

# Έλεγχος ασφάλειας

1<sup>η</sup> εβδομαδιαία εργασία

**Φίλιππος Δουραχαλής**

**Χρήστος Αργυρόπουλος**

**Αλέξανδρος Κάρρας**

## Φάση 1. Μηχανές Αναζήτησης

Εργαλεία που χρησιμοποιήθηκαν:

- Google
- Shodan HQ
- netcraft

Αρχικά ανοίγουμε το site απευθείας στον browser και αναζητούμε πληροφορίες που θα μπορούσαμε να χρησιμοποιήσουμε στις επόμενες φάσεις, απευθείας μέσω αυτού. Τέτοιες πληροφορίες είναι μεταξύ άλλων, το αντικείμενο της σελίδας, το προσωπικό του εργαστηρίου, πληροφορίες τοποθεσίας, τηλέφωνα κτλ. Επίσης αναζητούμε το domain σε μηχανές αναζήτησης όπως το netcraft και το Shodan HQ για να βρούμε στοιχεία που θα μπορούσαν να είναι χρήσιμα στην συνέχεια. Το output των εργαλείων φαίνεται στην συνέχεια. Τέλος προβάλλαμε τον πηγαίο κώδικα της αρχικής σελίδας για να αναζητήσουμε frameworks που χρησιμοποιούνται και κλήσεις μεθόδων. Παρατηρούμε ότι η σελίδα χρησιμοποιεί JQuery για την φόρτωση στοιχείων της σελίδας και το Joomla, γεγονός που επιβεβαιώνει και το output των εργαλείων στην 4<sup>η</sup> φάση. Αναζητήσαμε επίσης σχόλια στον κώδικα, χωρίς να εντοπίσουμε κάποιο που παρουσίασε ιδιαίτερο ενδιαφέρον.

## Φάση 2. Google Hacking

Στην συγκεκριμένη φάση χρησιμοποιήσαμε την προχωρημένη αναζήτηση Google για να ανακαλύψουμε περισσότερες πληροφορίες σχετικά με τα endpoints του website, τα πιθανά χρήσιμα αρχεία που φιλοξενεί και τις σελίδες που θα μπορούσαμε να αξιοποιήσουμε, όπως σελίδες που απαιτούν αυθεντικοποίηση. Τα ερωτήματα που χρησιμοποιήσαμε ήταν τα ακόλουθα:

- site:infosec.aueb.gr filetype:log
- site:infosec.aueb.gr inurl:login OR inurl:signin OR intitle:login OR intitle:signin
- site:infosec.aueb.gr inurl:admin OR inurl:administrator
- site:infosec.aueb.gr intitle:"401" OR intitle:"Forbidden"
- ip:195.251.252.250
- filetype:pdf

Τα 4 πρώτα ερωτήματα δεν επιστρέφουν κανένα αποτέλεσμα. Ωστόσο για το τελευταίο υπάρχουν 483 αποτελέσματα, από όπου μπορούμε να εξάγουμε στοιχεία όπως:

- a) Τη φυσική τοποθεσία: Πατησίων 76, Αθήνα, 104 34, Ελλάδα
- b) Τους λοιπούς συνεργάτες που δεν φαίνονται στη λίστα Προσωπικού, τις συνεργασίες με φορείς/επιχειρήσεις/εκδοτικούς οίκους και Οργανισμούς από τις βάσεις δεδομένων των οποίων μπορούμε να αντλήσουμε επιπλέον στοιχεία, αποθηκευμένα. Από αυτά τα δεδομένα μπορούμε να εξάγουμε τις ακόλουθες πληροφορίες.

### Φάση 3. Social Networks

Σε αυτήν την φάση χρησιμοποιήσαμε κοινωνικά δίκτυα όπως LinkedIn, Facebook και Twitter για να αναζητήσουμε τα πρόσωπα που είχαμε βρει στις προηγούμενες φάσεις και να καταγράψουμε πληροφορίες όπως email, ενδιαφέροντα, τομείς απασχόλησης, θέση στους οργανισμούς όπου απασχολούνται κ.τ.λ.

### Φάση 4. Website footprinting

Εργαλεία που χρησιμοποιήθηκαν:

- Curl
- Nmap
- Dirbuster
- BurpSuite
- OWASP Zap
- WhatWeb
- ipinfo.io
- Shodan HQ
- Netcraft

