/CAkey.pem'
Enter PEM pass phrase:
```

Πανεπιστήμιο Πειραιώς  
Τμήμα Πληροφορικής



```
C:\ Command Prompt - openssl req -new -x509 -keyout private/Cakey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
C:\OpenSSL-Win32\bin>openssl req -new -x509 -keyout private/Cakey.pem -out certs/CAcert.pem -days 365 -config CAcnf.txt -sha1
Generating a 2048 bit RSA private key
....+
writing new private key to 'private/Cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GR]:GR
State or Province Name (full name) [Attica]:Attica
Locality Name (eg, city) [Athens]:Athens
Organization Name (eg, company) [University Of Piraeus]:University Of Piraeus
Organizational Unit Name (eg, section) [Informatics Department]:Informatics Department
Common Name (eg, YOUR name) [Unipi IT Security Lab Test CA]:Unipi IT Security Lab Test CA
Email Address [e-mail@unipi.gr]:kostastheos-13@hotmail.com
```

**Πανεπιστήμιο Πειραιώς**  
**Τμήμα Πληροφορικής**



```
C:\OpenSSL-Win32\bin>openssl x509 -in certs/CACert.pem -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
    ee:93:c:f:44:aa:f6:de:fa
Signature Algorithm: sha1WithRSAEncryption
Issuer: C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
Validity
    Not Before: Nov 20 13:36:19 2017 GMT
    Not After : Nov 20 13:36:19 2018 GMT
Subject: C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
            Modulus:
                00:d9:d6:37:f3:01:1f:28:64:a1:fa:bd:d8:36:94:
                2a:17:00:76:42:87:d6:31:b3:1b:10:e3:dd:a1:d9:
            1c:36:d8:08:8d:ff:b9:69:93:02:b9:d6:83:0a:
            f4:19:56:25:e2:44:8b:c2:64:4b:81:id:44:23:44:
            e9:7d:53:8c:f3:b6:77:20:88:57:de:ac:m4:8a:82:
            3c:a7:4c:3e:20:63:ed:42:02:02:dc:4c:6c:cb:
            b6:99:41:41:31:31:31:31:31:31:31:31:31:31:
            39:84:7c:66:d5:37:bd:7c:7a:ed:66:77:1b:37:ad:
            cc:6a:bd:ff:ff:5:bc:ad:6e:c2:72:db:75:f5:db:2f:
            5b:1b:09:a9:98:84:f6:56:25:4f:25:c7:77:45:b9:
            4b:91:93:fb:83:bc:43:99:6e:82:24:0b:3b:6b:00:
            b1:c0:76:e3:4c:aa:5a:3e:6a:ad:a8:79:61:60:e1:
            9b:5a:fd:c5:f6:00:53:74:08:5e:9b:14:9c:7c:fa:
            67:af:b4:5b:d4:10:e0:ca:7a:ba:68:0b:4c:dd:de:
            6a:03:a9:db:42:4e:b3:40:e7:7e:ca:ca:3b:95:e6:8d:
            d8:a5:21:ea:d1:a0:46:f0:98:34:7f:a1:73:d8:f3:
            80:63:90:cd:56:1b:ba:e1:b1:0a:d1:62:7a:26:ba:
            f0:a5
            Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Subject Key Identifier:
        1E:D2:FB:93:41:AD:AB:8F:9F:6F:C5:83:93:B4:80:4C:B6:FE:E5:52
    X509v3 Authority Key Identifier:
        keyid:1E:D2:FB:93:41:AD:AB:8F:9F:6F:C5:83:93:B4:80:4C:B6:FE:E5:52
        DirName:/C=GR/ST=Attica/L=Athens/O=University Of Piraeus/OU=Informatics Department/CN=Unipi IT Security Lab Test CA/emailAddress=kostastheos-13@hotmail.com
        serial:EE:93:CF:44:AA:F6:DE:FA
X509v3 Basic Constraints:
    CA:TRUE
X509v3 Key Usage:
    Certificate Sign, CRL Sign
Netscape Cert Type:
    SSL CA, S/MIME CA
```

```
C:\ Command Prompt
-----  

      SSL CA: /halWithRSAEncryption  

Signature Algorithm: sha1WithRSAEncryption  

67:19:6e:0f:2b:89:94:ac:19:52:6a:22:0e:47:52:3e:a3:23:  

a8:1c:a3:47:28:33:0c:fd:31:4f:30:38:92:e3:28:8d:3e:44:  

60:07:8c:a1:08:a0:04:a6:a9:b9:5b:f8:f5:fd:1c:24:f6:97:  

9d:0c:bd:b1:9e:ae:48:7a:58:59:d7:c5:2d:95:a3:9b:3e:56:  

27:73:c3:79:9d:35:14:40:fc:02:09:e9:d3:d1:c0:0c:3e:11:  

13:41:94:91:6e:25:55:32:b7:78:2b:0b:b2:47:88:25:83:e6:  

55:57:b7:d4:8d:c6:c3:7e:34:42:46:34:54:eb:b5:53:a6:91:45:  

98:70:94:34:43:c3:98:e2:70:3b:eb:54:f5:fb:9e:8f:5e:9d:  

b4:dd:09:05:68:77:32:6a:92:2d:2d:67:31:9e:2b:1d:a8:5d:  

f1:7a:18:af:ze:34:02:5b:09:04:00:25:e4:ac:9f:d1:eb:4f:  

bc:88:d5:09:74:10:95:e1:35:30:7a:cb:96:7f:0b:6c:8e:05:  

6e:6:f7:dc:da:99:91:7e:76:9a:86:df:a3:ba:aa:7a:fd:f1:ab:  

b5:38:5b:1b:10:10:c2:56:70:8e:44:74:72:8b:fd:7d:78:fd:4e:  

8d:11:fc:50:75:d6:81:34:e4:74:3c:9b:cb:b6:ee:d3:59:72:  

bc:dc:d9:22
-----  

----- BEGIN CERTIFICATE -----  

MIIFWTCCBEGgAwIBAgIJAQAGt2S9t7GM0AQCSqGSIb3DQEBBQUAMHdIQswCQYD  

VQQGEwJHJjEPMA0GA1UECAwGXRx0aWlnMg8wO0YDQVQHDazBgHgbmXtrjAcBgIV  

BaOfMFVuaxZlcnlpdHkgT2YpUGlyVMicZEMB0gAUUCwawSi5mb3JtYXKp3Mg  

RGWVXJ0BwVuDEWMQQA1UEAwdwW5pcGkSVQgU2VjzXOpdlkgTGflIFlrc13g  

Q0EXKTAnBgkqhkiG9w0BEMktvc3RhczR0ZW91LTzGhvdgHawhuY29tH8AX  

DTE9MTEyMDc2h2z1yXoXoDTE4MTEyIDE2h2YXQDowgcRkxzaJEcgNBAYTakSNQ8w  

QDYVQUDADAkBHRgv2Ex0AAMbgIVAcMBkFba6Vu:zeIeBwGAUeCgVwMsCpdMv  

C2:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  

----- END CERTIFICATE -----  

C:\OpenSSL-Win32\bin>
```



```
cov9fXj95I0R/FB11oE05HQ8m8u47tNZcrzU2SI=
-----END CERTIFICATE-----
RSA: Use -help for summary.
C:\OpenSSL-Win32\bin\lab>openssl rsa -in private/CAkey.pem -text
Enter pass phrase for private/CAkey.pem:
```

