

MISTIC

Seguridad en Bases de Datos

Arquitectura de Aplicaciones Web

Objetivo: Oxfam

Unai Gamarra Aguirre, DNI: 41515348A

APARTADO 1

Resumen Ejecutivo

La web de Oxfam tiene buena presentación. Lo primero que aparece es una sección principal, desde la que se puede pasar a otras como donativos, firmas, tienda o inscripción como socio.

A continuación, la información que hemos podido recabar sobre el sitio.

Nivel de Red

- Rangos de IP:

La página principal y sus alternativas (alias), se mueven entre la IP 104.17.122.180 y la 104.17.126.180, o sea las cinco que resultarían de aumentar el 122 hasta 126, ambas inclusive.

Además hemos encontrado direcciones de IPV6, también un rango comprendido entre 2606:4700::6811:7ab4 y 2606:4700::6811:7eb4, cambiando la tercera letra por el final (de "a" a "e").

- Puertos abiertos:

Hemos encontrado cuatro puertos abiertos:

- 80: HTTP. Puerto http normal.
- 443: HTTPS. Puerto http seguro (el que usa normalmente).
- 8080: HTTP-PROXY. Alternativa al puerto http normal.
- 8443: HTTPS-ALT. Alternativa al puerto http seguro.

- Aplicativos:

Hay varios formularios desarrollados en Javascript y que utilizan PHP, por ejemplo para hacer donativos o hacerse socio. Además hay una tienda online.

- CMS:

En la sección de firmas, hemos encontrado el Gestor de contenidos *Drupal*.

Nivel de Dominio

Oxfam ha contratado los servicios de la empresa Cloudflare, para el hosting de la web. Como consecuencia, los servidores son de dicha empresa.

- DNS:

Los servidores DNS que hemos encontrado son:

- 54.154.104.202
- 54.76.228.17

- Servidores:

A continuación una relación de servidores que alojan la web con sus IP:

- ns-46.awsdns-05.com, 205.251.192.46
- ns-834.awsdns-40.net, 205.251.195.66
- ns-1433.awsdns-51.org, 205.251.197.153
- ns-1765.awsdns-28.co.uk, 205.251.198.229

Hemos encontrado un dominio (airspace.com), perteneciente a la empresa "domainsbyproxy.com", que a su vez es de Cloudflare.

En al menos algunas secciones de la web se ha utilizado el servidor *Nginx*.

- Alias de hosting:
www.oxfamintermon.org es alias de 426027.group27.sites.hubspot.net, que a su vez es alias de group27.sites.hscoscdn20.net

Nivel de Aplicativo

- Intranet:

La IP de la Intranet que hemos encontrado es 77.240.125.4, está alojada en "intranet.oxfamintermon.org".

- Correo:

Hay dos servidores de correo en: mail.oxfamintermon.org y mx2.oxfamintermon.org. Con autenticación LDAP.

- Tecnologías:

Se han encontrado rastros de:

- PHP.
- JavaScript con Framework TweenMax 2.0.2 y diferentes librerías.
- Sistema operativo Debian.
- Servidor Web Apache 2.4.25.
- Framework para web Bootstrap.
- Widget FlexSlider para web.

- Comentarios:

Nivel de Cifrado

- Certificados:

Se han encontrado certificados SSL, con la entidad certificadora, el receptor y la clave pública.

APARTADO 2

Metodología utilizada y Evidencias

La metodología utilizada para elaborar la PEC ha consistido en utilizar las herramientas propuestas en la Guía OWASP de Pruebas para Recabar Información [1]. Siempre usando herramientas de tipo pasivo y no intrusivo, como se requería en el enunciado.

Además nos hemos apoyado en el foro de la asignatura y en los comentarios de los compañeros, para obtener conocimientos adicionales sobre herramientas que no están incluidas en la guía.

El análisis de la web ha sido exhaustivo y punto por punto de la guía OWASP. Ha habido herramientas que no hemos podido utilizar debido a fallos en configuraciones o puesta a punto.

Algunos de los puntos de la guía han sido redundantes o no aplicables al caso propuesto, por lo que se han omitido.

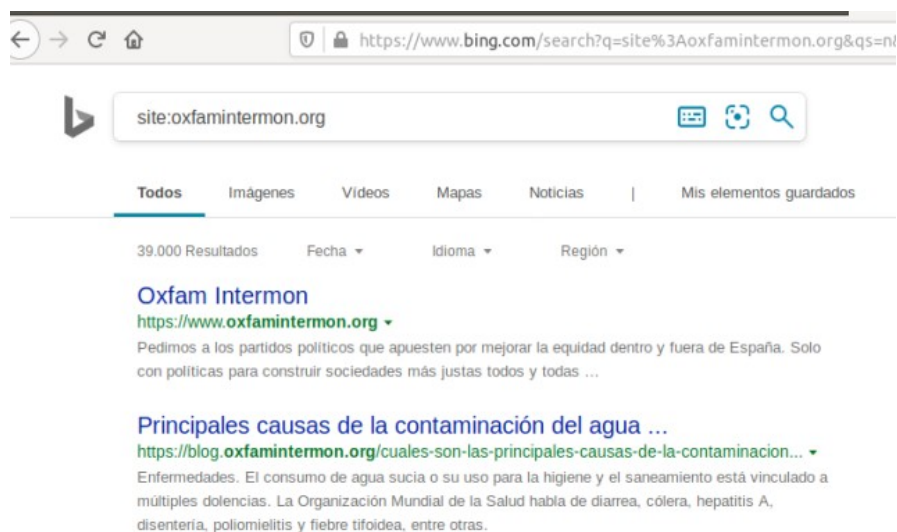
No hemos incluido resultados poco relevantes para la investigación.

A continuación pondremos las pruebas, con los resultados y la información útil obtenida en cada una de ellas.

