

Σύγχρονες Εφαρμογές Ασφάλειας

Ονοματεπώνυμο : Νικόλας Φιλιππάτος

AM: 1072754

Εργασία: 7η

- [Εργαλεία](#)
 - [Ασκήσεις](#)
 - [1. εγκατάσταση apache](#)
 - [2. Develop Website](#)
 - [3 FQDN](#)
 - [4 https connections](#)
 - [5. https redirection](#)
 - [6. firewall ports 443, 80](#)
 - [Strengthening Security](#)
 - [Mozilla Observer](#)
 - [SSL Labs](#)
 - [Support of ciphers](#)
 - [Security Headers](#)
 - [cryptcheck.fr](#)
-

Εργαλεία

1. Ανάλυση Ασφάλειας Ιστοσελίδων από την Mozilla.

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.

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

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

4. Ανάλυση χρήσης/υποστήριξης ciphersuites

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

Ασκησεις

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.
2. Χρησιμοποιώντας την έτοιμη σουίτα κατασκευής ιστοσελίδων joomla ή wordpress αναπτύξτε μια προσωποποιημένη ιστοσελίδα.
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.
4. Τροποποιείστε κατάλληλα τον web-server σας να υποστηρίζει https συνδέσεις.
5. Τροποποιείστε κατάλληλα τον web-server σας να υποστηρίζει redirection από http => https συνδέσεις.
6. Τροποποιείστε κατάλληλα το firewall σας να επιτρέπει πρόσβαση στα ports 443,80.

Διαμορφώστε τις παραμέτρους του λογισμικού Apache, για

- την μεγιστοποίηση της βαθμολογίας στο παρατηρητήριο της Mozilla. (<https://observatory.mozilla.org/>)
- Την υποστήριξη μόνο TLSv1.3 πρωτοκόλλου και μόνο των recommended cipher suite του TLS1.2. (<https://cryptcheck.fr/>)
- Μεγιστοποίηση της προστασίας των HTTP επικεφαλίδων (<https://securityheaders.com/>)
- Πραγματοποιήστε ανάλυση του πιστοποιητικού (<https://www.ssllabs.com/ssltest/>)

Υπόδειξη:

Τα αρχεία που πρέπει να τροποποιήσετε είναι:

```
/etc/apache2/apache2.conf (παραμετροποίηση http headere)
/etc/apache2/mods-enabled/ssl.conf (παραμετροποίηση ciphersuites)
/etc/apache2/sites-enabled/default-ssl.conf (εισαγωγή πιστοποιητικού που θα χρησιμοποιεί)
/etc/apache2/sites-enabled/000-default.conf (redirection)
```

Σημείωση:

Εκτός από το παρατηρητήριο της Mozilla μπορείτε να πειραματιστείτε με τα παρακάτω εργαλεία:

<https://github.com/drwetter/testssl.sh>

<https://github.com/narbehaj/ssl-checker>

<https://portswigger.net/burp/communitydownload> (Burp Suite Community Edition)

1. εγκατασταση apache

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
```

```
sudo systemctl start apache2
```

```
sudo systemctl enable apache2
```

2. Develop Website

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

Installing joomla

Installing php

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

Ελεγχουμε οτι η php εγκατασταθηκε σωστα

```
php -v
```

```
PHP 8.2.7 (cli) (built: Jun 9 2023 19:37:27) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.2.7, Copyright (c) Zend Technologies
    with Zend OPcache v8.2.7, Copyright (c), by Zend Technologies
```

Installing MariaDB

```
sudo apt install mariadb-server mariadb-client
```

Enabling MariaDB

```
sudo systemctl start mariadb
sudo systemctl enable mariadb
```

```
sudo systemctl status mariadb
```

Creating a new database and database user for the joomla installation

```
sudo mysql -u root
```

Run the following once connected to MariaDB shell

Username and passwords redacted.

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

Output :

```
MariaDB [(none)]> CREATE DATABASE db_name;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> CREATE USER username@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.152 sec)

