



# **Desafío No. 10**

Bootcamp DevOps 63703

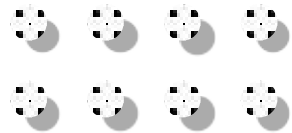
Presentado por:  
Marco Vanegas  
2023

## Ejercicio 1

1. Utilizar dig y whois.
2. Obtener la información del dominio vulnweb.com.
3. Utilizar Google.
4. Identificar qué sitios web están hosteados en vulnweb.com.



Illustrations by [Pixeltrue](#) on



1. En la terminal se ejecutó el comando “**dig** vulnweb.com”, con lo cual se obtuvo el siguiente resultado:

```
dev@dev-ThinkPad-T530:~$ dig vulnweb.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14134
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;vulnweb.com.                IN      A

;; ANSWER SECTION:
vulnweb.com.                1027    IN      A      44.228.249.3

;; ADDITIONAL SECTION:
vulnweb.com.                1027    IN      HINFO   "RFC8482" ""
vulnweb.com.                1027    IN      NS      ns1.eurodns.com.
vulnweb.com.                1027    IN      NS      ns4.eurodns.com.
vulnweb.com.                1027    IN      NS      ns3.eurodns.com.
vulnweb.com.                1027    IN      NS      ns2.eurodns.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 22 12:07:17 -05 2023
;; MSG SIZE rcvd: 157

dev@dev-ThinkPad-T530:~$
```

En la salida del comando se observa como datos principales la dirección IP a la que corresponde el dominio vulnweb.com, junto con los DNS (NS).

En la terminal se ejecutó el comando “**whois** vulnweb.com”, con lo cual se obtuvo el siguiente resultado:

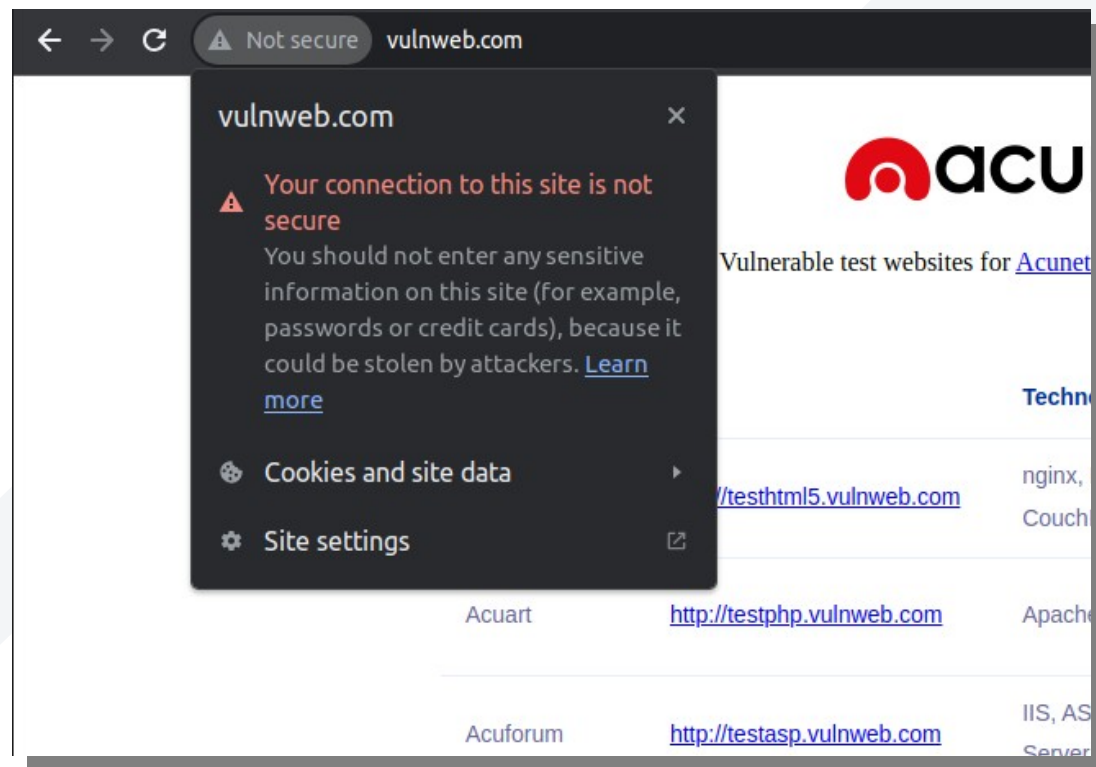
```
dev@dev-ThinkPad-T530:~$ whois vulnweb.com
Domain Name: VULNWEB.COM
Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2023-05-26T07:56:15Z
Creation Date: 2010-06-14T07:50:29Z
Registry Expiry Date: 2025-06-14T07:50:29Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
```

