

# **#SEGURIDAD Y ALTA DISPONIBILIDAD**

**@Práctica 3 \**



## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

### @ÍNDICE:

Introducción	2
objetivos	3
footprinting (búsqueda pasiva)	4
una mirada no tan rápida	5
siguiendo la huella con Google hacks	14
fingerprinting (búsqueda activa)	16
Dig	16
FOCA	17
Dominios	17
Metadata	18
conclusión	20
bibliografía	21
Recursos	21

**@INTRODUCCIÓN:**

En la realidad del mundo que experimentamos hoy las empresas que manejan información digitalizada están expuestas a que terceros se apropien de ella sin su conocimiento y/o consentimiento, vulnerando los deseos de la empresa y la ley estatal, pasando a ser posibles responsables subsidiarios de y portadores de una mancha ante la opinión pública que degradará su imagen, traducéndose en la pérdida de miles de euros.

Si bien la seguridad al 100% no existe, sí se pueden estudiar las vulnerabilidades existentes en el sistema y desarrollar/planificar una política interna que bloquee la información importante que permita explotar las vulnerabilidades.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

### @OBJETIVOS:

El propósito fundamental de ésta práctica es que el alumno sea consciente del paso previo a que un tercero obtenga la información digitalizada importante en una empresa, y que pasa por conocer como ése tercero obtiene información del entorno de tal empresa para acceder a sus recursos, e intentar a través del PenTest y con los medios a su alcance interferir en las maniobras que se puedan llevar acabo para tal fin.

Para el ejercicio intentaré obtener toda la información posible acerca del dominio **maridarioja.com**, identificando recursos tecnológicos, estructura y esquema de seguridad utilizado, para tener conciencia de las vulnerabilidades del mismo.

Para ello utilizaremos técnicas de Footprinting tanto *pasivo* como *activo* eligiendo para la realización de la práctica el dominio **maridarioja.com**.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

### @DESARROLLO \ Footprinting pasivo:

*El footprinting pasivo consiste en obtener información por cauces que no sean directamente la fuente. Podemos usar recursos públicos de búsqueda de información, recopilando la información directamente de la web del objetivo, buscadores e incluso revistas y periódicos.*

El objetivo que he seleccionado es el dominio **maridarioja.com**, unas personas que desean mostrar y poner al alcance de los demás los productos riojanos.



Imagen 1: Página de inicio de maridarioja.com

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

Ya soy conocedor del dominio, y voy a intentar saber quien lo posee a través de una consulta whois desde las herramientas de red de mi sistema:

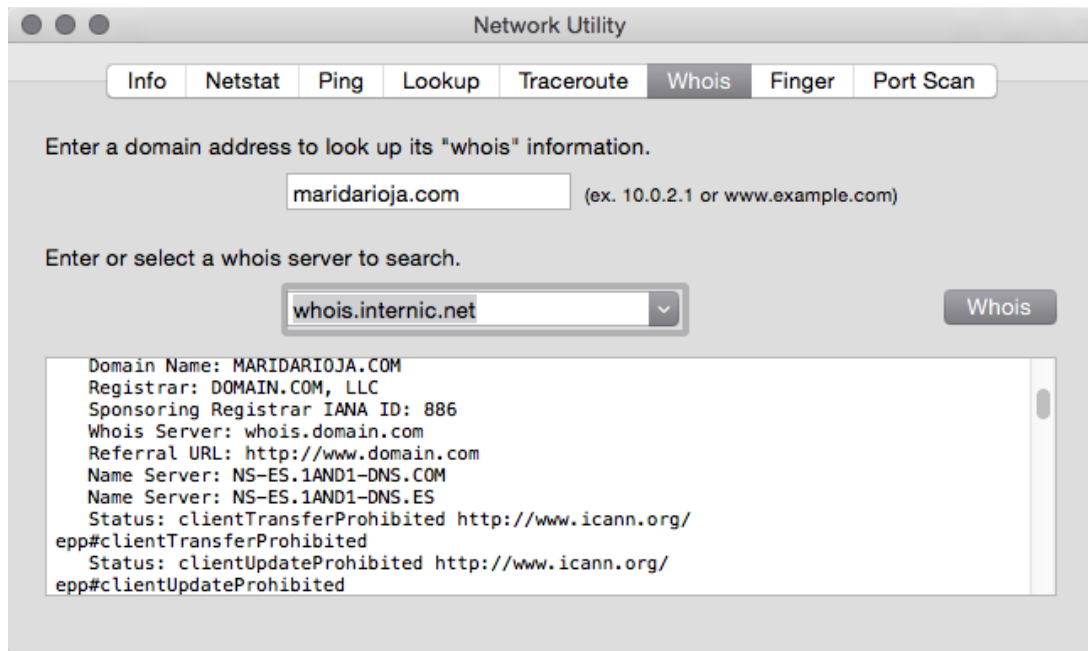


Imagen 2: Resultado sobre consulta whois

El registrante no permite que sus datos personales aparezcan en la consulta.

Del ejercicio de navegar por su sitio web ofrecen un teléfono móvil de contacto: XXXX.

Buscando en StreetView localizo el número de portal especificado, pero parece ser que no es una tienda física tradicional y que probablemente sea un piso, ya que no hay ningún establecimiento con el nombre del dominio en los alrededores.

Posteriormente en la página de Aviso Legal descubro un nombre y dirección completa con la misma dirección indicando un piso, concretamente el 6º A, así como el número de N.I.F. XXXXX.XXX-X que podría ser usado para diferentes propósitos, registrarse en casinos o casas de apuestas, abrir cuentas bancarias online, solicitar préstamos y/o créditos en diferentes servicios, realizar compras y ventas fraudulentas en distintos portales web...