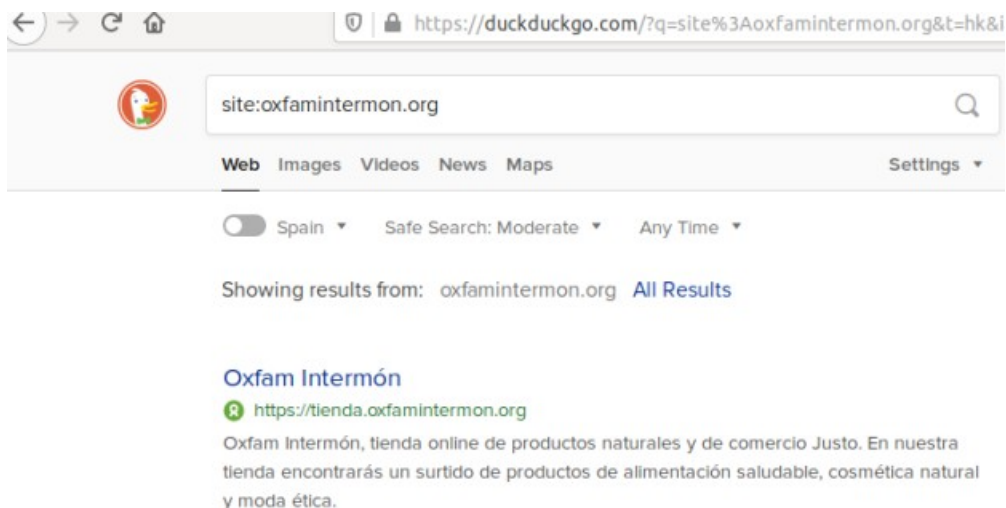
Objetivo: <https://www.oxfamintermon.org>

1. Búsquedas usando diferentes motores para descubrir fugas de información.

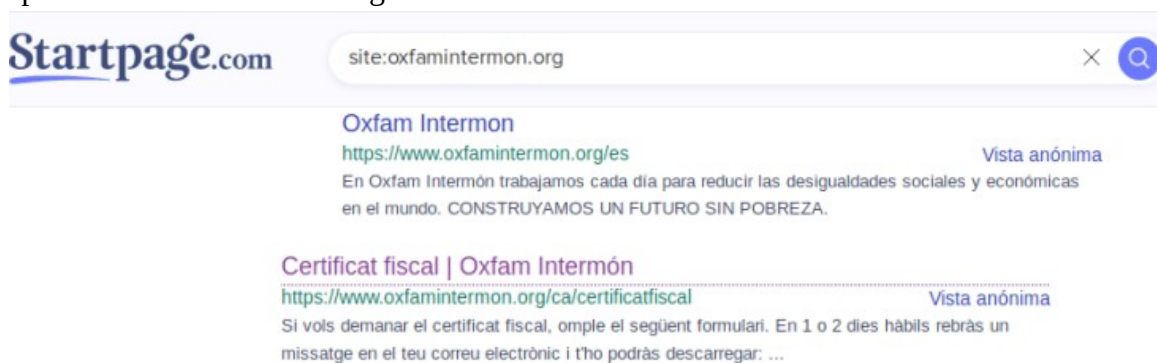
- Bing: Descubrimos un blog activo: <https://blog.oxfamintermon.org>



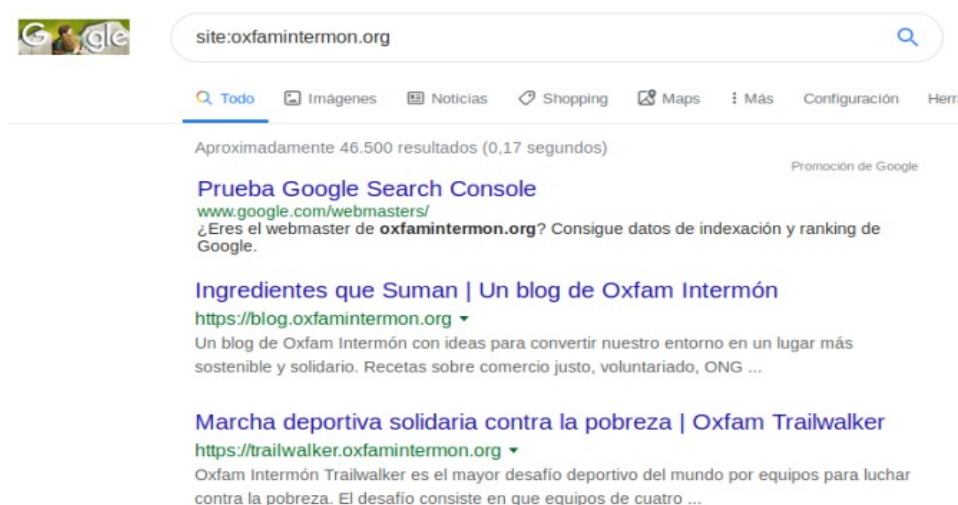
- Duck Duck Go: Hay una tienda en la página: <https://tienda.oxfamintermon.org>



- Startpage: Encontramos una sección con un formulario para pedir un informe fiscal: <https://web.oxfamintermon.org/ca/certificatfiscal>



- Google: En la versión *cached* de la página no hemos visto nada extraño. Haciendo una búsqueda con “site:oxfamintermon.org” vemos otra sección: trailwalker.



2. FingerPrinting del Servidor Web

2.1. NMAP [2]

Herramienta para escaneo de puertos y búsqueda de vulnerabilidades, con opciones activas o pasivas. En nuestro caso hemos utilizado la configuración básica, que es pasiva: nmap www.oxfamintermon.org

```
unai@unai-VirtualBox:~$ nmap www.oxfamintermon.org
Starting Nmap 7.60 ( https://nmap.org ) at 2019-11-09 03:21 CET
Nmap scan report for www.oxfamintermon.org (104.17.124.180)
Host is up (0.025s latency).
Other addresses for www.oxfamintermon.org (not scanned): 2606:4700::6811:7db4 2606:4700::6811:7ab4 2606:4700::6811:7cb4 2606:4700::6811:7eb4 2606:4700::6811:7fb4 104.17.125.180 104.17.126.180 104.17.123.
80 104.17.122.180
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```

Obtenemos la ip: 104.17.124.180 y 4 puertos abiertos (80, 443, 8080, 8443)

2.2. NETCAT

Comando de Unix para conectarse a una dirección y puerto especificados, para poder hacer peticiones por consola de comandos.

Haciendo Netcat a la IP obtenida, en el puerto 80 (*http*). Consultamos una cabecera de HTTP.