En esta primera parte se observa la información del vendedor del dominio junto con sus datos de contacto.

```
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
```

En esta parte se observa el nombre junto con los datos de contacto del propietario del dominio que coinciden con los datos del administrador y del técnico a cargo.

2. Mediante un navegador se ingresa al dominio vulnweb.com.



El dominio no cuenta con certificado de seguridad SSL, es decir, no cifra u oculta la información transmitida entre el usuario final y el servidor que aloja el sitio Web vulnweb.com.

3. Se realiza la búsqueda de archivos pertenecientes a vulnweb.com mediante el buscador de Google. Para ello se ingresó “site:vulnweb.com filetype:\*”, de esta forma se filtraron todos los archivos públicos correspondientes al dominio en cuestión.


← → ↻ google.com/search?q=site%3Avulnweb.com+filetype%3A\*&sca\_esv=da3b684943d773ac&ei=n0Fe2

Google

site:vulnweb.com filetype:\*

Q Todos Libros Imágenes Shopping Videos Más Herramientas


Cerca de 604 resultados (0,10 segundos)

vulnweb.com

http://testhtml5.vulnweb.com · Traducir esta página

SecurityTweets - HTML5 test website for Acunetix Web ...


This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...

vulnweb.com

http://testphp.vulnweb.com · pict... · Traducir esta página

Index of /pictures/


Index of /pictures/ ./ 1.jpg 11-May-2011 10:27 12426 1.jpg.tn 11-May-2011 10:27 4355 2.jpg 11-May-2011 10:27 3324 2.jpg.tn 11-May-2011 10:27 1353 3.jpg 11-May-2011 10:27 9692 3.jpg.tn 11-May-2011 10:27 3725 4.jpg 11-May-2011 10:27 13969 4.jpg.tn 11-May-2011 10:27 4615 5.jpg 11-May-2011 10:27 14228 5.jpg.tn 11-May-2011 10:27 4428 6.jpg 11-May-2011 10:27 11465 6.jpg.tn 11-May-2011 10:27 4345 7.jpg 11-May-2011 10:27 19219 7.jpg.tn 11-May-2011 10:27 6458 8.jpg 11-May-2011 10:27 50299 8.jpg.tn 11-May-2011 10:27 4139 WS\_FTP.LOG 23-Jan-2009 10:47 771 credentials.txt 23-Jan-2009 10:47 33 ipaddresses.txt 23-Jan-2009 12:59 52 path-disclosure-unix.html 08-Apr-2013 08:42 3936 path-disclosure-win.html 08-Apr-2013 08:41 698 wp-config.bak 03-Dec-2008 14:37 1535

vulnweb.com

http://testhtml5.vulnweb.com · re... · Traducir esta página

SecurityTweets - Acunetix Web Vulnerability Scanner

This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...

vulnweb.com

http://testhtml5.vulnweb.com · co... · Traducir esta página

← → ↻ Not secure | testphp.vulnweb.com/pictures/

Index of /pictures/

./		
1.jpg	11-May-2011 10:27	12426
1.jpg.tn	11-May-2011 10:27	4355
2.jpg	11-May-2011 10:27	3324
2.jpg.tn	11-May-2011 10:27	1353
3.jpg	11-May-2011 10:27	9692
3.jpg.tn	11-May-2011 10:27	3725
4.jpg	11-May-2011 10:27	13969
4.jpg.tn	11-May-2011 10:27	4615
5.jpg	11-May-2011 10:27	14228
5.jpg.tn	11-May-2011 10:27	4428
6.jpg	11-May-2011 10:27	11465
6.jpg.tn	11-May-2011 10:27	4345
7.jpg	11-May-2011 10:27	19219
7.jpg.tn	11-May-2011 10:27	6458
8.jpg	11-May-2011 10:27	50299
8.jpg.tn	11-May-2011 10:27	4139
WS_FTP.LOG	23-Jan-2009 10:47	771
credentials.txt	23-Jan-2009 10:47	33
ipaddresses.txt	23-Jan-2009 12:59	52
path-disclosure-unix.html	08-Apr-2013 08:42	3936
path-disclosure-win.html	08-Apr-2013 08:41	698
wp-config.bak	03-Dec-2008 14:37	1535