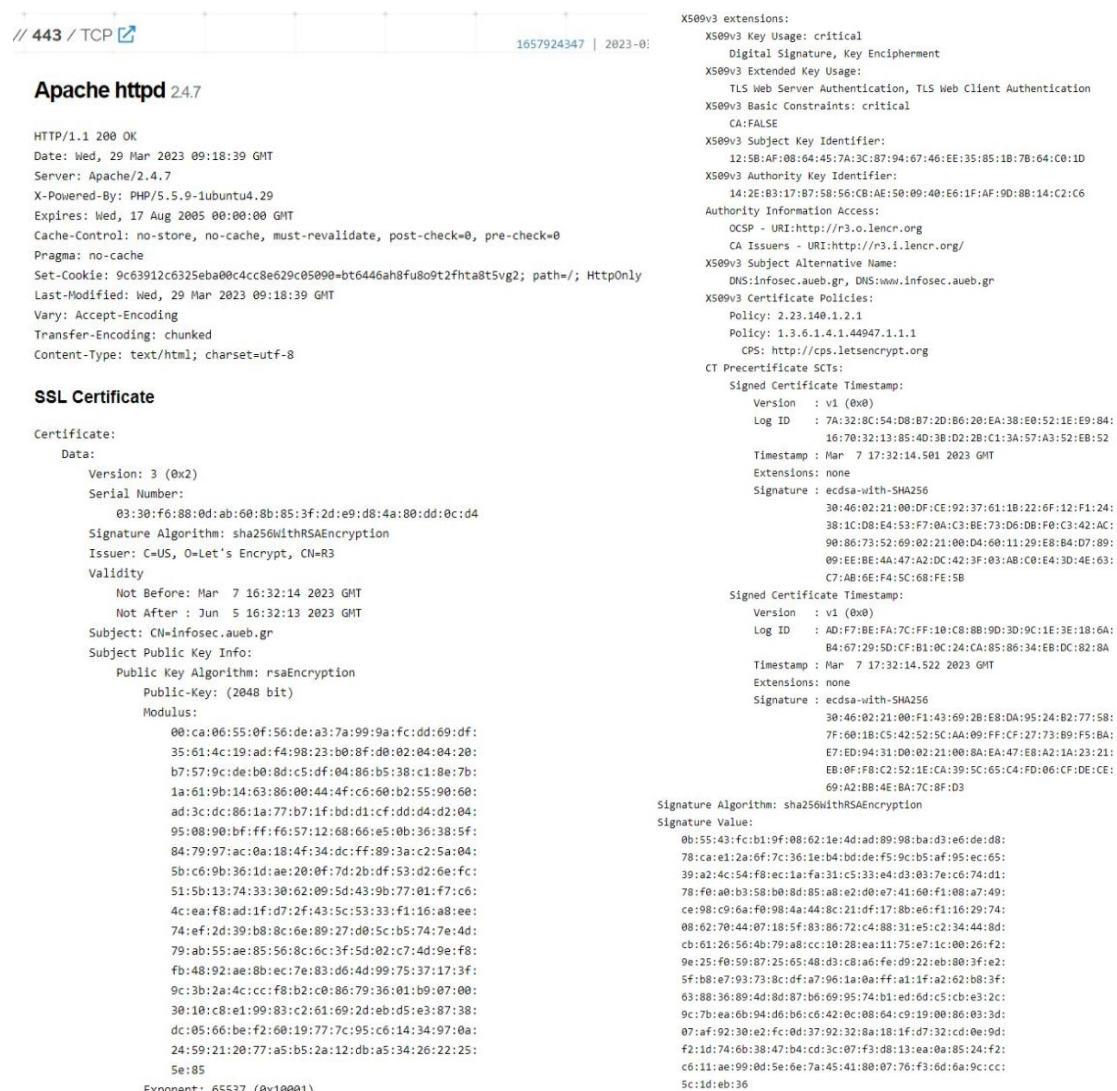
Το curl εμφανίζει τις ακόλουθες πληροφορίες για το domain:

```
(kali㉿kali)-[~]
└─$ curl -I https://infosec.aueb.gr -k
HTTP/1.1 200 OK
Date: Fri, 07 Apr 2023 13:14:17 GMT
Server: Apache/2.4.7
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 9c63912c6325eba00c4cc8e629c05090=iigmr8asb7d5mdrncgru7bkr3; path=/; HttpOnly
Last-Modified: Fri, 07 Apr 2023 13:14:17 GMT
Content-Type: text/html; charset=utf-8
```

Για να ανακαλύψουμε τις τεχνικές λεπτομέρειες, εκτελούμε την ακόλουθη εντολή στο nmap:

*"nmap -A -p- infosec.aueb.gr"*





[View Report](#) [View on Map](#)

**Product Spotlight:** Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

**Αρχική**  
195.251.252.250  
infosec.aueb.gr  
www.infosec.aueb.gr  
Athens University of  
Economics and Business  
Greece, Athens

#### SSL Certificate

Issued By:  
Common Name:  
**R3**

Organization:  
**Let's Encrypt**

Issued To:  
Common Name:  
**infosec.aueb.gr**

Supported SSL Versions:  
**SSLv3, TLSv1, TLSv1.1, TLSv1.2**

HTTP/1.1 200 OK  
Date: Wed, 29 Mar 2023 09:18:39 GMT  
Server: Apache/2.4.7  
X-Powered-By: PHP/5.5.9-1ubuntu4.29  
Expires: Wed, 17 Aug 2005 00:00:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Set-Cookie: 9c63912c6325eba00c4cc8e629c05090=bt6446ah8fu809t2fhta8t5vg2; path=/; HttpOnly

2023-03-29T09:19:02.932962Z

Figure 2 Shodan HQ results for infosec.aueb.gr

Χρησιμοποιήσαμε επίσης το BurpSuite για να χαρτογραφήσουμε τα διαθέσιμα endpoints. Το μειονέκτημά στην χρήση του συγκεκριμένου εργαλείου ωστόσο είναι ότι το αυτόματο scanning δεν είναι διαθέσιμο στο community edition, επομένως πρέπει χειροκίνητα να

εξερευνήσουμε τον ιστότοπο ώστε το Burp να συλλέξει πληροφορίες για αυτόν. Για τον λόγο αυτό χρησιμοποιήσαμε επίσης το OWASP Zarp, το οποίο μπορεί να αυτοματοποιήσει την διαδικασία για το website. Σε συνδυασμό με το DirBuster προσπαθήσαμε να ανακαλύψουμε κρυφά directories και subdomains που μπορεί να υπάρχουν. Τα αποτελέσματα των παραπάνω εργαλείων φαίνονται στην συνέχεια:

