

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 | 'Ασκηση 1 2.1 Εργαλείο 1 | 2 2 3 | | |
| 3 | 'Ασκηση 2 3.1 Εργαλείο 1 | | | |
| 4 | 'Ασκηση 3 4.1 Εργαλείο 1 | | | |

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 αρχετά πιο εχτενείς ελέγχους.

2 'Ασκηση 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 | Α |
| 2 | 2606:4700:0:0:0:6812:124b Ready | Sun, 18 Jun 2023 16:17:58 UTC Duration: 144.483 sec | Α |
| 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



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.

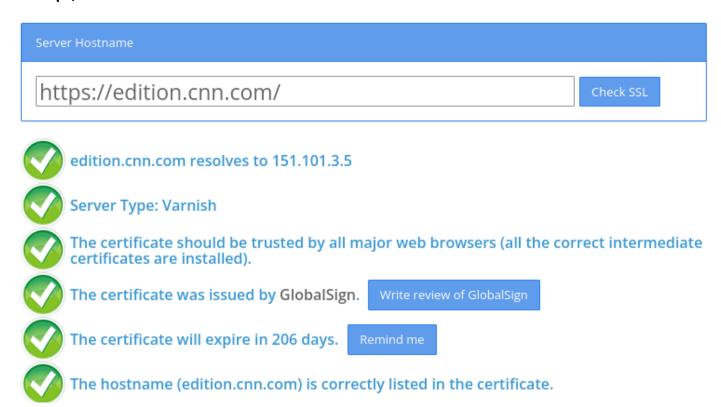
3 'Ασκηση 2

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 | Α |
| 2 | 151.101.3.5 Ready | Sun, 18 Jun 2023 16:27:36 UTC Duration: 103.446 sec | Α |

3.2 Εργαλείο 2



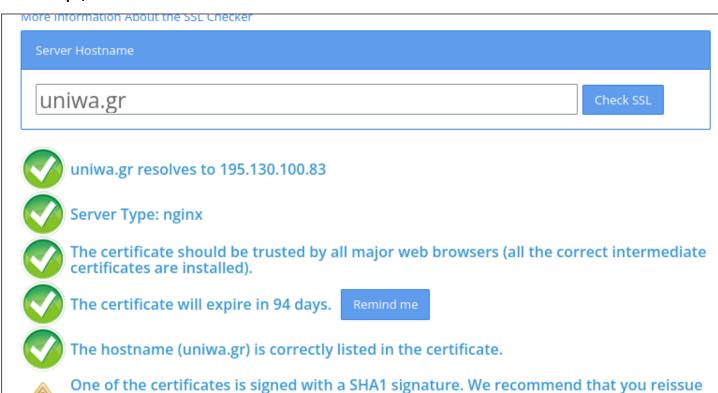
4 'Ασκηση 3

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

4.1 Εργαλείο 1

Certificate #1: RSA 2048 bits (SHA384withRSA) Server Key and Certificate #1 *.uniwa.gr Subject Fingerprint SHA256: c1346ac88e2b64869c90b79e2b27e49b2d51dc3fad08eb3d7cf362899053a491 Pin SHA256: Y1B5NyEBG6d/OQr3ud7gOt68AmSYWVAAu02um8lpluQ= Common names *.uniwa.gr Alternative names *.uniwa.gr uniwa.gr 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 GEANT OV RSA CA 4 Issuer AIA: http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt Signature algorithm SHA384withRSA Extended Validation Certificate Transparency Yes (certificate) OCSP Must Staple CRL, OCSP Revocation information CRL: http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl OCSP: http://GEANT.ocsp.sectigo.com Revocation status Good (not revoked) DNS CAA No (more info) Trusted Mozilla Apple Android Java Windows

4.2 Εργαλείο 2



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.