MariaDB [(none)]> GRANT ALL on db_name.* to username@localhost;
Query OK, 0 rows affected (0.011 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)
```

Download Joomla

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

Create the directory for the joomla

```
sudo mkdir /var/www/html/joomla
```

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

Changing the owner and the correct permissions

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

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

```
sudo systemctl restart apache2
```

Configuring the apache configuration file

```
sudo vim /etc/apache2/sites-available/joomla.conf
```


```
<VirtualHost *:80>
    ServerName nikolasfil.myddns.me
    ServerAdmin webmaster@nikolasfil.myddns.me
    ServerAlias www.nikolasfil.myddns.me
    DocumentRoot /var/www/html/joomla
    RewriteEngine On
    RewriteCond %{HTTPS} !=on
    RewriteCond %{HTTP_HOST} !^(localhost|127.0.0.1)
    RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>
```

Disabling the default configuration file, and enable the Joomla virtual host file :

```
sudo a2dissite 000-default.conf
```

```
sudo a2ensite joomla.conf
```

Acceding the site now will give this menu


 Login Data

Enter the real name of your Super User. *

Please fill in this field.

Set the username for your Super User account. *

Set the password for your Super User account. *



Enter at least 12 characters.

Enter the email address of the website Super User. *

Setup Database Connection >

3 FQDN

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.

Using Nolo, we get a domain for our cloud machine

Domain obtained:

nikolasfil.myddns.me

Modify Hostname: nikolasfil.myddns.me

IPv4 Address ⓘ

83.212.81.217

Last Update ⓘ

Dec 16, 2023
14:33 PST

☐ Offline ⓘ [Upgrade to Enhanced](#) to enable offline settings.

MX Records

[+ Add MX Records](#)

Set up a free domain with noip. Since the ip is static we only need to assign it once.

To set up let's encrypt we need Cerbot

```
sudo apt install snapd
```

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

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

Ran this to get only a certificate

```
sudo certbot --apache
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
```

```
Which names would you like to activate HTTPS for?
```

```
We recommend selecting either all domains, or all domains in a VirtualHost/server block.
```

```
1: nikolasfil.myddns.me
```

```
Select the appropriate numbers separated by commas and/or spaces, or leave input
```

```
blank to select all options shown (Enter 'c' to cancel):
```

```
Requesting a certificate for nikolasfil.myddns.me
```

```
Successfully received certificate.
```

```
Certificate is saved at: /etc/letsencrypt/live/nikolasfil.myddns.me-0001/fullchain.pem
```

```
Key is saved at: /etc/letsencrypt/live/nikolasfil.myddns.me-0001/privkey.pem
```

```
This certificate expires on 2024-03-17.
```

```
These files will be updated when the certificate renews.
```

```
Certbot has set up a scheduled task to automatically renew this certificate in the background.
```

```
Deploying certificate
```

```
Successfully deployed certificate for nikolasfil.myddns.me to /etc/apache2/sites-available/joomla-le-ssl.conf
```

```
Congratulations! You have successfully enabled HTTPS on https://nikolasfil.myddns.me
```

```
If you like Certbot, please consider supporting our work by:
```

```
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
```

```
* Donating to EFF: https://eff.org/donate-le
```

The following command is for updating to be able to get an email for expiring services

```
cerbot update_account --email your@mail.com
```

So now on the `/etc/letsencrypt/live/nikolasfil.myddns.me/` we have our files.

And our site is secure :

nikolasfil.myddns.me

Security

nikolasfil.myddns.me

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

[Learn more](#)

Certificate is valid

Certificate Viewer: nikolasfil.myddns.me

General

Details

Issued To

Common Name (CN)

Organization (O)

Organizational Unit (OU)

nikolasfil.myddns.me

<Not Part Of Certificate>

<Not Part Of Certificate>

Issued By

Common Name (CN)

Organization (O)

Organizational Unit (OU)

R3

Let's Encrypt

<Not Part Of Certificate>

Validity Period

Issued On

Expires On

Tuesday, December 19, 2023 at 1:10:59 AM

Monday, March 18, 2024 at 1:10:58 AM

SHA-256 Fingerprints

Certificate

Public Key

63de7382e3e4896af536b899924873773ed255d4f5b0bb3e8de93fa2093cf92

d349997838a42a8e4ab83bc0e6ea3223940f48e8b8d020cb646f5431ee065900

4 https connections

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

Αλλαζουμε το αρχαιο των available sites που προβαλλει το joomla

