

Seguridad y pentesting de servidores de datos

PEC 2

Arquitectura de las aplicaciones web

UOC - MISTIC

Pablo Riutort Grande

9 de noviembre de 2020

Índice

1. Resumen ejecutivo	3
1.0.1. Capa de red	3
1.0.2. Capa de aplicación	3
2. Metodología utilizada	4
2.1. Búsqueda mediante motores de búsqueda para el descubrimiento de fugas de información (OTG-INFO-001)	4
2.2. Fingerprint del servidor web (OTG-INFO-002)	4
2.3. Revisión de metadatos en busca de fuga de información (OTG-INFO-003)	5
2.4. Enumeración de aplicaciones en el servidor web (OTG-INFO-004)	5
2.5. Mapear rutas de ejecución a través de la aplicación (OTG-INFO-007)	5
2.6. Fingerprint del framework de la aplicación (OTG-INFO-008)	5
2.7. Fingerprint de la aplicación (OTG-INFO-009)	6
A. Evidencias	7
A.1. OTG-INFO-001	7
A.2. OTG-INFO-002	9
A.3. OTG-INFO-003	11
A.4. OTG-INFO-004	12
A.4.1. nmap scan	13
A.5. OTG-INFO-007	15
A.6. OTG-INFO-008	15
A.7. OTG-INFO-009	16

Índice de figuras

1. Operador “site: uoc.edu” con Google, Duck Duck Go y Startpage.com	7
2. Mediante el operador site:uoc.edu intitle:“index of” podemos encontrar varios archivos del servidor e incluso scripts	8
3. Detalle de resultados con Shodan	9
4. Detalle de resultados con Shodan sobre el host multimedia.uoc.edu (213.73.35.33)	10
5. Resultados con Shodan sobre uoc.edu en el puerto 80	10
6. Resultados de la búsqueda de uoc.edu en Netcraft	10
7. Listado de archivos de robots.txt y análisis de tags meta en el index.html	11
8. SpiderFoot saca información relevante del dominio, incluído algunas cuentas de email que pertenecen a fugas de datos.	12
9. Grafo de Maltego sobre el dominio de uoc.edu y vista en detalle del bloque de red encontrado	13
10. Escaneo de la web por parte de Nikto	13
11. Resultados de ZAP sobre el dominio www.uoc.edu. Muestra la request de tipo GET sobre el recurso robots.txt	15
12. Alertas detectadas para este nodo	15
13. Análisis de fingerprinting del framework con whatweb	15
14. Análisis de fingerprinting del framework con wappalyzer	16
15. Cookies de la página web	16

1. Resumen ejecutivo

Se ha hecho un análisis del portal de la universidad de la UOC de manera pasiva para determinar las medidas de seguridad presentes y otras características.

1.0.1. Capa de red

A nivel de red el sitio se mueve en el rango de IPs 213.73.40.0/24 con algunas aplicaciones abiertas y otras filtradas:

Puerto	Servicio
22	ssh
25	smtp
515	printer
3306	mysql
53	domain
8400	cvd (servicios de backup)
8402	abarsd (servicios de backup)
6881	bittorrent-tracker
...	...

En el rango de IPs se han encontrado un total de 23 hosts, entre algunos de ellos están los servidores de DNS y de correo:

- portugal.uoc.es (213.73.40.8)
- tibet_dnsex.uoc.es (213.73.40.9)
- nepal_dnsex.uoc.es (213.73.40.10)
- tibet.uoc.es (213.73.40.45) (Servidor de DNS)
- tibet_dns.uoc.es (213.73.40.46)
- nepal.uoc.es (213.73.40.47) (Servidor de DNS)
- nepal_dns.uoc.es (213.73.40.48)
- croacia_campus.uoc.es (213.73.40.49)
- www.uoc.edu (213.73.40.210)
- cv.uoc.edu (213.73.40.211)
- 73-40-242.uoc.es (213.73.40.242)
- eduroam.uoc.edu (213.73.40.249)
- ...
- aspmx5.googlemail.com (Correo)
- aspmx.l.googlemail.com (Correo)
- ...

1.0.2. Capa de aplicación

La aplicación utiliza varias tecnologías, entre ellas se han encontrado evidencias de:

- Librerías y Frameworks: jQuery, Mustache, WordPress
- Apache y algunos módulos del mismo (ModLayout)
- Analíticas: Google Analytics, Hotjar

- Lenguajes: PHP, Python, JavaScript y MySQL
- Uso de cifrado SSL: Se usa la redirección del tráfico http a https.
- Sistemas operativos: Ubuntu, Debian
- Gestores de tráfico (f5 Big-IP).

Vulnerabilidades

En ese nivel se han encontrado algunas vulnerabilidades o malas configuraciones que pueden ser explotables, algunas son:

- Se han encontrado direcciones de correo en el sistema que se sabe que pertenecen a fugas de información.
- Vulnerabilidades conocidas de Apache recogidas en CVE (CVE-2017-7679, CVE-2017-9798...)
- Headers mal configurados con riesgos de clickjacking y cross-site-scripting.
- Cookies atributos ausentes, sin flags de seguridad o con sobreinformación.

2. Metodología utilizada

La metodología utilizada ha sido la recomendada por la OWASP en su guía de *Testing Information Gathering* (OTG-INFO)[1]. Siguiendo esta guía de forma libre se ha realizado un análisis pasivo del portal web de esta universidad (www.uoc.edu) y extraído información de la misma.

A continuación se describe en más detalle este análisis siguiendo los apartados de la guía.

2.1. Búsqueda mediante motores de búsqueda para el descubrimiento de fugas de información (OTG-INFO-001)

Este primer paso de la guía consiste en recabar información del sitio utilizando motores de búsqueda y operadores especiales que nos permiten acceder a funcionalidades avanzadas.