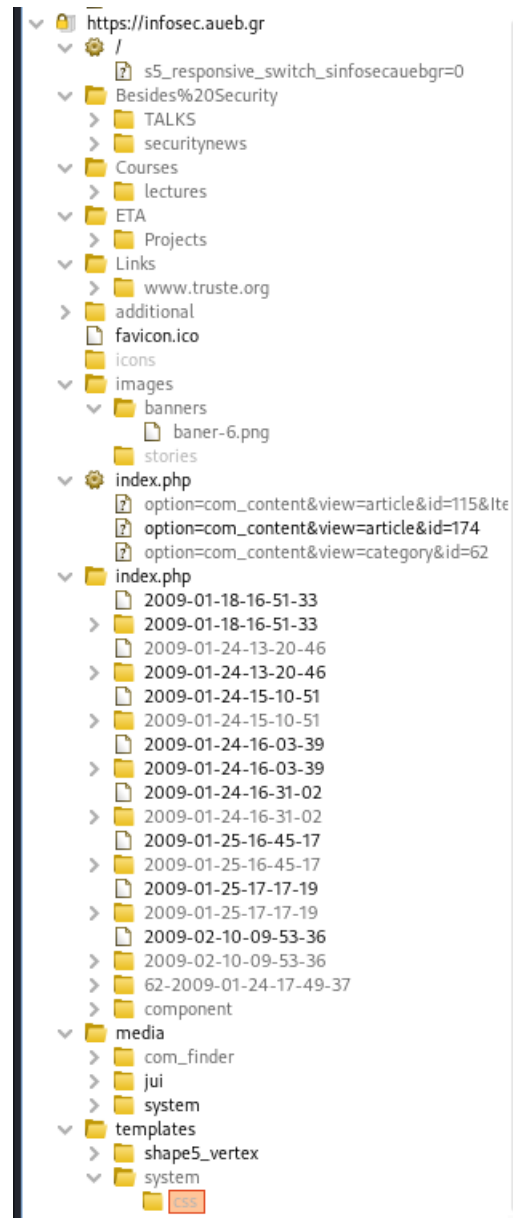


Figure 3 Burp directory listing for infosec.aueb.gr

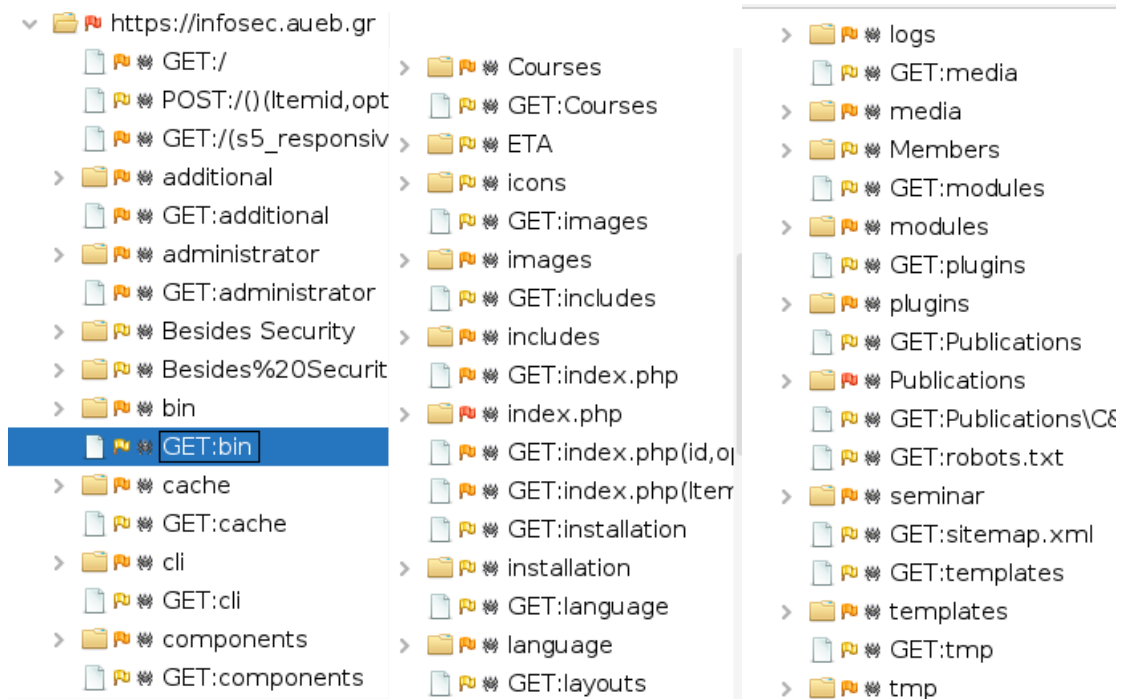


Figure 4 OWASP Zap directory listing for infosec.aueb.gr

```
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
File found: /index.php - 200
Dir found: /index.php/ - 200
File found: /index.php/2009-01-18-16-51-33/ - 200
Dir found: /index.php/2009-01-18-16-51-33/ - 200
File found: /index.php/2009-01-18-16-51-33/2009-01-18-17-09-15 - 200
File found: /index.php/2009-01-18-16-51-33/2009-01-24-11-44-12 - 200
File found: /index.php/2009-01-18-16-51-33/2009-01-18-17-13-22 - 200
File found: /index.php/2009-01-24-15-10-51 - 200
Dir found: /index.php/2009-01-24-15-10-51/ - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-46-21 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-46-52 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-47-22 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-47-52 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-48-27 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-48-57 - 200
File found: /index.php/2009-01-24-15-10-51/posters - 200
File found: /index.php/2009-01-24-15-10-51/2013-03-28-10-19-43 - 200
File found: /index.php/2009-01-24-15-10-51/2012-11-24-15-42-99 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-49-25 - 200
File found: /index.php/2009-01-24-15-10-51/2009-01-24-15-50-17 - 200
File found: /index.php/2009-01-25-16-45-17 - 200
Dir found: /index.php/2009-01-25-16-45-17/ - 200
File found: /index.php/2009-01-25-16-45-17/2009-01-25-16-52-56 - 200
File found: /index.php/2009-01-25-16-45-17/2009-01-25-17-00-19 - 200
File found: /index.php/2009-01-24-13-20-46/ - 200
Dir found: /index.php/2009-01-24-13-20-46/ - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55 - 200
Dir found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/ - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-20-19-16-12 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-56-20 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-56-57 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-57-53 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2022-03-01-14-58-21 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-58-20 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-58-19 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-14-53-55/2015-12-28-09-58-42 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-15-00-17 - 200
Dir found: /index.php/2009-01-24-13-20-46/2009-01-24-15-00-17/ - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-15-00-17/2015-12-28-10-00-19 - 200
File found: /index.php/2009-01-24-13-20-46/2009-01-24-15-02-17 - 200
File found: /index.php/2009-01-24-13-20-46/seminario-gpd - 200
File found: /index.php/2009-01-24-16-03-39 - 200
Dir found: /index.php/2009-01-24-16-03-39/ - 200
File found: /index.php/2009-01-24-16-03-39/-sites - 200
File found: /index.php/2009-01-24-16-03-39/2009-01-24-16-05-15 - 200
File found: /index.php/2009-01-24-16-31-02 - 200
Dir found: /index.php/2009-01-24-16-31-02/ - 200
File found: /index.php/2009-01-24-16-31-02/2009-01-24-16-31-42 - 200
File found: /index.php/2009-01-24-16-31-02/2009-01-24-16-32-31 - 200
File found: /index.php/2009-02-10-09-53-36 - 200
Dir found: /index.php/2009-02-10-09-53-36/ - 200
File found: /index.php/2009-02-10-09-53-36/2011 - 200
File found: /index.php/2009-02-10-09-53-36/2010 - 200
File found: /index.php/2009-02-10-09-53-36/2009 - 200
File found: /index.php/2009-02-10-09-53-36/2008 - 200
File found: /index.php/2009-02-10-09-53-36/2007 - 200
File found: /index.php/2009-02-10-09-53-36/2006 - 200
File found: /index.php/2009-01-25-17-17-19 - 200
Dir found: /index.php/62-2009-01-24-17-49-37/ - 200
DirBuster Stopped
```

