EDGAR ALVARADO

DEVOPS BOOTCAMP

DESAFIO 18

OBJETIVO

Realizar pruebas sobre sistemas informáticos de la misma forma que podría hacerla una persona malintencionada.

Conocer las debilidades de la infraestructura, a fin de poder solucionarlas, antes de que una persona malintencionada pudiera aprovecharse de ellas.

Ejecutar pruebas con un excelente nivel de ética, debido a que es muy probable que, durante las pruebas, se descubran vulnerabilidades que podrían ser explotadas para obtener beneficios económicos, más allá de los acordados.

Objeto de estudio: Sitio http://vulnweb.com/

GOOGLE

1. Identificar los sitios web están hosteados (al menos 5) en

http://vulnweb.com/

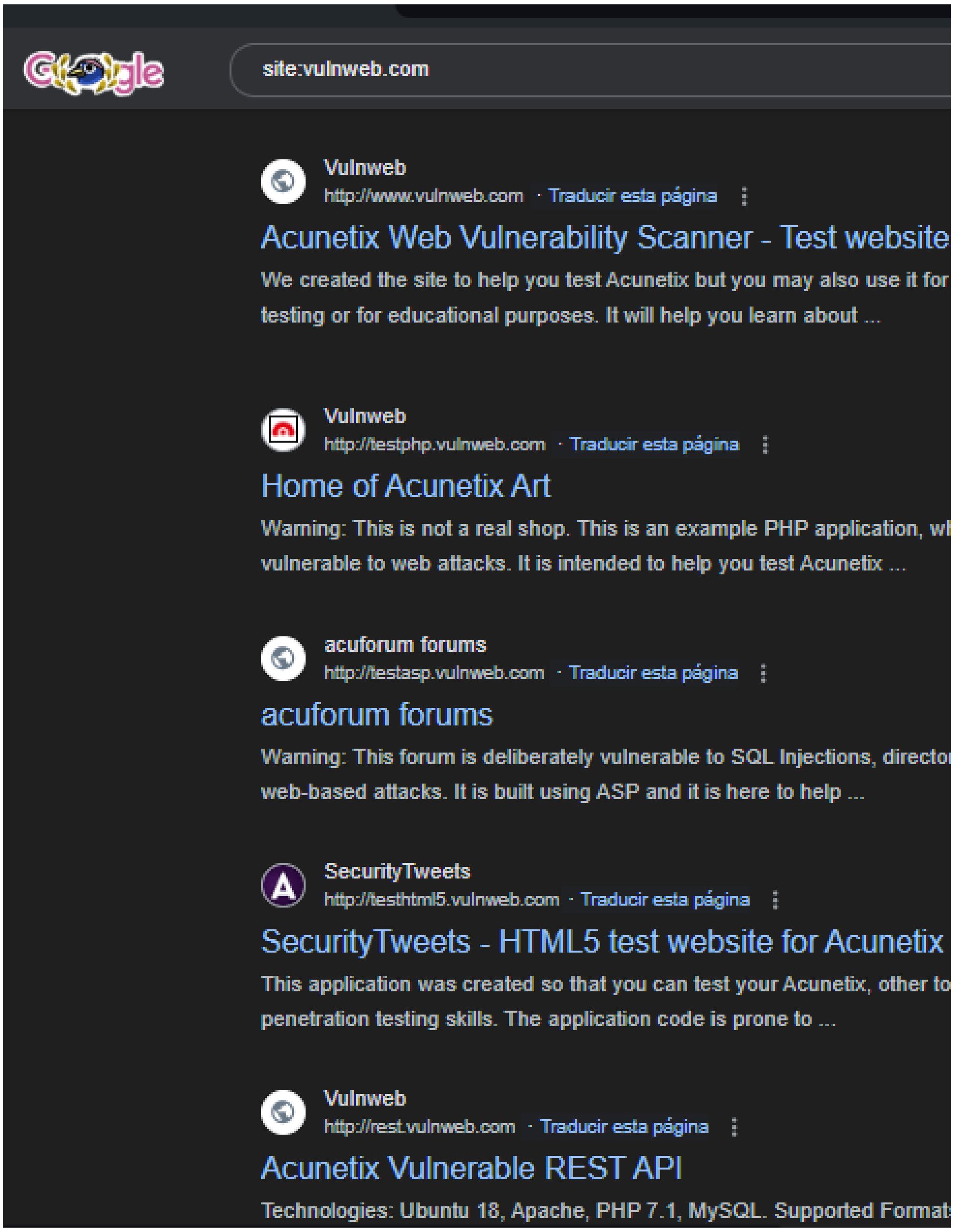
http://www.vulnweb.com/

http://testphp.vulnweb.com/

http://testasp.vulnweb.com/

http://testhtml5.vulnweb.com/

http://rest.vulnweb.com/



site:vulnweb.com

Vulnweb
http://www.vulnweb.com · Traducir esta página

Acunetix Web Vulnerability Scanner - Test website

We created the site to help you test Acunetix but you may also use it for testing or for educational purposes. It will help you learn about ...

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

Home of Acunetix Art

Warning: This is not a real shop. This is an example PHP application, wl vulnerable to web attacks. It is intended to help you test Acunetix ...

acuforum forums
http://testasp.vulnweb.com · Traducir esta página

acuforum forums

Warning: This forum is deliberately vulnerable to SQL Injections, directo web-based attacks. It is built using ASP and it is here to help ...