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

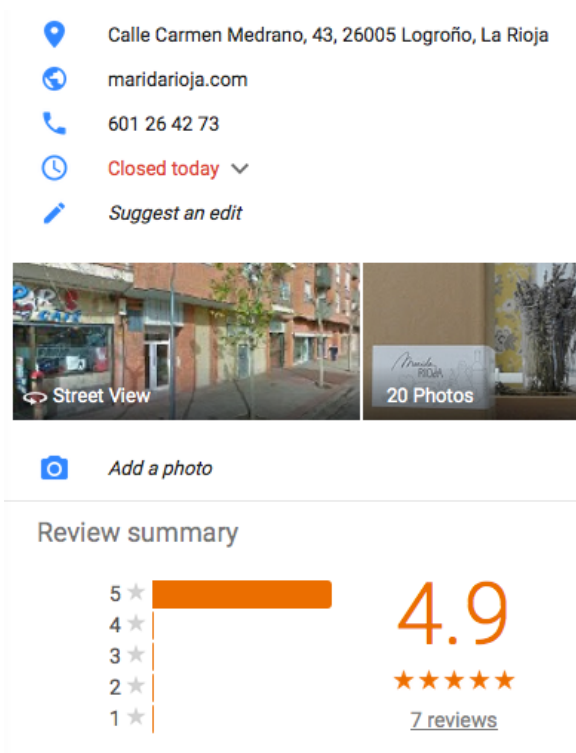


Imagen 3: En los alrededores de la dirección especificada no se encuentra el establecimiento indicado.



Imagen 4: Localización del contacto de la tienda en Google StreetView.

Aparentemente el sitio web es de tamaño pequeño. Sin más dilación lo primero que hago es navegar por el sitio web, y descubrir algún error en los enlaces así como echar un ojo al código fuente de las páginas.

En la página <http://maridarioja.com/tiendaonline/es/33-productos-ecologicos> descubro que la tienda online, está realizada con Prestashop:

```
29 var fb = $("#left_share_fb");
30 if (fb.length > 0)
31   fb.hide();
32 };</script><script type="text/javascript">/* * 2007-2015 PrestaShop * * NOTICE OF LICENSE * * This source file is subject to the Academic Free License
33
34 var user_options = {
```

Imagen 5: Observo en la línea 32 que el tienda online usa Prestashop.



## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

Y es más, mirando la información de la página desde el navegador en la misma url, descubro la versión de PrestaShop:

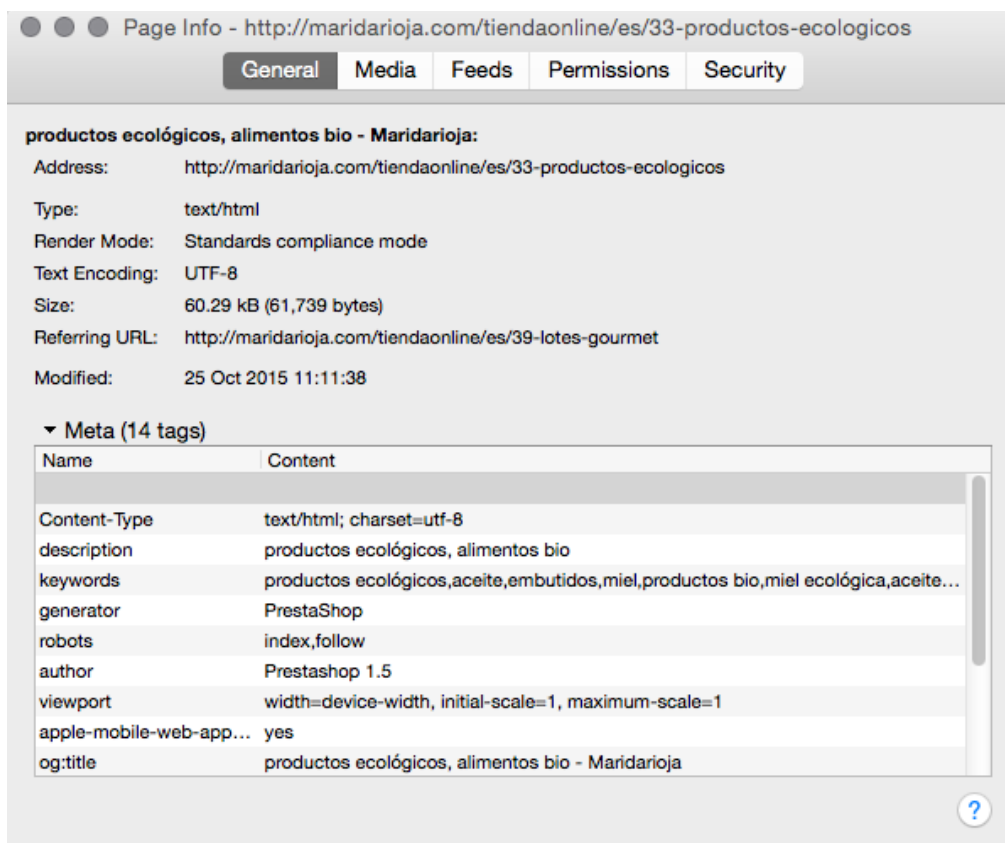


Imagen 6: La tienda usa la versión Prestashop 1.5

Con esta información puedo buscar algún tipo de exploit, inyección sql, que me permita acceder al Back End de la aplicación, o que me permita explotar algún módulo de pago online, o intentar una inyección HTML en la misma:

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

About 10,400 results (0.44 seconds)

### PrestaShop <= 1.5.1 Persistent XSS - Exploits Database

<https://www.exploit-db.com/exploits/22430/> ▼

Nov 2, 2012 - PrestaShop <= 1.5.1 Persistent XSS. Webapps exploit for php platform.

