PASSIVE RECONNAISSANCE REPORT

Assignment 2 - Cyber Security Internship

Target Domain: vulnweb.com

Date: September 9-10, 2025

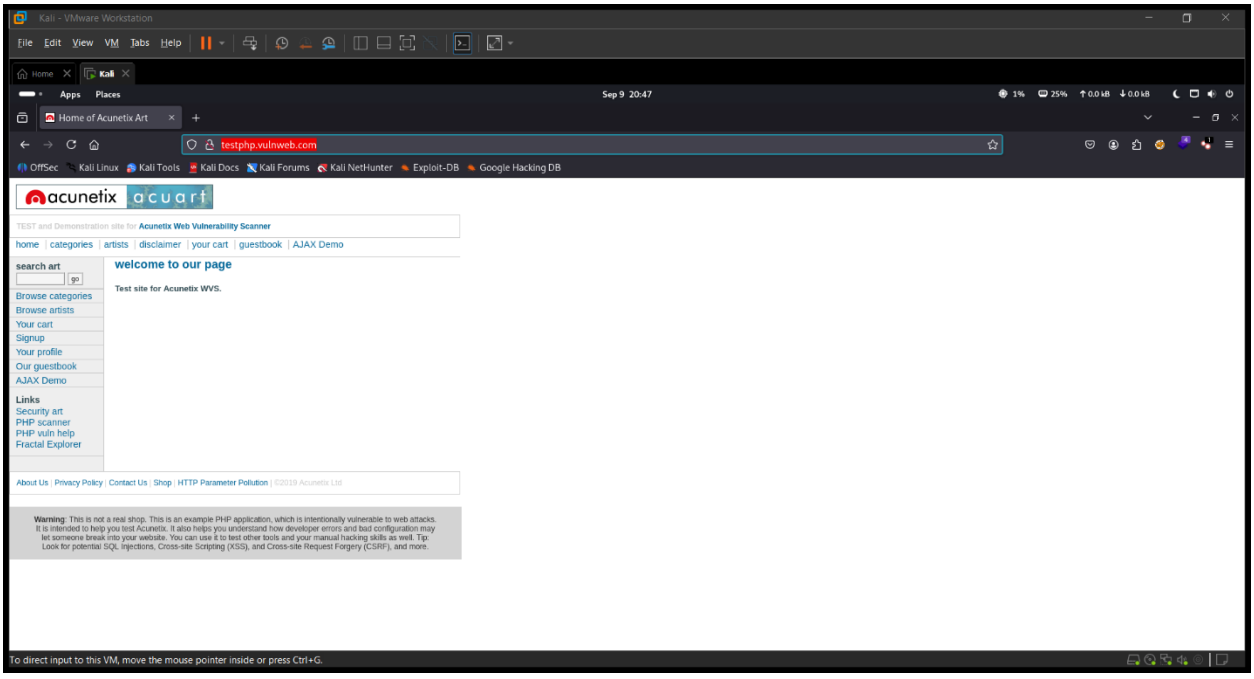
Performed By: Om Barot

Tools Used: Kali Linux

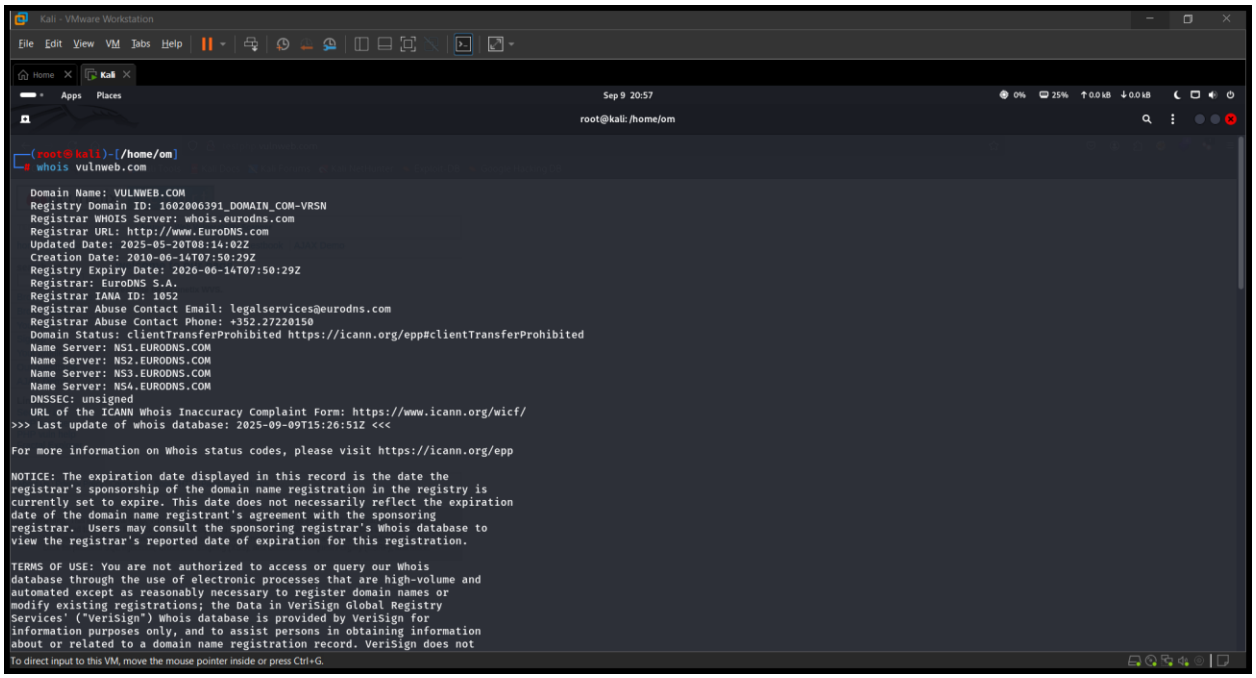
1. Target Domain Selection

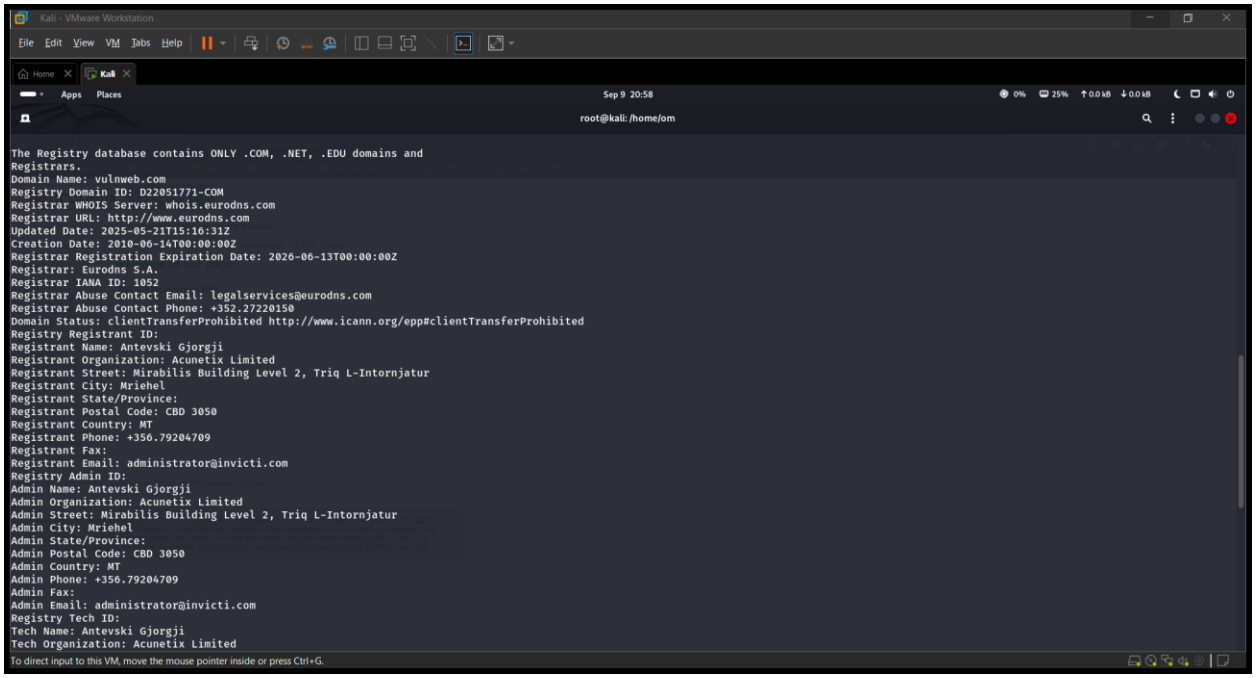
Target: vulnweb.com

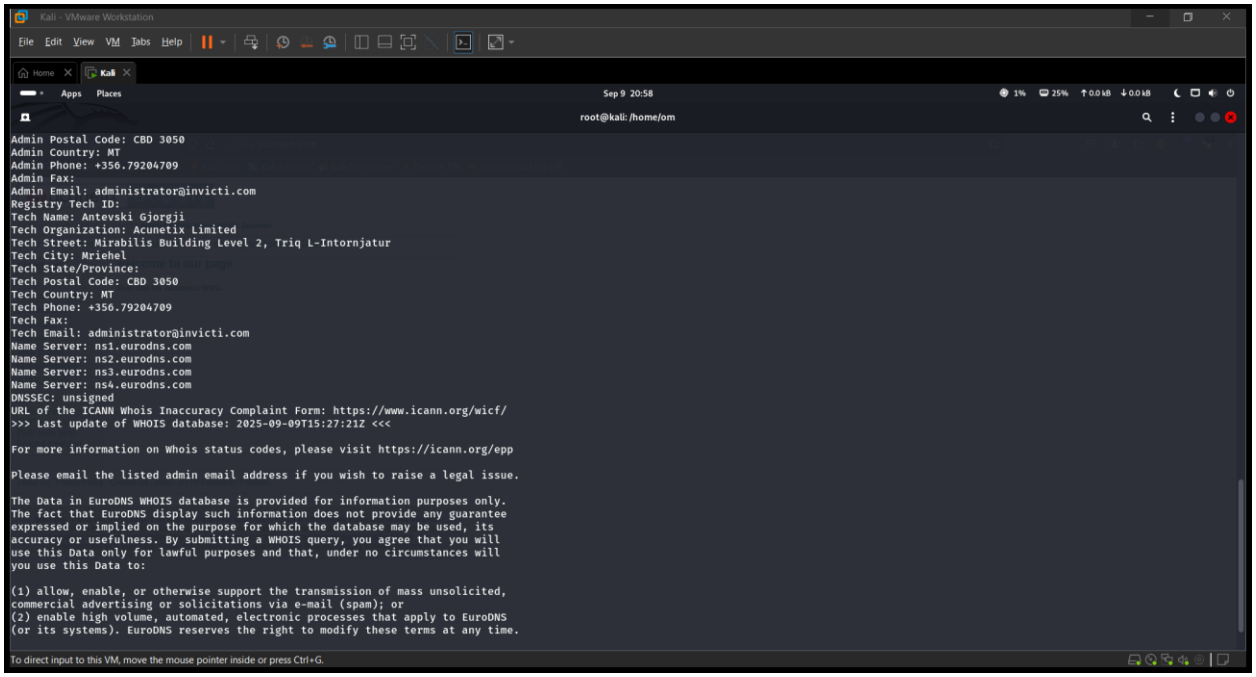
Justification: Selected vulnweb.com as it is a legitimate testing domain owned by Acunetix Limited, specifically designed for security testing and educational purposes. This ensures ethical and legal compliance with the assignment requirements.