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

SecurityTweets - HTML5 test website for Acunetix

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

Vulnweb
http://rest.vulnweb.com · Traducir esta página

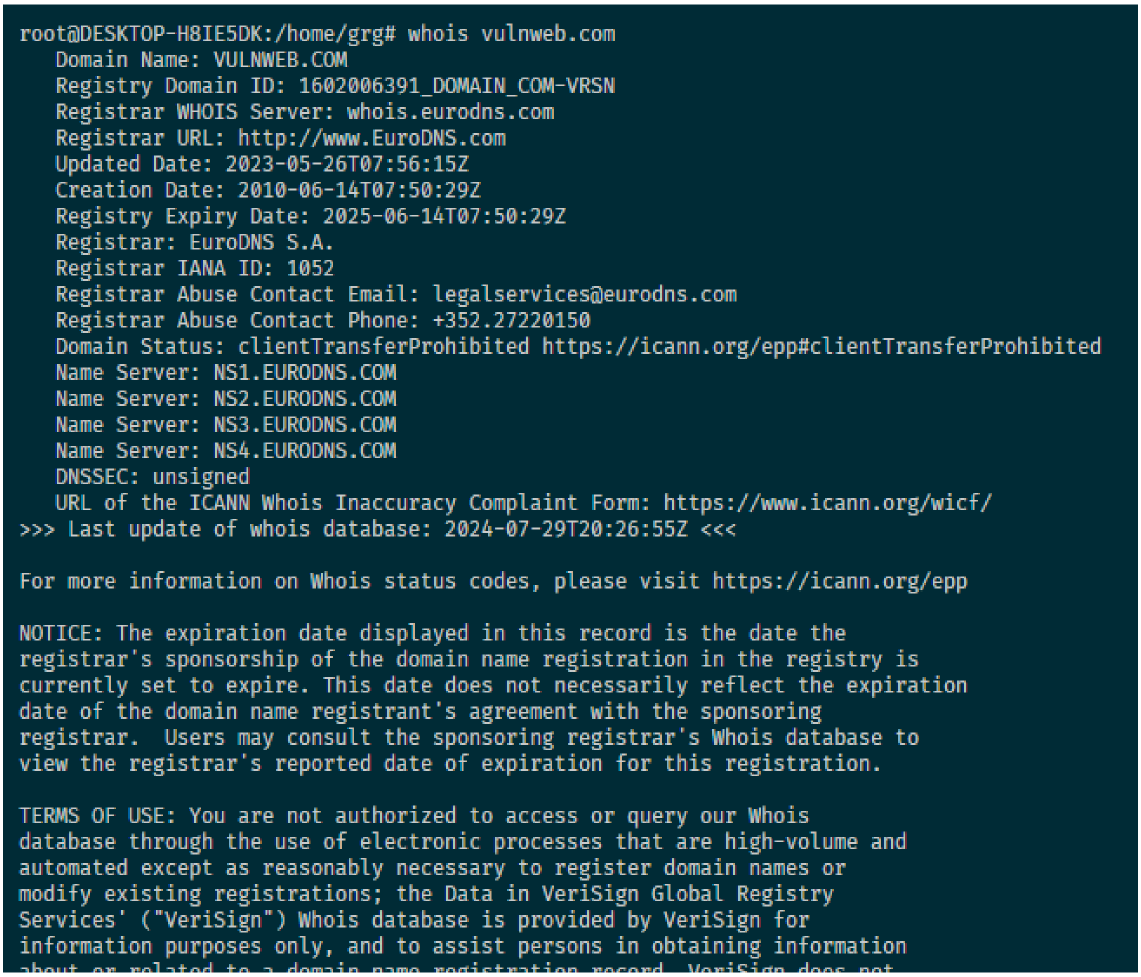