### Mpay24 PrestaShop Payment Module 1.5 - Exploit-DB

<https://www.exploit-db.com/exploits/34586/> ▼

Sep 8, 2014 - Mpay24 PrestaShop Payment Module Multiple Vulnerabilities.

CVE-2014-2008. Webapps exploit for php platform.

### CVE-2014-2008 : SQL injection vulnerability in confirm.php ...

[www.cvedetails.com/cve/CVE-2014-2008/](http://www.cvedetails.com/cve/CVE-2014-2008/) ▼

Aug 5, 2015 - EXPLOIT-DB 34586 Mpay24 PrestaShop Payment Module 1.5 - Multiple Vulnerabilities Author:Eldar Marcussen Release Date:2014-09-08 ...

### Haunt IT: [EN] PrestaShop 1.5.4.1 HTLM Injection

[hauntit.blogspot.com/2013/05/en-prestashop-1541-htlm-injection.html](http://hauntit.blogspot.com/2013/05/en-prestashop-1541-htlm-injection.html) ▼

May 2, 2013 - and yes, this vulnerability exists in admin's part of application. ;) \*

UPDATE \* After a few minutes I've got the idea how to extend this html ...

*Imagen 7: Resultado de la búsqueda "Exploit for Prestashop 1.5".*

Lo más probable es que existan muchísimas vulnerabilidades de ésta versión de PrestaShop, ya que actualmente han publicado la versión 1.6.1.2, y ésta empresa no la tiene actualizada. Además sabemos que hubo cambios importantísimos en Prestashop en dónde hay plugins que no son compatibles con esta nueva versión, y que probablemente los desarrolladores hayan abandonado las mejoras y actualizaciones para la versión 1.5, la actual de la tienda.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

El sitio web también cuenta con un blog, e intuyo que lo más probable es que use un gestor estándar como WordPress, para ello compruebo en una página cualquier la información de la misma desde el navegador:

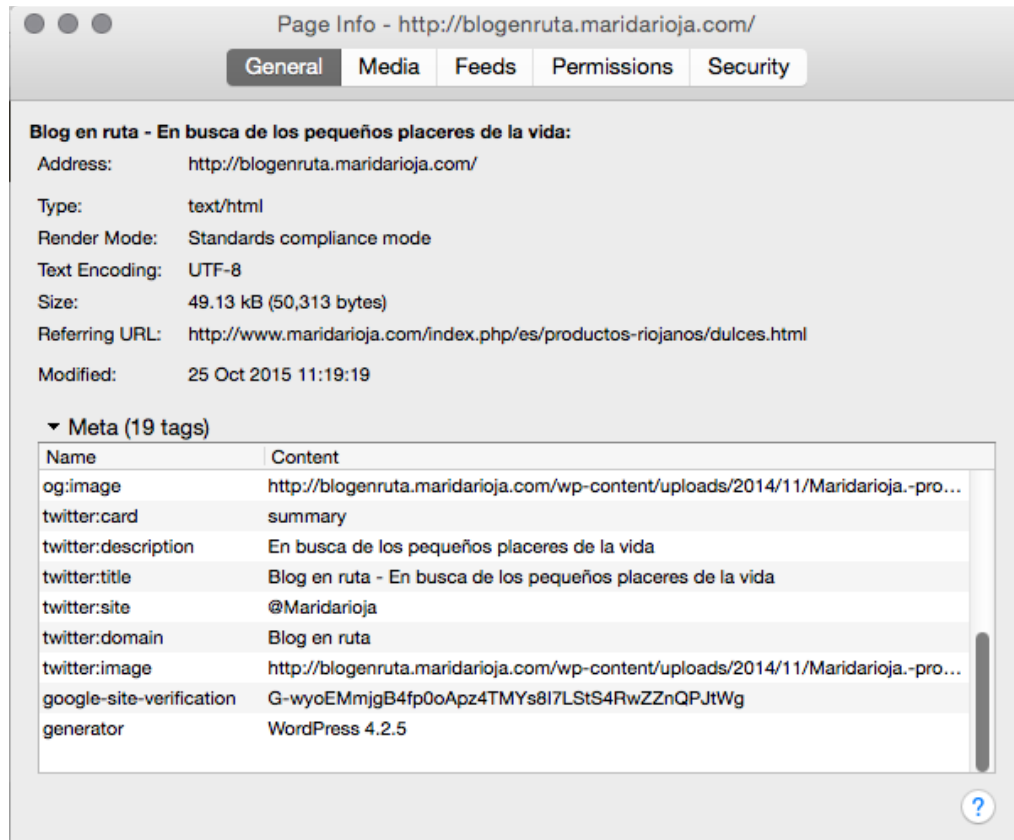


Imagen 8: Vemos que la sección del blog usa WordPress 4.2.5

La versión actual de WordPress es la versión 4.3.1. He buscado exploits conocidos para la versión de la web, pero descubro que aunque no está actualizada a la última versión los exploits conocido han sido solucionados según el sitio web <http://www.wordpressexploit.com/>. En cualquier caso habría que investigar el tema un poco más en profundidad.

El resto del sitio web está desarrollado con php y aparentemente usa un gestor de contenidos que no alcanzo a intuir desde el visionado del código fuente de la página. Me baso en que tiene una estructura muy bien definida. Así que cojo un trozo del mismo (/templates/cleanlogic/css/ie fixes.css.php) y lo busco en google, a ver si me arroja algún resultado en el que aparezca un gestor de contenidos. Descubro que es Joomla:

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

[rupadan.es QUIENES SOMOS information and statistics ...](#)

[rupadan.es.siteis.net/](#) ▾ [Translate this page](#)

[if lt IE 9]> <link rel="stylesheet" href="/templates/cleanlogic/css/ie\_fixes.css.php" type="text/css" /> <![endif--> <!--[if lt IE 9]> <style> body, #siteWrapper, header, ...