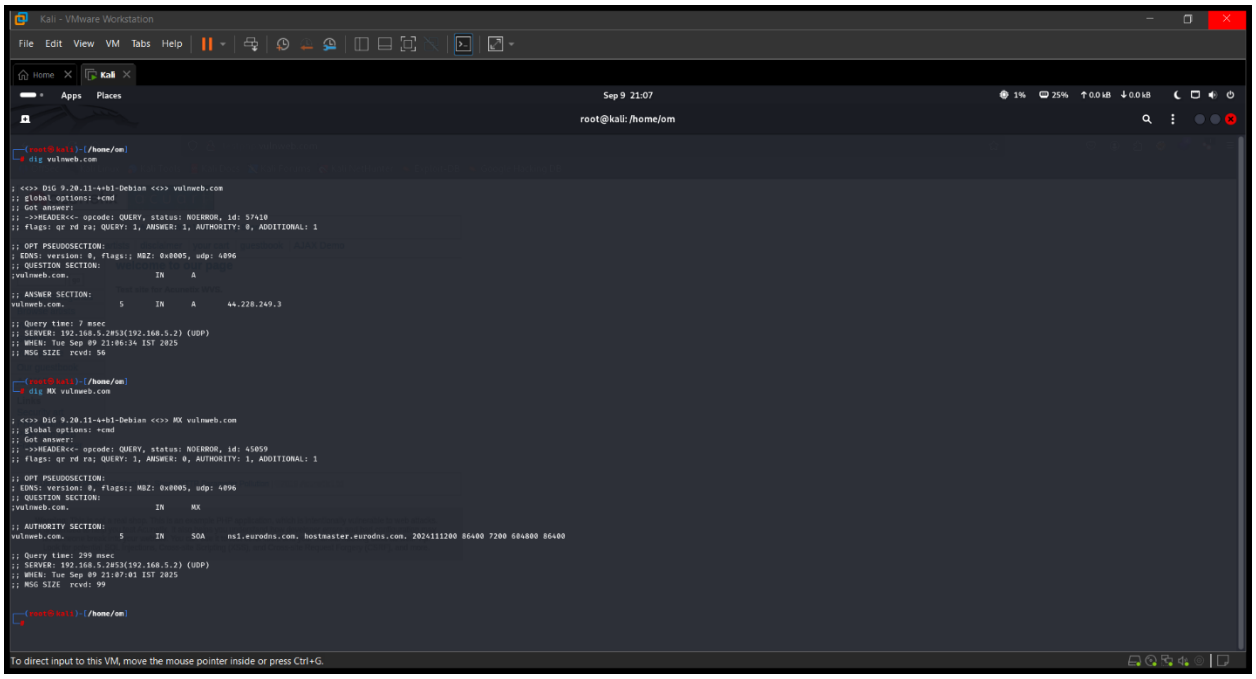


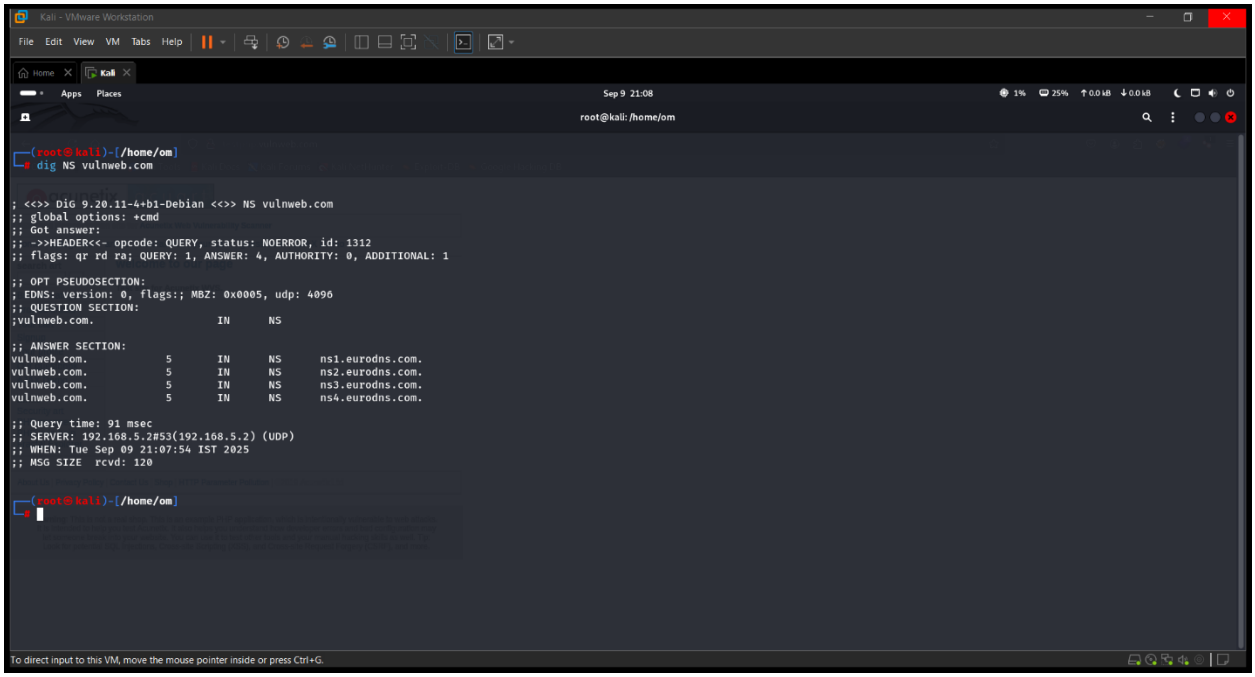
2. WHOIS & DNS Findings

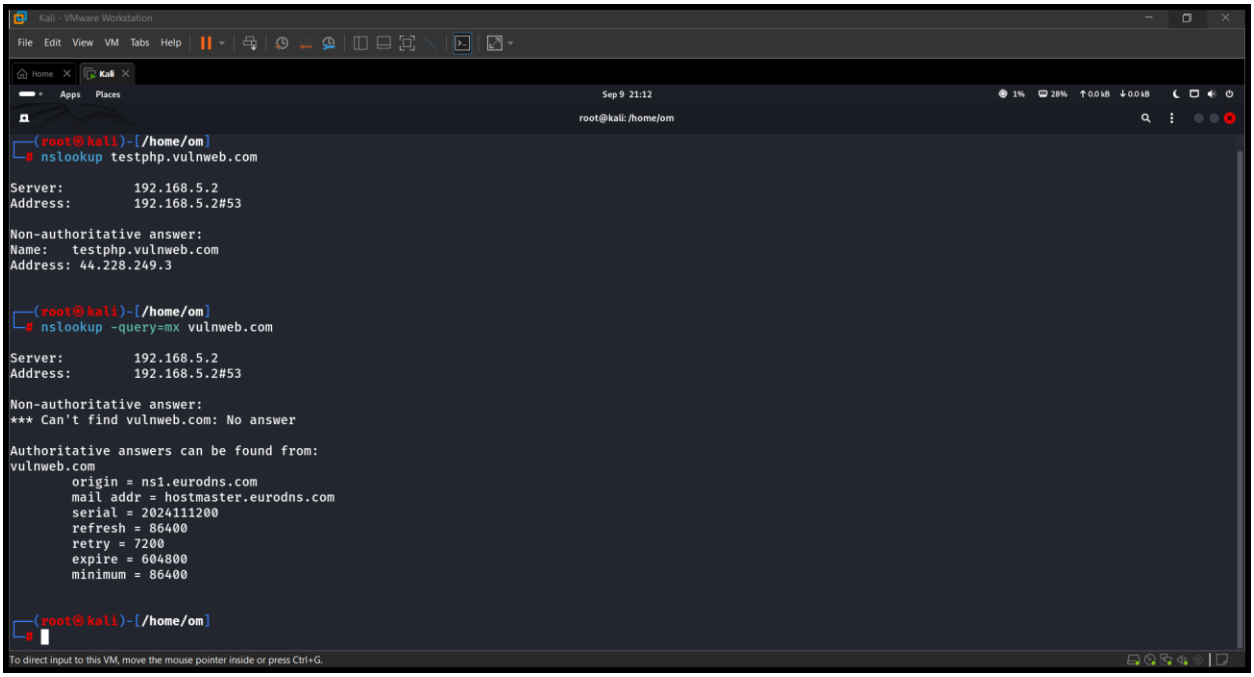


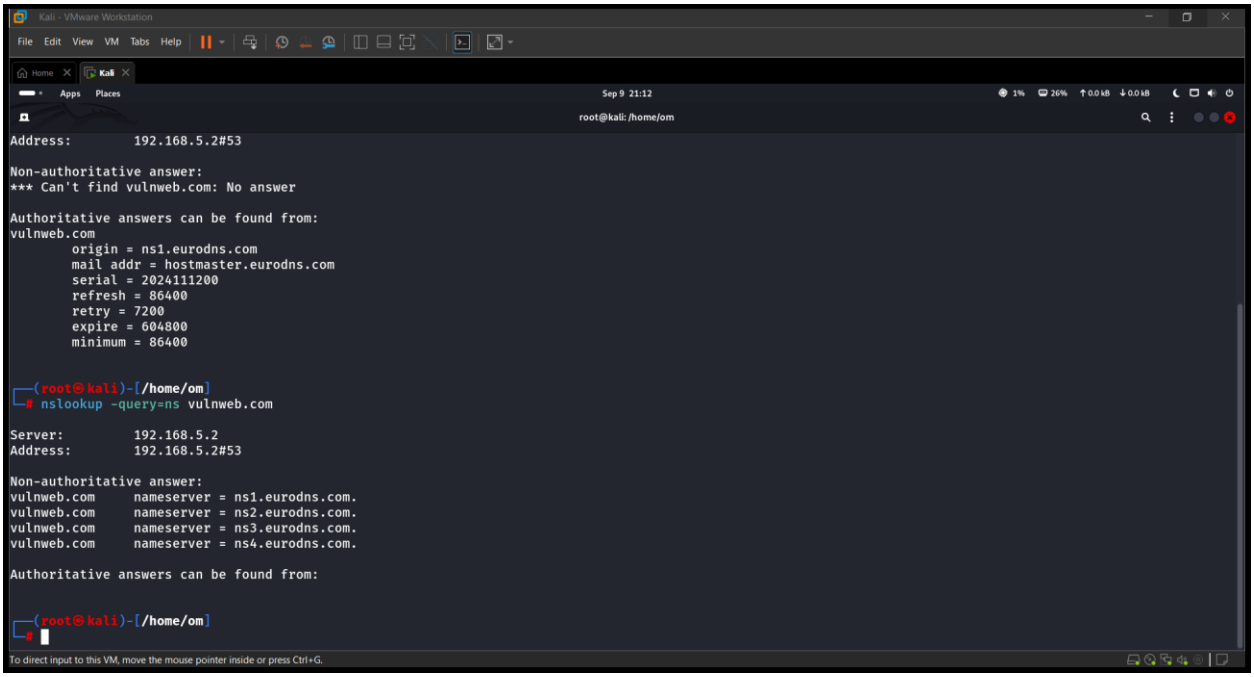



Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 20:58
root@kali: /home/om
Admin Postal Code: CBD 3050
Admin Country: MT
Admin Phone: +356.79204709
Admin Fax:
Admin Email: administrator@invicti.com
Registry Tech ID:
Tech Name: Antevski Gjorgji
Tech Organization: Acunetix Limited
Tech Street: Mirabilis Building Level 2, Triq L-Intornjatur
Tech City: Mriehel
Tech State/Province:
Tech Postal Code: CBD 3050
Tech Country: MT
Tech Phone: +356.79204709
Tech Fax:
Tech Email: administrator@invicti.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: 2025-09-09T15:27:21Z <<<
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.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 21:07
root@kali: /home/om
┌──(root㉿kali)-[/home/om]
└─# dig vulnweb.com
; <<>> DiG 9.20.11-4+b1-Debian <<>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57410
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;vulnweb.com. IN A
;; ANSWER SECTION:
vulnweb.com. 5 IN A 44.228.249.3
;; Query time: 7 msec
;; SERVER: 192.168.5.2#53(192.168.5.2) (UDP)
;; WHEN: Tue Sep 09 21:06:34 IST 2025
;; MSG SIZE rcvd: 56
┌──(root㉿kali)-[/home/om]
└─# dig MX vulnweb.com
; <<>> DiG 9.20.11-4+b1-Debian <<>> MX vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45059
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;vulnweb.com. IN MX
;; AUTHORITY SECTION:
vulnweb.com. 5 IN SOA ns1.eurodns.com. hostmaster.eurodns.com. 2024111200 86400 7200 604800 86400
;; Query time: 299 msec
;; SERVER: 192.168.5.2#53(192.168.5.2) (UDP)
;; WHEN: Tue Sep 09 21:07:01 IST 2025
;; MSG SIZE rcvd: 99
┌──(root㉿kali)-[/home/om]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 21:08
