



Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

7η Εργασία

Ονοματεπώνυμο: Αγησίλαος Κολλιόπουλος

Αριθμός Μητρώου: 1072803

Τμήμα: HMTY

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:

Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

7η Εργασία – Ασφάλεια Web-Εφαρμογών.

Εργαλεία

1. Ανάλυση Ασφάλειας Ιστοσελίδων από την Mozilla.

Το παρατηρητήριο της Mozilla αναλύει τις ευπάθειες μιας ιστοσελίδας και βοηθάει διαχειριστές συστημάτων και επαγγελματίες ασφαλείας πώς να διαμορφώσουν τους ιστότοπούς τους με ασφάλεια και ασφάλεια.

<https://observatory.mozilla.org/>

2. Ανάλυση επικεφαλίδων HTTP.

Η εταιρεία <https://probely.com/> εξειδικεύεται στην ανάπτυξη σαρωτών ευπαθειών web εφαρμογών και API για προγραμματιστές. Διατηρεί το site <https://securityheaders.com/> που βοηθάει την προστασία από κακόβουλες ενέργειες επί των HTTP headers.

Οι επικεφαλίδες HTTP αφήνουν τον πελάτη και τον διακομιστή να ανταλλάξουν πρόσθετες πληροφορίες με ένα HTTP request ή response. Μια επικεφαλίδα HTTP αποτελείται από το case-insensitive όνομα της, ακολουθούμενη από ένα “:”, και μετά την τιμή του.

3. Ανάλυση πιστοποιητικού

Η εταιρεία <https://www.ssllabs.com/> παρέχει εργαλεία ανάλυσης του πρωτοκόλλου ασφαλείας SSL πχ *SSL Labs APIs, SSL/TLS Deployment Best Practices, SSL Server Test, HTTP Client Fingerprinting Using SSL Handshake Analysis, SSL Client Test, etc* (<https://www.ssllabs.com/projects/index.html>)

Παρέχει δωρεάν την ανάλυση ενός πιστοποιητικού μιας ιστοσελίδας:

<https://www.ssllabs.com/ssltest/>

(μπορείτε να αναλύσετε και τον browser σας:

<https://www.ssllabs.com/ssltest/viewMyClient.html>)

4. Ανάλυση χρήσης/υποστήριξης ciphersuites

Η ιστοσελίδα <https://cryptcheck.fr/> αναλύει ποια ciphersuites υποστηρίζει μια web-εφαρμογή.



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Εργασία

1. Στην εικονική μηχανή που ήδη έχετε στην υπηρεσία του okeanos-knossos εγκαταστήστε το λογισμικό Apache (<https://httpd.apache.org/>). Το λογισμικό είναι από τα πλέον γνωστά και ευρέως χρησιμοποιούμενα λογισμικά για υλοποίηση web- Servers.

sudo apt install apache2

2. Χρησιμοποιώντας την έτοιμη σουίτα κατασκευής ιστοσελίδων joomla ή wordpress αναπτύξτε μια προσωποποιημένη ιστοσελίδα.

Πρώτα εγκαθιστούμε την PHP με τα εξής:

sudo apt install php php-common php-curl php-fpm php-imap php-cli php-xml php-zip php-mbstring php-gd php-mysql

Έπειτα κατεβάζουμε ένα σύστημα διαχείρισης βάσης δεδομένων. Εδώ επιλέγουμε το MariaDB:

sudo apt install mariadb-server mariadb-client

Φτιάχνουμε τη βάση και ένα χρήστη-διαχειριστή για την εγκατάσταση του Joomla. Συνδεόμαστε στο shell του MariaDB ως εξής:

sudo mysql -u root

Εκεί τρέχουμε με τη σειρά τις παρακάτω εντολές (username, password, name κατ' επιλογήν):

**CREATE DATABASE name;
CREATE USER 'username'@localhost IDENTIFIED BY 'password';
GRANT ALL on name.* to username@localhost;
FLUSH PRIVILEGES;
EXIT**

Κατεβάζουμε Joomla:

wget https://downloads.joomla.org/cms/joomla4/4-3-4/Joomla_4-3-4-Stable-Full_Package.zip

sudo mkdir /var/www/html/Joomla

sudo unzip Joomla_4-3-4-Stable-Full_Package.zip -d /var/www/html/joomla

Δίνουμε τα κατάλληλα permissions:

sudo chown -R www-data:www-data /var/www/html/joomla

sudo chmod -R 755 /var/www/html/joomla

sudo systemctl restart apache2.service

Φτιάχνουμε ένα configuration αρχείο για το apache:

```
<VirtualHost *:80>  
    ServerAdmin webmaster@localhost  
    ServerName agiskol.ddns.net  
    ServerAlias www.agiskol.ddns.net  
    DocumentRoot /var/www/html/joomla  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
</VirtualHost>
```

Και το ενεργοποιούμε, αφού ελέγξουμε:

sudo apache2ctl configtest

sudo a2ensite *.conf



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

3. Εκδώστε ένα δωρεάν FQDN (πχ από εδώ: www.dnsexit.com) και εισάγετε το στον web-server σας. Εκδώστε ένα δωρεάν certificate από τον οργανισμό Let's Encrypt και ρυθμίστε το κατάλληλα στον web-server σας.

Πήραμε το domain **agiskol.ddns.net** στην ip της εικονικής μηχανής, το οποίο και προσθέσαμε στο conf αρχείο, όπως εξηγήθηκε στο προηγούμενο ερώτημα.