Concretamente hemos utilizado el operador **site:uoc.edu** que restringe los resultados de la búsqueda al dominio de la página que nos interesa analizar [Ver A.1].

Existen ciertas páginas que normalmente no aparecerían en una búsqueda convencional, pero si aplicamos los operadores podemos sacar información interesante, como es el caso de la página <http://lpg.uoc.edu/IATE/> que se ha encontrado mediante el operador **site:uoc.edu intitle:"index of"** [Fig. 2].

2.2. Fingerprint del servidor web (OTG-INFO-002)

Este paso consiste en averiguar el tipo y versiones del servidor web. La idea es observar los datos de las cabeceras que devuelve el servidor

Shodan es un motor de búsqueda especializado en dispositivos conectados a internet [2]. Podemos utilizar este motor para hacer una búsqueda especializada de la página de UOC en el puerto 80 "**hostname:uoc.edu port:80**" y obtener información sobre los dispositivos que tengan que ver con este dominio [Fig. 3]. Shodan nos enseña la cabecera de las respuestas del servidor y nos pone qué software utiliza el servidor web: Apache/2.4.18 y Sistema operativo Ubuntu [Fig. 5]. Además, entre los dispositivos se han encontrado evidencias de otras tecnologías como jQuery Migrate, Wordpress, PHP y MySQL así como algunas vulnerabilidades conocidas [Fig. 5].

Otra herramienta que se ha utilizado es Netcraft que nos da un análisis muy variado del dominio introducido como la dirección IP, dónde está hosteada la red, qué trackers tiene y algunas tecnologías que se utilizan en el servidor [Fig. 6].

Finalmente, hemos visto que el dominio www.uoc.edu redirige el tráfico a https, vale la pena inspeccionar los certificados que se intercambian con el dominio con el comando

```
1 openssl s_client -connect uoc.edu:443
```

Vemos que en la respuesta se produce un handshake satisfactorio y nos devuelve el certificado del servidor para proceder con la conexión de manera segura.

2.3. Revisión de metadatos en busca de fuga de información (OTG-INFO-003)

Este apartado consiste en revisar datos del servidor para entender qué paths (o rutas) tiene actualmente. Para esto, un archivo muy útil suele ser el robots.txt ya que indica a los buscadores qué rutas no tienen que se indexadas por los buscadores. Podemos descargar este fichero con el comando `wget` y observar una primera vista de las aplicaciones que esconde el dominio [Ver A.3].

Otra acción que se recomienda en este paso es consultar los metadatos de la página, para eso podemos consultar los tags META de la sección HEAD del documento HTML.

2.4. Enumeración de aplicaciones en el servidor web (OTG-INFO-004)

Se ha utilizado la herramienta SpiderFoot para hacer una búsqueda sobre el dominio. SpiderFoot permite el descubrimiento de los recursos que pertenecen a un dominio y monitorizarlos [6]. Se ha realizado un scanner de tipo footprint que consiste en entender el perímetro de la red del objetivo, las entidades asociadas y otra información, en cambio, el pasivo pretende recopilar tanta información como sea posible sin tocar el objetivo o sus afiliados [Ver 8].

Para este paso también se ha utilizado la herramienta llamada Maltego, la cual genera un grafo de entidades y conexiones entre ellas a través de un dominio dado [4]. Mediante este grafo podemos sacar mucha información precisa y la relación que hay entre las entidades de manera catalogada: Servidores de DNS, servidores de correo, direcciones, personas, etc.

Finalmente, la guía también recomienda el uso de Nikto para detectar vulnerabilidades conocidas en servidores web [9]. Con esta herramienta podemos ver que existen riesgos de clickjacking y cross-site-scripting debido a la mala configuración de headers.

A través de la información que hemos obtenido hasta ahora se puede realizar un escaneo aún más exhaustivo con `nmap`. `Nmap` es una herramienta de exploración de puertos y escáner con múltiples opciones [8]. Para este ejercicio se ha ejecutado el comando sobre el rango de IPs encontrado con Maltego [Ver A.4.1].

```
1 nmap 213.73.40.0/24
```

Este comando nos da mucha información de todas las IPs del rango como distintas aplicaciones en distintos servidores como impresoras, protocolos de correo, ftp, ssh, etc.

2.5. Mapear rutas de ejecución a través de la aplicación (OTG-INFO-007)

Este proceso consiste en entender la estructura de la aplicación y su disposición en la red. Para este paso se ha utilizado ZAP (Zed Attack Proxy). ZAP es una herramienta de pentesting de OWASP diseñada para testear aplicaciones web [5]. Con esta herramienta podemos automatizar el proceso de descubrimiento de URLs de forma sencilla mediante spiders que recorren el dominio, ZAP registra la URL, el método utilizado (Verbo HTTP), la request enviada y la response. De esta forma, se consigue un mapa de toda la aplicación y sus rutas [Ver A.5].

ZAP, además, catalogará los diferentes niveles de riesgo que se haya podido encontrar [Ver. 12]; entre ellos ha encontrado mala configuración del cross domain, mala configuración de cookies, headers ausentes, etc.

2.6. Fingerprint del framework de la aplicación (OTG-INFO-008)

Esta tarea consiste en intentar averiguar el framework que se esté utilizando en el servidor web para la aplicación. Típicamente las aplicaciones basadas en web utilizan frameworks para facilitar tareas que de otra forma serían muy costosas de desarrollar y mantener, sin embargo, con estos frameworks también existen riesgos de seguridad que vale la pena conocer y mitigar. Conocer también las configuraciones típicas de este framework para saber si se han realizado correctamente es un proceso importante para el fingerprinting.

Para este paso se ha utilizado la herramienta Whatweb que reconocerá las tecnologías utilizadas en el servidor web tales como CMS o librerías de JavaScript [10], en el caso de la página de la UOC ha encontrado [Ver 13]:

- Se trata de un servidor Apache
- Hay una mención a un framework llamado ModLayout. Esto lo sabemos por el header no estándar de “X-Powered-By” típicamente designado para esto [11].