root@kali: /home/om
(root㉿kali)-[/home/om]
dig NS vulnweb.com
; <<>> DiG 9.20.11-4+b1-Debian <<>> NS vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1312
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;vulnweb.com. IN NS
;; ANSWER SECTION:
vulnweb.com. 5 IN NS ns1.eurodns.com.
vulnweb.com. 5 IN NS ns2.eurodns.com.
vulnweb.com. 5 IN NS ns3.eurodns.com.
vulnweb.com. 5 IN NS ns4.eurodns.com.
;; Query time: 91 msec
;; SERVER: 192.168.5.2#53(192.168.5.2) (UDP)
;; WHEN: Tue Sep 09 21:07:54 IST 2025
;; MSG SIZE rcvd: 120
(root㉿kali)-[/home/om]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 21:12
root@kali: /home/om
(root㉿kali)-[/home/om]
nslookup testphp.vulnweb.com
Server: 192.168.5.2
Address: 192.168.5.2#53
Non-authoritative answer:
Name: testphp.vulnweb.com
Address: 44.228.249.3
(root㉿kali)-[/home/om]
nslookup -query=mx vulnweb.com
Server: 192.168.5.2
Address: 192.168.5.2#53
Non-authoritative answer:
*** Can't find vulnweb.com: No answer
Authoritative answers can be found from:
vulnweb.com
origin = ns1.eurodns.com
mail addr = hostmaster.eurodns.com
serial = 2024111200
refresh = 86400
retry = 7200
expire = 604800
minimum = 86400
(root㉿kali)-[/home/om]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



WHOIS Information

Based on the WHOIS lookup results:

- **Domain Name:** vulnweb.com
- **Registrar:** EuroDNS S.A.
- **Creation Date:** June 14, 2010
- **Expiry Date:** June 14, 2026
- **Registrant:** Acunetix Limited
- **Organization Address:** Mirabilis Building Level 2, Triq L-Intornjatur, Mriehel, Malta (CBD 3050)
- **Admin Contact:** administrator@invicti.com
- **Phone:** +356.79204709

DNS Records Analysis

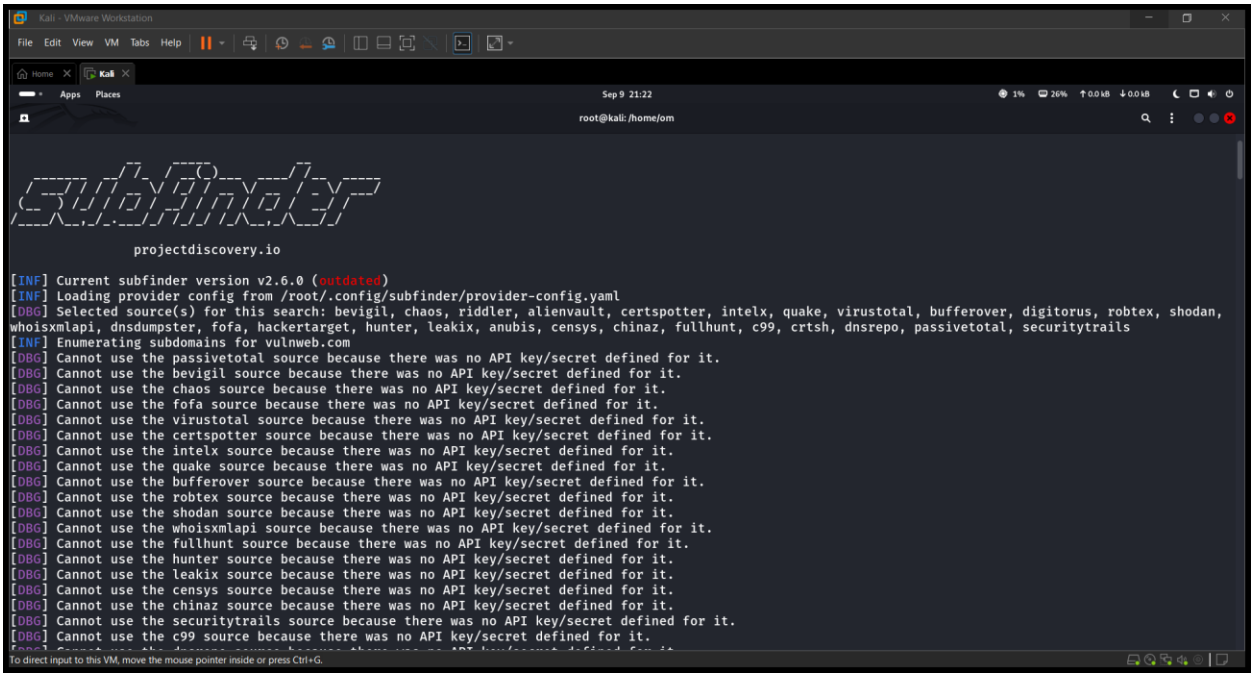
DNS enumeration using dig and nslookup revealed:

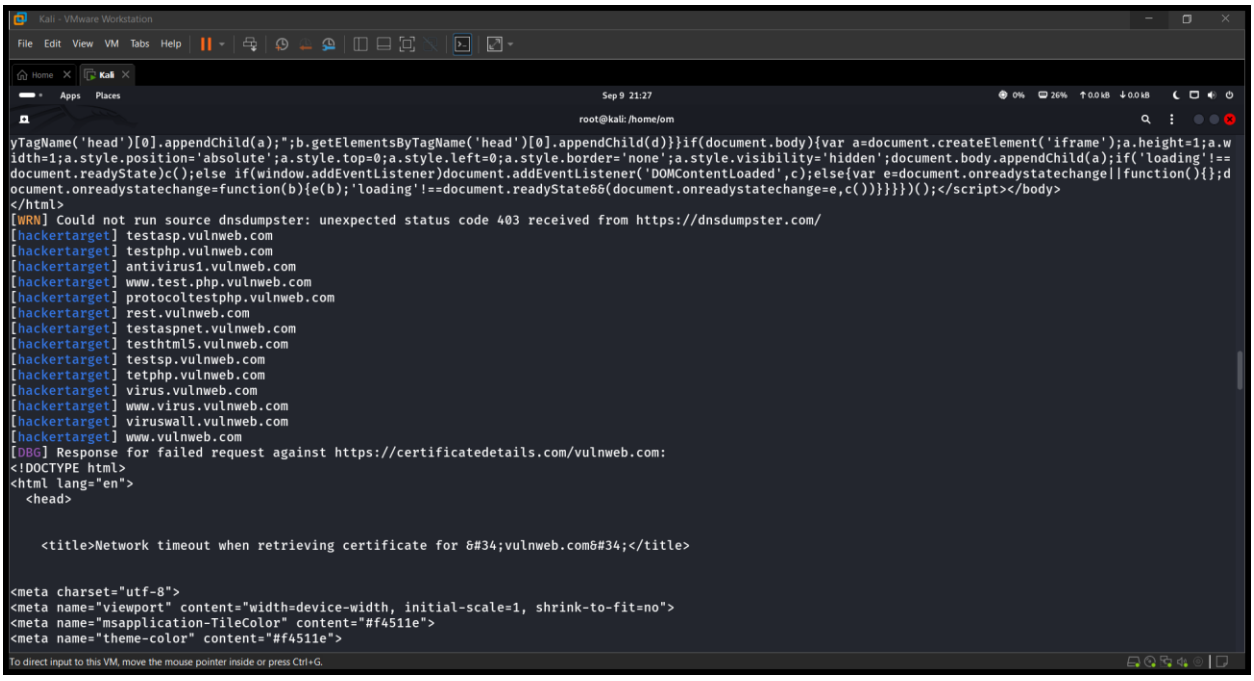
- **A Record:** 44.228.249.3
- **Name Servers:**