```
unai@unai-VirtualBox:~$ nc 104.17.124.180 80
HEAD / HTTP/1.0

HTTP/1.1 400 Bad Request
Date: Sat, 09 Nov 2019 02:48:42 GMT
Content-Type: text/html
Content-Length: 155
Connection: close
Server: cloudflare
CF-RAY: 532c780a083ad675-MAD
```

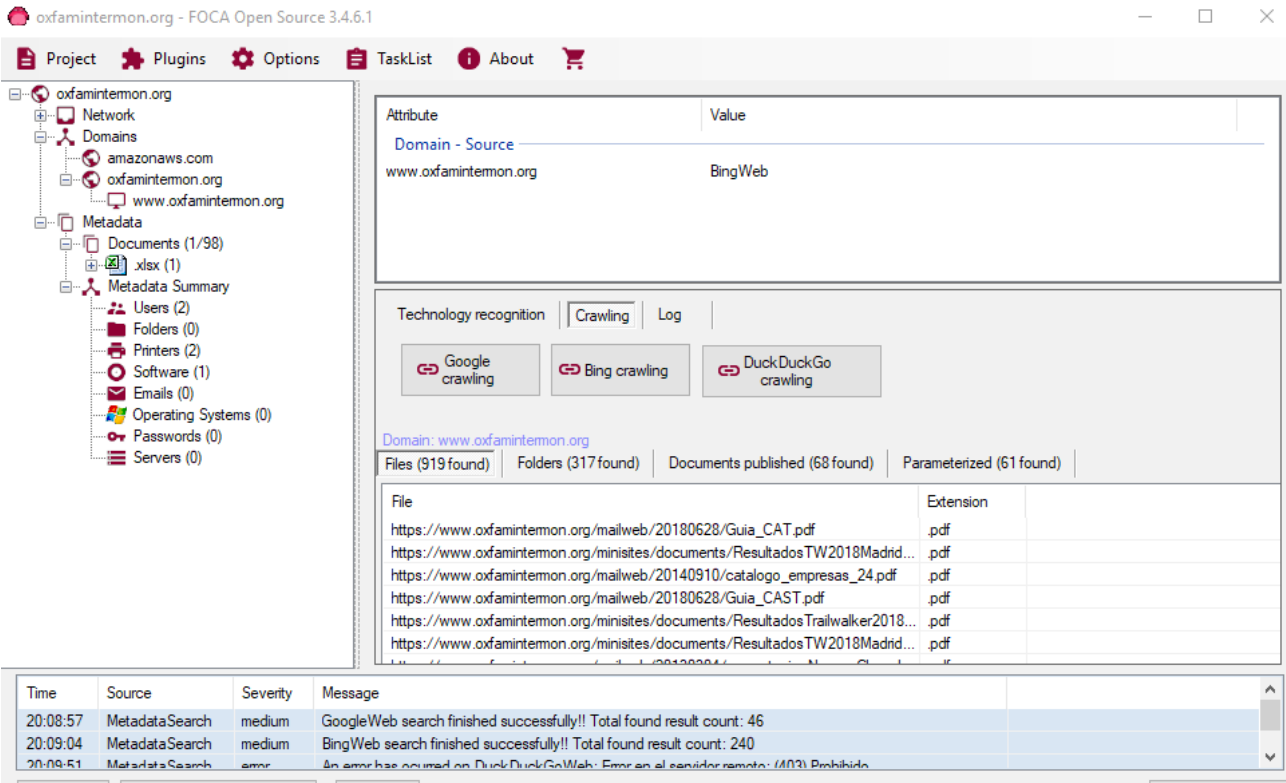
Nos deniega la petición y dice que el servidor es Cloudflare, una empresa de gestión de servidores y DNS.

Parece que Oxfam ha contratado los servicios de dicha empresa para que aloje su web y gestione la seguridad de la misma.

2.3. FOCA [3]

Es una herramienta que explora el dominio y obtiene información sobre la estructura y los ficheros accesibles.

Hemos encontrado mucha información sobre la estructura de la web y archivos colgados (pdf, excel) .



También nos ha dado las IP de los servidores DNS:

IP Addresses - Source	
54.154.104.202	DuckDuckGoWeb > DNS resolution [54.154.104.202]
54.154.104.202	BingWeb > Inferred by www.oxfamintemon.org [oxfamintemon.org] > DNS resol...
54.76.228.17	BingWeb > Inferred by www.oxfamintemon.org [oxfamintemon.org] > DNS resol...
54.76.228.17	DuckDuckGoWeb > DNS resolution [54.76.228.17]

Y el archivo Robots.txt:

```
User-agent: *
Disallow: /_hcms/preview/
Disallow: /hs/manage-preferences/
```

En este caso solo no permite el acceso a dos directorios, uno de los cuales parece ser para gestionar preferencias.

Tras descargar todos los documentos (PDF, html y excel) que hemos encontrado y analizar la meta información (*Metadata*); hemos encontrado 15 usuarios, 180 directorios, 2 impresoras y 19 programas distintos utilizados.

Los directorios no han sido de mucha utilidad, ya que muchos son de fuera de la web.
El resto de datos quizá sean útiles:

- Usuarios

Attribute	Value
All users found (15) - Times found	
Name	usuario
Name	Sandra Ameller Masuet
Name	aramachandran
Name	Ibertrand
Name	cuentas1
Name	pcorcuera
Name	pcorcuera
Name	Peter
Name	omunoz
Name	Tim Brown
Name	Diego Alejo Vázquez Pimentel, Iñigo Macías Aymar y Max Lawson
Name	Diego Alejo Vázquez Pimentel, Iñigo Macías Aymar y Max Lawson
Name	mpuigdelivol
Name	Mpresa
Name	margimon

- Impresoras

Attribute	Value
All printers found (2) - Times found	
Printer Name	\\NIGER\P2B
Printer Name	\\NIGER\P2A


- Software

Attribute	Value
All software found (19) - Times found	
Software	doPDF Ver 7.2 Build 363 (Windows 7 Home Premium Edition (SP 1) - Version: 6....
Software	Adobe Illustrator CS6 (Macintosh)
Software	Adobe PDF Library 10.01
Software	Microsoft Office
Software	PScript5.dll Version 5.2.2
Software	Acrobat Distiller 8.3.1
Software	FreeHand MX: pictwpstops filter 1.0
Software	Acrobat Distiller 7.0
Software	Adobe InDesign CC 2015 (Macintosh)
Software	Adobe PDF Library 15.0
Software	Adobe Illustrator CC 2014 (Macintosh)
Software	Adobe PDF Library 11.00
Software	Microsoft Office 2007
Software	Microsoft? Publisher 2016
Software	Adobe InDesign CC (Macintosh)
Software	Adobe PDF Library 10.0.1
Software	Microsoft Office 2003
Software	Adobe PDF Library 11.0
Software	GPL Ghostscript 8.15

2.4. NETCRAFT [4]

Es un buscador con múltiples opciones, entre las que destacan las opciones para testeo de seguridad.

Nos da bastante información, como que el gestor de la red es Cloudflare, el nombre del servidor y un historial de direcciones IP.



Site report for www.oxfamintermon.org

Search...

Netcraft Extension

Home

Download Now!

Report a Phish

Site Report

Top Reporters

Incentives for reporters

Phishiest TLDs

Phishiest Countries

Phishiest Hosters

Phishiest Certificate Authorities

Phishing Map

Takedown Map

Most Popular Websites

Branded Extensions

Tell a Friend

Phishing & Fraud

Phishing Site Feed

Hosting Phishing Alerts

SSL CA Phishing Alerts

Protection for TLDs against Phishing and Malware

Deceptive Domain Score

Bank Fraud Detection

Phishing Site Countermeasures

Extension Support

FAQ

Glossary

Contact Us

Report a Bug

Tutorials

Installing the Extension

Using the Extension

Lookup another URL:

Enter a URL here

Share

Background

Site title	Oxfam Intermon	Date first seen	October 2013
Site rank		Primary language	Spanish
Description	En Oxfam Intermon trabajamos cada día para reducir las desigualdades sociales y económicas en el mundo. CONSTRUYAMOS UN FUTURO SIN POBREZA		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.oxfamintermon.org	Netblock Owner	Cloudflare, Inc.
Domain	oxfamintermon.org	Nameserver	ns-1765.awsdns-28.co.uk
IP address	104.17.125.180 (VirusTotal)	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	2606:4700:0:0:0:0:6811:7db4	Reverse DNS	unknown
Domain registrar	pir.org	Nameserver organisation	whois.nic.uk
Organisation	Intermon Oxfam, ES	Hosting company	unknown
Top Level Domain	Organization entities (.org)	DNS Security Extensions	unknown
Hosting country	US		

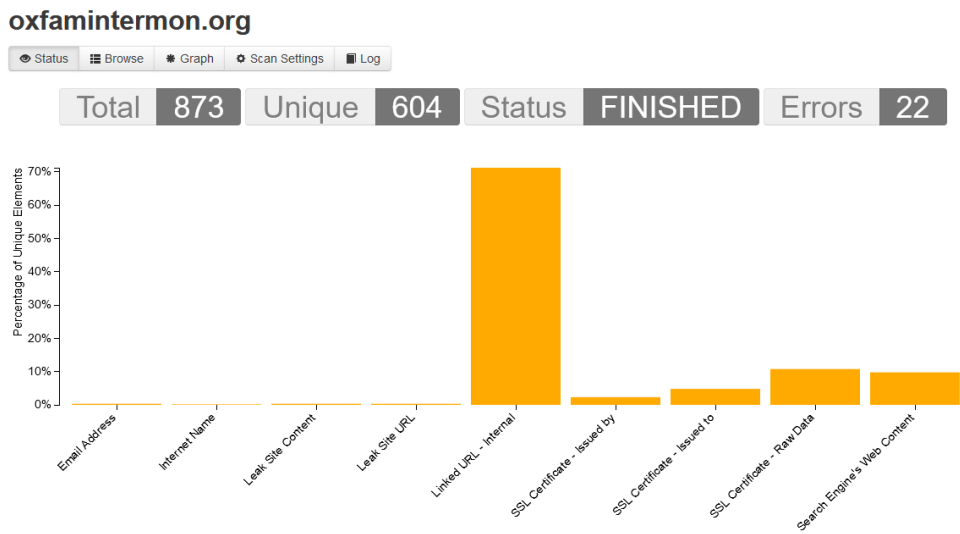
Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.124.180	Linux	cloudflare	9-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.126.180	Linux	cloudflare	8-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.125.180	Linux	cloudflare	7-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.124.180	Linux	cloudflare	6-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.122.180	Linux	cloudflare	5-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.123.180	Linux	cloudflare	4-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.126.180	Linux	cloudflare	4-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.124.180	Linux	cloudflare	3-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.126.180	Linux	cloudflare	2-Nov-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.124.180	Linux	cloudflare	2-Nov-2019

2.5 SPIDERFOOT [5]

Es una herramienta que, una vez instalada, permite utilizar un motor de búsqueda propio.

Ha devuelto muchos datos:



Entre ellos las entidades que proporcionan los certificados SSL:

oxfamintermon.org

Search results for 'SSL Certificate - Issued by':

Data Element	Source Data Element	Source Module	Identified
C=ES, ST=Illes Balears, L=Manacor, O=Soluciones Corporativas IP, SL, CN=Don Dominio / MrDomain RSA DV CA	[{"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"clientes.oxfamintermon.org","min_cert_id":2070016297,"min_entry_timestamp":"2019-11-04T08:44:16.001","not_before":"2019-11-04T07:44:15","not_after":"2020-02-02T07:44:15"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"clientes.oxfamintermon.org","min_cert_id":2070016267,"min_entry_timestamp":"2019-11-04T08:44:15.867","not_before":"2019-11-04T07:44:15","not_after":"2020-02-02T07:44:15"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"empleo-sede.oxfamintermon.org","min_cert_id":2039325833,"min_entry_timestamp":"2019-10-25T06:11:00.547","not_before":"2019-10-25T05:11:00","not_after":"2020-01-23T05:11:00"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"empleo-sede.oxfamintermon.org","min_cert_id":2034456493,"min_entry_timestamp":"2019-10-"}]	sfp_crt	2019-11-10 08:30:05

Y a quién le son proporcionados dichos certificados:

oxfamintermon.org

Search results for 'SSL Certificate - Issued to':

Data Element	Source Data Element	Source Module	Identified
C=ES, ST=Barcelona, L=Barcelona, O=FUNDACION INTERMON OXFAM FUNDACION PRIVADA, OU=Internet, OU=Terms of use at www.verisign.com/rpa (c)05, CN=www.oxfamintermon.org	[{"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"clientes.oxfamintermon.org","min_cert_id":2070016297,"min_entry_timestamp":"2019-11-04T08:44:16.001","not_before":"2019-11-04T07:44:15","not_after":"2020-02-02T07:44:15"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"clientes.oxfamintermon.org","min_cert_id":2070016267,"min_entry_timestamp":"2019-11-04T08:44:15.867","not_before":"2019-11-04T07:44:15","not_after":"2020-02-02T07:44:15"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"empleo-sede.oxfamintermon.org","min_cert_id":2039325833,"min_entry_timestamp":"2019-10-25T06:11:00.547","not_before":"2019-10-25T05:11:00","not_after":"2020-01-23T05:11:00"}, {"issuer_ca_id":16418,"issuer_name":"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3","name_value":"empleo-sede.oxfamintermon.org","min_cert_id":2034456493,"min_entry_timestamp":"2019-10-"}]	sfp_crt	2019-11-10 08:30:21

También nos ha proporcionado la estructura interna de la web, con los directorios; esta información ya ha sido obtenida anteriormente (2.1 - FOCA) por lo que no la hemos repetido aquí.

Los certificados, con sus claves públicas:

oxfamintermon.org

StatusBrowseGraphScan SettingsLog

Search...

Browse > SSL Certificate - Raw Data

<input type="checkbox"/> Data Element	Source Data Element	Source Module	Identified
<div><div><input type="checkbox"/></div><div>Certificate: Data: Version: 3 (0x2) Serial Number: 01:04:c5:6a:b9:28:e8:79:1a:02:4e:65:41:68:db:70 Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, ST=CA, L=San Francisco, O=CloudFlare, Inc., CN=CloudFlare Inc RSA CA-1 Validity Not Before: May 7 00:00:00 2018 GMT Not After : May 7 12:00:00 2019 GMT Subject: C=US, ST=MA, L=Cambridge, O=HubSpot, Inc., CN=sumate.oxfamintermon.org Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:f3:80:45:41:04:29:48:0d:67:28:0c:03:f4:de: f0:eb:0e:ca:ae:fa:a7:90:e9:1d:47:ca:cd:0c:0a: a1:dd:a8:f9:e1:5b:8d:b8:66:22:e5:fd:fa:59:5d: 4f:1a:89:29:74:19:69:2c:62:d3:f2:c0:f7:09:31: 17:d3:c5:3d:3a:a7:f7:1f:72:2b:26:55:11:b1:7a: 78:9a:98:d0:c0:90:49:3d:b8:39:47:6f:18:41:ac:</div></div>	oxfamintermon.org	sfp_crt	2019-11-10 08:30:14

Y detalles sobre los elementos Javascript que hay en la web, ha contabilizado 59.

Además de accesos a dos ficheros con información sobre la estructura de dominios de la web:

1. <code>activismo.oxfamintermon.org</code>	16. <code>mail.oxfamintermon.org</code>
2. <code>algomasqueunregalo.oxfamintermon.org</code>	17. <code>mkt.oxfamintermon.org</code>
3. <code>blog.oxfamintermon.org</code>	18. <code>mx2.oxfamintermon.org</code>
4. <code>clientes.oxfamintermon.org</code>	19. <code>recursos.oxfamintermon.org</code>
5. <code>empleo-f2f.oxfamintermon.org</code>	20. <code>sa.oxfamintermon.org</code>
6. <code>empleo-general.oxfamintermon.org</code>	21. <code>smscrm.intermonoxfam.org</code>
7. <code>empleo-internacional.oxfamintermon.org</code>	22. <code>sumate.oxfamintermon.org</code>
8. <code>empleo-sede.oxfamintermon.org</code>	23. <code>tienda.oxfamintermon.org</code>
9. <code>empleo-voluntariado.oxfamintermon.org</code>	24. <code>trackings.oxfamintermon.org</code>
10. <code>erecruiting.oxfamintermon.org</code>	25. <code>trailwalker.oxfamintermon.org</code>
11. <code>eureka.oxfamintermon.org</code>	26. <code>web.oxfamintermon.org</code>
12. <code>fidelizacion.oxfamintermon.org</code>	27. <code>www.oxfamintermon.org</code>
13. <code>hubspot.oxfamintermon.org</code>	28. <code>www.tienda.oxfamintermon.org</code>
14. <code>imagenesypalabras.oxfamintermon.org</code>	
15. <code>intranet.oxfamintermon.org</code>	

Hemos ido probando cada entrada de la lista en el navegador:

- La entrada 14 nos ha dado un mensaje de afiliado no encontrado.
- La entrada 15 nos ha dado la IP de la intranet (77.240.125.4).
- La entrada 20 nos lleva a una pantalla de login de Pulse Connect Secure, mirando el código fuente de la página vemos que hay un *Realm* oculto de LDAP.