Figure 5 Dirbuster directory listing for infosec.aueb.gr

Τέλος με το WhatWeb παίρνουμε αντίστοιχες πληροφορίες για τον server, όπως το λογισμικό και την έκδοση που τρέχει



```
(kali㉿kali)-[/opt/WhatWeb]
$ ./whatweb infosec.aueb.gr
http://infosec.aueb.gr [302 Found] Apache[2.4.7], Country[GREECE][GR], HTTPServer[Apache/2.4.7], IP[195.251.252.250], RedirectLocation[https://infosec.aueb.gr/], Title[302 Found]
https://infosec.aueb.gr/ [200 OK] Apache[2.4.7], Bootstrap, Cookies[9c63912c6325eba00c4cc8e629c05090], Country[GREECE][GR], HTML5, HTTPServer[Apache/2.4.7], HttpOnly[9c63912c6325eba00c4cc8e629c05090], IP[195.251.252.250], JQuery, probably Joomla[com_content], probably Mambo[com_content], Meta-Author[Administrator], MetaGenerator[ Joomla! - Open Source Content Management], PHP[5.5.9-1ubuntu4.29], Script[text/javascript], Title[Αρχική], X-Powered-By[PHP/5.5.9-1ubuntu4.29]
```

Figure 1 WhatWeb results for infosec.aueb.gr

## Φάση 5. E-mail footprinting

Εργαλεία που χρησιμοποιήθηκαν:

- theHarvester
- Gmail
- Ipinfo.io

Χρησιμοποιήσαμε το theHarvester για να προσπαθήσουμε να βρούμε πληροφορίες για το domain, ωστόσο δεν είχαμε κάποιο αποτέλεσμα.

Χρησιμοποιούμε το Gmail για να αναλύσουμε τον header ενός μηνύματος που έχει σταλεί από την διεύθυνση geostergior@aub.gr προκειμένου να εξάγουμε όσες περισσότερες πληροφορίες μπορούμε σχετικά με τον αποστολέα, το domain και τους e-mail servers.