Acunetix Vulnerable REST API

Technologies: Ubuntu 18, Apache, PHP 7.1, MySQL. Supported Format

DIG & WHOIS

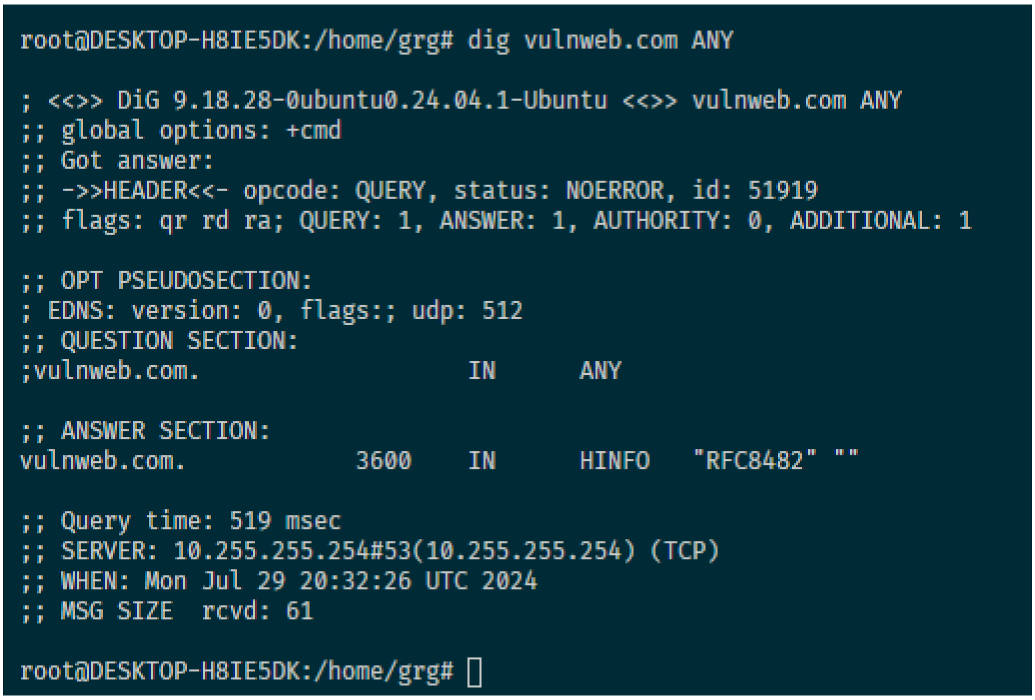
2. Obtener información del dominio principal http://vulnweb.com/