- Se trata de un servidor F5-BigIP.

Finalmente, se ha utilizado la herramienta Wappalyzer para identificar otras tecnologías que se puedan estar utilizando [12]. En la página de la UOC se ha encontrado el uso de la librería jQuery y el framework JavaScript de Mustache [Ver 14].

2.7. Fingerprint de la aplicación (OTG-INFO-009)

Conocer los componentes de la aplicación que se está testeando es también importante y reduce el esfuerzo de un test más exhaustivo puesto que se tiene una idea de los componentes de la aplicación. Para entender la aplicación un buen sitio donde mirar son las cookies que genera la aplicación y buscar pistas en el código HTML.

En las cookies podemos observar la presencia de las aplicaciones de análisis de Hotjar y Google Analytics [13] [Ver 15]. Existen cookies propias que dan pistas de la naturaleza de la aplicación que presenta el servidor web, como la llamada `_utmv` cuyo valor describe al tipo de usuario que utiliza la aplicación (`TipusUsuari=UOC %2FESTUDIANT`).

En cuanto al análisis del código HTML no se han encontrado pistas o patrones que delaten a un framework o describan una aplicación.

Anexo

A. Evidencias

A.1. OTG-INFO-001

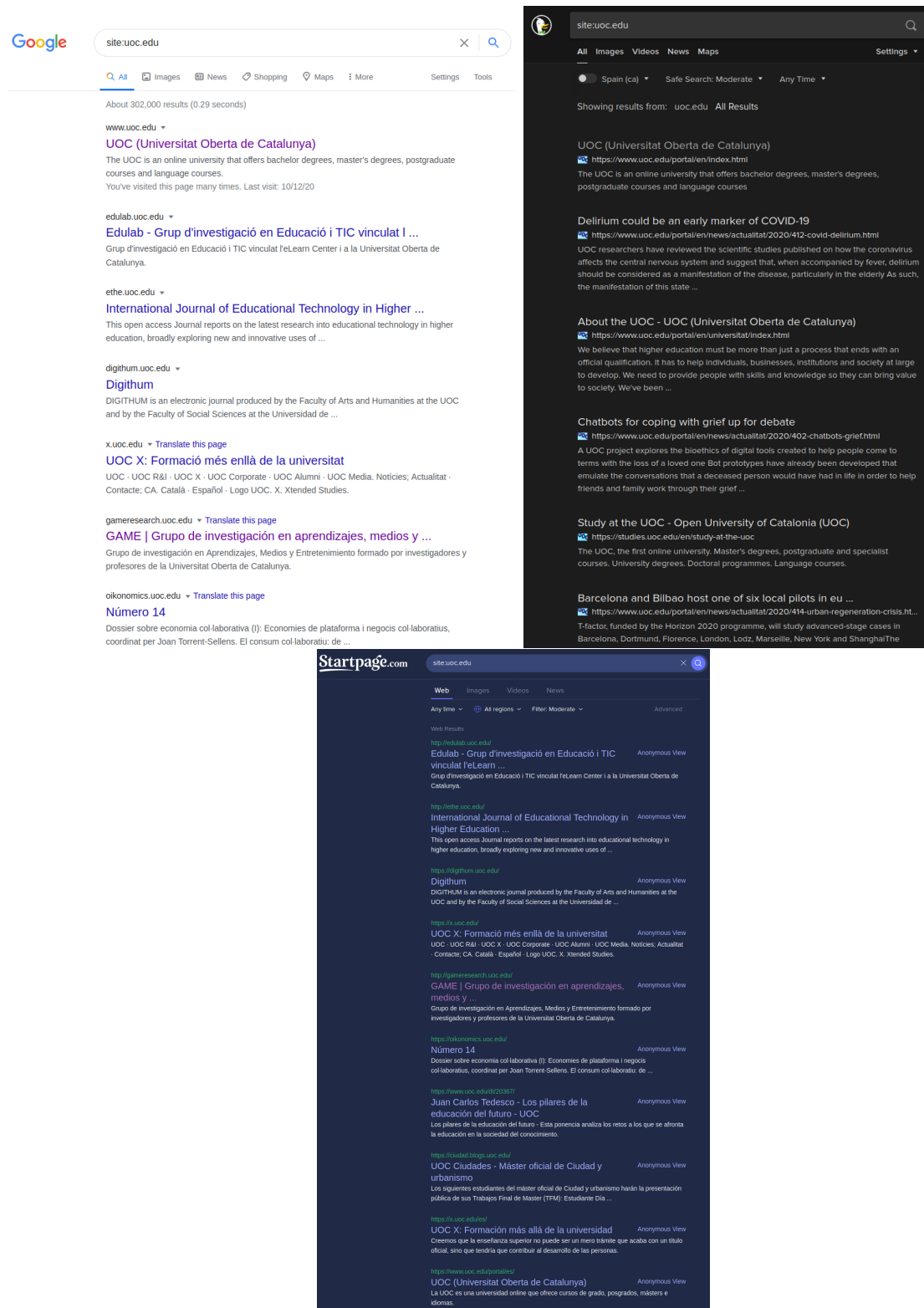


Figura 1: Operador “site: uoc.edu” con Google, Duck Duck Go y Startpage.com

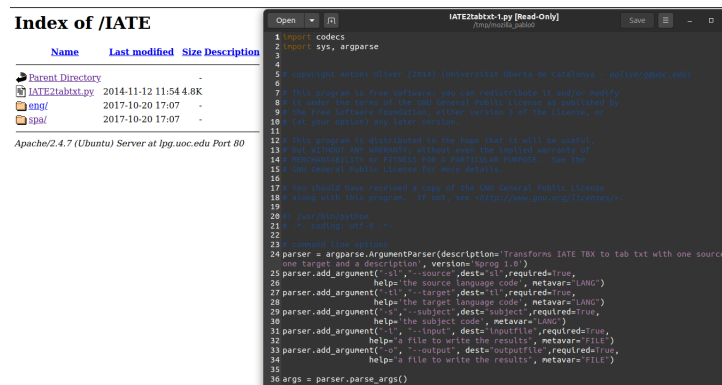


Figura 2: Mediante el operador site:uoc.edu intitle:“index of” podemos encontrar varios archivos del servidor e incluso scripts