Αναγνωριστικό μηνυμάτων	<4cdcf11ef00efc7cd441ac7773a8ed95@eclass.aueb.gr>
Διημερομηνήθηκε στις:	27 Μαρτίου 2023 στις 5:15 μ.μ. (Παραδόθηκε μετά από 2 δευτερόλεπτα)
Από:	"GEORGIOS STERGIOPOYLOS (μέσω: Open eClass του Οικονομικού Πανεπιστημίου Αθηνών)" <geostergiop@aub.gr>
Προς:	
Θέμα:	Μήνυμα εκπαιδευτή (INF447 - Έλεγχος Ασφάλειας 2023 - Ανακοίνωση)
SPF:	PASS με IP 195.251.255.106 <a href="#">Μάθετε περισσότερα</a>
DKIM:	'PASS' με τον τομέα aueb.gr <a href="#">Μάθετε περισσότερα</a>
DMARC:	'PASS' <a href="#">Μάθετε περισσότερα</a>
<p>Received: from 2023:a8a:55a:0:0:0:0 with SMTP ID y2c5cp51549780ct; Mon, 27 Mar 2023 07:15:10 -0700 (PDT) X-Google-Smtp-Source: AKy350a1943rVexqiaM02K/vXJ0s1RbkG3RyQ1ZmX8pqnHbvvKRB7uZz5QHvC9T3BEj6I/7FNU X-Received: by 2002:aad7:c948:0:b0:4fe:94a2:81be with SMTP ID h8-20020aa7c94800000b004fe94a281b6m11251712edt.7.1679926518466; Mon, 27 Mar 2023 07:15:10 -0700 (PDT) ARC-Seal: i=1; a=rsa-sha256; t=1679926510; cv=none; d=google.com; s=arc-20160816; b=YtU6URC4K0NHb0d9j2GdoB02rqGbE6oa1eCq7eHe6Ksvz40ZidxRAagN3109A3uJf 5tqHf3qBKVpoc31BH0f751rv/1ZNGMttDf/53wEf/H0N1Uy/Ny4uwwf882E9qhHf Ppy1/3Q9fZRF5S0q/1Fk6pYkU03C2G51DAuP/cN1nVUxy6d02jg1G8UuicgqK0TW TVpABq/cLm115bwnK5Z9MEHNM5d0DXXyI2V999Peet7Qs07/WkEh1Yxduh6Tmm6p2 59m6bI/CHOSG5/1UOFU4UvUeR0K8B0752uAZ6Ec1K4Pt0BJvLbtPv0FdG+SVQhX4b598 PILg== ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=mlme-version;from:subject:date:message-id:dkim-signature; b=h-bvUkX9SEZ9mcgpcv+P7j3Wf1E6dt4fcpq8W9M9y5; b=NfIgU1Vld28Jcheh/ps06pYGCpF3K9c5S9hBqJ8u1BK9amxaGw5DhQf95AR4 tqdG6wH61y1fNSubXFCgdUKZjyIvEfuGfZapbCf8v6c3IBC+142Qz1E+STP4ZG08ZXx Exu1CL+KpPfmcSV5H2m15F/En+plnH4HbftV8tVPB1sATAR3rK6cPcsU197Jhf/it8 68A1kHk1fxbhu9GctC9U0DM0wE5+6TbWfYmukbwggt72BstDv0v1KpV8u7HmNA3JU 0053990mL/fXZFSH5L+gXRK1I+/4wEwZY3B8Nu7BP8ZCEB5uXyK0h7Kwd0zBpxcVt+ KZ7A== ARC-Authentication-Results: i=1; mx.google.com; dkim=pass header.i=@aub.gr header.s=@01901 header.b=SUzRVfnt; spf=pass (google.com: domain of geostergiop@aub.gr designates 195.251.255.106 as permitted sender) smtp.mailfrom=geostergiop@aub.gr; dmarc=pass (p=NONE sp=NONE ds=NONE) header.From=aueb.gr Return-Path: &lt;geostergiop@aub.gr&gt; Received: from blade-b3-vm-relay.servers.aueb.gr (blade-b3-vm-relay.servers.aueb.gr. [195.251.255.106]) by mx.google.com with ESMTP ID a19-20020a1709064a5300b0093331f6c1ff518752972ejv.159.2023.03.27.07.15.10 for &lt;philip.d1510@gmail.com&gt;; Mon, 27 Mar 2023 07:15:10 -0700 (PDT) Received-SPF: pass (google.com: domain of geostergiop@aub.gr designates 195.251.255.106 as permitted sender) client-ip=195.251.255.106; Authentication-Results: mx.google.com; dkim=pass header.i=@aub.gr header.s=@01901 header.b=SUzRVfnt; spf=pass (google.com: domain of geostergiop@aub.gr designates 195.251.255.106 as permitted sender) smtp.mailfrom=geostergiop@aub.gr; dmarc=pass (p=NONE sp=NONE ds=NONE) header.From=aueb.gr Received: from blade-al-vm-smt servers.aueb.gr (blade-al-vm-smt.servers.aueb.gr [195.251.255.217]) by blade-b3-vm-relay.servers.aueb.gr (Postfix) with ESMTP ID DF61F2534; Mon, 27 Mar 2023 17:15:09 +0300 (EEST) DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=aueb.gr; s=@01901; t=1679926509; bh=Hirac/f68c8SmGjQuRUxhd13sGk8/RF1nIdtEtfM4; h=Date:Subject:From:From; b=SUzRVfnt0lnnGBEXZ8tsjtanGT9RgAPt/UfntlnRm6MqYVLMhJnp98EIA2I1 xfC69vUu+0Hkn0tqJCNcK3LECR0u/PwU/axhRblyf5x11Wp03waGn80Zm85g5eh pWf3JhV4VH8p9QzCccqHw/0d5um1k68h7JUNfUfpU28dCEgoz4Bn5yk5y6k gfu0mqZCk+vtEed48KkSdof54sfyfw4d52WdQYx5+UasD81dR07syeh2080p 1X6DzWahovf0LbArN2EQ+psY9zzMz93rMa1sW8N1Rj2q1j4t2IdzAHeC1j1j1 LSHauWwB9Naa== Received: from OpenEclass-web.servers.aueb.gr (openeclass-web.servers.aueb.gr [195.251.255.227]) (using TLSv1.2 with cipher ADH-AES256-GCM-SHA384 (256/256 bits)) (No client certificate required) (Authenticated sender: noclass); by blade-al-vm-smt.servers.aueb.gr (Postfix) with ESMTPS ID 103fD43C; Mon, 27 Mar 2023 17:15:09 +0300 (EEST) Received: by OpenEclass-web.servers.aueb.gr (Postfix, from userid 33) ID F2408081551; Mon, 27 Mar 2023 17:15:08 +0300 (EEST) Message-ID: &lt;4cdcf11ef00efc7cd441ac7773a8ed95@eclass.aueb.gr&gt; Date: Mon, 27 Mar 2023 17:15:08 +0300 Subject: Μήνυμα εκπαιδευτή (INF447 - Έλεγχος Ασφάλειας 2023 - Ανακοίνωση) From: "GEORGIOS STERGIOPOYLOS (μέσω: Open eClass του Οικονομικού Πανεπιστημίου Αθηνών)" &lt;geostergiop@aub.gr&gt; MIME-Version: 1.0 Content-Type: multipart/alternative; boundary=" " swift v4 1679926508 6e3b037f3e42fc661a15504ff6928cf - "</p>	

Figure 2 Gmail header analysis

Από την παραπάνω εικόνα μπορούμε να κάνουμε trace της διαδρομής που ακολούθησε το e-mail μέχρι να το παραλάβουμε και να χαρτογραφήσουμε την υποδομή του aueb.gr.

## Φάση 6. Έρευνα ανταγωνισμού

Δεν εντοπίσαμε πληροφορίες που θα μπορούσαν να αξιοποιηθούν στην συγκεκριμένη φάση για το συγκεκριμένο domain.