[www.servkent.co.uk/templates/cleanlogic-for-joomla...](#)

A description for this result is not available because of this site's robots.txt – learn more.

[citysafari.nl/templates/cleanlogic-for-joomla-3.x/...](#)

A description for this result is not available because of this site's robots.txt – learn more.

[www.gastronom-ibb.de/templates/cleanlogic/css/ie\\_f...](#)

A description for this result is not available because of this site's robots.txt – learn more.

*Imagen 9: Google.es asocia la cadena al gestor de contenidos Joomla.*

Soy más explícito en la búsqueda (joomla /templates/cleanlogic/css/ie\_fixes.css.php):

About 143 results (0.28 seconds)

**Topic: Page layout problems with CleanLogic template (4/5 ...**

<https://crosstec.org/...joomla-templates/82867-page-layout-problems-wit...> ▾

Re: Page layout problems with CleanLogic template 1 year 9 months ago #105576 ...  
\\templates\\cleanlogic-for-joomla-3.x\\css\\layout.css.php ... Es scheitert schon beim IE  
10, welcher ja leider in Win 8 (für die, die noch kein Upgrade auf 8.1 ...

**js syntax error with cleanlogic on IE - BreezingForms**

<https://crosstec.org/...joomla-templates/92250-js-synta...> ▾ [Translate this page](#)

while didn't send charset in header for `css.php` file that was requested by `css3-mediaqueries.js`. And now fixed by force apache to utf-8. alternative it's possible to ...

**Joomla! • View topic - [SOLVED] Remove "font size - bigger ...**

[forum.joomla.org > ... > Joomla! 1.5 > Templates for Joomla! 1.5 ▾](#)

Jul 11, 2010 - 19 posts - 9 authors

Edit the following `css` entry as shown that is available in the file `layout.css` located in ...  
of code available in the file `index.php` located in the directory `\\templates\\beez`. .... I work  
in Firefox and check IE to make sure it matches. ... I was wondering if there was an  
additional fix that could be added to this guide for ...

**225+ Best responsive free joomla templates**

<https://www.designsrazzi.com/2015/free-joomla-templates/> ▾

Best free **joomla templates** for 2015 are released constantly, some free, some premium. ... edited `index.php`, `templateDetails.xml` and `html` folder .... Important menu **CSS fixes**, Webkit / Chrome / Safari relevant. ... Fixed an issue with showing third level menu items in IE8 and IE9. .... **CleanLogic J3.x Free Joomla Template**.

*Imagen 10: Los resultados de esta búsqueda son más concretos.*

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

Lo que no puedo concretar todavía es qué versión de Joomla está instalada y buscar posibles exploits.

En una de las páginas me ratifica este hecho:

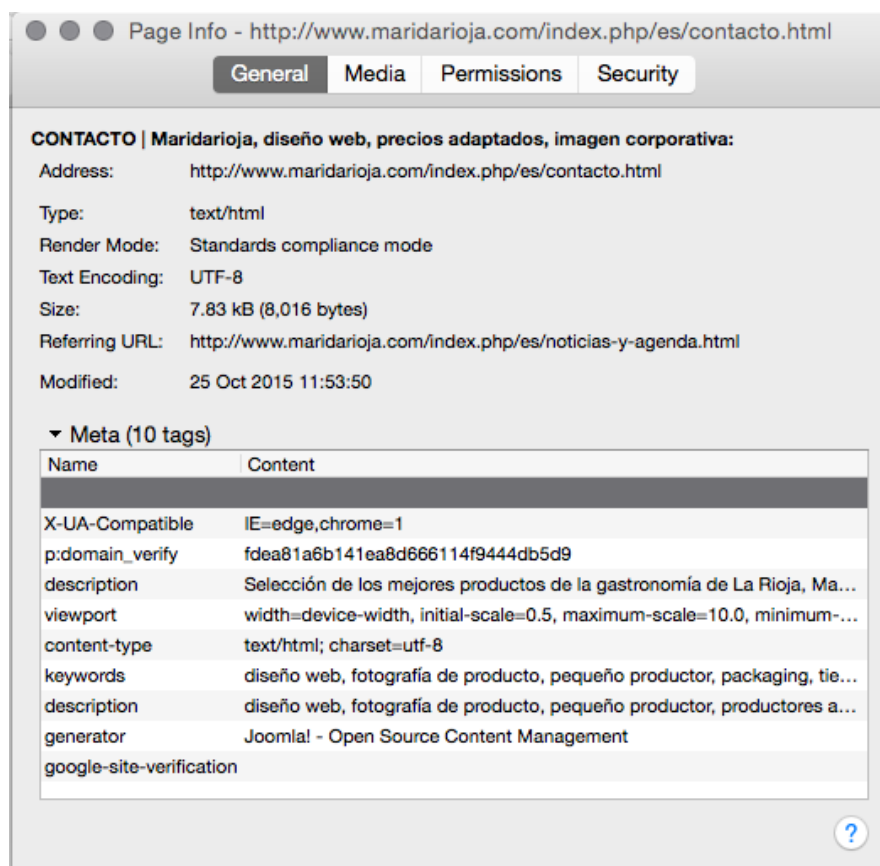


Imagen 11: Firefox me indica que la página ha sido generada con Joomla.