```
<input id="realm_16" type="hidden" name="realm" value="LDAP Realm">
```

- La entrada 24 nos enseña información que podrían no querer mostrar:

Prova Trackings

- [Open campanya 1, id_bp 12345](#)
- [Click campanya 1, id_bp 12345, id_tracking 10](#)
- [Open campanya 2, id_bp 67890](#)
- [Click campanya 2, id_bp 67890, id_tracking 20](#)
- [Open campanya 3, id_bp 98765](#)
- [Click campanya 3, id_bp 98765, id_tracking 30](#)
- [Open campanya 4, id_bp 54321](#)
- [Click campanya 4, id_bp 54321, id_tracking 40](#)

Hemos inferido la dirección del correo web (*mailweb*), a la que se puede acceder desde el navegador:



Index of /mailweb

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[DIR]	20111024/	2019-10-02 13:27	-	
[DIR]	20111117/	2019-10-02 13:27	-	
[DIR]	20111128A/	2019-10-02 13:27	-	
[DIR]	20111219/	2019-10-02 13:27	-	

Dentro de cada carpeta están las webs e imágenes que corresponden a cada una de las secciones del dominio.


3. Revisar los Meta archivos del Servidor Web

El fichero robots.txt ya ha sido previamente obtenido, está en <https://www.oxfamintermon.org/robots.txt>

```
User-agent: *
Disallow: /_hcms/preview/
Disallow: /hs/manage-preferences/
```

Para todos los agentes de búsqueda, prohíbe el acceso a dos directorios.
Hemos intentado acceder a los directorios que pertenecen a la misma ruta sin éxito.

También hemos obtenido el fichero robots.txt de uno de los servidores (<https://cdn2.hubspot.net/robots.txt>)