A.2. OTG-INFO-002

403 Forbidden 213.73.35.9 multimedia.uoc.edu Analysed on 2020-11-02 11:18:18 GMT Spain, Barcelona	HTTP/1.1 403 Forbidden Date: Sun, 02 Nov 2020 11:18:18 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 276 Content-Type: text/html; charset=iso-8859-1
Titulacions de l'àmbit multimèdia 213.73.35.9 multimedia.uoc.edu Analysed on 2020-11-02 09:04:08 GMT Spain, Barcelona jQuery Migrate	HTTP/1.1 200 OK Date: Sat, 07 Nov 2020 09:04:08 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: pll_language=ca; expires=Sun, 07-Nov-2021 09:04:08 GMT; Max-Age=31536000; path=/ Link: <http://multimedia.uoc.edu/wp-json/?>; rel="https://api.w.org/" Vary: Accept-Encoding Transfer-Encoding: chunk...
213.73.35.20 Universitat Oberta de Catalunya Analysed on 2020-10-30 07:37:18 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Fri, 30 Oct 2020 07:37:17 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 21 Content-Type: text/html; charset=UTF-8
301 Moved Permanently 213.73.35.9 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-04 14:48:55 GMT Spain, Barcelona	HTTP/1.1 301 Moved Permanently Date: Wed, 04 Nov 2020 14:48:55 GMT Server: Apache Location: https://x.uoc.edu/ Content-Length: 226 Content-Type: text/html; charset=iso-8859-1 Set-Cookie: BIGipServerportal_webserver=785833488.28488.0000; path=/; Httponly
213.73.35.43 emissari.uoc.edu emissari.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-12-04 05:57:28 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Wed, 04 Nov 2020 09:57:17 GMT Server: Apache/2.4.18 Last-Modified: Wed, 25 Nov 2015 07:57:57 GMT ETag: "17-52558d1091a0a" Accept-Ranges: bytes Content-Length: 23 Content-Type: text/html
403 Forbidden 213.73.37.245 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-04 21:59:18 GMT Spain, Barcelona	HTTP/1.1 403 Forbidden Date: Wed, 04 Nov 2020 22:03:03 GMT Server: Apache/2.2.22 (Debian) Vary: Accept-Encoding Content-Length: 281 Content-Type: text/html; charset=iso-8859-1
213.73.40.211 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-06 09:59:40 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Fri, 06 Nov 2020 09:59:54 GMT Server: Apache Last-Modified: Fri, 14 Jan 2011 08:47:11 GMT ETag: "56-49ca7ae341cd" Accept-Ranges: bytes Content-Length: 86 Access-Control-Allow-Origin: * Connection: close Content-Type: text/html Set-Cookie: BIGipServercvu_webserver=1...
302 Found 213.73.35.9 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-06 17:40:44 GMT Spain, Barcelona	HTTP/1.1 302 Found Date: Fri, 30 Oct 2020 17:40:44 GMT Server: Apache Location: https://213.73.35.4/ Content-Length: 284 Content-Type: text/html; charset=iso-8859-1
301 Moved Permanently 213.73.35.9 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-05 17:34:39 GMT Spain, Barcelona	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 05 Nov 2020 17:34:38 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://einstgit.uoc.edu/443/
Universitat Oberta de Catalunya 213.73.35.205 multimedia.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-11-05 13:46:33 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Fri, 30 Oct 2020 19:41:24 GMT Server: Apache/2.4.7 (Ubuntu) Last-Modified: Thu, 05 Mar 2020 13:46:33 GMT ETag: "11e4-5a81bc3c684e" Accept-Ranges: bytes Content-Length: 4588 Access-Control-Allow-Origin: * Connection: close Content-Type: text/html
Apache2 Ubuntu Default Page: It works 213.73.35.9 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-10-27 05:00:14 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Thu, 22 Oct 2020 15:14:24 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Thu, 01 Feb 2016 08:33:41 GMT ETag: "2cfe-56422748b3679" Accept-Ranges: bytes Content-Length: 11518 Vary: Accept-Encoding Content-Type: text/html
213.73.35.34 www.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-10-27 05:00:14 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Tue, 27 Oct 2020 05:00:13 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 14 May 2018 08:12:27 GMT ETag: "11-56c268be443cf" Accept-Ranges: bytes Content-Length: 17 Content-Type: text/html
Universitat Oberta de Catalunya 213.73.35.205 multimedia.uoc.edu Universitat Oberta de Catalunya Analysed on 2020-10-29 05:59:23 GMT Spain, Barcelona	HTTP/1.1 200 OK Date: Tue, 29 Oct 2020 05:59:18 GMT Server: Apache/2.4.7 (Ubuntu) Last-Modified: Thu, 05 Mar 2020 13:46:33 GMT ETag: "11e4-5a81bc3c684e" Accept-Ranges: bytes Content-Length: 4588 Access-Control-Allow-Origin: * Connection: close Content-Type: text/html Set-Cookie: UOC=lg...

Figura 3: Detalle de resultados con Shodan

Web Technologies

jQuery

jQuery Migrate

MySQL

PHP

WordPress

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2017-7679

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVE-2017-9798

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthorized OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVE-2016-1546

The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.