WHOIS



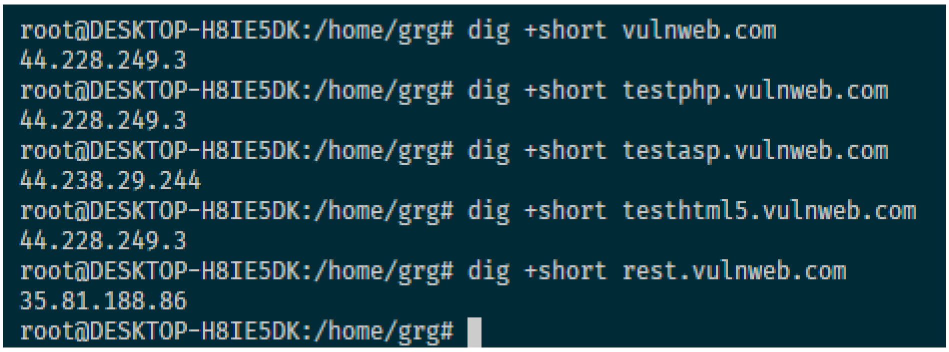
```
root@DESKTOP-H8IE5DK:/home/grg# whois vulnweb.com
   Domain Name: VULNWEB.COM
   Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.eurodns.com
   Registrar URL: http://www.EuroDNS.com
   Updated Date: 2023-05-26T07:56:15Z
   Creation Date: 2010-06-14T07:50:29Z
   Registry 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.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: 2024-07-29T20:26:55Z <<<

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
```

DIG



```
root@DESKTOP-H8IE5DK:/home/grg# dig vulnweb.com ANY

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> vulnweb.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51919
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;vulnweb.com.                   IN      ANY

;; ANSWER SECTION:
vulnweb.com.            3600    IN      HINFO   "RFC8482" ""

;; Query time: 519 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (TCP)
;; WHEN: Mon Jul 29 20:32:26 UTC 2024
;; MSG SIZE  rcvd: 61

root@DESKTOP-H8IE5DK:/home/grg# 
```

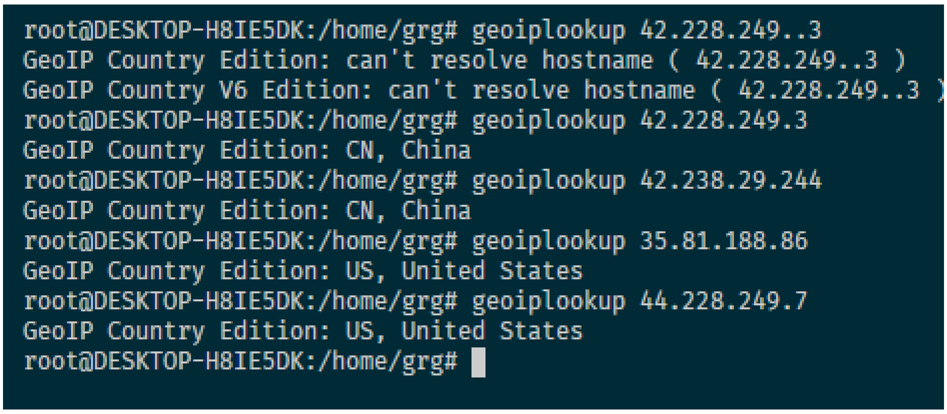
3. Identificar direcciones IP de cada uno de los sitios hospedados (al menos 5) en http://vulnweb.com/



```
root@DESKTOP-H8IE5DK:/home/grg# dig +short vulnweb.com
44.228.249.3
root@DESKTOP-H8IE5DK:/home/grg# dig +short testphp.vulnweb.com
44.228.249.3
root@DESKTOP-H8IE5DK:/home/grg# dig +short testasp.vulnweb.com
44.238.29.244
root@DESKTOP-H8IE5DK:/home/grg# dig +short testhtml5.vulnweb.com
44.228.249.3
root@DESKTOP-H8IE5DK:/home/grg# dig +short rest.vulnweb.com
35.81.188.86
root@DESKTOP-H8IE5DK:/home/grg# 
```

GEOIP

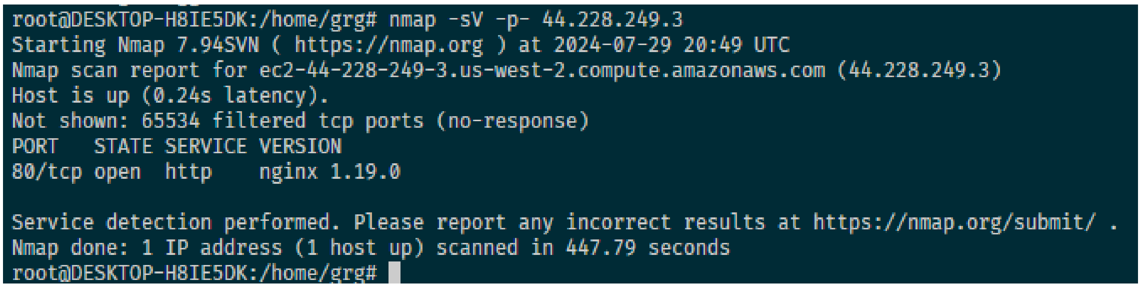
4. Identificar la geolocalización de cada dirección IP encontrada en los puntos anteriores.