```
Command Prompt
exponent2:
7:34:48:59:2e:d1:3a:f8:4e:8f:17:e2:ad:71:94:
Sc:9b:ef:37:f2:b5:d2:73:b6:ff:cd:ad:3d:c5:f5:
99:a1:0f:06:1e:d2:c7:e0:1d:89:38:63:30:2a:ba:
ba:a0:0d:ee:56:67:9d:e5:3b:d4:e3:7a:72:47:bb:
e3:f8:a5:53:e9:3b:b2:48:57:f7:d5:53:8c:93:96:
4d:bc:bb:f1:b7:09:5a:8d:42:0d:a6:33:15:4d:8f:
e5:3e:0e:b5:c1:e5:d6:74:b2:26:b4:94:65:b0:aa:
55:d2:1b:49:03:ac:23:59:f4:aa:d1:9f:c3:3f:26:
74:9a:3d:c9:2f:bd:3b:bd
coefficient:
22:19:ec:d2:04:79:f1:2c:45:97:40:a6:ba:59:75:
35:3e:e2:11:96:32:55:92:38:1c:80:86:31:56:44:
90:98:93:53:1e:cd:2a:7c:c4:b7:f7:09:08:4a:1a:
6c:30:85:3e:0d:d1:33:41:f2:62:c9:02:54:52:96:8c:
dd:7c:4c:1f:fd:4a:36:26:eb:4d:cc:di:08:0a:86:
3e:21:0d:18:18:37:49:5f:a5:8d:63:91:42:64:61:
ca:ed:1b:34:di:5a:36:0b:7b:da:af:7e:05:es:23:
fc:dd:42:ac:cb:f9:49:e2:cc:10:8d:13:38:58:38:47:
f2:f6:db:83:5b:9d:60:64
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MTEPAWCAQEAE2Q38ufFkGSh+3WnpQnFtB2QoFmMhMhEd7dodkChjtwjiaj/
uleYArnkgpwR+VY14kSLwmRlgR1E10tFv0Wxt3LYBXTxuoxio18p0w/UuA70JIC
S3zKbLSw0HtBje5uWdyo2cAySH5hx1t9eFrHt7ngNM3Mar3/oBytbs7y23X1
2y92ku0paT1T2V16t3dRbhLkZp7g7x2m0mJaS7awc.xubjTkpaPqatq1HnyGob
ju3F9gBtDmNvxs:cfppm7R81BbgynoqalBM3d5a6NbK6QDd+juVs3oy5h4q
0aBg83jgF6f2p2POAs7RaB6eK0W6Jn+rwa0TDAAQBaIBAQCT00eg1le0l0l0r
f6:zqFDH23n3BYBLUMLwh1v.F1OpSwkNyTcZRZvgutlhb71kBBqAg70FxzdZrn0
9M7xElz10Mp7U3mtz2k103v5G69M-1k+VwRA1DXJ9mbApAbYyyOhkkMv
08crgpeja1sMT3DySwHgtB3dMVEfM1C1k1B6Yhr+Fz2pxRbVHTcx0pdvgd
/jzg21h53uoxryJMu6f47+v+10Y3dg1lyMrqzgbwP806fT016tIX99tSw1uMtXm
/jUbhy1cVUDIDnduh0KMa9n0Bf5u9b5d1nJVP8Vqyj8s1ckxdzHdCRKDw
z20vPwRmk9bwUYGeUyicobOs92be3j94yMuh/Cp1PxWdHxxGsIN16gYqtwxI98
8Gz1SUDm+Y6j9Ab16t0wus1DAAC41ch84154x9d9TckjXPNUCfE1MHA9G0BAos
VggbNm32pUuHGSvRdnOrMktx2dM0Lvx615/XBqnxkA0HURkA+AduADtYS
QnWt1xMw1t1u2678apsk045Tgvxk7ZQ2Z0WnQ10Erpmu9y50a2poa/PFQ53h6
rn0yhnbrzr+BuHegowg7W7zNE2Cr+34V21xp/FzogBAnVq1B1ly2wInFqC18Y
z:8L/umgkixOyfjckK6fZdrhBKI/EN+u1u9dpdAOX7T7L1N0iQr1.BXbxXp0UC
r3kk35D1pkq70/A1x073infxqf+A5WnQkiz7r1V9CYveu9suJaJgptfjxZ8
f19Q1dCPnyf010x0B5H1qFaGAFz1tws7R0vh0jxfirGUXJxvhl/bbn02/82k
/.c/mamEPH7Sx+Ad1tjhMycq6uqWV71zneu07106cke74/11t7:kshX9V7tj10W
Tby78m.Wn0lDyaFu2PpeMoch1lin1Sjy-SU2bCqJ1B5Q01nngtfw+8ed1t9j
ys7tV0d+yG1gewBNhxLENx0KA6w0XUPluRnTvkJggc1YVksQ0JNTHs0q8pS3
cHkA5hpS04U+0MxQd01052z02dfeWf5k02ju7zNfHoCoY/f1BNGdfZXMWNY5FC
eHk3R3r90v0Zc3var24yP81MKstn12BcNe2hYOfFy9ruW51gBA=
```

-----END RSA PRIVATE KEY-----

2) Δημιουργία και πιστοποίηση κλειδιών για server: Δημιουργήστε ένα ζεύγος κλειδιών για έναν web server. Στη συνέχεια φτιάξτε ένα έτοιμα certificate signing request (csr) προς την δοκιμαστική API ώστε να υπογράψει το πιστοποιητικό του server, αντίστοιχα με το εργαστηριακό παράδειγμα. Όμως θα πρέπει να τροποποιήσετε κατάλληλα το αρχείο



διαμόρφωσης της API ώστε το πιστοποιητικό του server να περιλαμβάνει τα αντίστοιχα constraints (key usage και extended key usage) που αντιστοιχούν σε έναν server, όπως φαίνεται στο[1].

