02 RECONNAISSANCE PRACTICE

OBJECTIVE:

Perform passive OSINT on vulnweb (vulnweb.com / testphp.vulnweb.com), enumerate assets and subdomains, identify exposed services and tech stack, and document all findings for handoff to active testing.

SCOPE & RULES OF ENGAGEMENT

- **Target:** vulnweb.com and its subdomains (e.g., testphp.vulnweb.com).
- **Allowed activity:** OSINT (WHOIS, DNS, Shodan searches, Maltego transforms, Wappalyzer).

1. DOMAIN INFORMATION (WHOIS & DNS)

Domain: vulnweb.com

Commands:

whois vulnweb.com

dig +short NS vulnweb.com

dig +short vulnweb.com A

```
┌──(kali㉿kali)-[~]
└─$ 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: 2025-05-20T08:14:02Z
   Creation Date: 2010-06-14T07:50:29Z
   Registry Expiry Date: 2026-06-14T07:50:29Z
   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: 2025-10-08T17:59:01Z <<<
```

```
┌──(kali㉿kali)-[~]
└─$ dig +short NS vulnweb.com
ns3.eurodns.com.
ns4.eurodns.com.
ns2.eurodns.com.
ns1.eurodns.com.
```

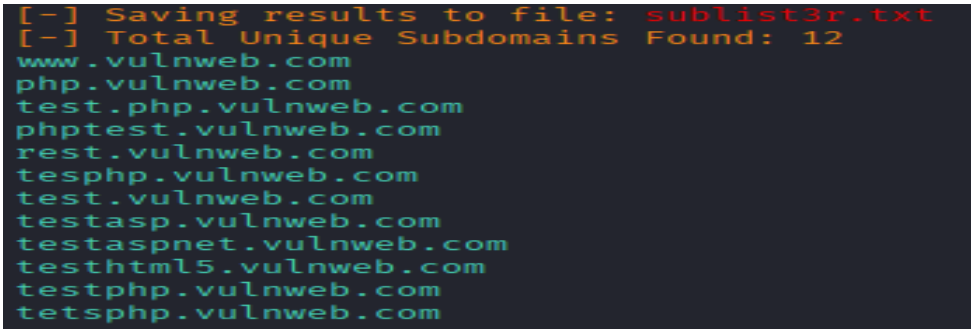
```
┌──(kali㉿kali)-[~]
└─$ dig testphp.vulnweb.com A +short
44.228.249.3
```

2. SUBDOMAIN ENUMERATION

Tools / commands:

subfinder -d vulnweb.com -o subfinder.txt

sublist3r -d vulnweb.com -o sublist3r.txt



VALIDATED SUBDOMAINS:

- testphp.vulnweb.com
- vulnweb.com
- testasp.culnweb.com

3. EXPOSED SERVICES & BANNERS

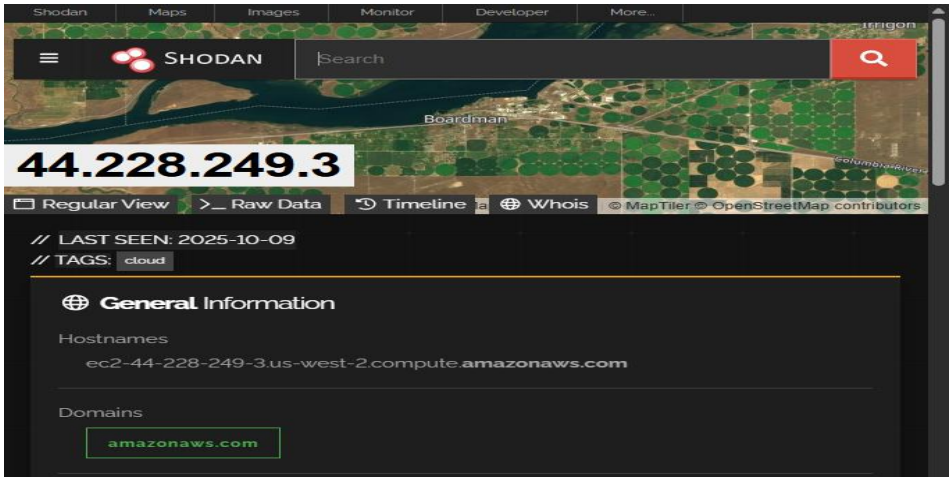
Steps:

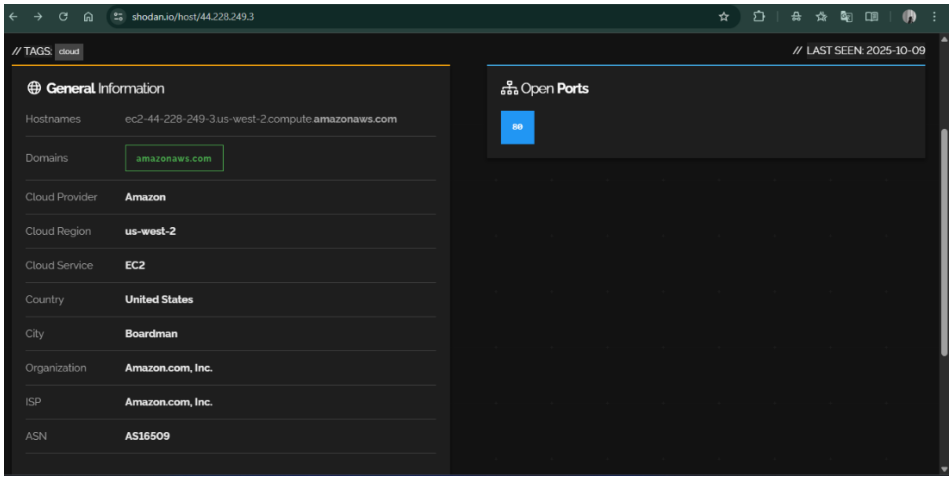
- Use curl -I to check HTTP headers for each host.
- Use Shodan web UI to check indexed banners for IPs/hostnames.