```
User-agent: *
Disallow: /hub/53/Increase_Volunteer_Involvement_in_2013.pdf
Disallow: /hub/53/an_introductory_guide_to_facebook_for_business.pdf
Disallow: /hub/53/Final_62_Social_Media_Tips_from_Around_the_World_Ebook.pdf
Disallow: /hub/53/Growing_Your_Nonprofit_HubSpot.pdf
Disallow: /hub/53/Inbound_Marketing_NEC_11_2_Final.pdf
Disallow: /hub/53/Template_-_Managing_and_Organizing_Google_AdWords_Campaigns.xlsx
Disallow: /hub/53/archive/docs/hubspot_business_grader_july.xlsx
Disallow: /hub/53/archive/docs/pdf_website_redesign_marketing_april-2009_webinar.pdf
```

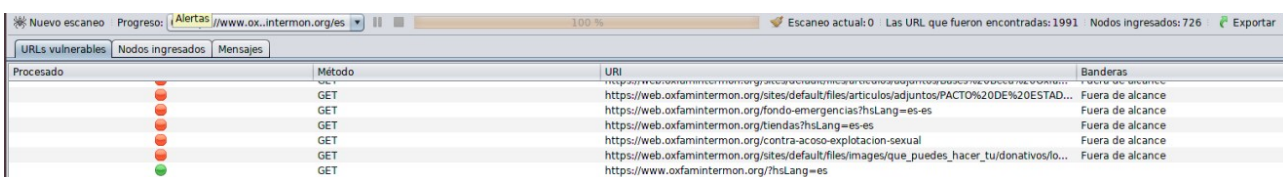
En este caso el fichero es muy completo a la hora de prohibir acceso a *crawlers* a la estructura interna de la web. De hecho es tan completo que da información sobre la misma estructura, poniendo de relieve multitud de archivos PDF y hojas de cálculo, además de parte de la organización de los directorios.

4. Enumeración de Aplicaciones en el Servidor Web

4.1 ZAP OWASP [6]

Herramienta de código libre para encontrar vulnerabilidades de seguridad.

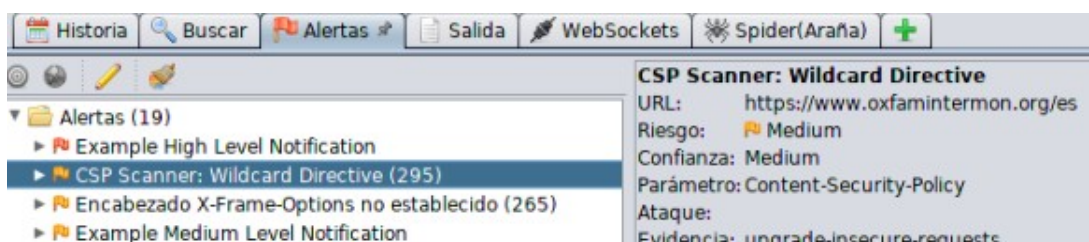
El escaneo pasivo tradicional (spider) ha encontrado 1991 URLs.



Procesado	Método	URI	Banderas
	GET	https://web.oxfamintermon.org/sites/default/files/articulos/adjuntos/PACTO%20DE%20ESTAD...	Fuera de alcance
	GET	https://web.oxfamintermon.org/fondo-emergencias/hsLang=es-es	Fuera de alcance
	GET	https://web.oxfamintermon.org/tiendas/hsLang=es-es	Fuera de alcance
	GET	https://web.oxfamintermon.org/contras-acoso-explotacion-sexual	Fuera de alcance
	GET	https://web.oxfamintermon.org/sites/default/files/images/que_puedes_hacer_tu/donativos/fo...	Fuera de alcance
	GET	https://www.oxfamintermon.org/hsLang=es	

En la sección de alertas nos advierten de dos posibles vulnerabilidades de nivel medio:


- El Encabezado X-Frame-Options no está establecido, que serviría para proteger contra ataques de tipo “Clickjacking”.
- Las directivas o bien permiten el uso de comodines, o no están definidas, o definidas demasiado ampliamente: script-src, style-src, img-src, etc.



Además hay muchas alertas de nivel bajo e informativas, pero no nos centraremos en ellas.

4.2. NETCRAFT [7]



Búsqueda de DNS en Netcraft, nos dice el bloque de red y que corre sobre un sistema operativo Linux – Debian

	Site	Site Report	First seen	Netblock	OS
1.	www.oxfamintermon.org		october 2013	amazon data services ireland limited	linux - debian

4.3. DOMAINTOOLS.COM – REVERSE IP [8]

Nos da un dominio: airspace.com

Reverse IP Lookup Results – 1 domain hosted on IP address 104.17.124.180

Domain	View Whois Record	Screenshots
1. airspace.com		

Mirando el whois, vemos que es de Cloudflare:

Name Servers	LARA.NS.CLOUDFLARE.COM (has 18,546,634 domains) TONY.NS.CLOUDFLARE.COM (has 18,546,634 domains)
Tech Contact	Registration Private Domains By Proxy, LLC DomainsByProxy.com, Scottsdale, Arizona, 85260, us airspace.com@domainsbyproxy.com (p) 14806242599 (f) 14806242598

4.4. WEBHOSTING.INFO [9]

Obtenemos más nombres de servidores registrados.

```
Registrant Organization: Intermon Oxfam
Registrant State/Province: BARCELONA
Registrant Country: ES
Name Server: NS-1433.AWSDNS-51.ORG
Name Server: NS-46.AWSDNS-05.COM
Name Server: NS-1765.AWSDNS-28.CO.UK
Name Server: NS-834.AWSDNS-40.NET
```

4.5. DNSSTUFF.COM [10]

Nos da los mismos nombres que el anterior, con las IP.

Results for Target: oxfamintermon.org

```
Created Date : 2012-05-02T08:51:55Z
Updated Date : 2019-04-25T23:22:42Z
WHOIS Server: whois.pir.org
```

Discovered Nameservers

```
NS-1433.AWSDNS-51.ORG | 205.251.197.153
NS-46.AWSDNS-05.COM | 205.251.192.46
NS-1765.AWSDNS-28.CO.UK | 205.251.198.229
NS-834.AWSDNS-40.NET | 205.251.195.66
```

Registrar Information

Acens Technologies, S.L.U.

Please note these results are obtained from third party databases (whois.pir.org)

Contact Information

Registrant

```
Intermon Oxfam
BARCELONA
ES
```


4.6. NIKTO [11]

Utilidad que busca vulnerabilidades y puertos abiertos, programada en PERL.

Encuentra varias vulnerabilidades y zonas sin proteger adecuadamente, además de la interfaz del servidor Apache, que está protegida o prohibida.

```

unai@unai-VirtualBox:~/Descargas/nikto-master/program$ perl nikto.pl -h www.oxfamintermon.org
- Nikto v2.1.6
-----
+ Target IP:      104.17.124.180
+ Target Hostname: www.oxfamintermon.org
+ Target Port:    80
+ Message:       Multiple IP addresses found: 104.17.124.180, 104.17.125.180, 104.17.122.180, 104.17.126.180, 104.17.123.180
+ Start Time:    2019-11-11 04:19:42 (GMT1)
-----
+ Server: cloudflare
+ 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
+ Uncommon header 'x-hs-https-only' found, with contents: worker
+ 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 fashion to the MIME type
+ Root page / redirects to: https://www.oxfamintermon.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-trace' found, with contents: 2B38265D5B207DA9C984390468EC8F95E925827F62000000000000000000000000
+ Allowed HTTP Methods: HEAD, POST, GET, OPTIONS
-----
+ /server-status: Apache server-status interface found (protected/forbidden)
+ 7920 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2019-11-11 04:24:22 (GMT1) (280 seconds)
-----
+ 1 host(s) tested

```

4.7. HOST

Comando de Unix para consulta de DNS.

Aquí obtenemos un par de alias para la web, con más aplicaciones de host sacamos las Ips de los Alias.