```
C:\Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl req -new -config CAcnf.txt -nodes -keyout private/serverKey.pem -out req/server.csr -days 365 -md5
```

```
C:\Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl req -new -config CAcnf.txt -nodes -keyout private/serverKey.pem -out server.csr -days 365 -md5
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'private/serverKey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GR]:GR
State or Province Name (full name) [Attica]:Attica
Locality Name (eg, city) [Athens]:Athens
Organization Name (eg, company) [University Of Piraeus]:University Of Piraeus
Organizational Unit Name (eg, section) [Informatics Department]:Informatics Department
Common Name (eg, YOUR name) [Unipi IT Security Lab Test CA]:Konstantinos
Email Address [e-mail@unipi.gr]:kostastheos-13@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []::pappouli13

C:\OpenSSL-Win32\bin\lab>
```

```
C:\Administrator: Command Prompt
C:\OpenSSL-Win32\bin\lab>openssl rsa -in private/serverKey.pem -text
```

**Πανεπιστήμιο Πειραιώς**  
**Τμήμα Πληροφορικής**



```

Administrator: Command Prompt
exponent12:
6e:40:c4:2b:f1:b1:86:60:7d:ec:59:41:79:28:
2b:6f:c5:11:a1:8c:89:55:26:dd:4e:2d:d8:49:e9:
c1:e9:f1:a9:bc:61:09:e2:85:5d:bc:df:36:26:18:
ed:3e:6f:b4:dc:f6:01:26:81:34:be:6e:4c:9a:ad:
7e:da:a5:40:08:76:fa:65:b3:63:97:49:16:f1:c7:
00:ed:8b:78:04:f9:03:a8:3d:ef:de:ab:36:7e:85:
a8:d7:26:6f:b0:06:a0:0c:e7:f3:18:ed:36:6c:e7:
67:ba:17:1a:99:93:b2:88:02:3b:82:49:f0:f3:53:
df:01:52:01:4a:3c:e6:c9

coefficient:
39:af:4f:db:81:10:12:89:21:b8:01:2f:52:13:31:
ba:7c:54:af:03:09:59:20:74:b6:d0:4f:4d:5c:b7:
85:f2:d2:23:70:3f:d4:0e:f2:a9:58:66:c2:2c:94:
9e:20:ad:18:2b:7e:4f:74:8f:14:94:f0:bc:ca:02:
00:0d:28:60:2f:c3:74:cd:9d:47:8e:a0:63:4b:36:
9f:ee:73:74:eb:fa:28:12:c1:a2:98:fb:cf:06:72:
42:0c:f3:98:fa:0b:43:ed:64:ca:5f:f0:02:03:db:58:
8a:da:0e:67:01:75:6a:db:f0:7c:b0:41:24:c1:fc:
eb:bb:84:41:d8:1d:62:10:1b

writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxvh-SH13b1jygwCwXpzi1mKOiyQeBmJPK6ARsW9P?+on
97010fx7WmXbXkE-SGAGKoMcGg862yE5yOJFTM4Vv+v7i1QWf3IcbhD
+g+10iyw7eMly703/vK5nppjg0h2lO7n+ed0ijz=4MKYwep/XfQouzGR8Sp5
SEWltvymrniLZZAV0WVYpoxOK,g1whEyMCPBBeu11bLw+SdSnsk0g656
fIsqzvz5167FOk6stg2+y5LkwpxUSHC61QWfAYXyeZuhhaF476921xvOnu
pr277CTO1p2QVlgAFRRPvL10LR43ZCmkC5TN/q0DAQABao1BAc:c549:yphnYKCSR
86k8Bu/EpfT0bYl37CRVghMnwQVsU5B7MtKvJ1M1ik7w8q1dXl:00873t0J0T2
1J90LqA9R14um0ljd4u1JgDRFM-Uf88g92Bp5d2KlqrLLJ0g2f0Ypap8ze4Yh0wR
v8xhAGU17956ekxdi+7xK5n1h86FUFBtAa1AV69qZuhofG1uoh1XvWzexiyK
DaFgvLWX11Frxe95Q5uB5Ymfx1090101511f7ap08gg+9lF511t+hPwfWvOr+j6m
pd32fJgy+KoB02u+C+To:VWlqpldvF5dukN7oc1+q3v-Bh+i1g1b8N8suVaDoV
yxKHIECeyEAOPUf7QHAvvUJupmLlfwohdvYgsee2dWl4+d+94L87dNsttu80VSQ
4q0nf0TuVykfAuyk/K0T32+vMs29MG8xF1z:3/4YEkrXwEc:005cWaX8hNlL
4pYOsniKAUdqAc114cmkkqC/P/Sf1/9U1DPUx0g0Htsv/caGbdapTxccgYEa208z
11YXZfQV32uSehGr8LDHKSG1cK5:fy4xpLVdAY2Kb10q8114HF2ff7rADGUl
c+g1zjX0lobr5ka1nDfw2j4uC0Z96j+rNGh51TRG+M1xr8U1R1Fnd22Qwz6V
eu15pxB18VwAXjv2fHx3fThpkYkzv383:8cgYEAQ1QVksQsR0ldv+E+TgN/B
secev1sVX3XznN6VckLwqoZKtnazf0yYdm955zefspXe2AQ2GV99fkWChmp5xq
2un7kbpuPcsbsn6XQVK0MTQZD+cNBc3dM4Q2IGPOKNTwu901EpKmeH5I6CeZ
GtJvr1bpG1Yfe6n25vem%0gYBuUQ077/tlhmBn7f1BeDgb8URoyYVSndi3Y
Q0nb72Gqge1Aoqv82JhjtPm+03PVtob0vw5Mnq1+zqVAChb6zbNjB6kWccA
7Yt4BPkdq3v3ks2fw0lyZvAagD0fZgQ2b0dnuhcamZoyia17gknw81PFAVIB
SjzmyK8Bgdmgw9BEBK1IbgL11THbpV80DCVkgdLbQ701ctYx0iWp9008q1Y
Zu1s134pRgrfK90jxu8LzKAgQDKGAwvTlNle0GgILMp/uc3Tr+igSwakY+88G
ckINP85jg0CptMfgafpPw1rlmc:BoWr-Y+nywQ5TB/u4QjdgdynAb

-----END RSA PRIVATE KEY-----
C:\OpenSSL-Win32\bin\lab>

```



### Δημιουργία έμπιστης αρχής πιστοποίησης (CA)

```
c:\>cd CA
c:\CA>set RANDFILE=rand
```

```
C:\CA>openssl req -new -keyout cakey.pem -out careq.pem -config C:\OpenSSL-Win64\bin\openssl.cfg
```