CVE-2018-1312

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Figura 4: Detalle de resultados con Shodan sobre el host multimedia.uoc.edu (213.73.35.33)

```
HTTP/1.1 200 OK
Date: Thu, 22 Oct 2020 15:14:24 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Thu, 01 Feb 2018 08:33:41 GMT
ETag: "2cf6-5642274083679"
Accept-Ranges: bytes
Content-Length: 11510
Vary: Accept-Encoding
Content-Type: text/html
```

Figura 5: Resultados con Shodan sobre uoc.edu en el puerto 80

Background

Site title

UOC

Date first seen

March 2001

Site rank

85355

Netcraft Risk Rating

Not Present

Description

La UOC es una universidad online que ofrece cursos de grados, posgrados, másters e idiomas.

Primary language

Spanish

Network

Site

http://www.uoc.edu

Domain

uoc.edu

Netblock Owner

UOC Data Network

Nameserver

tibet.uoc.es

Hosting company

UOC.es

Domain registrar

unknown

Hosting country

ES

Nameserver organisation

unknown

IPv4 address

213.73.40.242

Organisation

unknown

IPv4 autonomous systems

AS15633

DNS admin

root@tibet.uoc.es

IPv6 address

Not Present

Top Level Domain

Educational entities (.edu)

IPv6 autonomous systems

Not Present

DNS Security Extensions

unknown

Reverse DNS

73-40-242.uoc.es

IP delegation

IPv4 address (213.73.40.242)

IP range

Country

Name

Description

0.0.0.0-255.255.255.255

N/A

IANA-BLK

The whole IPv4 address space

Figura 6: Resultados de la búsqueda de uoc.edu en Netcraft

10

A.3. OTG-INFO-003

```
pablo@fossa:~$ wget https://www.uoc.edu/robots.txt; head robots.txt
--2020-11-08 17:55:14-- https://www.uoc.edu/robots.txt
Resolving www.uoc.edu (www.uoc.edu)... 213.73.40.242
Connecting to www.uoc.edu (www.uoc.edu)[213.73.40.242]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2577 (2.5K) [text/plain]
Saving to: 'robots.txt.1'

robots.txt.1      100%[=====] 2,52K  --KB/s   in 0,01s

2020-11-08 17:55:14 (168 KB/s) - 'robots.txt.1' saved [2577/2577]

User-agent: *
Disallow: /*?
Disallow: /masters/
Allow: /masters/oficiales/ing/913.pdf
Disallow: /web/
Allow: /web/esp/art/uoc/molina102/molina102.pdf
Disallow: /symposia/
Allow: /symposia/dret-tic2012/pdf/4.6.carrizosa-esther-y-gallardo-jose.pdf
Allow: /symposia/dret-tic2011/pdf/4.carrizosa-prieto-esther_gallardo_ballesteros_jose.pdf
Allow: /symposio/pau/art/Milhelni.pdf

pablo@fossa:~$ wget www.uoc.edu > index.html
--2020-11-08 18:36:50-- http://www.uoc.edu/
Resolving www.uoc.edu (www.uoc.edu)... 213.73.40.242
Connecting to www.uoc.edu (www.uoc.edu)[213.73.40.242]:80.. connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.uoc.edu/ [following]
--2020-11-08 18:36:50-- https://www.uoc.edu/
Connecting to www.uoc.edu (www.uoc.edu)[213.73.40.242]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1      [ <=> ] 0,84K  --KB/s   in 0,001s

2020-11-08 18:36:50 (15,6 MB/s) - 'index.html.1' saved [9054]

pablo@fossa:~$ grep "<meta" index.html.1
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<meta name="robots" content="all" />
<meta name="author" content="Universitat Oberta de Catalunya" />
<meta name="keywords" content="estudis, graus, masters, e-learning,
recerca, innovacio, universitat, online, catalunya, idiomes, postgrau,
campus virtual, matricula, internet" />
<meta name="description" content="La UOC es una universidad online
que ofrece cursos de grados, posgrados, masters e idiomas." />
<meta name="google-site-verification" content="MEQNfigU7C_jXHQkTogLlMqlwOLFkBMHYLAUHVCMWuxk" />
pablo@fossa:~$
```

Figura 7: Listado de archivos de robots.txt y análisis de tags meta en el index.html

A.4. OTG-INFO-004

UOC FINISHED

Summary Browse Graph Scan Settings Log

Type	Unique Data Elements	Total Data Elements
Account on External Site	26	26
Affiliate - Company Name	6	11
Affiliate - Domain Name	5	13
Affiliate - Domain Whois	5	5
Affiliate - Email Address	24	96
Affiliate - Internet Name	13	13
Affiliate Description - Abstract	3	3
Affiliate Description - Category	20	21
BGP AS Membership	1	2
Co-Hosted Site	3	3
Co-Hosted Site - Domain Name	3	3
Co-Hosted Site - Domain Whois	1	1
Country Name	4	10
Credit Card Number	1	5
DNS SPF Record	1	1
DNS TXT Record	4	4
Domain Name (Parent)	1	1
Domain Whois	1	1
Email Address	4	11
Email Address - Generic	1	1
Email Gateway (DNS MX Records)	7	7
Hacked Email Address	9	9

UOC FINISHED

Summary Browse Graph Scan Settings Log

Browse / Hacked Email Address

Data Element	Source Data Element	Source Module
<input type="checkbox"/> aroure@uoc.edu [Unknown]	aroure@uoc.edu	sfp_emailrep
<input type="checkbox"/> aroure@uoc.edu [dropbox.com]	aroure@uoc.edu	sfp_citadel
<input type="checkbox"/> aroure@uoc.edu [luminpdf.com]	aroure@uoc.edu	sfp_citadel
<input type="checkbox"/> aroure@uoc.edu [onlinerspambot]	aroure@uoc.edu	sfp_citadel
<input type="checkbox"/> aroure@uoc.edu [verifications.io]	aroure@uoc.edu	sfp_citadel
<input type="checkbox"/> msuriyach@uoc.edu [Unknown]	msuriyach@uoc.edu	sfp_emailrep
<input type="checkbox"/> msuriyach@uoc.edu [luminpdf.com]	msuriyach@uoc.edu	sfp_citadel
<input type="checkbox"/> uocbarcelona@uoc.edu [Unknown]	uocbarcelona@uoc.edu	sfp_emailrep
<input type="checkbox"/> uocbarcelona@uoc.edu [bit.ly]	uocbarcelona@uoc.edu	sfp_citadel

Figura 8: SpiderFoot saca información relevante del dominio, incluido algunas cuentas de email que pertenecen a fugas de datos.