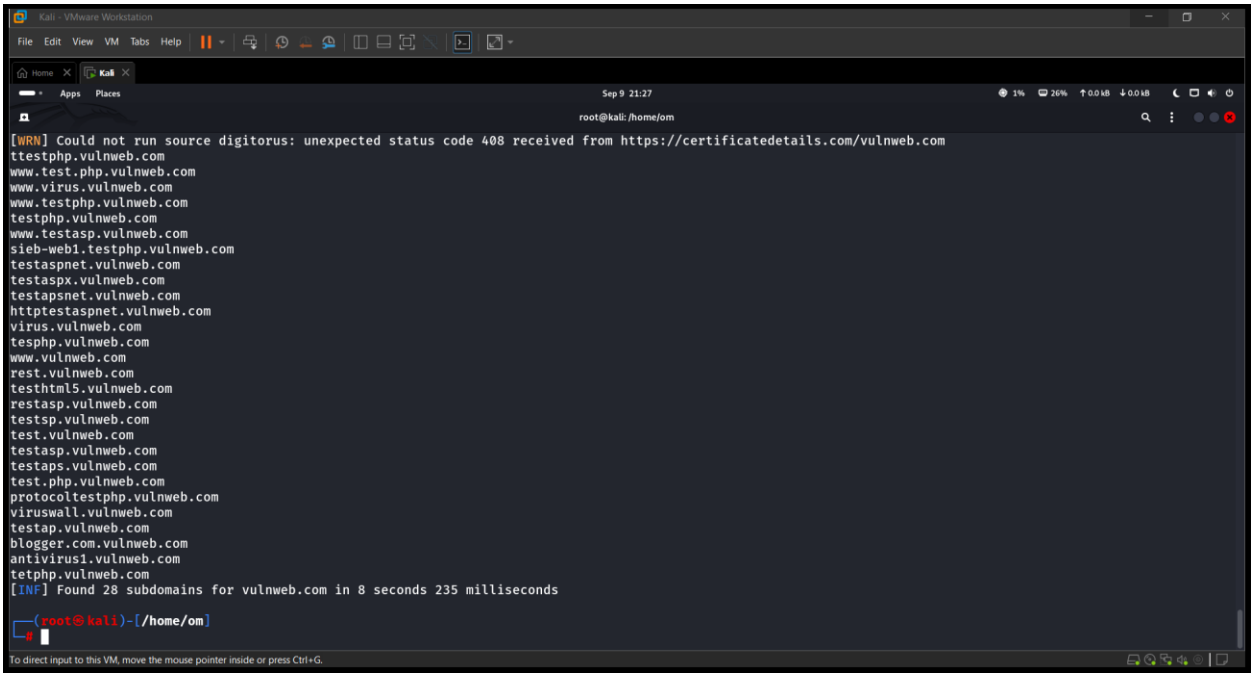
    - ns1.eurodns.com
    - ns2.eurodns.com
    - ns3.eurodns.com
    - ns4.eurodns.com
- **MX Records:** No mail exchange records found
- **Infrastructure:** Hosted on Amazon AWS (ASN 16509)

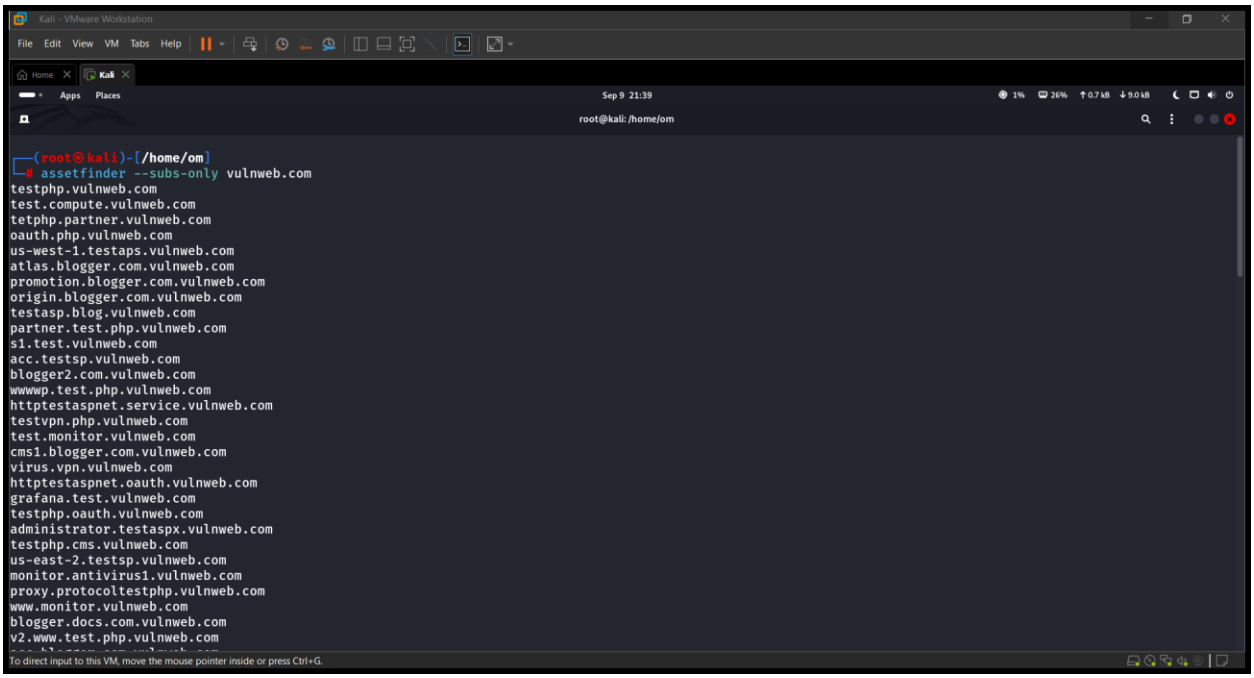
3. Subdomains Discovered

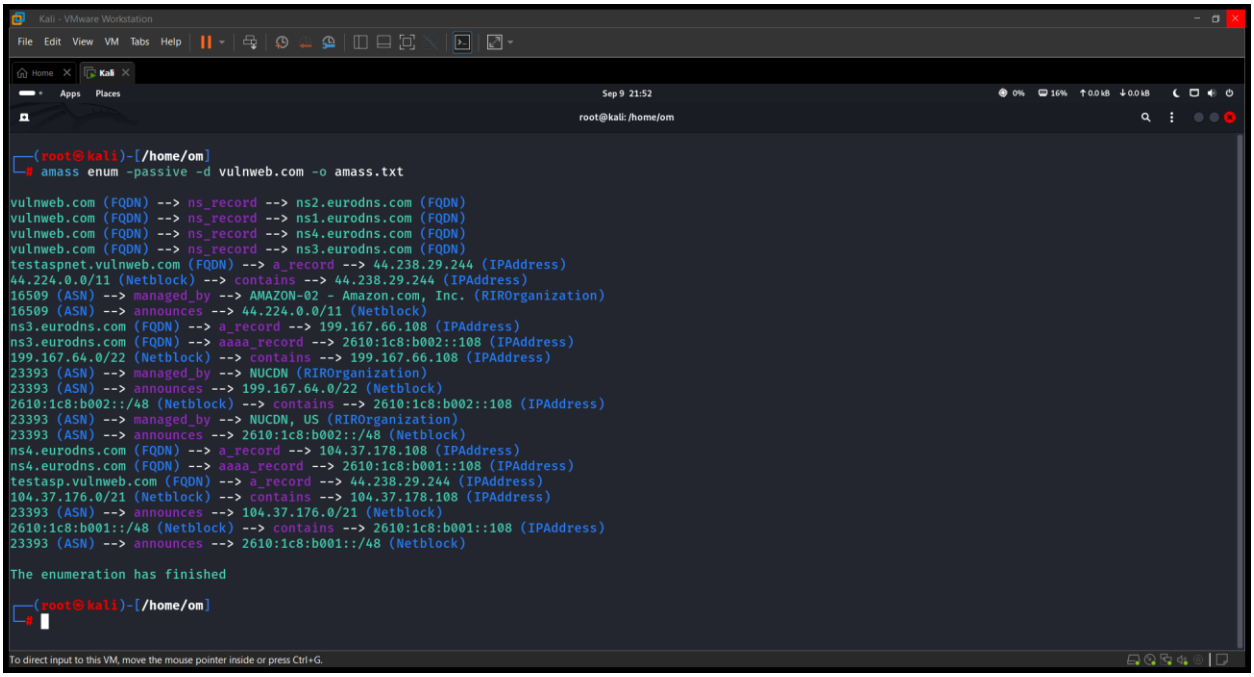
Using subfinder, assetfinder, and amass, the following **28 primary subdomains** were identified:






Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 21:27
root@kali: /home/om
[WRN] Could not run source digitorus: unexpected status code 408 received from https://certificatedetails.com/vulnweb.com
ttestphp.vulnweb.com
www.test.php.vulnweb.com
www.virus.vulnweb.com
www.testphp.vulnweb.com
testphp.vulnweb.com
www.testasp.vulnweb.com
sieb-web1.testphp.vulnweb.com
testaspnet.vulnweb.com
testaspx.vulnweb.com
testapsnet.vulnweb.com
httptestaspnet.vulnweb.com
virus.vulnweb.com
tesphp.vulnweb.com
www.vulnweb.com
rest.vulnweb.com
testhtml5.vulnweb.com
restasp.vulnweb.com
testsp.vulnweb.com
test.vulnweb.com
testasp.vulnweb.com
testaps.vulnweb.com
test.php.vulnweb.com
protocoltestphp.vulnweb.com
viruswall.vulnweb.com
testap.vulnweb.com
blogger.com.vulnweb.com
antivirus1.vulnweb.com
tetphp.vulnweb.com
[INF] Found 28 subdomains for vulnweb.com in 8 seconds 235 milliseconds
(root@kali)-[/home/om]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 9 21:39
root@kali: /home/om
(root@kali)-[/home/om]
assetfinder --subs-only vulnweb.com
testphp.vulnweb.com
test.compute.vulnweb.com
tetphp.partner.vulnweb.com
oauth.php.vulnweb.com
us-west-1.testaps.vulnweb.com
atlas.blogger.com.vulnweb.com
promotion.blogger.com.vulnweb.com
origin.blogger.com.vulnweb.com
testasp.blog.vulnweb.com
partner.test.php.vulnweb.com
s1.test.vulnweb.com
acc.testsp.vulnweb.com
blogger2.com.vulnweb.com
wwwwp.test.php.vulnweb.com
httptestaspnet.service.vulnweb.com
testvpn.php.vulnweb.com
test.monitor.vulnweb.com
cms1.blogger.com.vulnweb.com
virus.vpn.vulnweb.com
httptestaspnet.oauth.vulnweb.com
grafana.test.vulnweb.com
testphp.oauth.vulnweb.com
administrator.testaspx.vulnweb.com
testphp.cms.vulnweb.com
us-east-2.testsp.vulnweb.com
monitor.antivirus1.vulnweb.com
proxy.protocoltestphp.vulnweb.com
www.monitor.vulnweb.com
blogger.docs.com.vulnweb.com
v2.www.test.php.vulnweb.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Active Testing Applications:

- **testphp.vulnweb.com** - PHP vulnerable web application
- **testasp.vulnweb.com** - ASP vulnerable web application
- **testaspnet.vulnweb.com** - ASP.NET vulnerable web application
- **testhtml5.vulnweb.com** - HTML5 testing application
- **rest.vulnweb.com** - REST API testing endpoint