De momento he encontrado que el sitio web usa tres gestores de contenido para diferentes apartados del sitio. Ahora voy a investigar si hay copias del sitio en archive.org.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

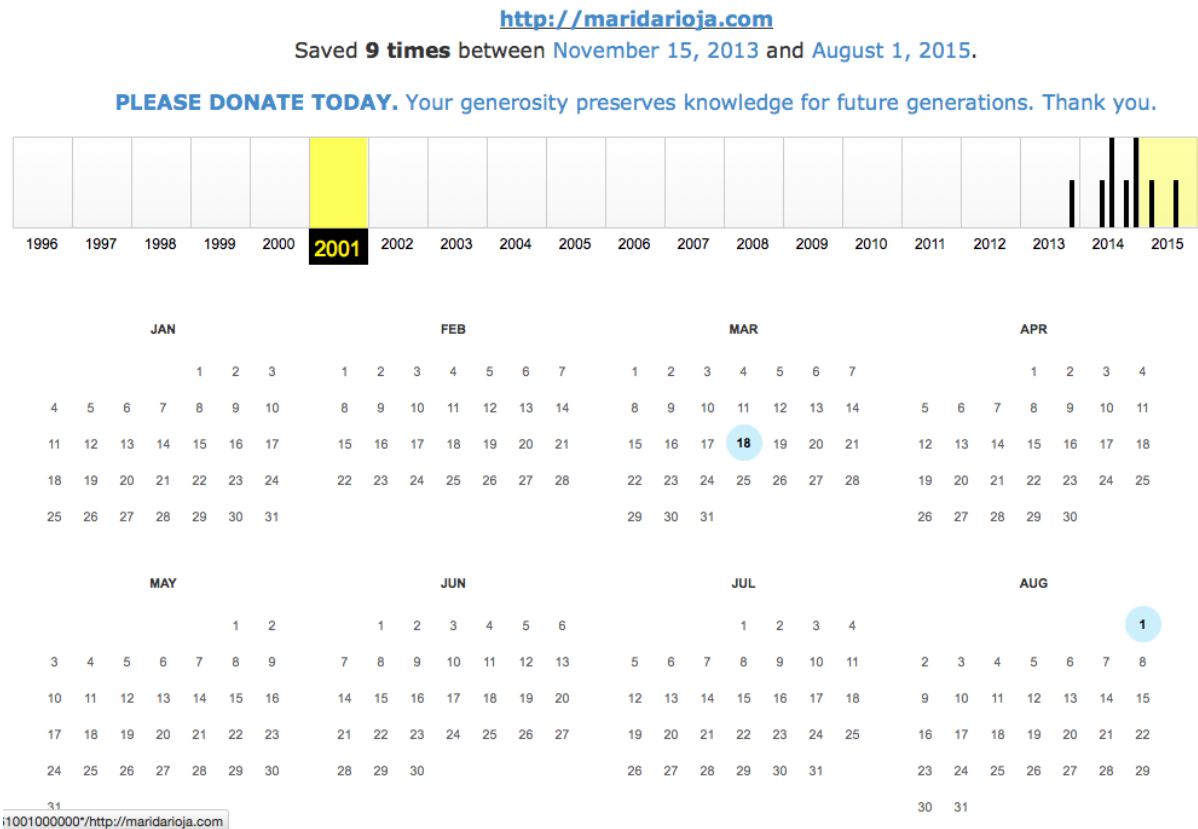


Imagen 12: El sitio de maridarioja.com en archive.org

Puedo observar que el dominio investigado tiene nueve copias realizadas a lo largo de tres años. Buscando en las copias no se ha encontrado información relevante.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

Voy a enfocarme en obtener información del sitio usando las Google Hacks.

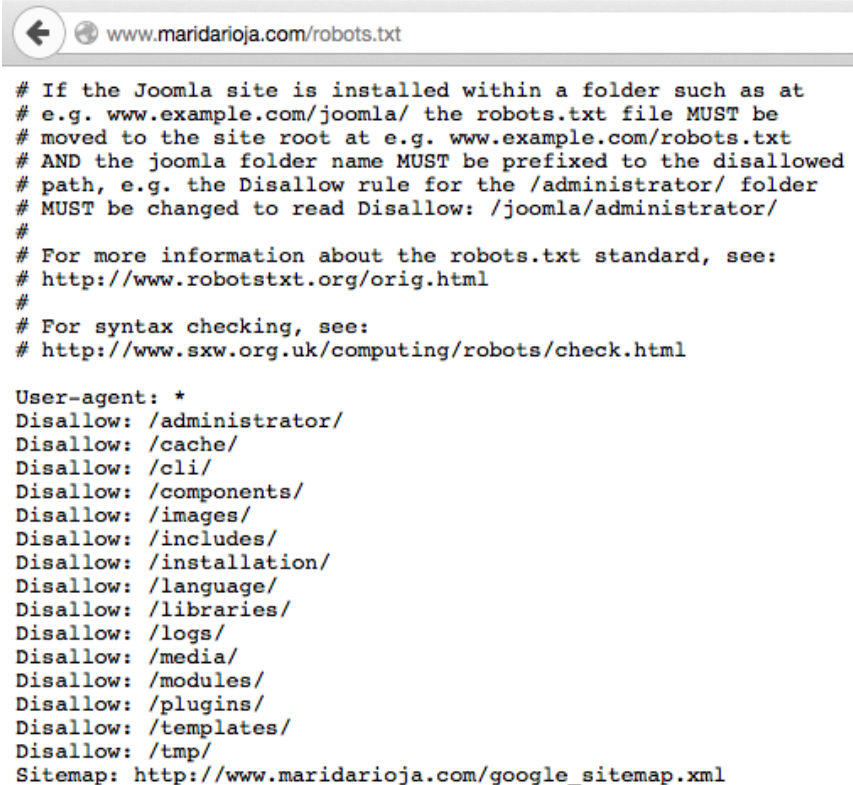
Realizo una búsqueda del dominio con el hack "site" de la siguiente manera:

site:maridarioja.com

Y obtengo en el resultado un archivo importante: robots.txt

```
If the Joomla site is installed within a folder such as at # e.g. ...  
www.maridarioja.com/robots.txt  
# If the Joomla site is installed within a folder such as at # e.g. www.example.com  
/joomla/ the robots.txt file MUST be # moved to the site root at e.g. ...
```