```
C:\CA>openssl x509 -signkey cakey.pem -req -days 3650 -in careq.pem -out caroot.cer -extensions v3_ca
```

Signature algorithm name: SHA1withRSA  
Version: 1

Here are the screen shots:

The first screenshot shows the 'Certificate Information' tab, which displays a warning message: 'This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.' It also shows the 'Issued to' field as 'Test CA', 'Issued by' as 'Test CA', and 'Valid from' and 'Valid to' dates.

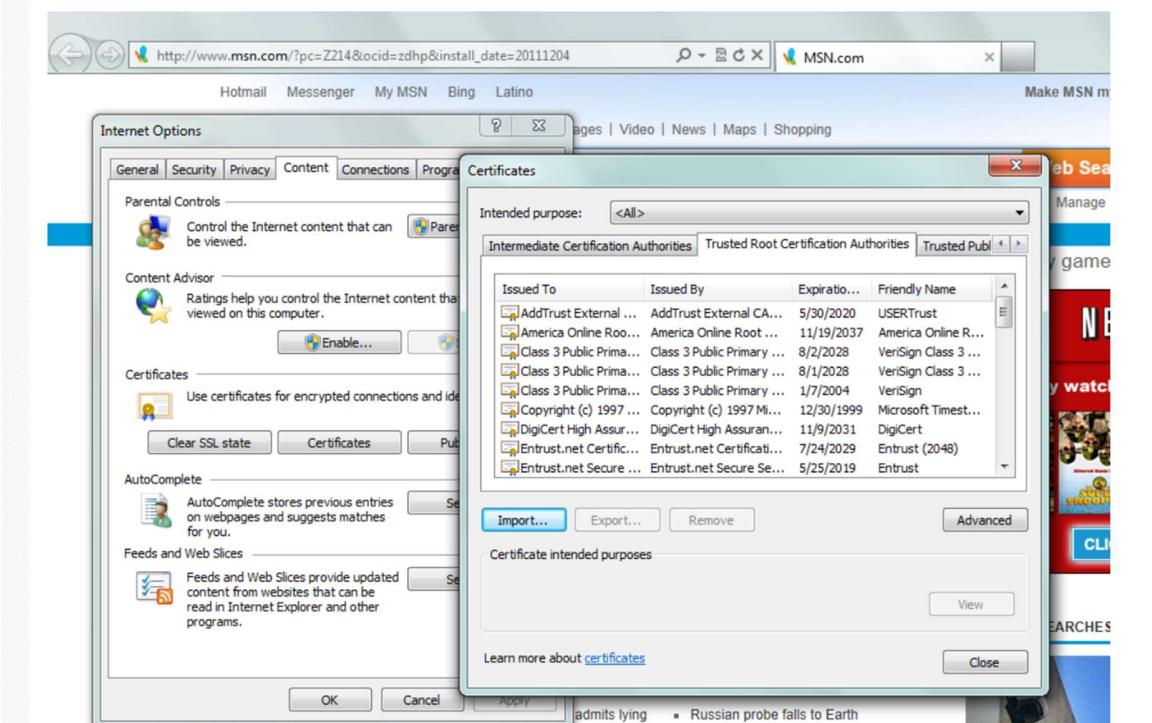
The second screenshot shows the 'Details' tab, listing certificate fields and their values. Key entries include:

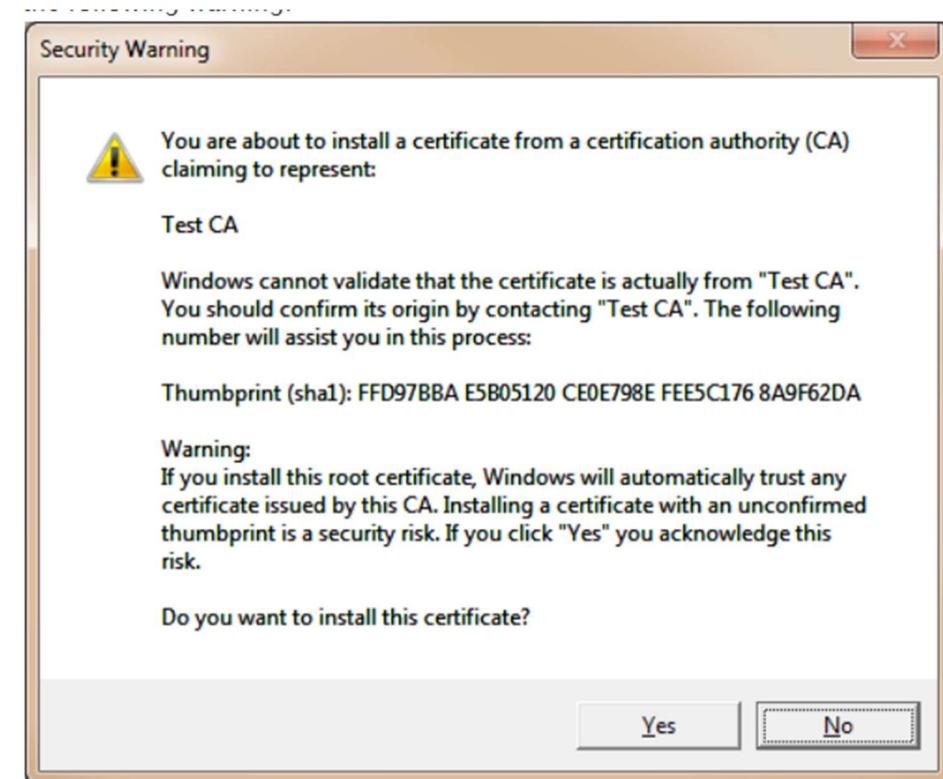
Field	Value
Signature hash algorithm	sha1
Issuer	admin@testca.com, Test CA, ...
Valid from	Friday, January 20, 2012 11:20:00
Valid to	Monday, January 17, 2022 11:20:00
Subject	admin@testca.com, Test CA, ...
Public key	RSA (1024 Bits)
Thumbprint algorithm	sha1
Thumbprint	ff:fd:7b:ha:e5:h0:51:20:ce:0e

The third screenshot shows the 'Certification Path' tab, which lists the 'Certification path' as 'Test CA'.



Open IE and click on **Internet Options->Content->Certificates->Trusted Root Certification Authorities**







Name	Date modified	Type	Size
❑ .rnd	11/26/2018 9:28 PM	RND File	1 KB
❑ cakey	11/26/2018 9:28 PM		2 KB
❑ careq	11/26/2018 9:30 PM		2 KB
❑ caroot	11/26/2018 9:31 PM	Security Certificate	2 KB
❑ rand	11/26/2018 9:44 PM	File	1 KB
❑ serial	12/17/2018 4:49 A...	Text Document	1 KB
❑			

Στην συνέχεια υπογράφω με το έμπιστο πιστοποιητικό μου το δικό μου πιστοποιητικό.

Administrator: Command Prompt