← → ↻ Not secure | testphp.vulnweb.com/CVS/

Index of /CVS/

./		
Entries	11-May-2011 10:27	1
Entries.log	11-May-2011 10:27	1
Repository	11-May-2011 10:27	8
Root	11-May-2011 10:27	1

← → ↻ Not secure | testphp.vulnweb.com/.idea/

Index of /.idea/

./		
scopes/	13-Nov-2012 13:29	-
acuart.inl	20-Apr-2012 08:22	292
encodings.xml	20-Apr-2012 08:22	171
misc.xml	20-Apr-2012 08:22	266
modules.xml	20-Apr-2012 08:22	275
ycs.xml	20-Apr-2012 08:22	173
workspace.xml	20-Apr-2012 08:23	12473



4. En este punto se requiere encontrar todos los subdominios de vulnweb.com, para ello se empleó el buscador de Google y los términos de búsqueda “site:vulnweb.com -www”.

The screenshot shows a Google search interface in an Incognito browser window. The search bar contains the query "site:vulnweb.com -www". Below the search bar, there are navigation links for "Todos", "Libros", "Noticias", "Imágenes", "Videos", "Más", and "Herramientas". The search results are displayed below the navigation links, showing a list of results for "vulnweb.com". The first result is "Index of /pictures/" with a snippet "Index of /pictures/ .. / 1.jpg 11-May-2011 10:27 12426 1.jpg.tn 11-May-2011 10:27 4355 2.jpg 11-May-2011 10:27 3324 2.jpg.tn 11-May-2011 10:27 1353 3.jpg ...". The second result is "SecurityTweets - Acunetix Web Vulnerability Scanner" with a snippet "This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...". The third result is "HTML5 test website for Acunetix Web Vulnerability Scanner." with a snippet "This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...". The fourth result is "vulnweb.com" with a snippet "http://testhtml5.vulnweb.com > like · Traducir esta página". On the right side of the search results, there is a yellow box with the text "Looking for results in English?" and three links: "Change to English", "Continuar usando español", and "Configuración del idioma".

google.com/search?q=site%3Avulnweb.com+-www&sca\_esv=da3b684943d773ac&ei=G0xeZYerI-aOwbkP4-aSOA&ved=0ahUKEwjHpL\_modiCAXV... ☆ Incognito

Google site:vulnweb.com -www

Acceder

Todos Libros Noticias Imágenes Videos Más Herramientas SafeSearch

Cerca de 427 resultados (0.21 segundos)

**vulnweb.com**  
http://testphp.vulnweb.com > pict... · Traducir esta página

**Index of /pictures/**  
Index of /pictures/ .. / 1.jpg 11-May-2011 10:27 12426 1.jpg.tn 11-May-2011 10:27 4355 2.jpg 11-May-2011 10:27 3324 2.jpg.tn 11-May-2011 10:27 1353 3.jpg ...

**vulnweb.com**  
http://testhtml5.vulnweb.com > re... · Traducir esta página

**SecurityTweets - Acunetix Web Vulnerability Scanner**  
This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...

**vulnweb.com**  
http://testhtml5.vulnweb.com > co... · Traducir esta página

**HTML5 test website for Acunetix Web Vulnerability Scanner.**  
This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to ...

**vulnweb.com**  
http://testhtml5.vulnweb.com > like · Traducir esta página

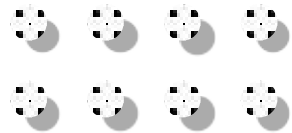
Looking for results in English? X  
Change to English  
Continuar usando español  
Configuración del idioma

## Ejercicio 2

1. Utilizar dig.
2. Identificar la dirección IP de cada uno de los sitios.
3. Utilizar la herramienta geoip.
4. Identificar la geolocalización de cada dirección IP.
5. Utilizando nmap, obtener cualquier información adicional, como puertos abiertos.