```

unai@unai-VirtualBox:~/Descargas/spiderfoot-2.12.0-src/spiderfoot-2.12$ host -t
ns www.oxfamintermon.org
www.oxfamintermon.org is an alias for 426027.group27.sites.hubspot.net.
426027.group27.sites.hubspot.net is an alias for group27.sites.hscoscdn20.net.
unai@unai-VirtualBox:~/Descargas/spiderfoot-2.12.0-src/spiderfoot-2.12$

```

```

unai@unai-VirtualBox:~/Descargas/spiderfoot-2.12.0-src/spiderfoot-2.12$ host -l
www.oxfamintermon.org 426027.group27.sites.hubspot.net

;; Connection to 104.17.126.180#53(104.17.126.180) for www.oxfamintermon.org failed: timed out.

```

```

unai@unai-VirtualBox:~/Descargas/spiderfoot-2.12.0-src/spiderfoot-2.12$ host -l
www.oxfamintermon.org 426027.group27.sites.hscoscdn20.net

;; Connection to 104.17.123.180#53(104.17.123.180) for www.oxfamintermon.org failed: timed out.

```

4.8. NSLOOKUP

Herramienta de Unix para conectarse a servidores y obtener información.

Obtenemos nombres de servidores y rangos de Ips.

```
unai@unai-VirtualBox:~/Descargas$ nslookup
> www.oxfamintermon.org
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.oxfamintermon.org canonical name = 426027.group27.sites.hubspot.net.
426027.group27.sites.hubspot.net canonical name = group27.sites.hscoscdn20.net.
Name:   group27.sites.hscoscdn20.net
Address: 104.17.123.180
Name:   group27.sites.hscoscdn20.net
Address: 104.17.122.180
Name:   group27.sites.hscoscdn20.net
Address: 104.17.124.180
Name:   group27.sites.hscoscdn20.net
Address: 104.17.126.180
Name:   group27.sites.hscoscdn20.net
Address: 104.17.125.180
Name:   group27.sites.hscoscdn20.net
Address: 2606:4700::6811:7eb4
Name:   group27.sites.hscoscdn20.net
Address: 2606:4700::6811:7bb4
Name:   group27.sites.hscoscdn20.net
Address: 2606:4700::6811:7db4
Name:   group27.sites.hscoscdn20.net
Address: 2606:4700::6811:7cb4
Name:   group27.sites.hscoscdn20.net
Address: 2606:4700::6811:7ab4
>
```

Hemos podido obtener los servidores de intercambio de correo.

```
> set type=MX
> oxfamintermon.org
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
oxfamintermon.org mail exchanger = 20 mail.oxfamintermon.org.
oxfamintermon.org mail exchanger = 10 mx2.oxfamintermon.org.
```

Usando los servidores de google como base (8.8.8.8), hemos obtenido el origen de DNS (cloudflare).

```
> www.oxfamintermon.org
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.oxfamintermon.org canonical name = 426027.group27.sites.hubspot.net.
426027.group27.sites.hubspot.net canonical name = group27.sites.hscoscdn20.net.

Authoritative answers can be found from:
hscoscdn20.net
  origin = jerry.ns.cloudflare.com
  mail addr = dns.cloudflare.com
  serial = 2032503029
  refresh = 10000
  retry = 2400
  expire = 604800
  minimum = 3600
```

Si buscamos los nombres de los servidores, también los obtenemos.

```
unai@unai-VirtualBox:~/Descargas$ nslookup -querytype=NS oxfamintermon.org
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
oxfamintermon.org nameserver = ns-46.awsdns-05.com.
oxfamintermon.org nameserver = ns-834.awsdns-40.net.
oxfamintermon.org nameserver = ns-1433.awsdns-51.org.
oxfamintermon.org nameserver = ns-1765.awsdns-28.co.uk.
```


5. FingerPrint del Framework de la Aplicación Web

5.1. Analizar Cabeceras HTTP

Lo hemos hecho con *netcat*, herramienta previamente presentada (2.2.).

El campo *X-Powered-By* ha sido desactivado, por lo que no hemos conseguido información del framework de la aplicación web por ahí.

Han debido manipular las cabeceras para que no muestren información sensible.

5.2. Análisis de Cookies

Mirando una de las cookies observamos que el servidor es “*nginx*” [12]



Análisis de Código HTML

No parece haber fugas de información en los comentarios.

5.3. WHATWEB [13]

Nos dice que se han movido permanentemente los servidores a Cloudflare.

```
https://www.oxfamintermon.org [301 Moved Permanently] CloudFlare, Cookies[__cfduid,__cfduid],
Country[UNITED STATES][US],
HTTPServer[cloudflare],
HttpOnly[__cfduid,__cfduid],
IP[104.17.124.180],
RedirectLocation[https://www.oxfamintermon.org/es],
Strict-Transport-Security[max-age=0],
UncommonHeaders[cf-cache-status,cf-ray,access-control-allow-credentials,expect-ct,x-oxfamintermon],
https://www.oxfamintermon.org/es [200 OK] CloudFlare, Cookies[__cfduid,__cfduid],
Country[UNITED STATES][US],
Email[info@OxfamIntermon.org],
Google-Analytics[Universal] [UA-2835792-1],
HTML5, HTTPServer[cloudflare],
HttpOnly[__cfduid,__cfduid],
IP[104.17.126.180],
jQuery[1.11.2],
Meta-Author[Fundación Oxfam Intermón],
MetaGenerator[HubSpot],
Open-Graph-Protocol[website],
Script[text/javascript],
Strict-Transport-Security[max-age=0],
Title[Oxfam Intermón],
UncommonHeaders[cf-cache-status,cf-ray,access-control-allow-credentials,content-security-policy],
X-Powered-By[HubSpot],
X-UA-Compatible[IE=edge]
```

5.4. BLINDELEPHANT [14]

Aplicación para Unix que se conecta a un servidor y compara los *fingerprints* que recibe con una base de datos.

No ha podido comprobar ningún archivo, daban errores 404.
Han debido restringir correctamente el acceso a dichos archivos.