```
C:\OpenSSL-Win32\bin\lab>openssl ca -config CAcnf.txt -policy policyAnything -cert certs/CAcert.pem -keyfile private/CAkey.pem -out certs/serverCert.pem -infiles server.csr
```

**Πανεπιστήμιο Πειραιώς**  
**Τμήμα Πληροφορικής**



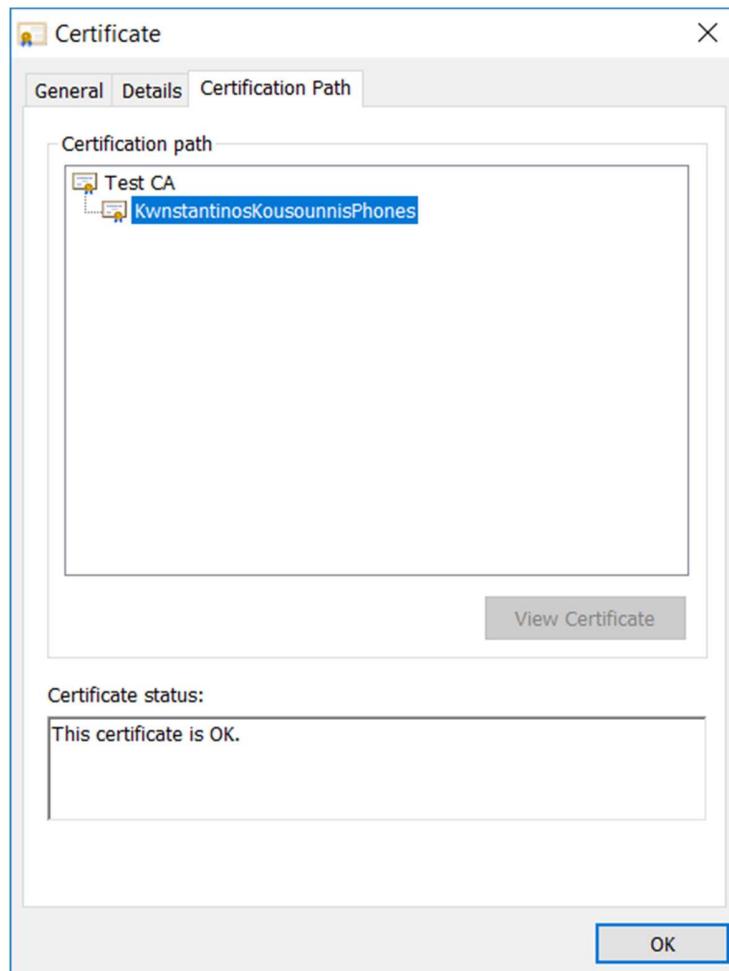
```
C:\OpenSSL-Win32\bin\lab>openssl ca -config CAcnf.txt -policy policy_anything -cert certs/CAcert.pem -keyfile private/CAkey.pem -out certs/serverCert.pem -infiles server.csr
Using configuration from CAcnf.txt
Enter pass phrase for private/CAkey.pem:
Can't open index.txt.attr for reading, No such file or directory
10436:error:02001002:system library:fopen:No such file or directory:crypto\bio\bss_file.c:74:fopen('index.txt.attr','r')
10436:error:20060080:BIO routines:BIO_new_file:no such file:crypto\bio\bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'GR'
stateOrProvinceName   :ASN.1 12:'Attica'
localityName          :ASN.1 12:'Athens'
organizationName      :ASN.1 12:'University Of Piraeus'
organizationalUnitName:ASN.1 12:'Informatics Department'
commonName            :ASN.1 12:'Konstantinos'
emailAddress          :IA5STRING:'kostastheos-13@hotmail.com'
Certificate is to be certified until Nov 19 17:34:16 2022 GMT (1825 days)
Sign the certificate? [y/n]:y

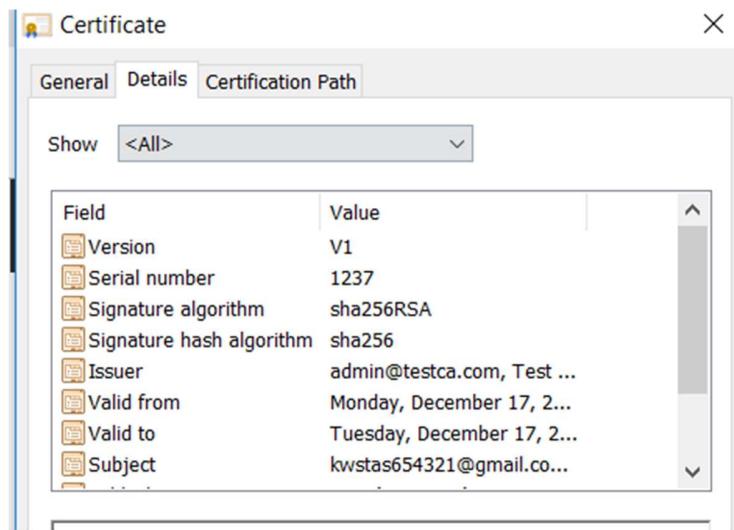
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\OpenSSL-Win32\bin\lab>
```

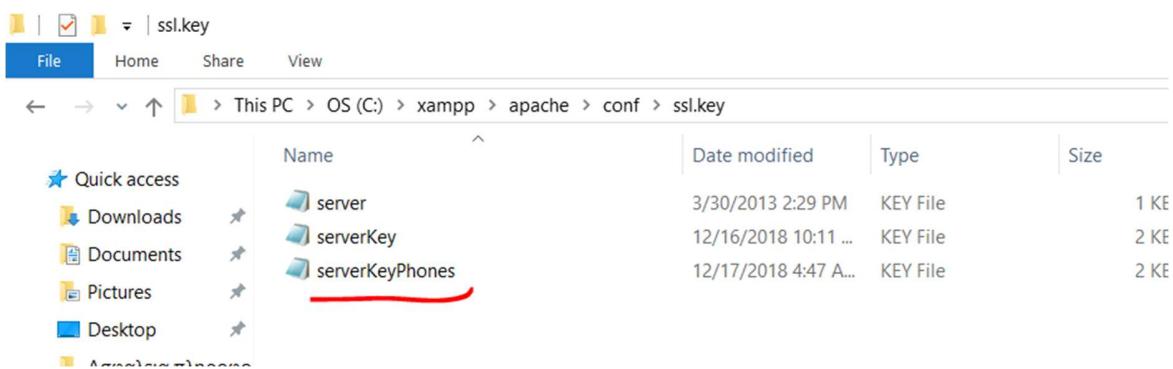
```
C:\OpenSSL-Win32\bin\lab>openssl x509 -subject -issuer -enddate -noout -in ./certs/serverCert.pem
subject=C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Konstantinos, emailAddress = kostastheos-13@hotmail.com
issuer=C = GR, ST = Attica, L = Athens, O = University Of Piraeus, OU = Informatics Department, CN = Unipi IT Security Lab Test CA, emailAddress = kostastheos-13@hotmail.com
notAfter=Nov 19 17:34:16 2022 GMT