Imagen 13: Resultado de la búsqueda con Google hack "site:maridarioja.com"



```
# If the Joomla site is installed within a folder such as at  
# e.g. www.example.com/joomla/ the robots.txt file MUST be  
# moved to the site root at e.g. www.example.com/robots.txt  
# AND the joomla folder name MUST be prefixed to the disallowed  
# path, e.g. the Disallow rule for the /administrator/ folder  
# MUST be changed to read Disallow: /joomla/administrator/  
#  
# For more information about the robots.txt standard, see:  
# http://www.robotstxt.org/orig.html  
#  
# For syntax checking, see:  
# http://www.sxw.org.uk/computing/robots/check.html  
  
User-agent: *  
Disallow: /administrator/  
Disallow: /cache/  
Disallow: /cli/  
Disallow: /components/  
Disallow: /images/  
Disallow: /includes/  
Disallow: /installation/  
Disallow: /language/  
Disallow: /libraries/  
Disallow: /logs/  
Disallow: /media/  
Disallow: /modules/  
Disallow: /plugins/  
Disallow: /templates/  
Disallow: /tmp/  
Sitemap: http://www.maridarioja.com/google_sitemap.xml
```

Imagen 14: Contenido del archivo Robots.txt bado el dominio.

El resultado de ésta búsqueda permite a un extraño conocer el directorio desde el que acceder al login la administración del sitio. Además veo que sigue teniendo online el directorio

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

/installation, que si bien es probable que esté protegido por contraseña es un aliciente para intentar maniobras extrañas.

Usaré el siguiente comando "site:maridarioja.com filetype:txt", y obtengo:

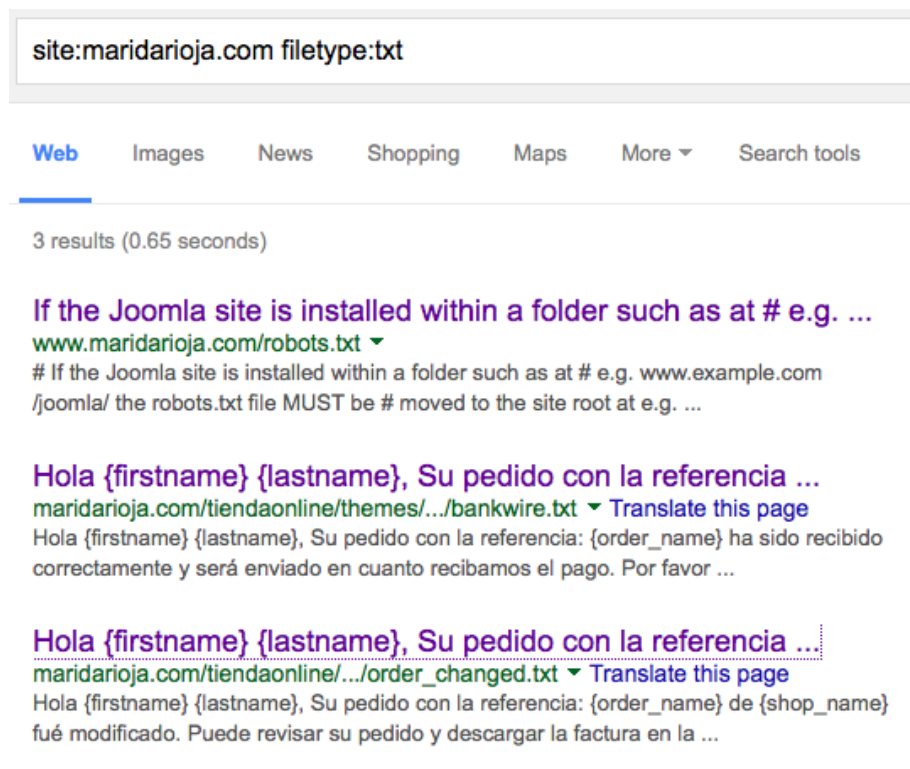


Imagen 15: Resultado de hacker "site:maridarioja.com filetype:text".

Vemos el archivo robots.txt comentado anteriormente y dos plantillas de la tienda online PrestaShop, que si bien se puede acceder a las plantillas para ver su código este no es manipulable.



## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

En este tipo de búsqueda lo interesante sería encontrar alguna contraseña tanto en el código fuente de un documento como documentos ocultos. Pero después de usar diversos comandos no se encuentra ninguna vulnerabilidad aprovechable. A continuación los comandos:

site:maridarioja.com filetype:pdf



Imagen 16: Resultado del hack "site:maridarioja.com filetype:pdf".

site:maridarioja.com filetype:png

site:maridarioja.com filetype:gif

-No arrojan ningún resultado.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

### @DESARROLLO \ Fingerprinting activo:

El Footprinting activo consiste en interactuar con la tecnología del objetivo. Para ello se usan diferentes aplicaciones que permiten obtener datos sobre el entorno informático.