## Φάση 7. WHOIS footprinting

Εργαλεία που χρησιμοποιήθηκαν:

- <https://who.is/whois/infosec.aueb.gr>
- <https://networking.ringofsaturn.com/Tools/whois.php>
- [https://bgp.he.net/ip/195.251.252.250#\\_whois](https://bgp.he.net/ip/195.251.252.250#_whois)
- <https://ipinfo.io/195.251.252.250>

Χρησιμοποιούμε την σελίδα <https://ipinfo.io/195.251.252.250> για να βρούμε περισσότερες πληροφορίες σχετικά με το domain, τον κάτοχό της και το AS (Autonomous System) στο οποίο ανήκει καθώς και την διεύθυνση email στην οποία μπορούμε να απευθυνθούμε για να αναφέρουμε προβλήματα. Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο στην περίπτωση που θα θέλαμε να κάνουμε κάποια επίθεση social engineering. Επίσης μπορούμε να ερευνήσουμε περισσότερο το AS για να ανακαλύψουμε περισσότερες πληροφορίες για το domain ανώτερου επιπέδου (aueb.gr), όπως τον κάτοχό του, τα IP blocks και ειδικότερα όλες τις διευθύνσεις που έχουν δεσμευτεί, τις πληροφορίες που παρέχονται από το WHOIS API, όπως φαίνεται παρακάτω:

# 195.251.252.250

🇬🇷 Athens, Attica, Greece

🔍 Search an IP or AS number	
Summary >	
Geolocation	
Privacy	
ASN	
Company	
Abuse	

Summary	
ASN	AS8611 - Athens University of Economics and Business
Hostname	www.infosec.aueb.gr
Range	195.251.248.0/21
Company	Athens University of Economics and Business
Hosted domains	0
Privacy	⊗ False
Anycast	⊗ False
ASN type	Education
Abuse contact	abuse@aueb.gr



# AS8611

Athens University of Economics and Business · aueb.gr

## AS8611 – Athens University of Economics and Business

Country	 Greece
Website	<a href="https://aueb.gr">aueb.gr</a>
Hosted domains	16
Number of IPs	4,096
ASN type	Education
Allocated	53 years ago on Jan 01, 1970
Updated	5 years ago on Nov 15, 2017

## IP Address Ranges

IPv4 Ranges IPv6 Ranges




NETBLOCK	COMPANY	NUM OF IPS
<a href="https://whois.ripe.net/ip/195.251.232.0/22">195.251.232.0/22</a>	 Athens University of Economics and Business	1,024
<a href="https://whois.ripe.net/ip/195.251.248.0/21">195.251.248.0/21</a>	 Athens University of Economics and Business	2,048
<a href="https://whois.ripe.net/ip/83.212.204.0/22">83.212.204.0/22</a>	 Athens University of Economics and Business	1,024

Figure 3 ipinfo.io results for infosec.aueb.gr

Αντίστοιχες πληροφορίες λαμβάνουμε ψάχνοντας απευθείας στις σελίδες

<https://who.is/whois/infosec.aueb.gr>,

<https://networking.ringofsaturn.com/Tools/whois.php> και

[https://bgp.he.net/ip/195.251.252.250#\\_whois](https://bgp.he.net/ip/195.251.252.250#_whois)

```

aut-num: AS8611
as-name: UNSPECIFIED
org: ORG-AUOE1-RIPE
import: from AS5408 action pref=100; accept ANY
import: from AS1241 action pref=200; accept ANY
import: from AS3323 action pref=300; accept ANY
export: to AS5408 announce AS8611
export: to AS1241 announce AS8611
export: to AS3323 announce AS8611
default: to AS5408 action pref=100; networks ANY
default: to AS1241 action pref=200; networks ANY
default: to AS3323 action pref=300; networks ANY
admin-c: CK150-RIPE
admin-c: YA334-RIPE
tech-c: AN2938-RIPE
status: ASSIGNED
mnt-by: RIPE-NCC-END-MNT
mnt-by: AS8611-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2017-11-15T09:12:56Z
source: RIPE
sponsoring-org: ORG-GRaT1-RIPE
abuse-email: abuse@aueb.gr
abuse-c: AN2938-RIPE
abuse-org: ORG-GRaT1-RIPE

organisation: ORG-AUOE1-RIPE
org-name: Athens University of Economics and Business
country: GR
org-type: OTHER
address: Athens University of Economics and Business
address: Patission 76
address: 10434
address: Athens
address: GREECE
e-mail: noc@aueb.gr
abuse-c: AN2938-RIPE
mnt-ref: AUEB-NOC
mnt-ref: GRNET-NOC
mnt-by: AUEB-NOC

remarks: For complains about abuse, spam etc:
abuse-mailbox: abuse@aueb.gr
remarks: -----
mnt-by: AS8611-MNT
mnt-by: GRNET-NOC
nic-hdl: AN2938-RIPE
created: 2007-06-13T11:32:23Z
last-modified: 2014-04-07T08:59:47Z
source: RIPE

created: 2014-04-07T08:51:10Z
last-modified: 2022-12-01T17:07:18Z
source: RIPE

role: AUEB NOC
address: Network Operation Center,
address: Athens University of Economics and Business
address: 76 Patission St., 10434,
address: Athens, Greece
phone: +30 210 8203900
fax-no: +30 210 8203909
e-mail: noc@aueb.gr
admin-c: CK150-RIPE
admin-c: YA334-RIPE
tech-c: YA334-RIPE
tech-c: CK150-RIPE
remarks: -----
remarks: For complains about abuse, spam etc:
abuse-mailbox: abuse@aueb.gr
remarks: -----
mnt-by: AS8611-MNT
mnt-by: GRNET-NOC
nic-hdl: AN2938-RIPE
created: 2007-06-13T11:32:23Z
last-modified: 2014-04-07T08:59:47Z
source: RIPE

role: AUEB NOC
address: Network Operation Center,
address: Athens University of Economics and Business
address: 76 Patission St., 10434,
address: Athens, Greece
phone: +30 210 8203900
fax-no: +30 210 8203909
e-mail: noc@aueb.gr
admin-c: CK150-RIPE
admin-c: YA334-RIPE
tech-c: YA334-RIPE
tech-c: CK150-RIPE
remarks: -----