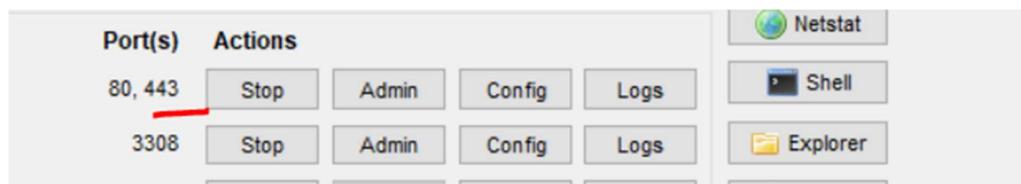
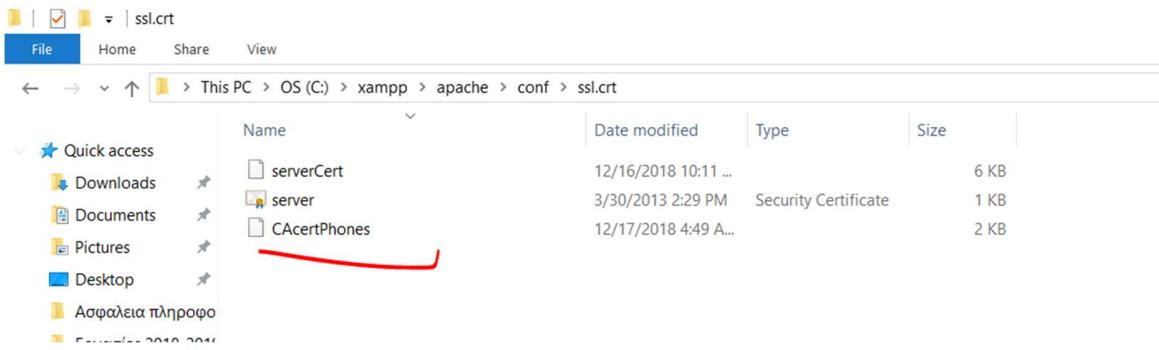
C:\OpenSSL-Win32\bin\lab>
```





Οπως βλέπουμε έχω υπογράψει το πιστοποιητικό μου **KwnstantinosKousounnisPhones** με το **test ca** στην συνέχεια τα αποθηκευω και ενεργοποιώ το ssl στον xampp μου.





Πηγή:<https://sites.google.com/site/ddmwsst/create-your-own-certificate-and-ca>

**3.Να υλοποιείστε ένα μηχανισμό αυθεντικοποίησης (user authentication), πχ. username,password, one-time password, certificate based κτλ. και ελέγχου πρόσβασης (authorization), πχ. LDAP-based, identity management, certificate based, group-based, role-based κτλ. (Σημείωση: αυτό το βήμα θα αποτελεί επέκταση της 4ης άσκησης).**

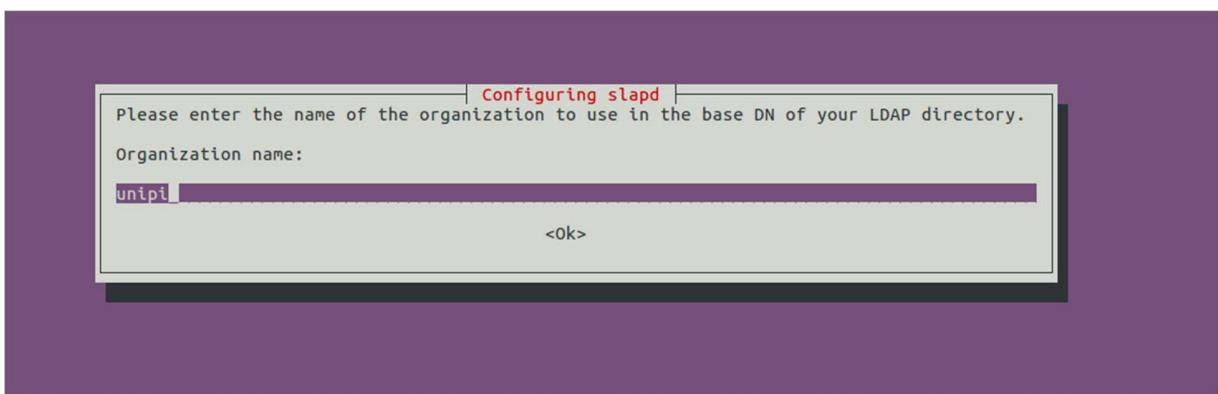
Δημιουργούμε ένα **ldapserver unipi.gr**



```
root@server:/# dpkg-reconfigure slapd
```

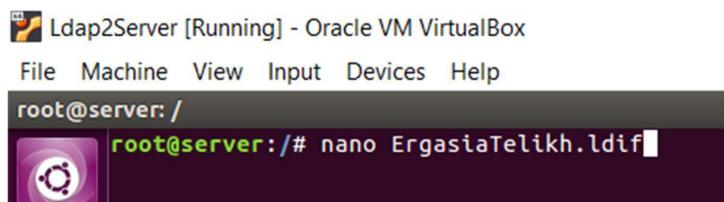


**Δίνουμε το όνομα του server μας**



Η εργασία μου αφορά μια ιστοσελίδα πώλησης Κινητών Τηλεφώνων η οποία ιστοσελίδα έχει administrator και Users.

Δημιουργώ ενα ldif αρχείο όπως και παραπάνω και φτιάχνω αντιστοιχα μια δομή για την Ιστοσελίδα μου.





Ldap2Server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@server: /

GNU nano 2.5.3

```
dn:ou=DepartmentPhoneSales,dc=unipi,dc=gr
objectClass:organizationalUnit
ou:DepartmentPhoneSales

dn:ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass:organizationalUnit
ou:Admins

dn:uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass/inetOrgPerson
cn:Kwnstantinos
sn:Kousounnis
mail:kwstas654321@gmail.com
uid:Admin1

dn:ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype:add
objectClass:organizationalUnit
ou:Users

dn:uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr
changetype: add
objectClass:inetOrgPerson
cn:Lena
sn:Tsoukala
mail:lena@gmail.com
Userpassword:123
uid:User1
```

Δημιουργώ ενα organizational unit με όνομασια admins και μεσα σε αυτον τον Καταλογό φτιαχνω ενα Unit τύπου Users.

Βαζω έναν admin:Kwnstantino Kousounni

Και ένα User:Lena Tsoukala με κωδικό για τον User

root@server: /

```
root@server:/# nano ErgasiaTelikh.ldif
root@server:/# nano ErgasiaTelikh.ldif
root@server:/# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaTelikh.ldif
```

Τρέχω την εντολή για να παρει ο Server τα στοιχεία.



