



Πανεπιστήμιο Δυτικής Αττικής
Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Υπολογιστών

Εργαστήριο Ασφάλειας στην Τεχνολογία της Πληροφορίας – Εργασία 5

Χρήστος Μαργιώλης – 19390133

Ιούνιος 2023

Περιεχόμενα

1	Εργαλεία	2
2	Άσκηση 1	2
2.1	Εργαλείο 1	2
2.2	Εργαλείο 2	3
3	Άσκηση 2	3
3.1	Εργαλείο 1	3
3.2	Εργαλείο 2	4
4	Άσκηση 3	4
4.1	Εργαλείο 1	5
4.2	Εργαλείο 2	6

1 Εργαλεία

Τα δύο εργαλεία που χρησιμοποιήθηκαν για την εργασία είναι το

- <https://www.ssllabs.com/ssltest>
- <https://www.sslshopper.com/ssl-checker.html>

Το πρώτο εργαλείο πραγματοποιεί αρκετά πιο εκτενείς ελέγχους.

2 Άσκηση 1

Το ηλεκτρονικό μαγαζί που θα ελεγχθεί είναι το skroutz.gr.

2.1 Εργαλείο 1

SSL Report: www.skroutz.gr

Assessed on: Sun, 18 Jun 2023 16:25:15 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	2606:4700:0:0:0:6812:134b Ready	Sun, 18 Jun 2023 16:15:33 UTC Duration: 144.930 sec	A
2	2606:4700:0:0:0:6812:124b Ready	Sun, 18 Jun 2023 16:17:58 UTC Duration: 144.483 sec	A
3	104.18.19.75 Ready	Sun, 18 Jun 2023 16:20:23 UTC Duration: 146.218 sec	A+
4	104.18.18.75 Ready	Sun, 18 Jun 2023 16:22:49 UTC Duration: 145.916 sec	A+

2.2 Εργαλείο 2

Server Hostname

Check SSL

These results were cached from June 15, 2023, 10:02 am PST to conserve server resources.

If you are diagnosing a certificate installation problem, you can get uncached results by [clicking here](#).



skroutz.gr resolves to 185.6.76.42



The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).



The certificate will expire in 145 days.

[Remind me](#)



The hostname (skroutz.gr) is correctly listed in the certificate.

3 Άσκηση 2

Η ειδησεογραφική σελίδα που θα ελεγχθεί είναι το CNN.


3.1 Εργαλείο 1


	Server	Test time	Grade
1	151.101.195.5 Ready	Sun, 18 Jun 2023 16:25:53 UTC Duration: 103.358 sec	A
2	151.101.3.5 Ready	Sun, 18 Jun 2023 16:27:36 UTC Duration: 103.446 sec	A


3.2 Εργαλείο 2


Server Hostname

Check SSL


 edition.cnn.com resolves to 151.101.3.5

 Server Type: Varnish


 The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).

 The certificate was issued by GlobalSign.

Write review of GlobalSign

 The certificate will expire in 206 days.

Remind me


 The hostname (edition.cnn.com) is correctly listed in the certificate.

4 Άσκηση 3


Η πανεπιστημιακή σελίδα που θα ελεγχθεί είναι το uniwa.gr.

4.1 Εργαλείο 1

Certificate #1: RSA 2048 bits (SHA384withRSA)



Server Key and Certificate #1



Subject	*.uniwa.gr Fingerprint SHA256: c1346ac88e2b64869c90b79e2b27e49b2d51dc3fad08eb3d7cf362899053a491 Pin SHA256: Y1B5NyEBG6d/OQr3ud7gOt68AmSYWVAAu02um8lpluQ=
Common names	*.uniwa.gr
Alternative names	*.uniwa.gr uniwa.gr
Serial Number	60ca8d4620e4e3275fe361197a43cdbb
Valid from	Tue, 20 Sep 2022 00:00:00 UTC
Valid until	Wed, 20 Sep 2023 23:59:59 UTC (expires in 3 months and 2 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GEANT OV RSA CA 4 AIA: http://GEANT.crl.sectigo.com/GEANTOVRSA4.crl
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://GEANT.crl.sectigo.com/GEANTOVRSA4.crl OCSP: http://GEANT.ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

4.2 Εργαλείο 2

[More information About the SSL Checker](#)

Server Hostname

Check SSL



uniwa.gr resolves to 195.130.100.83



Server Type: nginx



The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).



The certificate will expire in 94 days.

Remind me



The hostname (uniwa.gr) is correctly listed in the certificate.



One of the certificates is signed with a SHA1 signature. We recommend that you reissue or replace this certificate with one that uses a SHA-2 signature. Contact your SSL provider about how to do this. [Read more about the SHA-1 deprecation here.](#)