Για να χρησιμοποιήσουμε το Let's Encrypt, εγκαθιστούμε το Certbot:

```
sudo apt install snapd
```

```
sudo snap install --classic certbot
```

```
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

Τρέχουμε την εντολή:

```
sudo certbot --apache
```

Θα μας ζητηθεί ένα email, συμφωνία με Terms και έπειτα θα εντοπίσει το domain μας και θα εκδώσει το πιστοποιητικό, προσθέτοντάς το παράλληλα στο αρχείο **-le-ssl.conf*

4. Τροποποιείτε κατάλληλα τον web-server σας να υποστηρίζει https συνδέσεις.

Τροποποιούμε το αρχείο **-le-ssl.conf*, που προέκυψε μετά την έκδοση του πιστοποιητικού, στο */etc/apache2/sites-available/* ως εξής:

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName agiskol.ddns.net
    ServerAlias www.agiskol.ddns.net
    DocumentRoot /var/www/html/joomla
    <Directory /var/www/html/joomla>
        Allowoverride all
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLCertificateFile /etc/letsencrypt/live/agiskol.ddns.net/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/agiskol.ddns.net/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf
</VirtualHost>
```

5. Τροποποιείτε κατάλληλα τον web-server σας να υποστηρίζει redirection από http => https συνδέσεις.

Τροποποιούμε το αρχείο στο */etc/apache2/sites-enabled/* ως εξής:

```
<VirtualHost *:80>
    ServerName agiskol.ddns.net
    Redirect permanent / https://agiskol.ddns.net/
</VirtualHost>
```

Επανεκκινούμε το apache2.service



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

6. Τροποποιείτε κατάλληλα το firewall σας να επιτρέπει πρόσβαση στα ports 443,80.

Προσθέτουμε τους εξής κανόνες:

```
iptables -A firewall.rules -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A firewall.rules -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Ισχυροποίηση Ασφάλειας

Κάνοντας ένα αρχικό scan και ακολουθώντας τις προτάσεις του Mozilla Observatory, προσθέτουμε τα εξής στο `/etc/apache2/conf-enabled/security.conf`:

```
Header set X-Frame-Options "SAMEORIGIN"
Header set X-XSS-Protection "1;mode=block"
Header set X-Content-Type-Options: "nosniff"
Header always set Content-Security-Policy: "frame-ancestors 'self';script-src 'strict-dynamic'
'nonce-rAnd0m123' 'unsafe-inline'
http: https;;object-src 'none';base-uri 'none';require-trusted-types-for 'script';report-uri
https://csp.example.com;"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
Header always set Referrer-Policy "strict-origin"
Header always set Permissions-Policy "geolocation=(),midi=(),sync-
xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=
(),fullscreen=(self),payment=()"
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;SameSite=Strict;
```

Ενεργοποιούμε τα headers, security.conf και επανεκκινούμε το apache2.service:

```
sudo a2enmod headers
```

```
sudo a2enconf security.conf
```

```
sudo systemctl restart apache2.service
```


Τέλος αλλάζουμε το `/var/www/html/joomla/robots.txt`

- Μεγιστοποίηση της βαθμολογίας στο παρατηρητήριο της Mozilla.

Observatory
moz://a

[HTTP Observatory](#) [TLS Observatory](#) [SSH Observatory](#) [Third-](#)

Scan Summary



Host:	agiskol.ddns.net
Scan ID #:	45993742 (unlisted)
Start Time:	December 31, 2023 1:43 AM
Duration:	1870 seconds
Score:	115/100
Tests Passed:	11/11

Εικόνα 1: Grade from Mozilla Observatory



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

- Υποστήριξη μόνο TLSv1.3 πρωτοκόλλου και μόνο των recommended ciphersuite του TLS1.2.

[HTTPS] agiskol.ddns.net (31/12/2023 00:07:54 +00:00)

A+


83.212.72.199 : 443 (agiskol.ddns.net)

Name	Key exchange	Authentication	Encryption				MAC		PFS
			Type	Key size	Block size	Mode	Type	Size	
TLSv1.2									
<div><input checked="" type="checkbox"/> ECDHE-ECDSA-AES128-GCM-SHA256</div>	ECDH	ECDSA	AES	128	128	GCM	SHA256	256	PI
<div><input checked="" type="checkbox"/> ECDHE-ECDSA-AES256-GCM-SHA384</div>	ECDH	ECDSA	AES	256	128	GCM	SHA384	384	PI
<div><input checked="" type="checkbox"/> ECDHE-ECDSA-CHACHA20-POLY1305</div>	ECDH	ECDSA	CHACHA20	256	stream	AEAD	POLY1305	128	PI

Εικόνα 2: Grade from Cryptcheck

- Μεγιστοποίηση της προστασίας των HTTP επικεφαλίδων

Security Report Summary



Site: <https://agiskol.ddns.net/>

IP Address: 83.212.72.199

Report Time: 31 Dec 2023 11:57:50 UTC

Headers: ☒ Content-Security-Policy ☒ Referrer-Policy ☒ Permissions-Policy ☒ X-Frame-Options
☒ X-Content-Type-Options ☒ Strict-Transport-Security


Advanced: Wow, amazing grade! Perform a deeper security analysis of your website and APIs: [Try it](#)

Εικόνα 3: Grade from Securityheaders

- Ανάλυση του πιστοποιητικού

Summary

Overall Rating



Certificate: 100

Protocol Support: 100

Key Exchange: 80

Cipher Strength: 80

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.3.

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0xc1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_AES_256_GCM_SHA384 (0xc1302)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0xc1303)	ECDH x25519 (eq. 3072 bits RSA)	FS	256

TLS 1.2 (server has no preference)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp521r1 (eq. 15360 bits RSA)	FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp521r1 (eq. 15360 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a9)	ECDH secp521r1 (eq. 15360 bits RSA)	FS	256

Εικόνα 4: Grade from SSLlabs