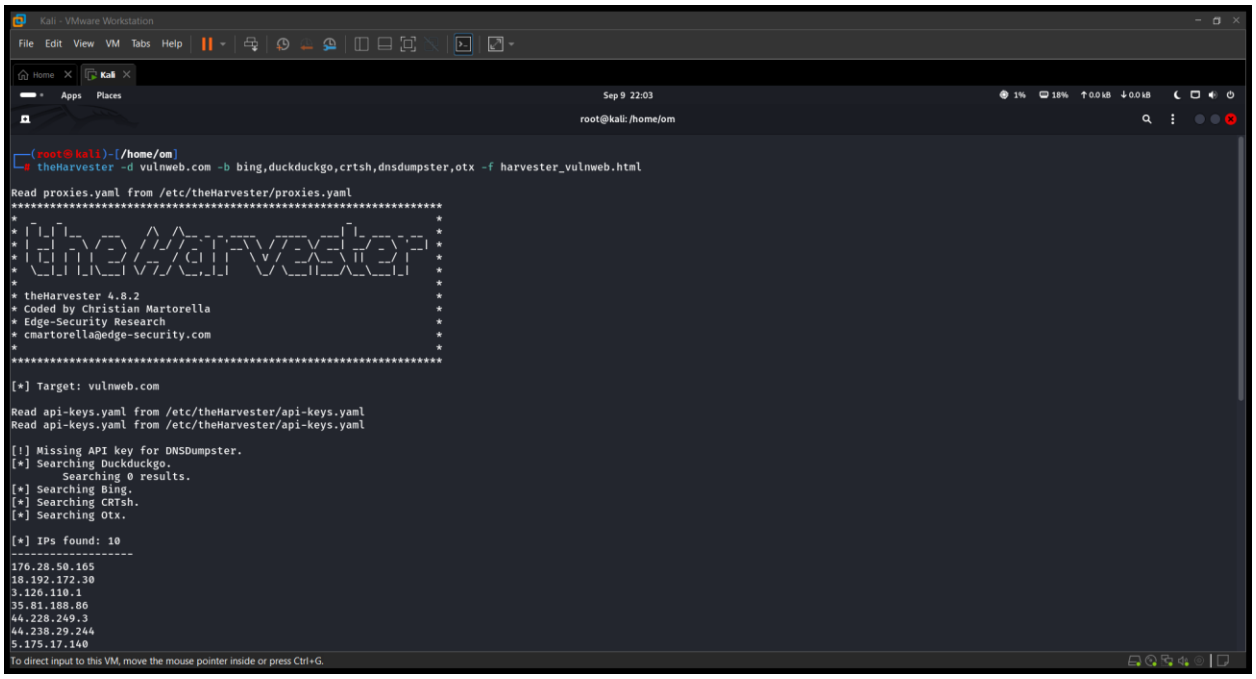
Additional Subdomains:

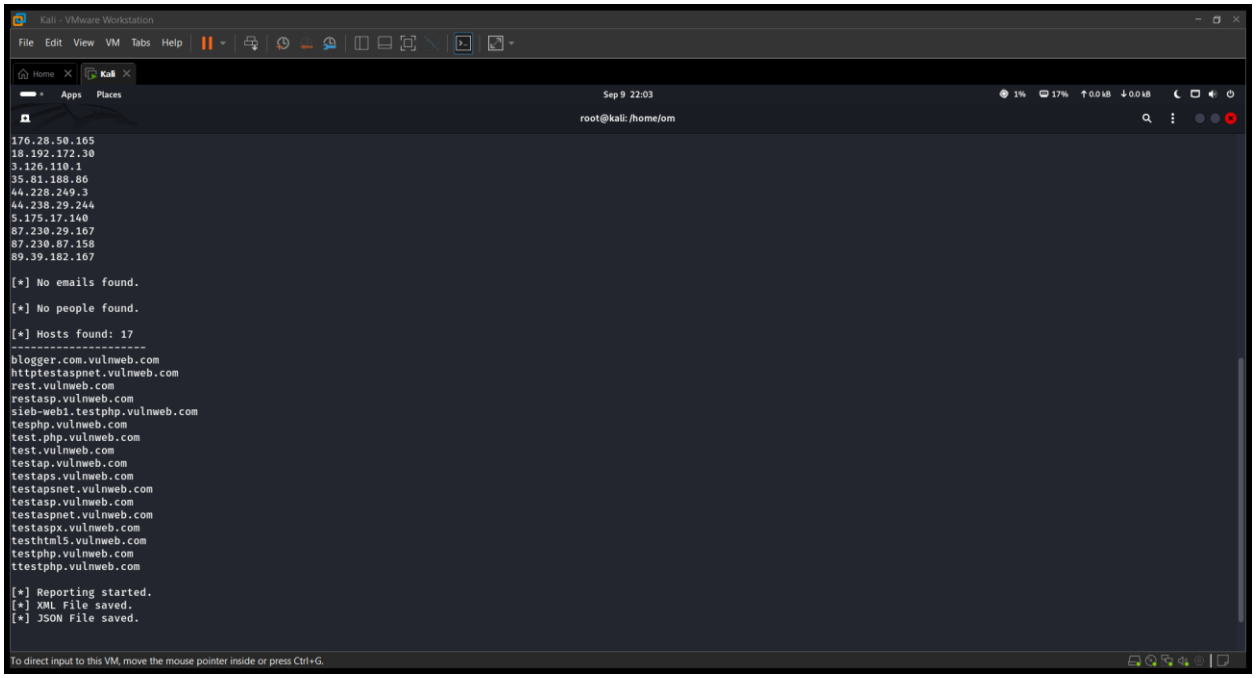
- blogger.com.vulnweb.com
- virus.vulnweb.com
- antivirus1.vulnweb.com
- viruswall.vulnweb.com
- test.vulnweb.com
- www.vulnweb.com
- protocoltestphp.vulnweb.com
- sieb-web1.testphp.vulnweb.com

Total Infrastructure: Over 100+ subdomains discovered including development, testing, and service-specific endpoints.

4. Email IDs & Employee Data

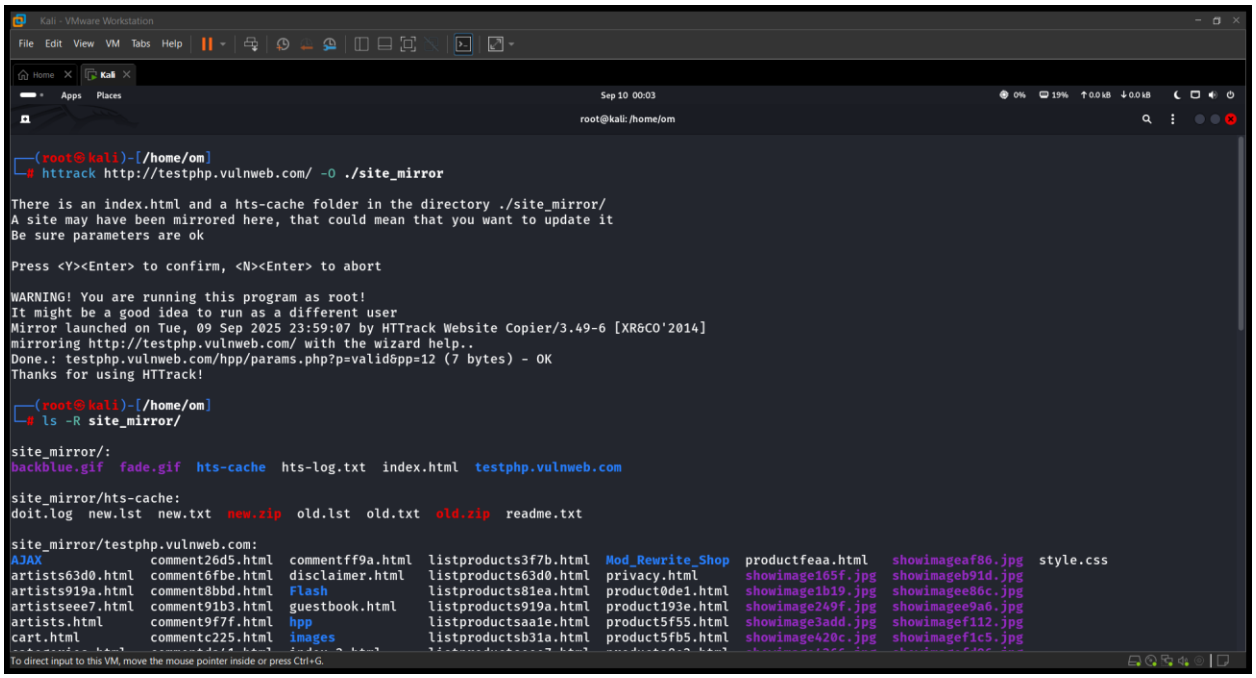
TheHarvester Results:

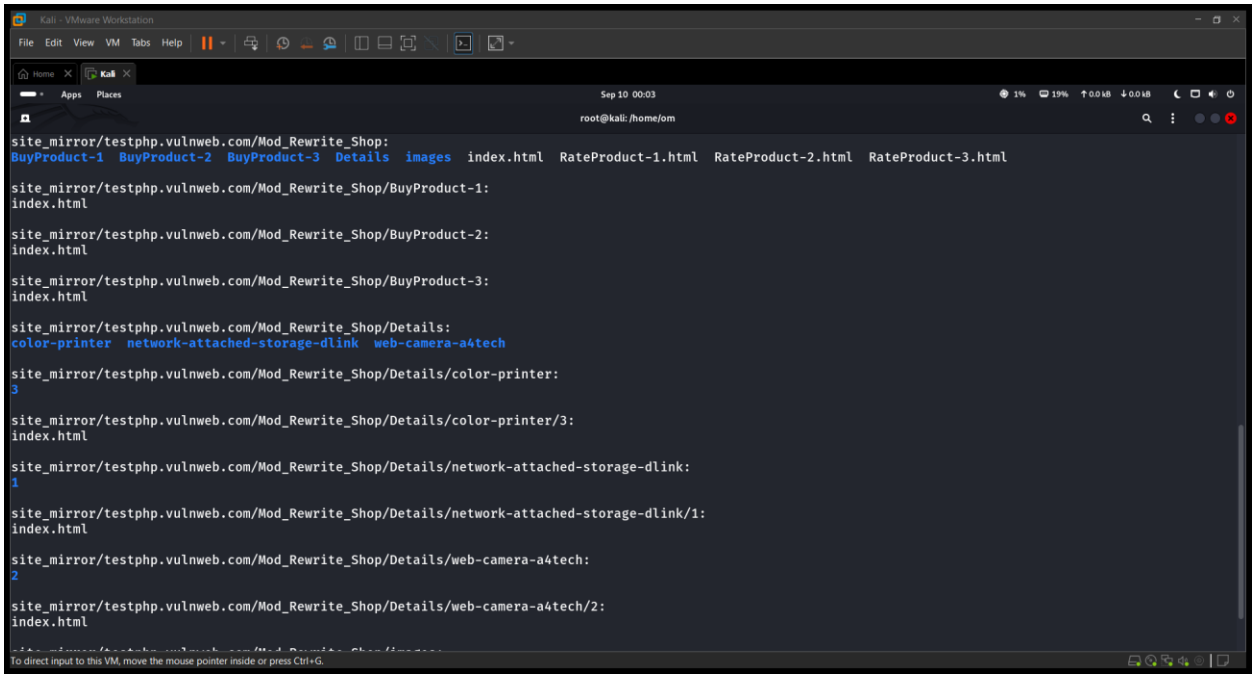


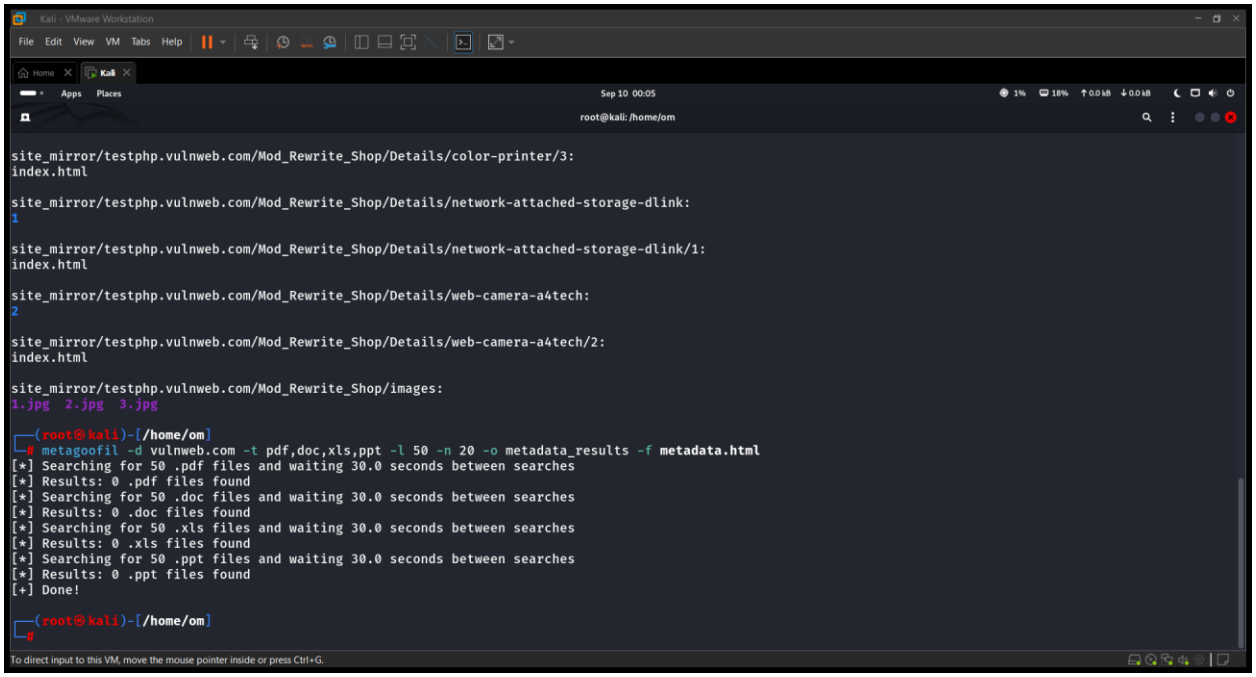


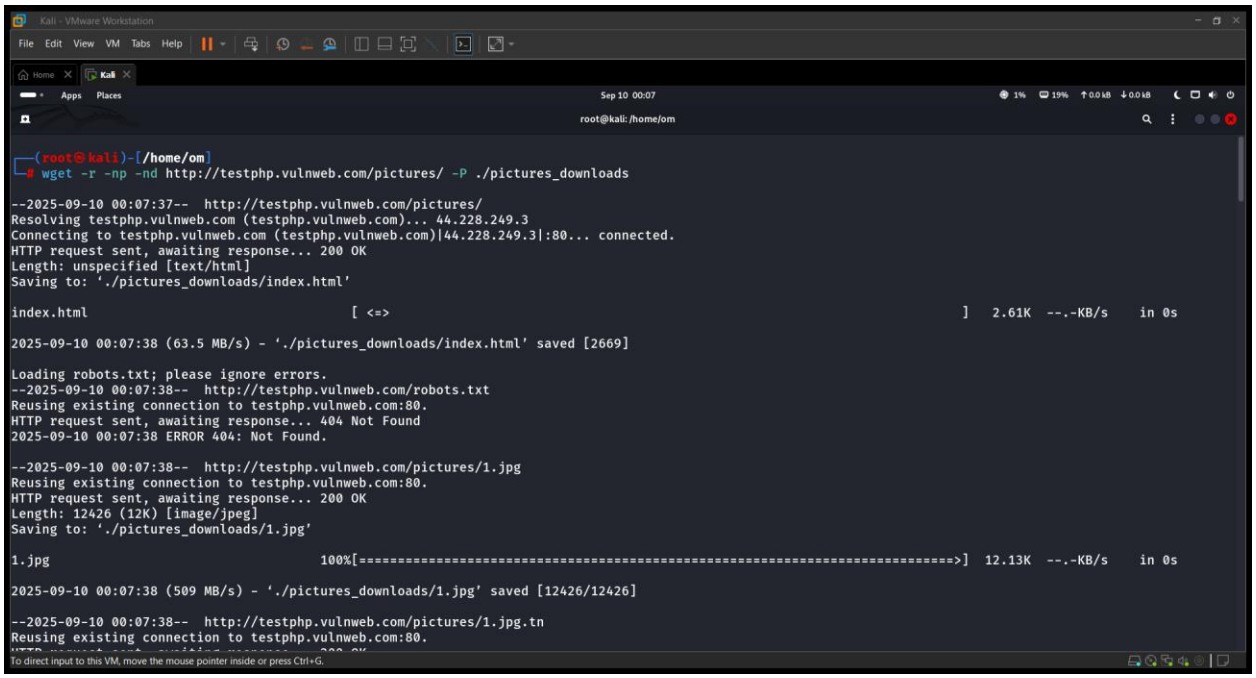
- **Command Used:** `theharvester -d vulnweb.com -b bing,duckduckgo,crtsh,dnsdumpster,otx`
- **Hosts Discovered:** 17 unique hostnames
- **IP Addresses:** 10 unique IP addresses ranging from 3.126.110.1 to 176.28.50.165
- **Email Addresses:** No personal email addresses discovered (expected for testing domain)
- **Contact Found:** administrator@invicti.com (from WHOIS data)