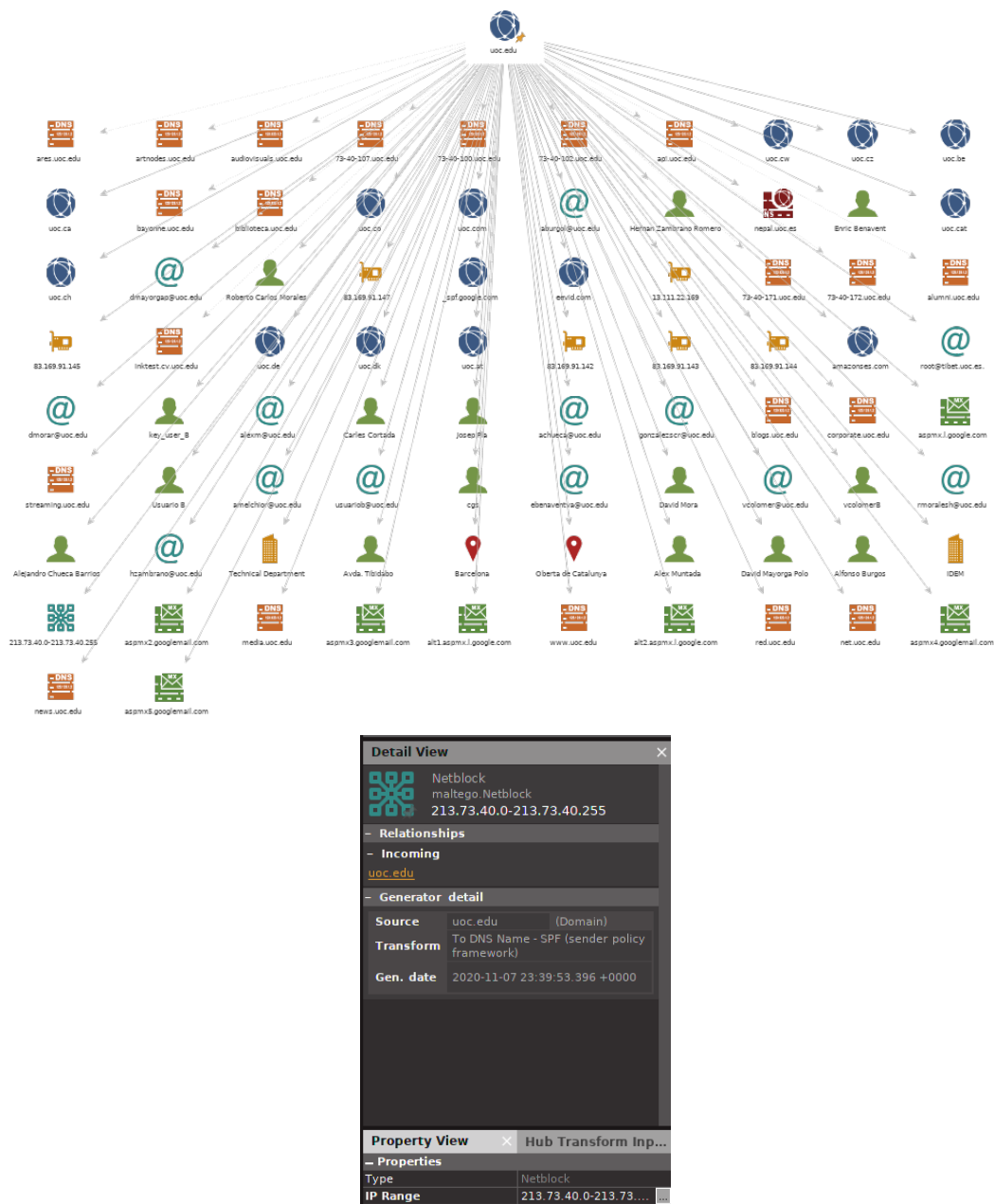


Figura 9: Grafo de Maltego sobre el dominio de uoc.edu y vista en detalle del bloque de red encontrado

```
kali@kali:~$ nikto -h www.uoc.edu
- Nikto v2.1.6

+ Target IP: 213.73.40.242
+ Target Hostname: www.uoc.edu
+ Target Port: 80
+ Start Time: 2020-11-08 22:59:06 (GMT0)

+ Server: BigIP
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
IME type
+ Root page / redirects to: https://www.uoc.edu/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Figura 10: Escaneo de la web por parte de Nikto

A.4.1. nmap scan