Commands:

curl -I https://testphp.vulnweb.com/

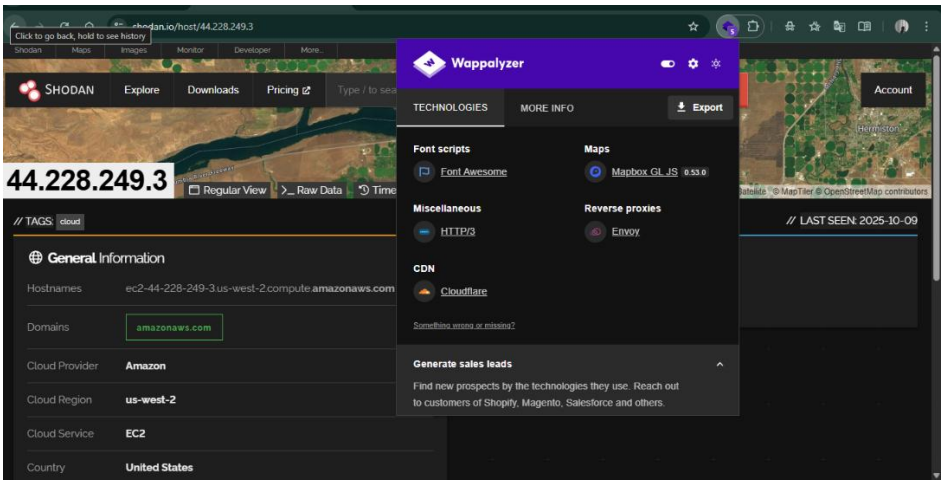
shodan host 44.228.249.3





4. TECHNOLOGY IDENTIFICATION

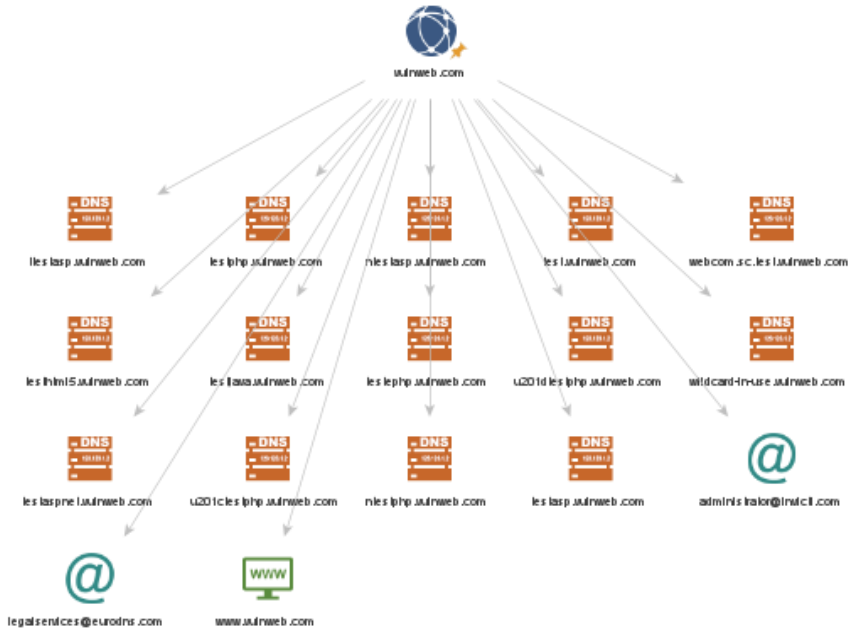
Tools: Wappalyzer browser extension to inspect Server and X-Powered-By headers.



5. MALTEGO GRAPHING

Transforms to run:

- Domain → To DNS names
- Domain → To certificates
- Certificate → To IP address



6. ASSET MAPPING (TABLE)

Timestamp	Tool	Finding
2025-10-09 20:10:00	WHOIS	Domain vulnweb.com
2025-10-09 20:15:00	DNS	testphp.vulnweb.com
2025-10-09 20:25:00	CT logs	Certificate: testphp.vulnweb.com
2025-10-09 20:40:00	Subfinder	Subdomains: testphp.vulnweb.com
2025-10-09 21:00:00	Wappalyzer	PHP, Apache
2025-10-09 21:15:00	Maltego	Passive graph attached
2025-10-09 21:30:00	Shodan	banners for IP

7. CHECKLIST

- WHOIS
- Subdomains enumeration (subfinder)
- Tech stack documention (Wappalyzer)
- Shodan banners capture
- Maltego graph.

8. RECON SUMMARY

Performed passive OSINT on vulnweb.com/testphp.vulnweb.com: WHOIS identified domains, DNS resolution confirmed test hosts, Wappalyzer and headers indicate a PHP/Apache stack, and Maltego passive transforms mapped certificates to IPs. Results compiled for informed, scoped active testing.