```

root@server:/# ldapadd -a -x -D "cn=admin,dc=unipi,dc=gr" -w 123456 -H ldap:// -f ErgasiaTelikh.ldif
adding new entry "ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
adding new entry "uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr"
root@server:/

```

Και μπορούμε να δούμε οπως και πρίν αν έχει δημιουργηθει η ιεραρχία στον phpLDAPadmin.

The screenshot shows the phpLDAPadmin interface. On the left, there's a tree view of the LDAP structure under 'My LDAP Server'. A red box highlights the tree structure. On the right, there's a detailed view of the 'ou=Admins' object. A second red box highlights the 'Create a child entry' option in the sidebar. The sidebar also lists other actions like Refresh, Switch Template, Copy or move this entry, Rename, Show internal attributes, Export, Delete this entry, Compare with another entry, Add new attribute, and Export subtree. At the bottom, there are fields for 'objectClass' (set to 'organizationalUnit') and 'ou' (set to 'Admins').



## Ελεγχω και τον κωδικό του Χρήστη

The screenshot shows a dual-browser setup. On the left, a 'Password Checker Tool' window displays a comparison between two password entries, with a green 'Passwords match!' message. On the right, an 'Ldapwiki: Microsoft Active Directory' window shows the user 'Lena' with attributes: 'cn' set to 'Lena', 'Email' set to 'lena@gmail.com', 'objectClass' listing 'inetOrgPerson' (structural), and a 'Password' field which is currently empty. Red boxes highlight the 'Compare' button in the checker tool and the 'Password' field in the LDAP editor.

Συνδέση του Ldap με την Εφαρμογή μου.

Πάω στον Path που έχω εγκαταστήσει το xampp και δημιουργώ ένα php αρχείο.



File   Home   Share   View				
This PC > OS (C:) > xampp > htdocs				
	Name	Date modified	Type	Size
Quick access	dashboard	12/10/2018 2:47 PM	File folder	
Downloads	ErgasiaAp	12/10/2018 7:45 PM	File folder	
Documents	img	12/10/2018 2:47 PM	File folder	
Pictures	webalizer	12/10/2018 2:47 PM	File folder	
DATA (D:)	xampp	12/10/2018 2:47 PM	File folder	
Desktop	applications	10/19/2017 6:09 A...	Chrome HTML Do...	4 KB
ΕργασίαΣΔΒΔ-2018	bitnami	2/27/2017 11:36 A...	CSS File	1 KB
Εργασίες, 2018-2019	favicon	7/16/2015 6:32 PM	Icon	31 KB
OneDrive	index	7/16/2015 6:32 PM	PHP File	1 KB
This PC	Idapserver	12/10/2018 6:27 PM	PHP File	1 KB
3D Objects				



Και Μιλάω στον στον server μου με πορτα 192.168.94.3

ldapserver.php - Microsoft Visual Studio

FILE EDIT VIEW PROJECT DEBUG TEAM TOOLS TEST ANALYZE WINDOW HELP

ldapserver.php X

```
<?php
$ldap_dn = "cn=admin,dc=unipi,dc=gr";
$ldap_password = "123456";
$ldaptree = "ou=DepartmentPhoneSales,dc=unipi,dc=gr";
$ldapconn = ldap_connect("192.168.94.3");
ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);
$result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);
if($result) {
    $search = ldap_search($ldapconn,$ldaptree, "(cn*)") or die ("Error");
    $data = ldap_get_entries($ldapconn, $search);
    print_r($data);
} else {echo "Invalid user/pass or other errors!"};|
```

Ανοίγουμε την ιστοσελίδα του xampp και βλέπουμε τον ldap server.

localhost/ldapserver.php

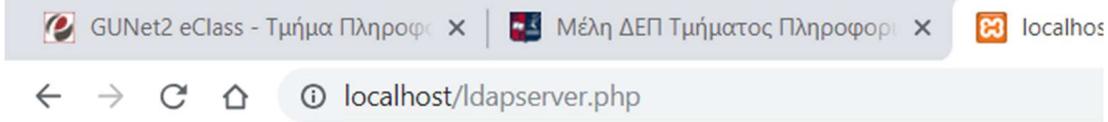
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

```
Array ( [count] => 2 [0] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass [cn] => Array ( [count] => 1 [0] => Kwnstantinos ) [1] => cn [sn] => Array ( [count] => 1 [0] => Kousounnis ) [2] => sn [mail] => Array ( [count] => 1 [0] => kwsstas654321@gmail.com ) [3] => mail [uid] => Array ( [count] => 1 [0] => Admin1 ) [4] => uid [count] => 5 [dn] => uid=Admin1,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) [1] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass [cn] => Array ( [count] => 1 [0] => Lena ) [1] => cn [sn] => Array ( [count] => 1 [0] => Tsoukala ) [2] => su [mail] => Array ( [count] => 1 [0] => lena@gmail.com ) [3] => mail [userpassword] => Array ( [count] => 1 [0] => 123 ) [4] => userpassword [uid] => Array ( [count] => 1 [0] => User1 ) [5] => uid [count] => 6 [dn] => uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) )
```



Στην ουσία μου δίνει όλα τα αποτελέσματα που έχω αποθηκευσει στον server αυτός ο κώδικας

Στην τελική έργασία θα ελέγχω τους χρήστες που έχω με τον server μου.



For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

```
Array ( [count] => 2 [0] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson [mail] => Array ( [count] => 1 [0] => kwstas654321@gmail.com ) [3] => mail [uid] => Array ( [objectclass] => Array ( [count] => 1 [0] => inetOrgPerson ) [0] => objectclass lena@gmail.com ) [3] => mail [userpassword] => Array ( [count] => 1 [0] => 123 ) [4] => uid=User1,ou=Users,ou=Admins,ou=DepartmentPhoneSales,dc=unipi,dc=gr ) )
```

Στην Ιστοσελίδα μου έχω τοις αντίστοιχες συνδέσεις.



The screenshot shows a web browser window with the title "Title". The address bar indicates the URL is <https://localhost/ErgasiaAp/login.html>. The page content includes a navigation bar with links for "Αρχική", "Είσοδος χρήστη", and "Εγγραφή". Below this is a login form with fields for "Όνομα Χρήστη:" and "Κωδικός:", and a "Login" button. To the right of the form is a large blue decorative graphic of a stylized building or bridge. Below the form is a code editor window displaying the following PHP code:

```

    }
} else {
    echo "Invalid user/pass or other errors!";
}

```

Έχω ένα αρχείο με το οποίο κάνω την σύνδεση μου.

Για την εγγραφή χρηστών πηγαίνω στον ldap και δημιουργώ στο κλαδή Member τους χρήστες μου.

Στην συνέχεια για να συνδεθώ με τα στοιχεία μου πηγαίνω και ελεγχω αν υπαρχουν τα στοιχεία μέσα στον ldap μου.



The screenshot shows a web browser window with the following details:

- Title Bar:** Title [x] +
- Address Bar:** https://localhost/ErgasiaAp/Menu.php
- Menu Bar:** Αρχική Παραγγελίες Αποσύνδεση
- Content Area:** A large white area containing the text "Welcomelena".
- Left Sidebar:** A vertical sidebar with a dark header bar containing the text "SmartPhones".

Οπως βλεπουμε παραπάνω ελέχγω αν υπάρχει το username και το password του αντίστοιχου χρήστη.