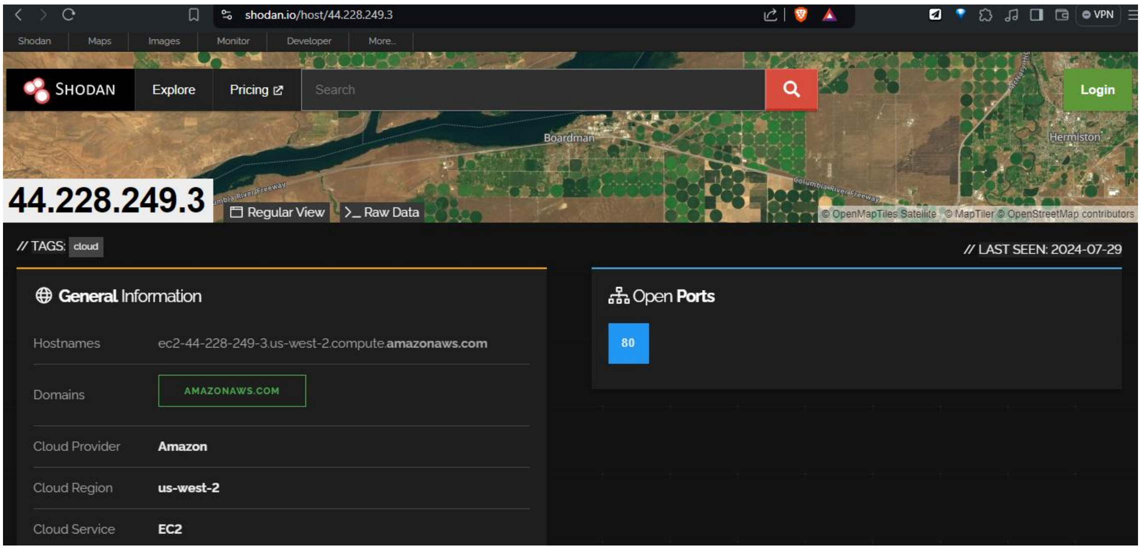
```
root@DESKTOP-H8IE5DK:/home/grg# geoiplookup 42.228.249..3
GeoIP Country Edition: can't resolve hostname ( 42.228.249..3 )
GeoIP Country V6 Edition: can't resolve hostname ( 42.228.249..3 )
root@DESKTOP-H8IE5DK:/home/grg# geoiplookup 42.228.249.3
GeoIP Country Edition: CN, China
root@DESKTOP-H8IE5DK:/home/grg# geoiplookup 42.238.29.244
GeoIP Country Edition: CN, China
root@DESKTOP-H8IE5DK:/home/grg# geoiplookup 35.81.188.86
GeoIP Country Edition: US, United States
root@DESKTOP-H8IE5DK:/home/grg# geoiplookup 44.228.249.7
GeoIP Country Edition: US, United States
root@DESKTOP-H8IE5DK:/home/grg# 
```

NMAP/SHODAN

5. Obtener cualquier información adicional, como puertos abiertos, por ejemplo.



```
root@DESKTOP-H8IE5DK:/home/grg# nmap -sV -p- 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 20:49 UTC
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.24s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 447.79 seconds
root@DESKTOP-H8IE5DK:/home/grg# 
```



44.228.249.3

// TAGS: cloud

// LAST SEEN: 2024-07-29

General Information

Hostnames ec2-44-228-249-3.us-west-2.compute.**amazonaws.com**

Domains AMAZONAWS.COM

Cloud Provider **Amazon**

Cloud Region **us-west-2**

Cloud Service **EC2**

Open Ports

80