A continuación voy a obtener todos los datos que pueda del objetivo con el comando dig contra el servidor DNS 8.8.8.8 de Google:

```
NetStandard:~ oscar$ dig ANY @8.8.8.8 maridarioja.com

; <=> DiG 9.8.3-P1 <=> ANY @8.8.8.8 maridarioja.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50132
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;maridarioja.com.          IN      ANY

;; ANSWER SECTION:
maridarioja.com.          21599   IN      NS      ns-es.1and1-dns.es.
maridarioja.com.          21599   IN      NS      ns-es.1and1-dns.biz.
maridarioja.com.          21599   IN      SOA     ns-es.1and1-dns.es. hostmaster.1and1.com. 2015101201 28800 7200 604800 600
maridarioja.com.          3599    IN      MX      10 mx01.1and1.es.
maridarioja.com.          21599   IN      NS      ns-es.1and1-dns.com.
maridarioja.com.          21599   IN      AAAA    2001:8d8:1001:19b:c1f9:85e5:ac42:d829
maridarioja.com.          21599   IN      NS      ns-es.1and1-dns.org.
maridarioja.com.          3599    IN      A       217.160.227.103
maridarioja.com.          3599    IN      MX      10 mx00.1and1.es.

;; Query time: 99 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Oct 25 16:41:29 2015
;; MSG SIZE rcvd: 306
```

Imagen 17: Resultado del comando dig sobre el dominio maridarioja.com

La dirección IP de la línea IN A pertenece al servidor web del dominio que nos ocupa.

A → Especifica la dirección IPv4 y se utiliza para convertir nombres de dominio en IP's.

HINFO → Permite adquirir información específica sobre la CPU y OS de un host.

MX → Indica un servidor de intercambio de correo.

SOA → Indica la información básica sobre una zona DNS, incluido el servidor DNS primario, contacto administración y número de serie del dominio.

Por desgracia, mi objetivo tiene los servidores DNS externos, por lo que no podré realizar DNS cache Snooping. Tengo el mismo problema con el servidor de correo. Es lo que tiene elegir al azar.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

Nuestro objetivo es una empresa pequeña que sólo tiene contratado un hosting, cuya seguridad depende de una gran empresa de hosting, con lo que no tengo mucho más que investigar, salvo descubrir dónde está alojado el dominio web, SO que utiliza, servidor web que ofrece el servicio, subdominios que cuelguen del raíz...

Para ello voy a usar la aplicación F.O.C.A.

El uso de esta aplicación me indica que el dominio maridarioja.com está alojado en los servidores de la empresa [mialojamiento.es](http://mialojamiento.es). También nos indica los cuatro subdominios que tiene el principal ([ftp.maridarioja.com](http://ftp.maridarioja.com), [prueba.maridarioja.com](http://prueba.maridarioja.com), [pruebas.maridarioja.com](http://pruebas.maridarioja.com), [blogenruta.maridarioja.com](http://blogenruta.maridarioja.com)):

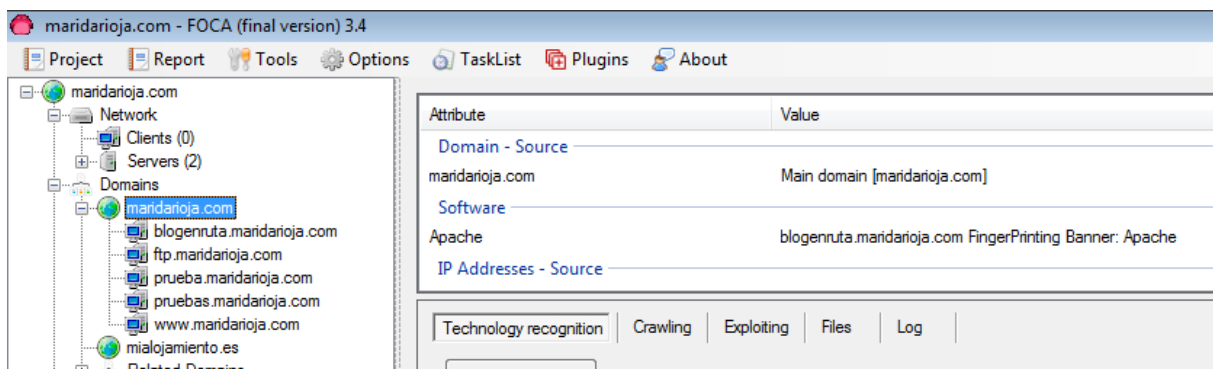


Imagen 18: El objetivo está alojado en los servidores de mialojamiento.es. Subdominios del objetivo.

Estos subdominios están accesibles, pero no contiene absolutamente nada en el directorio raíz, salvo el que provee el blog.

En la sección de metadata, rastreo el servidor en busca de archivos, encontrándome solamente uno. Anteriormente realizamos la misma operación con los Google Hacks, y encontramos un par de archivos pdf incrustados. Accedemos a ellos y los descargamos, añadiéndolos a continuación a la sección metadata para intentar encontrar datos relevantes:

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

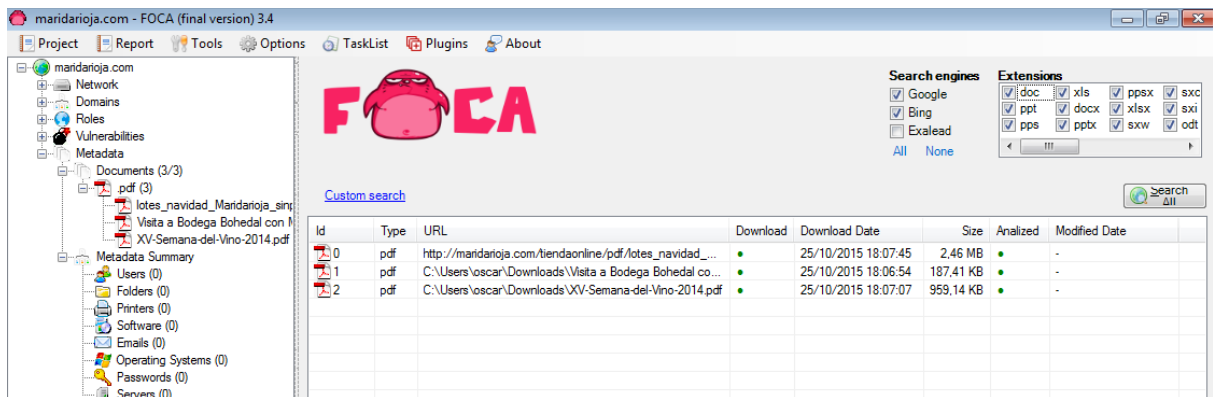


Imagen 19: Resultado de análisis de matedatos en FOCA.