```
unai@unai-VirtualBox:~/Descargas/blindelephant-code-r7-trunk/src$ BlindElephant.py https://www.oxfamintermon.org movabletype
Loaded /usr/local/lib/python2.7/dist-packages/blindelephant/dbs/movabletype.pkl with 101 versions, 2229 differentiating paths, and 216 version groups.
Starting BlindElephant fingerprint for version of movabletype at https://www.oxfamintermon.org

Hit https://www.oxfamintermon.org/mt-static/mt.js
File produced no match. Error: Detected Custom 404

Hit https://www.oxfamintermon.org/mt-static/js/tc/client.js
File produced no match. Error: Detected Custom 404
```

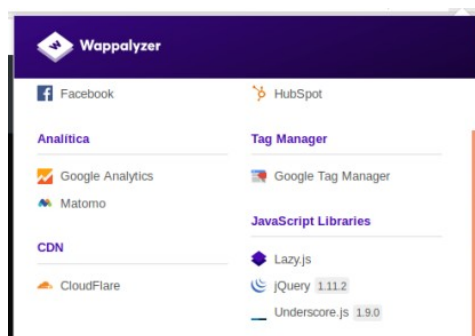
```
unai@unai-VirtualBox:~/Descargas/blindelephant-code-r7-trunk/src$ BlindElephant.py https://www.oxfamintermon.org drupal
Loaded /usr/local/lib/python2.7/dist-packages/blindelephant/dbs/drupal.pkl with 145 versions, 478 differentiating paths, and 434 version groups.
Starting BlindElephant fingerprint for version of drupal at https://www.oxfamintermon.org

Hit https://www.oxfamintermon.org/CHANGELOG.txt
File produced no match. Error: Detected Custom 404
```

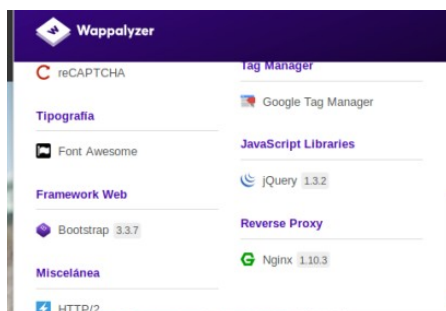
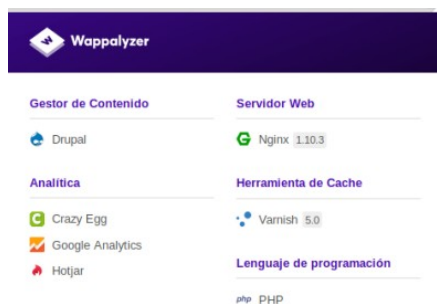
5.5. WAPPALYZER [15]

Es un plugin para Firefox que analiza los programas presentes en una web.

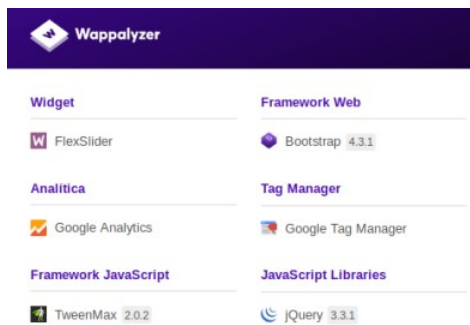
En la página de bienvenida (<https://www.oxfamintermon.org/es>) detecta varias cosas, entre ellas un widget de Facebook y librerías de Javascript.



En la sección de donativos (<https://web.oxfamintermon.org/es/donativos>) detecta varios elementos. A destacar el gestor de contenido (Drupal), el servidor web (Nginx 1.10.3), el lenguaje de programación (PHP) y el framework de la web (Bootstrap 3.3.7).

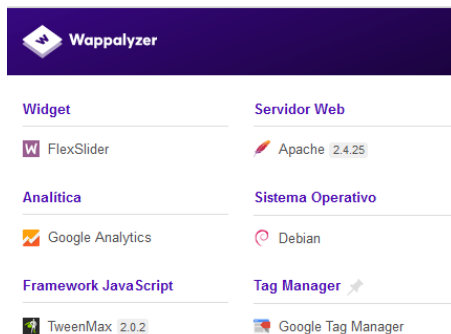


En la sección de firmas (<https://juntassomosvictoria.org/es>) detecta un framework para Javascript (TweenMax 2.0.2) y un Widget (FlexSlider). Cabe destacar que el framework de la web tiene una versión distinta al encontrado anteriormente en la página de donativos, ahora es Bootstrap 4.3.1 y antes era 3.3.7.



Las pruebas anteriores se han hecho con un Ubuntu en máquina virtual. Probando directamente con Windows en la página de firmas, hemos obtenido nueva información:

La versión del servidor web Apache es 2.4.25 y el sistema operativo es Debian.



Bibliografía y Enlaces

1. Guía OWASP de Pruebas para Recabar Información

[Consulta: 9 de Noviembre de 2019].

<https://www.owasp.org/index.php/Testing_Information_Gathering>

2. NMAP

[Consulta: 9 de Noviembre de 2019].

<<https://nmap.org/>>

3. FOCA – Organizaciones de FingerPrinting con Archivos Coleccionados

[Consulta: 9 de Noviembre de 2019].

<<https://www.elevenpaths.com/es/labstools/foca-2/index.html>>

4. NETCRAFT

[Consulta: 9 de Noviembre de 2019].

<<https://www.netcraft.com/>>

5. SPIDERFOOT

[Consulta: 9 de Noviembre de 2019].

<<https://www.spiderfoot.net/>>

6. ZAP OWASP

[Consulta: 9 de Noviembre de 2019].

<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

7. NETCRAFT

[Consulta: 9 de Noviembre de 2019].

<<https://searchdns.netcraft.com/>>

8. DOMAINTOOLS

[Consulta: 9 de Noviembre de 2019].

<<http://whois.domaintools.com/airspace.com>>

9. WEBHOSTING.INFO

[Consulta: 10 de Noviembre de 2019].

<<https://webhosting.info/whois/oxfamintermon.org>>

10. DNSSTUFF

[Consulta: 10 de Noviembre de 2019].

<<https://tools.dnsstuff.com/>>

11. NIKTO

[Consulta: 10 de Noviembre de 2019].

<<https://cirt.net/nikto2>>

12. NGINX

[Consulta: 10 de Noviembre de 2019].

<<https://www.nginx.com/resources/glossary/nginx/>>

13. WHATWEB

[Consulta: 10 de Noviembre de 2019].

<<https://www.whatweb.net/>>

14. BLINDELEPHANT

[Consulta: 11 de Noviembre de 2019].

<<http://blindelephant.sourceforge.net/>>

15. WAPPALYZER

[Consulta: 11 de Noviembre de 2019].

<<https://addons.mozilla.org/es/firefox/addon/wappalyzer/>>