Illustrations by [Pixeltrue](#) on





1. Teniendo en cuenta que ya se uso dig con el dominio vulnweb.com, ahora se realiza el mismo ejercicio pero con example.com.

```
dev@dev-ThinkPad-T530:~$ dig example.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25067
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 65494
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                31083   IN      A      93.184.216.34

;; Query time: 35 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 22 13:51:45 -05 2023
;; MSG SIZE rcvd: 56

dev@dev-ThinkPad-T530:~$
```

En la información se destaca la dirección IP del dominio, pero para este ejemplo no se imprimieron los DNS.

2. Para este numeral se identificará la dirección ip de vulnweb.com mediante la herramienta ping.

```
dev@dev-ThinkPad-T530:~$ ping vulnweb.com
PING vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=45 time=155 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=45 time=151 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=45 time=153 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=45 time=151 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=5 ttl=45 time=152 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=6 ttl=45 time=152 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=7 ttl=45 time=152 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=8 ttl=45 time=151 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=9 ttl=45 time=152 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=10 ttl=45 time=163 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=11 ttl=45 time=156 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=12 ttl=45 time=159 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=13 ttl=45 time=151 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=14 ttl=45 time=151 ms
```

IP: 44.228.249.3

3. En la terminal, mediante el comando “**geoiplookup** 44.228.249.3” se pudo determinar que la dirección IP pertenece a Estados Unidos.

```
dev@dev-ThinkPad-T530:~$ geoiplookup 44.228.249.3
GeoIP Country Edition: US, United States
dev@dev-ThinkPad-T530:~$
```

4. En este punto para la geolocalización de la dirección IP **44.228.249.3** se empleó la herramienta en línea ip2location.com.

The screenshot shows the IP2Location website interface. The browser address bar displays 'ip2location.com/demo/44.228.249.3'. The website header includes the IP2LOCATION logo, navigation links (Home, Products, Pricing, Resources, Contact, Log In), and a shopping cart icon showing '0 item | US\$0.00'. The main content area is titled 'IP Lookup Result' with a 'Share The Result' link. It is divided into two sections: 'Geolocation Data' and 'Proxy Data'. The 'Geolocation Data' section states it uses the 'IP2Location DB26 geolocation database' and lists various fields. A red arrow points to the 'Country' field, which is 'United States of America [US]'. The 'Proxy Data' section states it uses the 'IP2Proxy PX11 proxy database' and lists various fields, all of which are currently empty or show dashes.

Geolocation Data	
Permalink	<a href="https://www.ip2location.com/44.228.249.3">https://www.ip2location.com/44.228.249.3</a>
<input checked="" type="checkbox"/> IP Address	<a href="#">44.228.249.3</a>
<input type="checkbox"/> Country	<a href="#">United States of America [US]</a>
<input type="checkbox"/> Region	Oregon
<input type="checkbox"/> City	Portland
<input type="checkbox"/> Coordinates of City ⓘ	45.523459, -122.676465 (45°31'24"N 122°40'35"W)
<input type="checkbox"/> ISP	Amazon.com Inc.
<input type="checkbox"/> Local Time	22 Nov, 2023 11:14 AM (UTC -08:00)
<input type="checkbox"/> Domain	amazon.com
<input type="checkbox"/> Net Speed	(T1) Data Center/Transit
<input type="checkbox"/> IDD & Area Code	(1) 503

Proxy Data	
<input checked="" type="checkbox"/> IP Address	<a href="#">44.228.249.3</a>
<input type="checkbox"/> Anonymous Proxy	No
<input type="checkbox"/> Proxy Country	-
<input type="checkbox"/> Proxy Region	-
<input type="checkbox"/> Proxy City	-
<input type="checkbox"/> Proxy ISP	-
<input type="checkbox"/> Proxy Domain	-
<input type="checkbox"/> Proxy Usage Type	-
<input type="checkbox"/> Proxy Type	-
<input type="checkbox"/> Proxy ASN	-
<input type="checkbox"/> Threat	-

5. Con la herramienta nmap se escaneó la dirección IP 44.228.249.3 (nmap 44.228.249.3) para encontrar puertos abiertos, en este caso sólo se hallaba abierto el puerto 80.

```
dev@dev-ThinkPad-T530:~$ nmap 44.228.249.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-22 14:21 -05
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.19s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds
dev@dev-ThinkPad-T530:~$
```

Repositorio de GitHub donde se encuentra esta presentación:

<https://github.com/BambooThink/BootcampDevOps2023>