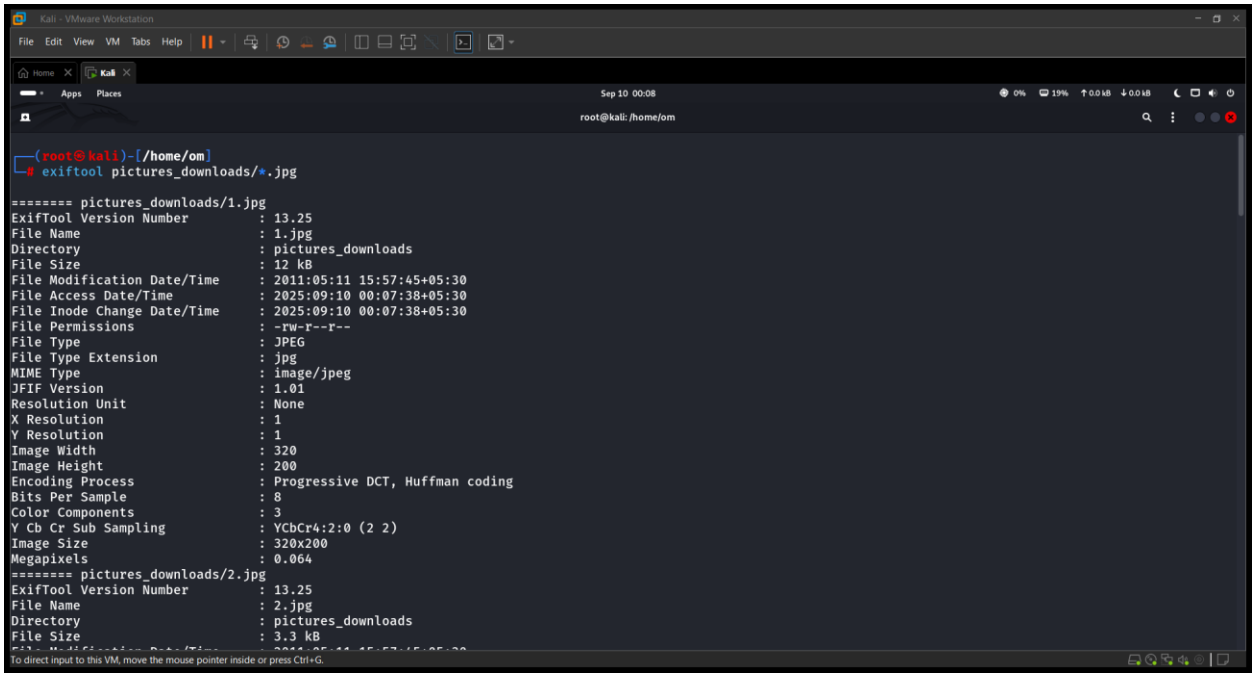
5. Metadata Information

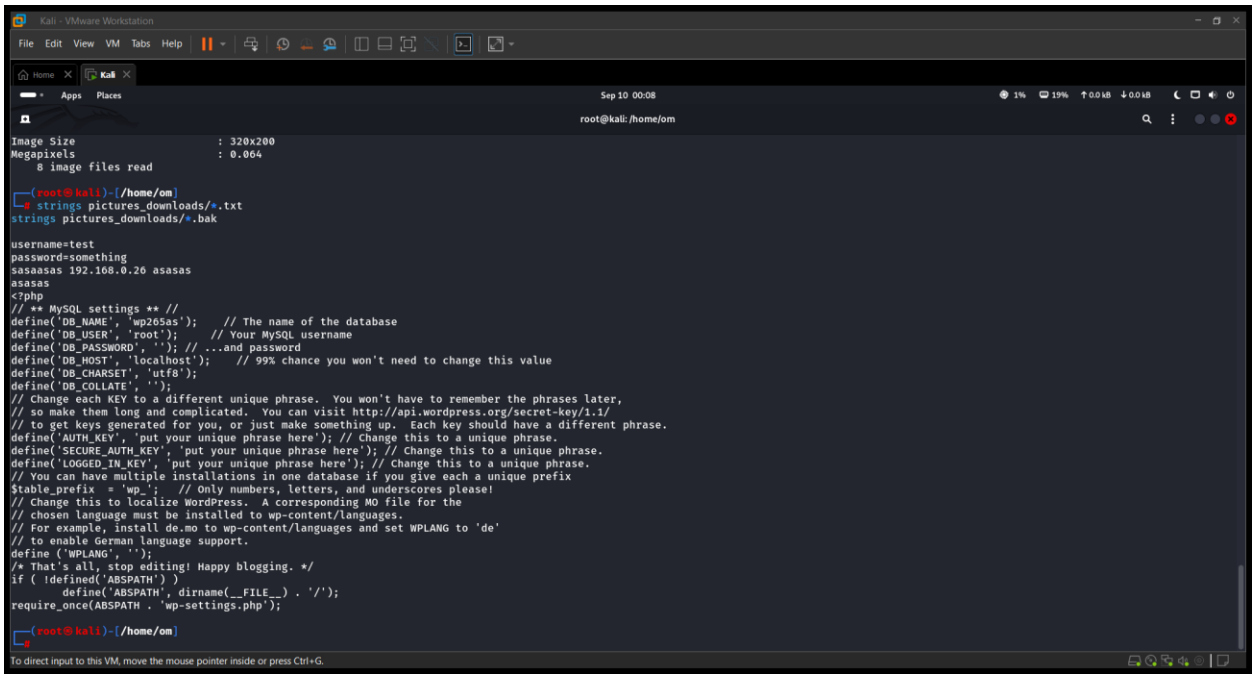





Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 10 00:05
root@kali: /home/om
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3:
index.html
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink:
1
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1:
index.html
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech:
2
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2:
index.html
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/images:
1.jpg 2.jpg 3.jpg
┌──(root㉿kali)-[/home/om]
└─# metagoofil -d vulnweb.com -t pdf,doc,xls,ppt -l 50 -n 20 -o metadata_results -f metadata.html
[*] Searching for 50 .pdf files and waiting 30.0 seconds between searches
[*] Results: 0 .pdf files found
[*] Searching for 50 .doc files and waiting 30.0 seconds between searches
[*] Results: 0 .doc files found
[*] Searching for 50 .xls files and waiting 30.0 seconds between searches
[*] Results: 0 .xls files found
[*] Searching for 50 .ppt files and waiting 30.0 seconds between searches
[*] Results: 0 .ppt files found
[+] Done!
┌──(root㉿kali)-[/home/om]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Apps Places
Sep 10 00:07
root@kali: /home/om
┌──(root㉿kali)-[/home/om]
└─# wget -r -np -nd http://testphp.vulnweb.com/pictures/ -P ./pictures_downloads
--2025-09-10 00:07:37-- http://testphp.vulnweb.com/pictures/
Resolving testphp.vulnweb.com (testphp.vulnweb.com)... 44.228.249.3
Connecting to testphp.vulnweb.com (testphp.vulnweb.com)|44.228.249.3|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘./pictures_downloads/index.html’
index.html [<=>] 2.61K --.-KB/s in 0s
2025-09-10 00:07:38 (63.5 MB/s) - ‘./pictures_downloads/index.html’ saved [2669]
Loading robots.txt; please ignore errors.
--2025-09-10 00:07:38-- http://testphp.vulnweb.com/robots.txt
Reusing existing connection to testphp.vulnweb.com:80.
HTTP request sent, awaiting response... 404 Not Found
2025-09-10 00:07:38 ERROR 404: Not Found.
--2025-09-10 00:07:38-- http://testphp.vulnweb.com/pictures/1.jpg
Reusing existing connection to testphp.vulnweb.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 12426 (12K) [image/jpeg]
Saving to: ‘./pictures_downloads/1.jpg’
1.jpg 100%[==========>] 12.13K --.-KB/s in 0s
2025-09-10 00:07:38 (509 MB/s) - ‘./pictures_downloads/1.jpg’ saved [12426/12426]
--2025-09-10 00:07:38-- http://testphp.vulnweb.com/pictures/1.jpg.tn
Reusing existing connection to testphp.vulnweb.com:80.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





Files Analyzed Using ExifTool:

Downloaded and analyzed multiple files from the target revealing:

Image Files:

- Multiple JPEG files (320x200 and 160x100 resolution)

- Creation dates: 2011-05-11
- No GPS or camera information embedded

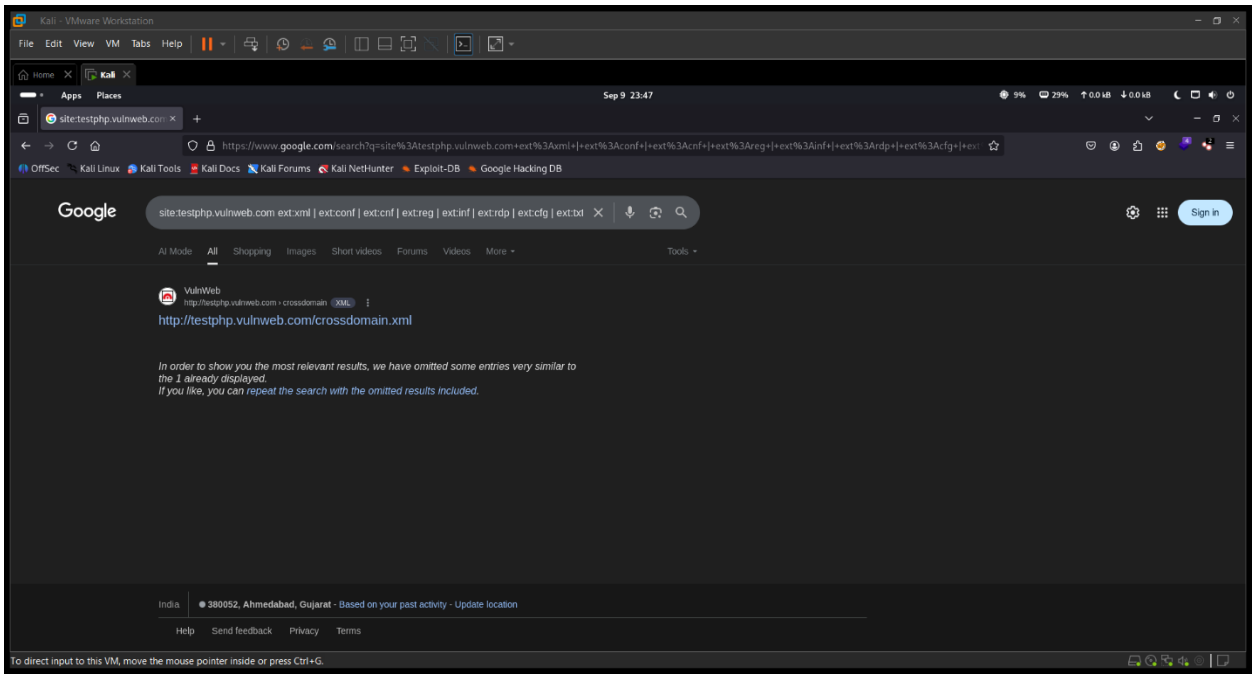
Sensitive Files Discovered:

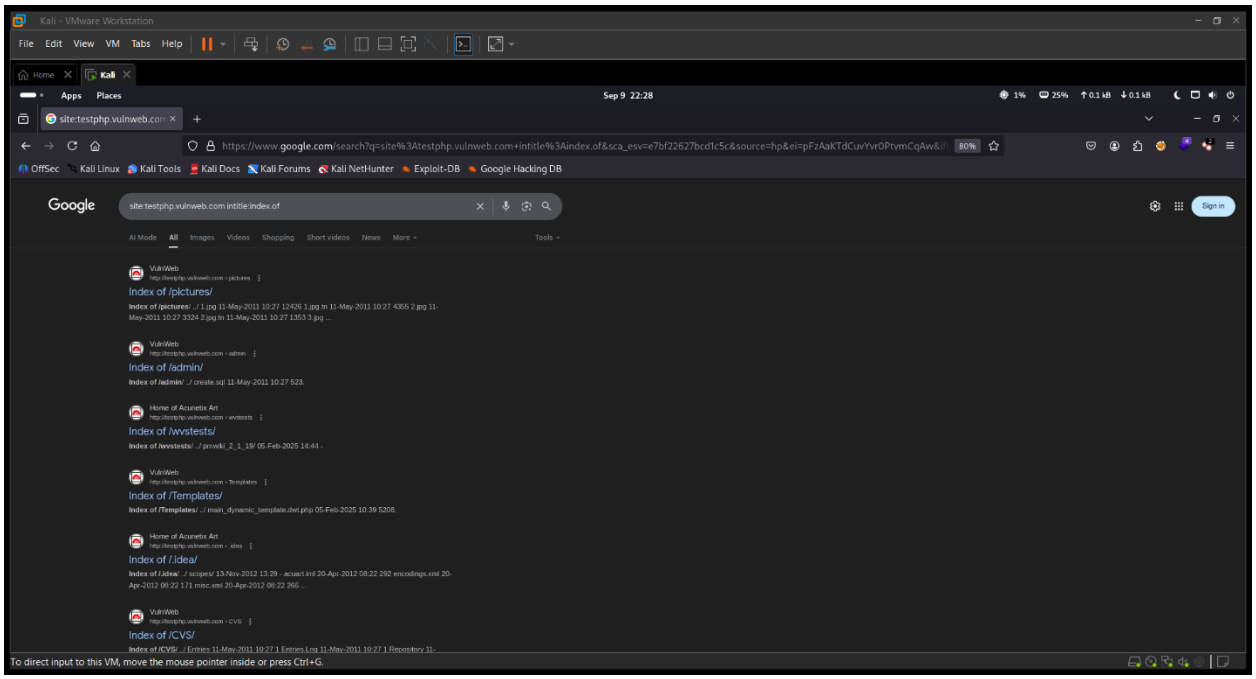
- **credentials.txt** - 33 bytes, potential credential storage
- **wp-config.bak** - WordPress configuration backup (1,535 bytes)
- **ipaddresses.txt** - IP address listing (52 bytes)
- **WS_FTP.LOG** - FTP transfer logs (771 bytes)
- **path-disclosure-unix.html** - System path disclosure examples
- **path-disclosure-win.html** - Windows path disclosure examples