En le imagen se ve que no se ha encontrado ningún usuario, directorio, impresoras, software con el que se han realizado, sistema operativo, password o servidor.

El sitio web cuenta con imágenes de productos. Voy a descargar unas cuantas y también las analizaré con F.O.C.A.

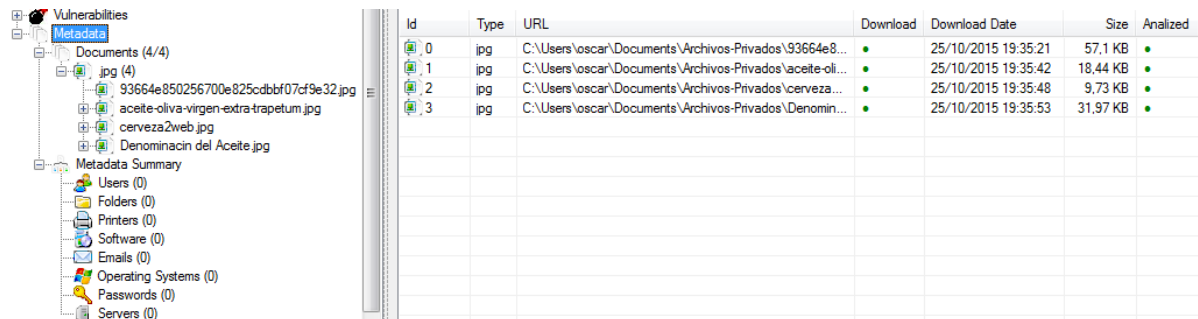


Imagen 20: Resultado de extración de Metas en archivos .jpg

Se puede observar que los archivos no contienen ningún metadato que informe sobre algún tipo de información.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

En la sección Vulnerabilidades / Juicy files puedo observar que el servidor web dónde está alojado el sitio web es Apache:

Attribute	Value
IP - Source	
217.160.227.103 [maridarioja.com]	IP range
Roles in IP	
Rol	Http
Rol	Https
Juicy files	
URL	http://blogenruta.maridarioja.com:80/robots.txt
URL	http://blogenruta.maridarioja.com/wp-admin/
FingerPrinting - HTTP	
217.160.227.103:80	Apache
217.160.227.103:443	Apache
blogenruta.maridarioja.com:443	Apache
blogenruta.maridarioja.com:80	Apache
HTML Title	
blogenruta.maridarioja.com:443	<title>Blog en ruta - En busca de los pequeños placeres de la vida</title>
blogenruta.maridarioja.com:80	<title>Blog en ruta - En busca de los pequeños placeres de la vida</title>
Domains in IP - Source	
maridarioja.com	Main domain [maridarioja.com]
ftp.maridarioja.com	Common Names [ftp.maridarioja.com]
s488801221.mialojamiento.es	Common Names [ftp.maridarioja.com] > DNS reverse resolution [s488801221.mialojamiento.es]
prueba.maridarioja.com	Common Names [prueba.maridarioja.com]
pruebas.maridarioja.com	Common Names [pruebas.maridarioja.com]
www.maridarioja.com	Common Names [www.maridarioja.com]
blogenruta.maridarioja.com	Main domain [maridarioja.com] > DNS resolution [217.160.227.103] > Bing IP Search [blogenruta.maridarioja.com]

Imagen 21: El hosting usa servicio Apache.

## #SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3

### @CONCLUSIÓN:

Si bien con estas herramientas se puede llegar a conocer la estructura informática, usuarios, direcciones de email..., la empresa que he investigado es pequeña y la infraestructura que usa consiste en un hosting alquilado a una compañía que se encarga de la seguridad. El programador y diseñador que han materializado la idea han reducido considerablemente las fuentes de información de las que obtener datos.

Un resumen:

D

En la página Aviso Legal aparece nombre y NIF de individuo, así como dirección. Estos datos no deberían aparecer, ya que ofrece una información que bien podría ser la de una gestora, y mantener el anonimato de cara a terceros.

Gestor de contenidos:

Gestor de blog:

Gestor tienda:

Estos tipos de gestores están sujetos a actualizaciones, tanto globales como específicos en los plugins, y deben de actualizarse por el bien de la seguridad.

La información está muy bien salvaguardada. Salvo los detalles comentados y la aplicación de posibles exploits a los gestores mencionados.

### @BIBLIOGRAFÍA:

-La Biblia del Footprinting.

### @RECURSOS:

## **#SEGURIDAD Y ALTA DISPONIBILIDAD \ Práctica 3**

[http://www.flu-project.com/2011/04/la-biblia-del-footprinting-ii-de-vii\\_1.html](http://www.flu-project.com/2011/04/la-biblia-del-footprinting-ii-de-vii_1.html)

<https://www.osi.es/es/actualidad/blog/2014/01/17/publicar-tu-dni-en-internet-no-es-una-buena-idea>