```

1 Nmap scan report for portugal.uoc.es (213.73.40.8)
2 Host is up (0.019s latency).
3 Not shown: 990 closed ports
4 PORT      STATE      SERVICE
5 22/tcp    open       ssh
6 25/tcp    open       smtp
7 53/tcp    filtered   domain
8 111/tcp   open       rpcbind
9 515/tcp   filtered   printer
10 873/tcp   filtered   rsync
11 1084/tcp  filtered   ansoft-lm-2
12 1971/tcp  filtered   netop-school
13 5678/tcp  open       rrac
14 8400/tcp  open       cvd
15
16 Nmap scan report for tibet_dnsex.uoc.es (213.73.40.9)
17 Host is up (0.019s latency).
18 Not shown: 995 closed ports
19 PORT      STATE      SERVICE
20 22/tcp    open       ssh
21 515/tcp   filtered   printer
22 5678/tcp  open       rrac
23 8400/tcp  open       cvd
24 8402/tcp  open       abarsd
25
26 :
27 :
28
29 Nmap scan report for eduroam.uoc.edu (213.73.40.249)
30 Host is up (0.017s latency).
31 Not shown: 995 closed ports
32 PORT      STATE      SERVICE
33 22/tcp    open       ssh
34 53/tcp    filtered   domain
35 111/tcp   open       rpcbind
36 515/tcp   filtered   printer
37 5678/tcp  open       rrac
38
39 Nmap scan report for 73-40-250.uoc.es (213.73.40.250)
40 Host is up (0.020s latency).
41 Not shown: 950 closed ports, 48 filtered ports
42 PORT      STATE      SERVICE
43 22/tcp    open       ssh
44 111/tcp   open       rpcbind
45
46 Nmap done: 256 IP addresses (23 hosts up) scanned in 1622.41 seconds

```

A.5. OTG-INFO-007

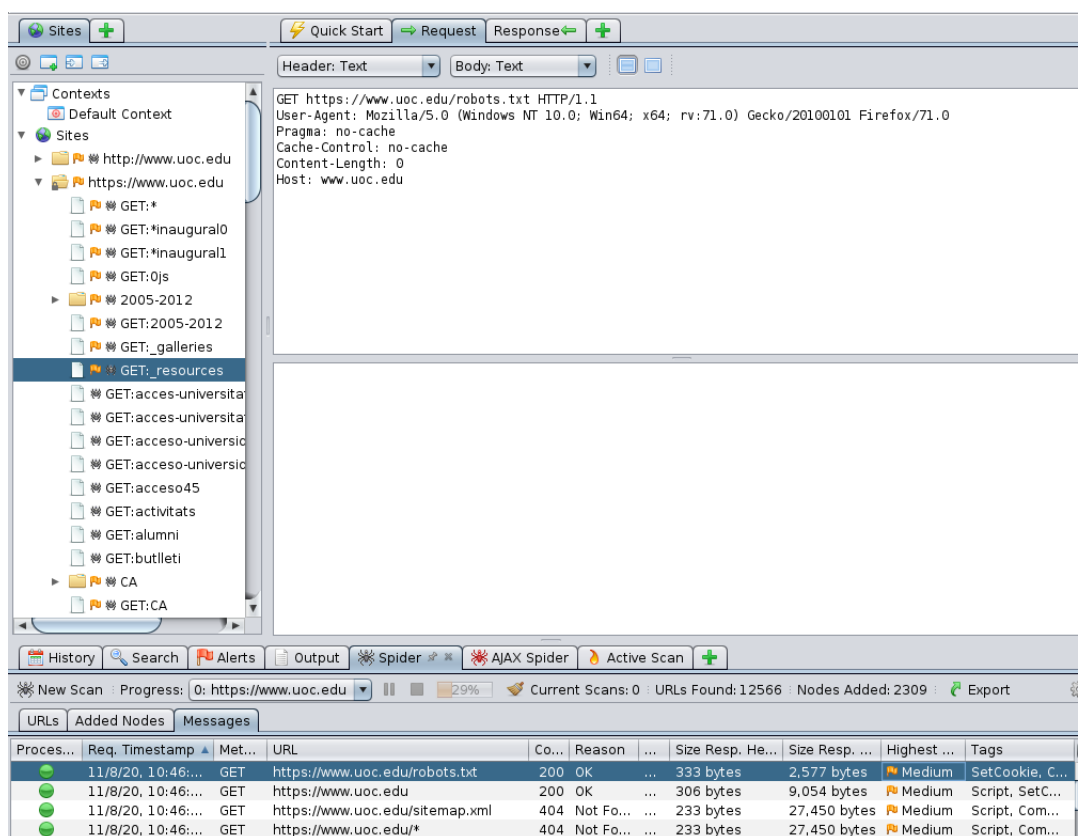


Figura 11: Resultados de ZAP sobre el dominio `www.uoc.edu`. Muestra la request de tipo GET sobre el recurso `robots.txt`

Alerts for This Node	
Generate Anti-CSRF Test FORM	Cross-Domain Misconfiguration
Invoke with Script...	Cookie Without SameSite Attribute
Compare 2 requests	X-Content-Type-Options Header Missing
Compare 2 responses	Incomplete or No Cache-control and Pragma HTTP Header Set
Save Raw	Cookie Without Secure Flag
	Timestamp Disclosure - Unix

Figura 12: Alertas detectadas para este nodo

A.6. OTG-INFO-008