```

34
35
36
37
38
39
$_SESSION['login_user'] = $username;
$_SESSION['login_password']=$password;
39
echo("<meta http-equiv=\"refresh\" content=\"0; URL='AdminMenu.php'\\" />"); 
40
} else {
41
echo("<meta http-equiv=\"refresh\" content=\"0; URL='InvalidMessage.html'\\" />"); 
42
}
43
}

```

Βλέπουμε ότι μπορούμε πλέον να συνδεθούμε αν υπάρχουν τα στοιχεία.

Επιπλέον έχουμε εναν διαχείριστη ο οποίος συνδέεται από εναν έλεγχο που κάνουμε στον Idapr μας στο κλαδί admin.



Title +

Αρχική Είσοδος χρήστη

Όνομα Διαχειριστή:

Κωδικός:



Στην  
συνέχεια  
έχουμε ενα

Προνομοιούχο διαχειριστή ο οποίος συνδέεται και δημιουργεί και διαγράφει διαχειριστές.



Screenshot of a web browser showing a login form and a user management table.

The browser title bar says "Title" and the address bar shows "https://192.168.0.102/ErgasiaAp/PrivilegeAdminMenu.php".

The page content includes:

- A login form with fields for "Όνομα Χρήστη:", "Κωδικός:", and "Επιθετο:".
- A "Εγγραφή" button.
- A table listing users with columns: Username, Surname, AdminPassword, and Delete.

Username	Surname	AdminPassword	
Admin2	Admin2	c8d30f3d9ed79ecce3a15ce9e5037a9b	<button>Delete</button>
Admin1	Admin1	ac5602aa1ba63ce6e1659e8cfcb45559	<button>Delete</button>

**4. Για τη λήψη δεδομένων εισόδου από τους χρήστες της εφαρμογής, να χρησιμοποιείστε συναρτήσεις οι οποίες επιβάλουν input filtering και validation, ανάλογα με το προγραμματιστικό περιβάλλον που επιλέξατε.**

Τοποθετούμε για πρόληψη σε Idap Injection φίλτρα τα οποία όταν εισάγει ο χρήστης ένα κείμενο φιλτράρονται για να μην περάσει ο χρήστης κώδικα μέσα στον Idap κατάλογο.



```
1 <?php
2 /**
3  * Created by PhpStorm.
4  * User: kwnstantinos
5  * Date: 1/25/2019
6  * Time: 3:19 AM
7 */
8 $username=($_POST['username']);
9 $username=ldapspecialchars($username);
10 $password=($_POST['password']);
11 $password=ldapspecialchars($password);
12 // $password="{SSHA}hiPVqfDJnaZjb5TSbByAh1jUMDEM4YFh";
13
14
15 function ldapspecialchars($string) {
16     $sanitized=array('\\\\' => '\\5c',
17                      '*' => '\\2a',
18                      '(' => '\\28',
19                      ')' => '\\29',
20                      "\x00" => '\\00');
21
22     return str_replace(array_keys($sanitized),array_values($sanitized),$string);
23 }
24
```



```

10
11     $username=$_POST['username'];
12     $username=ldapspecialchars($username);
13     $password=$_POST['password'];
14     $password=ldapspecialchars($password);
15
16     function ldapspecialchars($string) {
17         $sanitized=array('\\\\' => '\\5c',
18                         '*' => '\\2a',
19                         '(' => '\\28',
20                         ')' => '\\29',
21                         '\\x00' => '\\00');
22
23         return str_replace(array_keys($sanitized),array_values($sanitized),$string);
24     }

```

Οπως βλέπουμε βάζουμε την μέθοδο ldapspecialchars και φιλτραρούμε χαρακτήρες όπως \\, \*, (),\x00 η οποίοι είναι όλοι χαρακτήρες κώδικα του ldap μας



Arachni v1.5.1 - WebUI v0.5.12   Scans   Profiles   Dispatchers   Users

Scans / https://192.168.0.102/ErgasiaAp/Index.html

TOGGLE VISIBILITY OF: Comments

ACTIONS: Share, Full edit, Download report as: HTML, JSON, Marshal, XML, YAML, AFR

Edit description

The scan completed in 00:01:05.

### Issues [14]

All [14] \* Fixed [0] ✓ Verified [0] ⚡ Pending verification [0] ✗ False positives [0] ⓘ Awaiting review [0]

Listing all logged Issues.

TOGGLE BY SEVERITY: Reset, Show all, Hide all

URL	Input	Element
LDAP Injection 3		
Cross-Site Scripting (XSS) 1		
HTTP TRACE 1		
Missing "Strict-Transport-Security" header 1		
Password field with auto-complete 4		
Missing "X-Frame-Options" header 1		
Allowed HTTP methods 1		
Interesting response 2		
LDAP Injection 3		
Cross-Site Scripting (XSS) 1		
HTTP TRACE 1		
Missing "Strict-Transport-Security" header 1		
LDAP Injection 3		
Cross-Site Scripting (XSS) 1		
HTTP TRACE 1		
Missing "Strict-Transport-Security" header 1		

## 5. Να πραγματοποιείσετε αυτοματοποιημένο έλεγχο για την εύρεση επαθειών ασφάλειας (Σημείωση: αυτό το βήμα αποτελεί θα επέκταση της 7ης άσκησης).

Χρησημοποιώ το προγραμματιστηκό εργαλείο Arachni για να βρώ ευπάθειες στην ιστοσελίδα μου.

Έχουμε τα αντιστοιχα προβλήματα:

Ldap injection και μας ενημερώνει αναλυτικά για την κάθε ευπάθεια του συστήματος

Στην συνέχεια έχουμε xss πάλι κατα την εισαγωγή μας στον ldam.



localhost:9292/scans/6

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Arachni v1.5.1 - WebUI v0.5.12 Scans Profiles Dispatchers Users Administrator

TOGGLE VISIBILITY OF: Comments

ACTIONS: Share, Full edit, Download report as: HTML, JSON, Marshal, XML, YAML, AFR

https://192.168.1.8/ErgasiaAp/Index.html

Edit description

The scan completed in 00:01:08.

**Issues [6]**

All [6] \* Fixed [0] ✓ Verified [0] ⚡ Pending verification [0] ✗ False positives [0] ⓘ Awaiting review [0]

LISTING ALL LOGGED ISSUES

TOGGLE BY SEVERITY: Reset, Show all, Hide all

URL	Input	Element
HTTP TRACE 1		
Missing 'Strict-Transport-Security' header 1		
Missing 'X-Frame-Options' header 1		
Interesting response 2		
Allowed HTTP methods 1		

NAVIGATE TO: HTTP TRACE, Missing 'Strict-Transport-Security' header, Missing 'X-Frame-Options' header, Interesting response, Allowed HTTP methods

Διορθώνουμε στον κωδικα μας τα λάθοι αυτά τοποθετώντας input validation filters

Όπως βλέπουμε έχουμε διορθώσει τις ευπάθειες μας.