


Desafío 18 – Miriam Romitelli.

1. Identificar los sitios web hospedados en <http://vulnweb.com/>

Para identificar los sitios web alojados en <http://vulnweb.com/>, podemos utilizar herramientas como Nmap para escanear los subdominios o simplemente acceder al sitio y verificar manualmente los enlaces disponibles.

vulnweb.com			
			
Vulnerable test websites for Acunetix Web Vulnerability Scanner .			
Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

2. Obtener información del dominio principal <http://vulnweb.com/>

Utilizaremos herramientas como WHOIS para obtener detalles sobre el dominio principal:

```
#whois vulnweb.com
```

Esto nos dará información como el registrante del dominio, los servidores de nombres (DNS), etc.

```
ubuntu@ip-10-0-14-133:~$ 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: legal@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.EURODNS.COM
Name Server: NS2.EURODNS.COM
Name Server: NS3.EURODNS.COM
Name Server: NS4.EURODNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-07-07T21:09:46Z <<<
```

```
ubuntu@ip-10-0-14-133:~$ sudo apt install whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.22).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
ubuntu@ip-10-0-14-133:~$ ^C
ubuntu@ip-10-0-14-133:~$ ^C
ubuntu@ip-10-0-14-133:~$ 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
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Name Server: NS1.EUODNS.COM
Name Server: NS2.EUODNS.COM
Name Server: NS3.EUODNS.COM
Name Server: NS4.EUODNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of whois database: 2024-07-07T21:09:46Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: <http://www.eurodns.com>
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
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
Registry Admin ID:
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of WHOIS database: 2024-07-07T21:09:59Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

Please email the listed admin email address if you wish to raise a legal issue.

The Data in EuroDNS WHOIS database is provided for information purposes only. The fact that EuroDNS display such information does not provide any guarantee expressed or implied on the purpose for which the database may be used, its accuracy or usefulness. By submitting a WHOIS query, you agree that you will use this Data only for lawful purposes and that, under no circumstances will you use this Data to:

- (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam); or
- (2) enable high volume, automated, electronic processes that apply to EuroDNS (or its systems). EuroDNS reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by the above policy.

3. Identificar direcciones IP de cada uno de los sitios hospedados (al menos 5) en <http://vulnweb.com/>

Podemos usar DIG para obtener las direcciones IP de cada sitio:

dig site1.vulnweb.com +short

dig site2.vulnweb.com +short

y así sucesivamente para los otros sitios

```

ubuntu@ip-10-0-14-133:~$ dig http://testhtml5.vulnweb.com/ +short
ubuntu@ip-10-0-14-133:~$ dig testhtml5.vulnweb.com +short
44.228.249.3
ubuntu@ip-10-0-14-133:~$ dig testphp.vulnweb.com +short
44.228.249.3
ubuntu@ip-10-0-14-133:~$ dig testasp.vulnweb.com +short
44.238.29.244
ubuntu@ip-10-0-14-133:~$ dig testaspnet.vulnweb.com +short
44.238.29.244
ubuntu@ip-10-0-14-133:~$ dig rest.vulnweb.com +short
35.81.188.86

```

4. Identificar la geolocalización de cada dirección IP encontrada

Usaremos una herramienta de GEOIP como geoipllookup para encontrar la ubicación geográfica de cada dirección IP:
geoipllookup <dirección IP>

```

ubuntu@ip-10-0-14-133:~$ geoipllookup 44.228.249.3
GeoIP Country Edition: US, United States
ubuntu@ip-10-0-14-133:~$ geoipllookup 44.238.29.244
GeoIP Country Edition: US, United States
ubuntu@ip-10-0-14-133:~$ geoipllookup 35.81.188.86
GeoIP Country Edition: US, United States

```

5. Obtener información adicional como puertos abiertos usando NMAP o SHODAN

- **NMAP:** Escanear los sitios para obtener información sobre los puertos abiertos:

bash

Copiar código

nmap site1.vulnweb.com

nmap site2.vulnweb.com

y así sucesivamente

```

ubuntu@ip-10-0-14-133:~$ nmap testhtml5.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 21:26 UTC
Nmap scan report for testhtml5.vulnweb.com (44.228.249.3)
Host is up (0.064s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
ubuntu@ip-10-0-14-133:~$ nmap testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 21:27 UTC
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.060s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

```

```
ubuntu@ip-10-0-14-133:~$ nmap testasp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 21:28 UTC
Nmap scan report for testasp.vulnweb.com (44.238.29.244)
Host is up (0.064s latency).
rDNS record for 44.238.29.244: ec2-44-238-29-244.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
ubuntu@ip-10-0-14-133:~$ nmap testaspnet.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 21:28 UTC
Nmap scan report for testaspnet.vulnweb.com (44.238.29.244)
Host is up (0.063s latency).
rDNS record for 44.238.29.244: ec2-44-238-29-244.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
```

```
ubuntu@ip-10-0-14-133:~$ nmap rest.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 21:29 UTC
Nmap scan report for rest.vulnweb.com (35.81.188.86)
Host is up (0.064s latency).
rDNS record for 35.81.188.86: ec2-35-81-188-86.us-west-2.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.15 seconds
```

Estos pasos permitieron realizar pruebas de seguridad de manera ética en <http://vulnweb.com>, identificando posibles vulnerabilidades y asegurando que la infraestructura esté protegida antes de que pueda ser explotada por personas malintencionadas. Actuando con responsabilidad y dentro de los límites legales y éticos.