```

Figure 4 whois information for domain infosec.aueb.gr

## Φάση 8. DNS footprinting

Εργαλεία που χρησιμοποιήθηκαν:

- DNSEnum
- TheHarvester
- Who.is
- Nslookup
- netcraft

Αρχικά εισάγουμε το domain στο who.is για να πάρουμε DNS πληροφορίες, όπως το ποιος είναι ο authoritative name server, τις IP διευθύνσεις που είναι συσχετισμένες με το domain και τα canonical names του

infosec.aueb.gr

DNS Information

Whois

DNS Records

Diagnostics

DNS Records for infosec.aueb.gr

cache expires in 2 minutes and 43 seconds

Hostname	Type	TTL	Priority	Content
infosec.aueb.gr	SOA	1800		hermes.aueb.gr nameadm@aub.gr 2032021404 86400 3600 4838400 86400
infosec.aueb.gr	A	3600		195.251.252.250
infosec.aueb.gr	CNAME	3600		www.infosec.aueb.gr
www.infosec.aueb.gr	A	3600		195.251.252.250

Figure 5 whois DNS lookup of infosec.aueb.gr

## Παρόμοια δεδομένα παίρνουμε από το theHarvester

```
[*] Target: infosec.aueb.gr

[93m[!] Missing API key for binaryedge. [0m
[93m[!] Missing API key for Censys ID and/or Secret. [0m
[93m[!] Missing API key for fullhunt. [0m
[93m[!] Missing API key for Github. [0m
[93m[!] Missing API key for Hunter. [0m
[93m[!] Missing API key for Intelx. [0m
[93m[!] Missing API key for PentestTools. [0m
[93m[!] Missing API key for ProjectDiscovery. [0m
[93m[!] Missing API key for RocketReach. [0m
[93m[!] Missing API key for Securitytrail. [0m
[93m[!] Missing API key for virustotal. [0m
[93m[!] Missing API key for zoomeye. [0m
An exception has occurred: Cannot serialize non-str key None
[94m[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.r
Searching 0 results.
[94m[*] Searching Bing.
[94m[*] Searching Baidu.
Searching results.
[94m[*] Searching Certspotter.
[94m[*] Searching CRTsh.
[94m[*] Searching Duckduckgo.
[94m[*] Searching Hackertarget.
[94m[*] Searching Dnsdumpster.
[94m[*] Searching Otx.
[94m[*] Searching Qwant.
[94m[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host www.threatcrowd.
string indices must be integers
[94m[*] Searching Threatcrowd.
[94m[*] Searching Threatminer.
[94m[*] Searching Urlscan.
An exception has occurred: 0, message='Attempt to decode JSON with
[94m[*] Searching Sublist3r.
An exception has occurred: 0, message='Attempt to decode JSON with
[94m[*] Searching Omnisint.

[*] LinkedIn Links found: 0
-----

[*] IPs found: 1
-----
195.251.252.250

[*] No emails found.

[*] Hosts found: 5
-----
www.infosec.aueb.gr:195.251.252.250
```

Το output του nslookup είναι το ακόλουθο:

Server:	192.168.1.1
Address:	192.168.1.1#53

```
Non-authoritative answer:  
Name:   infosec.aueb.gr  
Address: 195.251.252.250  
infosec.aueb.gr canonical name = www.infosec.aueb.gr.
```

*Figure 6 nslookup of infosec.aueb.gr*

Τέλος εκτελέσαμε το TheHarvester και το DNSEnum στο domain ανώτερου επιπέδου aueb.gr προκειμένου να χαρτογραφήσουμε τα subdomains του και να ελέγξουμε αν υπάρχουν άλλα domains που σχετίζονται άμεσα με το infosec.aueb.gr (π.χ. aliases ή servers που μπορεί να χρησιμοποιεί).

```
(kali㉿kali)-[~]  
$ dnsenum aueb.gr  
dnsenum VERSION:1.2.6
```

### aueb.gr

#### Host's addresses:

aueb.gr.	120	IN	A	195.251.255.156
----------	-----	----	---	-----------------

#### Name Servers:

sns0.grnet.gr.	79818	IN	A	83.212.5.89
hermes.aueb.gr.	3600	IN	A	195.251.255.142
sns1.grnet.gr.	79818	IN	A	83.212.5.22

#### Mail (MX) Servers:

mx1.servers.aueb.gr.	3600	IN	A	195.251.255.213
mx2.servers.aueb.gr.	3600	IN	A	195.251.255.218