```
sudo vim /etc/apache2/sites-available/joomla-le-ssl.conf
```

```
<VirtualHost *:443>
    ServerName nikolasfil.myddns.me
    ServerAdmin webmaster@nikolasfil.myddns.me
    DocumentRoot /var/www/html/joomla
    ServerAlias www.nikolasfil.myddns.me
    <Directory /var/www/html/joomla>
        AllowOverride all
    </Directory>

    SSLCertificateFile /etc/letsencrypt/live/nikolasfil.myddns.me-0001/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/nikolasfil.myddns.me-0001/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf

</VirtualHost>
```

5. https redirection

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

Τροποποιουμε τα /etc/apache2/sites-enabled/ configuration files για να κανει http redirect

```
sudo vim joomla-le-ssl.conf
```

```
<VirtualHost *:80>
    ServerName nikolasfil.myddns.me
    Redirect permanent / https://nikolasfil.myddns.me
</VirtualHost>
```

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

6. firewall ports 443, 80

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

```
sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Based on [this](#) --conntrack superseded state .

Updating firewall

in `/etc/rc.local`

```
#!/bin/bash
```

```
# Clear out the firewall
```

```
iptables -t filter -F  
iptables -t filter -X
```

```
# Create a custom table
```

```
iptables -t filter -N fire.rules
```

```
# Accept every incoming that is already established or is Related
```

```
iptables -A fire.rules -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
# Accept ssh only from Uni IP and from house
```

```
iptables -A fire.rules -p tcp --dport 22 -s 150.140.0.0/16 -j ACCEPT
```

```
iptables -A fire.rules -p tcp --dport 22 -s 94.66.220.0/24 -j ACCEPT
```

```
# Have accepted only pubkey auth, because of problems with openvpn
```

```
# Change it so that it will be able to find the NAT
```

```
# Accept udp only on port 53
```

```
iptables -A fire.rules -p udp --dport 53 -j ACCEPT
```

```
# for apt
```

```
iptables -A fire.rules -p tcp --dport 53 -j ACCEPT
```

```
# Accept all the traffic from localhost
```

```
iptables -A fire.rules -p all -s 192.168.0.0/16 -j ACCEPT
```

```
iptables -A fire.rules -p all -s 127.0.0.1 -j ACCEPT
```

```
# Giving access to webserver
```

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

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

```
# Enabling the custom firewall
```

```
iptables -I INPUT -j fire.rules
```

```
iptables -I FORWARD -j fire.rules
```

```
# Policies
```

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT ACCEPT
```

```
sudo -s source /etc/rc.local
```

Strengthening Security

[infosec Mozilla](#)

Adding the following configurations to the apache2 server settings, per the results of the initial observatory.I

```
sudo vim /etc/apache2/conf-enabled/headers.conf
```

```
Header set X-Frame-Options "SAMEORIGIN"
Header set X-XSS-Protection "1;mode=block"
```

```
sudo vim /etc/apache2/conf-enabled/security.conf
```

```
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;
```

We enable the headers and security conf with :

```
sudo a2enconf headers
sudo a2enconf security
```

We can also disable them with

```
sudo a2disconf headers
```

Reload apache2

```
sudo systemctl reload apache2.service
```

Changed the `/var/www/html/joomla/robots.txt`