```
http://www.uoc.edu [301 Moved Permanently] Country[SPAIN][ES],
HTTPServer[BigIP],
IP[213.73.40.242],
RedirectLocation[https://www.uoc.edu/]
https://www.uoc.edu/ [200 OK] Apache, Cookies[BIGipServerportal_webserver],
Country[SPAIN][ES],
F5-BigIP, Frame, Google-Analytics [UA-1571980-1],
HTTPServer[Apache],
HttpOnly[BIGipServerportal_webserver],
IP[213.73.40.242],
Meta-Author[Universitat Oberta de Catalunya],
Script[text/javascript],
Title[UOC],
UncommonHeaders[access-control-allow-origin],
X-Powered-By[ModLayout/5.1]
```

Figura 13: Análisis de fingerprinting del framework con whatweb

Technology lookup

Find out what websites are built with

Instantly reveal the technology stack and contact details of any website, such as ecommerce platform, content management system or marketing automation tools.


 **Lookup**


Website URL or company name


http://www.uoc.edu


Q


Technologies (7)

 [jQuery](#) JavaScript libraries

 [Mustache](#) JavaScript frameworks

 [Apache](#) Web servers

 [Google Analytics](#) Analytics

 [Google Analytics](#) SaaS

Look up 5,000 websites at once with [Bulk lookup](#).

Automate lookups with the [Lookup API](#).

Get the free [browser extension](#).

Figura 14: Análisis de fingerprinting del framework con wappalizer

A.7. OTG-INFO-009

Cache Storage	Filter Items
https://vars.hotjar.com	
https://www.uoc.edu	
Cookies	
https://vars.hotjar.com	
https://www.uoc.edu	
Indexed DB	
https://vars.hotjar.com	
https://www.uoc.edu	
Local Storage	
https://vars.hotjar.com	
https://www.uoc.edu	
Session Storage	
https://vars.hotjar.com	
https://www.uoc.edu	

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
_utma		.uoc.edu	/	Wed, 09 Nov 2022 01:12:06 GMT	62	false	false
_utmb		.uoc.edu	/	Mon, 09 Nov 2020 01:42:06 GMT	31	false	false
_utmc		.uoc.edu	/	Session	15	false	false
_utmt		.uoc.edu	/	Mon, 09 Nov 2020 01:20:44 GMT	7	false	false
_utmv		.uoc.edu	/	Wed, 09 Nov 2022 01:12:06 GMT	53	false	false
_utmnz		.uoc.edu	/	Wed, 09 Dec 2020 01:12:06 GMT	76	false	false
_dc_gtm_UA-1571980-43		.uoc.edu	/	Mon, 09 Nov 2020 01:13:07 GMT	22	false	false
_fbp		.uoc.edu	/	Sat, 06 Feb 2021 02:31:15 GMT	32	false	false
_gat_gtag_UA_54150984_4		.uoc.edu	/	Sun, 08 Nov 2020 16:01:23 GMT	24	false	false
_gat_gtag_UA_121777415_1		.uoc.edu	/	Sat, 07 Nov 2020 22:25:16 GMT	25	false	false
_gat_UA-1571980-43		.uoc.edu	/	Mon, 09 Nov 2020 01:16:05 GMT	19	false	false
_ga		.uoc.edu	/	Sun, 08 Nov 2020 16:01:11 GMT	5	false	false
_ga		.uoc.edu	/	Wed, 09 Nov 2022 01:15:05 GMT	30	false	false
_gclau		.uoc.edu	/	Fri, 29 Jan 2021 15:27:59 GMT	32	false	false
_gid		.uoc.edu	/	Tue, 10 Nov 2020 01:15:05 GMT	31	false	false
_hjAbsoluteSessionInProgress		.uoc.edu	/	Mon, 09 Nov 2020 01:45:25 GMT	29	false	false
_hjid		.uoc.edu	/	Sun, 31 Oct 2021 15:27:59 GMT	41	false	false
_hjIncludedInPageviewSample		www.uoc.edu	/	Sun, 08 Nov 2020 01:39:15 GMT	28	false	false
_hjid		.uoc.edu	/	Session	11	false	false
ADRM		.uoc.edu	/	Session	84	false	true
BiGipServerportal_webserver		www.uoc.edu	/	Session	47	true	false
campusJWT		.uoc.edu	/	Session	1...	false	false
COOKIE_ORDERID		.uoc.edu	/	Sat, 07 Nov 2020 20:23:00 GMT	24	false	false
cto_bundle		.uoc.edu	/	Wed, 08 Dec 2021 05:22:55 GMT	233	false	false
III_ENCORE_PATRON		.uoc.edu	/	Session	24	false	false
III_EXPT_FILE		.uoc.edu	/	Session	20	false	false
III_SESSION_ID		.uoc.edu	/	Session	46	false	false
JSESSIONID		.uoc.edu	/iii/encore/	Session	42	true	false
SESSION_LANGUAGE		.uoc.edu	/	Session	19	false	false
source		.uoc.edu	/	Session	8	false	false
tipousuario		.uoc.edu	/	Tue, 02 Nov 2021 19:19:49 GMT	22	false	false
uocLanguage		.uoc.edu	/	Thu, 07 Nov 2020 01:12:08 GMT	13	false	false
user_id		.uoc.edu	/	Session	39	false	false

Figura 15: Cookies de la página web

Referencias

- [1] **Testing Information Gathering**
OWASP
https://wiki.owasp.org/index.php/Testing_Information_Gathering
- [2] **What is Shodan?**
Shodan - Help Center
<https://help.shodan.io/the-basics/what-is-shodan>
- [3] **Search Web by Domain**
Netcraft
<https://searchdns.netcraft.com/>
- [4] **Maltego is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks.**
Malego
<https://www.maltego.com/>
- [5] **Introducing ZAP**
OWASP ZAP
<https://www.zaproxy.org/getting-started/>
- [6] **SpiderFoot HX: OSINT for Professionals**
<https://www.spiderfoot.net/hx/>
- [7] **SpiderFoot 2.12 includes many new modules, including SecurityTrails, ARIN and Full-Contact.com among a number of improvements and bug fixes.**
SpiderFoot
<https://www.spiderfoot.net/spiderfoot-2-12-includes-many-new-modules/>
- [8] **Network exploration tool and security / port scanner**
nmap
<https://nmap.org/>
- [9] **Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items**
Nikto
<https://cirt.net/Nikto2>
- [10] **Identify the technology stack that powers a website and explore the Web of Things**
Whatweb
<http://www.morningstarsecurity.com/research/whatweb>
- [11] **What does “x-powered by” mean?**
Stack Overflow
<https://stackoverflow.com/questions/33580671/what-does-x-powered-by-mean>
- [12] **Identify technologies on websites**
Wappalyzer
<https://www.wappalyzer.com/>
- [13] **What is `var _gaq = _gaq || []`; for?**
Stack Overflow
<https://stackoverflow.com/questions/2538252/what-is-var-gaq-gaq-for>