#### Brute forcing with /usr/share/dnsenum/dns.txt:

archive.aueb.gr.	3600	IN	A	83.212.204.92
dns.aueb.gr.	3600	IN	CNAME	hermes.aueb.gr.
hermes.aueb.gr.	3576	IN	A	195.251.255.142
forum.aueb.gr.	3600	IN	CNAME	art.aueb.gr.
art.aueb.gr.	3600	IN	A	195.251.255.146
ftp.aueb.gr.	3600	IN	CNAME	video.aueb.gr.
video.aueb.gr.	3600	IN	A	195.251.253.200
hermes.aueb.gr.	3570	IN	A	195.251.255.142
infosec.aueb.gr.	2925	IN	CNAME	www.infosec.aueb.gr.
www.infosec.aueb.gr.	1580	IN	A	195.251.252.250
jobs.aueb.gr.	3600	IN	A	195.251.253.135
kibana.aueb.gr.	3600	IN	A	195.251.251.101
lists.aueb.gr.	3600	IN	A	195.251.255.212
mail.aueb.gr.	1257	IN	CNAME	imap.aueb.gr.
imap.aueb.gr.	618	IN	CNAME	imap.servers.aueb.gr.
imap.servers.aueb.gr.	618	IN	A	195.251.255.214
map.aueb.gr.	3600	IN	A	185.138.42.117
marketing.aueb.gr.	3600	IN	CNAME	dept.aueb.gr.
dept.aueb.gr.	303	IN	A	195.251.255.149
moniteur.aueb.gr.	3600	IN	A	195.251.248.143
mx.aueb.gr.	3600	IN	CNAME	s6.servers.aueb.gr.
s6.servers.aueb.gr.	3600	IN	A	195.251.255.146
mx2.aueb.gr.	3600	IN	CNAME	foomx.servers.aueb.gr.
foomx.servers.aueb.gr.	3600	IN	A	195.251.255.153
news.aueb.gr.	3600	IN	CNAME	mine.aueb.gr.
mine.aueb.gr.	3600	IN	A	195.251.255.12
nms.aueb.gr.	3600	IN	A	195.251.255.146
pop.aueb.gr.	156	IN	A	195.251.255.152
shop.aueb.gr.	3600	IN	A	135.181.171.50
sist.aueb.gr.	3600	IN	A	195.251.252.224
smtp.aueb.gr.	342	IN	A	195.251.255.215
stats.aueb.gr.	43200	IN	A	195.251.253.91
survey.aueb.gr.	3600	IN	A	83.212.168.201
vpn.aueb.gr.	3600	IN	CNAME	vpn.servers.aueb.gr.
vpn.servers.aueb.gr.	3600	IN	A	195.251.255.77
webmail.aueb.gr.	557	IN	A	195.251.255.118
www.aueb.gr.	61	IN	CNAME	www-cl.aueb.gr.
www-cl.aueb.gr.	3570	IN	A	195.251.255.156
www2.aueb.gr.	3600	IN	CNAME	users.aueb.gr.
users.aueb.gr.	3600	IN	A	195.251.255.230

Brute forcing with /usr/share/dnsenum/dns.txt:

archive.aueb.gr.	3600	IN	A	83.212.204.92
dns.aueb.gr.	3600	IN	CNAME	hermes.aueb.gr.
hermes.aueb.gr.	3576	IN	A	195.251.255.142
forum.aueb.gr.	3600	IN	CNAME	art.aueb.gr.
art.aueb.gr.	3600	IN	A	195.251.255.146
ftp.aueb.gr.	3600	IN	CNAME	video.aueb.gr.
video.aueb.gr.	3600	IN	A	195.251.253.200
hermes.aueb.gr.	3570	IN	A	195.251.255.142
infosec.aueb.gr.	2925	IN	CNAME	www.infosec.aueb.gr.
www.infosec.aueb.gr.	1580	IN	A	195.251.252.250
jobs.aueb.gr.	3600	IN	A	195.251.253.135
kibana.aueb.gr.	3600	IN	A	195.251.251.101
lists.aueb.gr.	3600	IN	A	195.251.255.212
mail.aueb.gr.	1257	IN	CNAME	imap.aueb.gr.
imap.aueb.gr.	618	IN	CNAME	imap.servers.aueb.gr.
imap.servers.aueb.gr.	618	IN	A	195.251.255.214
map.aueb.gr.	3600	IN	A	185.138.42.117
marketing.aueb.gr.	3600	IN	CNAME	dept.aueb.gr.
dept.aueb.gr.	303	IN	A	195.251.255.149
moniteur.aueb.gr.	3600	IN	A	195.251.248.143
mx.aueb.gr.	3600	IN	CNAME	s6.servers.aueb.gr.
s6.servers.aueb.gr.	3600	IN	A	195.251.255.146
mx2.aueb.gr.	3600	IN	CNAME	foomx.servers.aueb.gr.
foomx.servers.aueb.gr.	3600	IN	A	195.251.255.153
news.aueb.gr.	3600	IN	CNAME	mine.aueb.gr.
mine.aueb.gr.	3600	IN	A	195.251.255.12
nms.aueb.gr.	3600	IN	A	195.251.255.146
pop.aueb.gr.	156	IN	A	195.251.255.152
shop.aueb.gr.	3600	IN	A	135.181.171.50
sist.aueb.gr.	3600	IN	A	195.251.252.224
smtp.aueb.gr.	342	IN	A	195.251.255.215
stats.aueb.gr.	43200	IN	A	195.251.253.91
survey.aueb.gr.	3600	IN	A	83.212.168.201
vpn.aueb.gr.	3600	IN	CNAME	vpn.servers.aueb.gr.
vpn.servers.aueb.gr.	3600	IN	A	195.251.255.77
webmail.aueb.gr.	557	IN	A	195.251.255.118
www.aueb.gr.	61	IN	CNAME	www-cl.aueb.gr.
www-cl.aueb.gr.	3570	IN	A	195.251.255.156
www2.aueb.gr.	3600	IN	CNAME	users.aueb.gr.
users.aueb.gr.	3600	IN	A	195.251.255.230

```
(kali@kali)-[~]
$ dnsenum aueb.gr
dnsenum VERSION:1.2.6
```

— aueb.gr —

#### Host's addresses:

aueb.gr.	120	IN	A	195.251.255.156
----------	-----	----	---	-----------------

#### Name Servers:

sns0.grnet.gr.	79818	IN	A	83.212.5.89
hermes.aueb.gr.	3600	IN	A	195.251.255.142
sns1.grnet.gr.	79818	IN	A	83.212.5.22

#### Mail (MX) Servers:

mx1.servers.aueb.gr.	3600	IN	A	195.251.255.213
mx2.servers.aueb.gr.	3600	IN	A	195.251.255.218



## Φάση 9. Network footprinting

Εργαλεία που χρησιμοποιήθηκαν:

- nmap
- traceroute
- Gmail (e-mail trace analysis)
- DNSEnum

Χρησιμοποιήσαμε το output των παραπάνω εργαλείων, όπως φαίνεται στις προηγούμενες εικόνες, προκειμένου να χαρτογραφήσουμε τις υποδομές που χρησιμοποιεί ο ιστότοπος και την απόστασή μας από τον server.