```
sudo vim /var/www/html/joomla/robots.txt
```

```
# Stop all search engines from crawling this site
User-agent: *
Disallow: /
```

Disallow the whole directory and not specific folders, as it is still readable from attackers

Security Checkers

Mozilla Observer

[observatory](#)

Observatory

mozilla

HomeFAQStatisticsAbout

HTTP Observatory

TLS Observatory

SSH Observatory

Third-party Tests

Scan Summary

A⁺

Host:

nikolasfil.myddns.me

Scan ID #:

45658820

Start Time:

December 21, 2023 12:02 AM

Duration:

831 seconds

Score:

115/100

Tests Passed:

11/11

Recommendation

Initiate Rescan

Almost there!

Your current CSP policy allows the use of `'unsafe-inline'` inside of `style-src`. Moving `style` attributes into external stylesheets not only makes you safer, but also makes your code easier to maintain.

- Mozilla Web Security Guidelines (Content Security Policy)
- An Introduction to Content Security Policy
- Google CSP Evaluator

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Reason	Info
------	------	-------	--------	------

SSL Labs

[ssllabs](#)

Security Report Summary

A⁺

Site:

<https://nikolasfil.myddns.me/>

IP Address:

83.212.81.217

Report Time:

20 Dec 2023 22:07:19 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 Now

Configuration

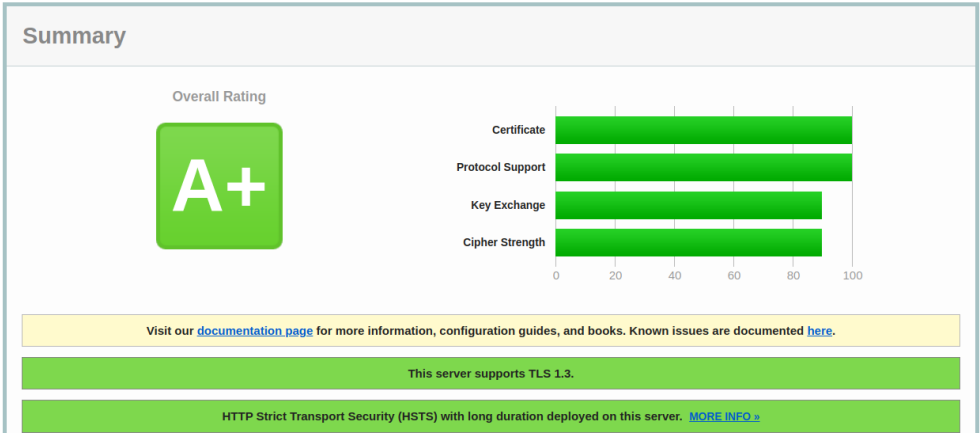
Protocols

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 (0x1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	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 (0xcca9)	ECDH secp521r1 (eq. 15360 bits RSA)	FS	256

Support of ciphers



Security Headers

[Security Headers](#)

Security Report Summary

A+

Site:

<https://nikolasfil.myddns.me/>

IP Address:

83.212.81.217

Report Time:

22 Dec 2023 16:44:27 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 Now

cryptcheck.fr

[cryptcheck](#)

[HTTPS] nikolasfil.myddns.me (22/12/2023 16:47:33 +00:00)

Refresh available at 17:47:33

A+ 83.212.81.217 : 443 (nikolasfil.myddns.me)

Name	Key exchange	Authentication	Encryption				MAC		
			Type	Key size	Block size	Mode	Type	Size	PFS
TLSv1.2									
■ ECDHE-ECDSA-AES128-GCM-SHA256	ECDH	ECDSA	AES	128	128	GCM	SHA256	256	PFS
■ ECDHE-ECDSA-AES256-GCM-SHA384	ECDH	ECDSA	AES	256	128	GCM	SHA384	384	PFS
■ ECDHE-ECDSA-CHACHA20-POLY1305	ECDH	ECDSA	CHACHA20	256	stream	AEAD	POLY1305	128	PFS