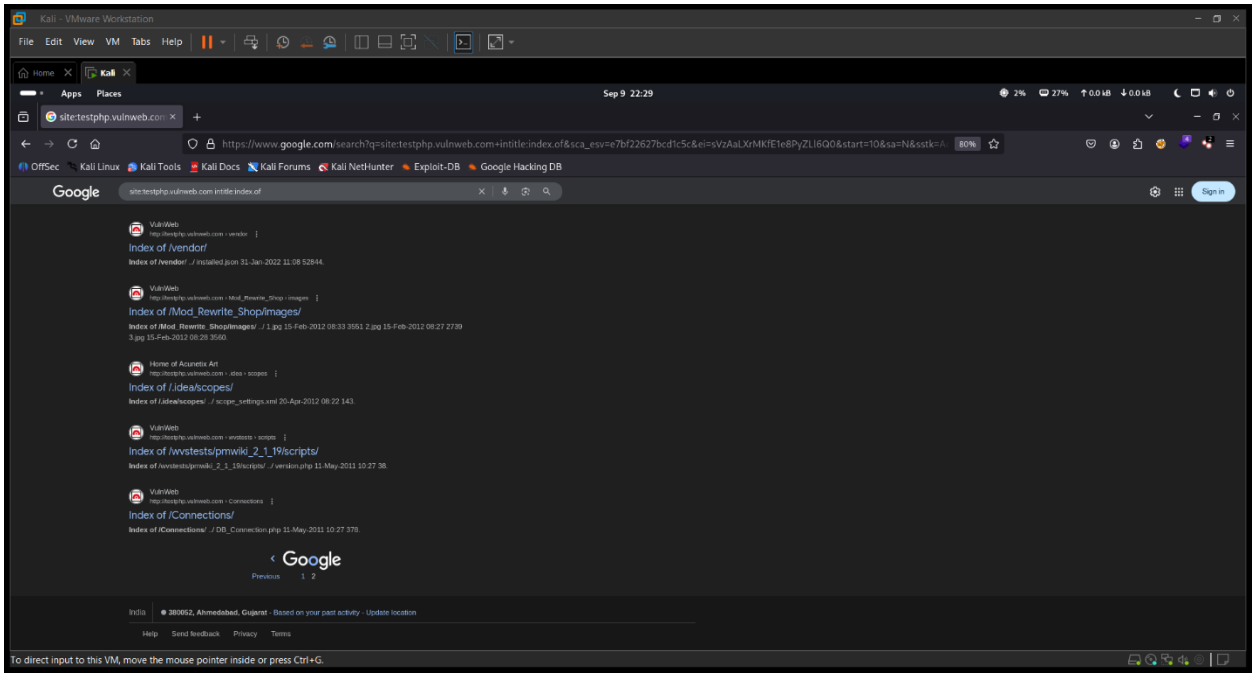
Key Metadata Findings:

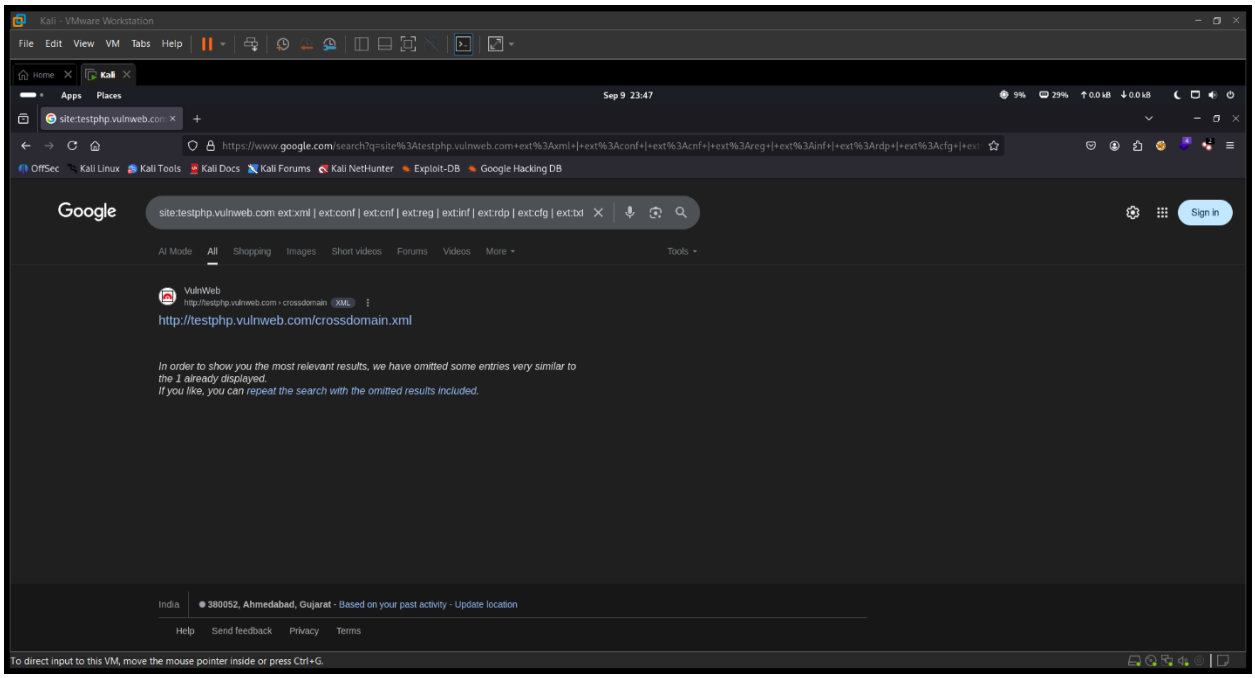
- Files date back to 2008-2013, indicating legacy systems
- Directory listing available at `/pictures/`
- Backup configuration files accessible

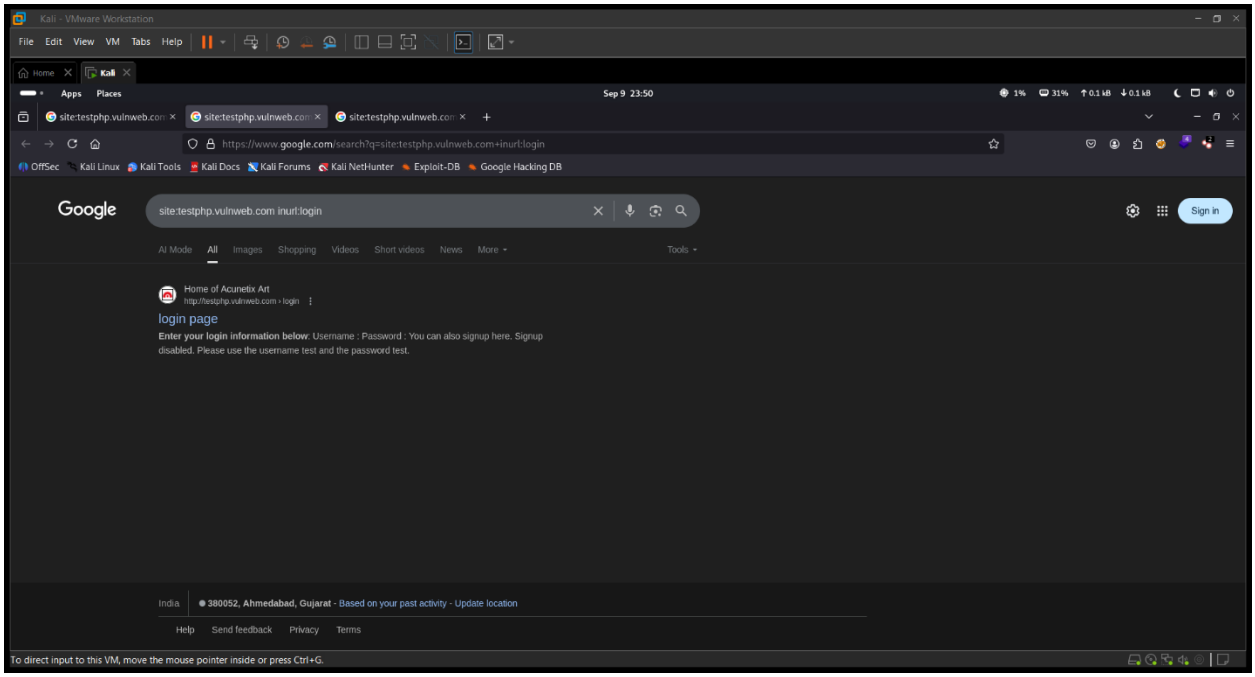
6. Google Dorks Attempted

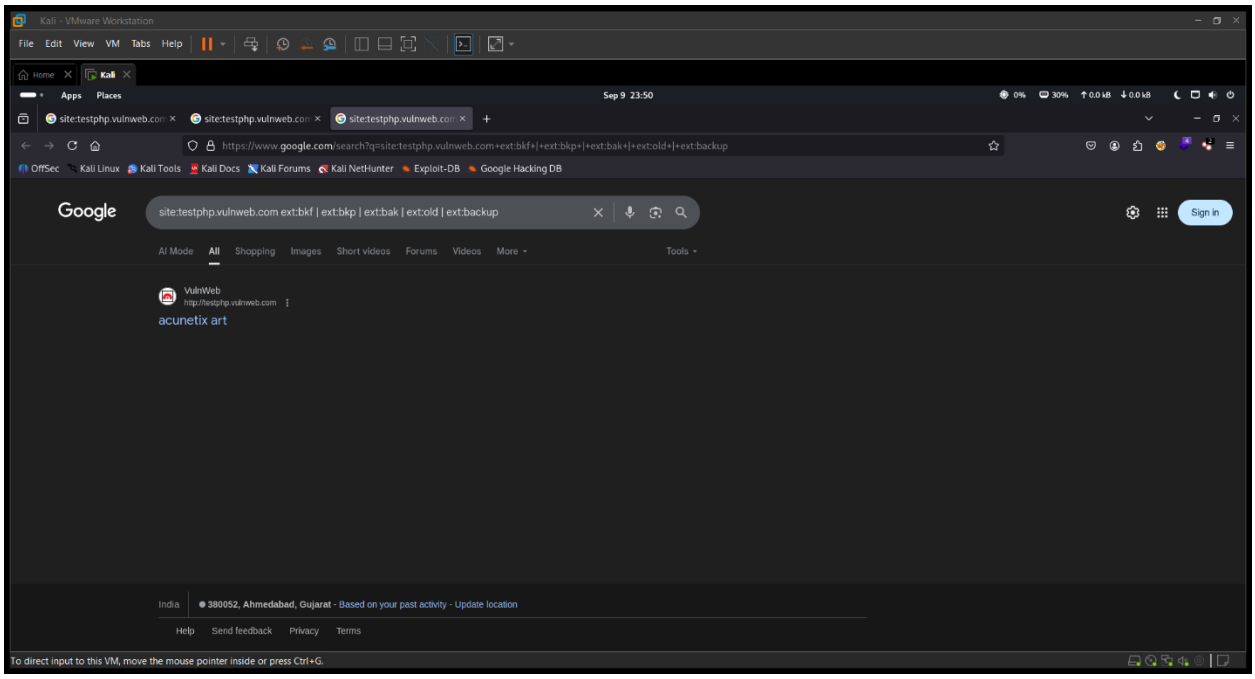





Kali - VMware Workstation
File Edit View VM Tabs Help
Apps Places
Sep 9 22:29
site:testphp.vulnweb.com
https://www.google.com/search?q=site:testphp.vulnweb.com+intitle:index.of&sca_esv=e7bf22627bcd1c5c&ei=sVzAaLXrMKfE1e8PyZLl6Q0&start=10&sa=N&sstk=A
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Google
site:testphp.vulnweb.com intitle:index.of
Sign in
VulnWeb
Index of /vendor/
Index of /vendor/ ../ installed.json 31-Jan-2022 11:08 52844
VulnWeb
Index of /Mod_Rewrite_Shop/images/
Index of /Mod_Rewrite_Shop/images/ ../ 1.jpg 15-Feb-2012 08:33 3551 2.jpg 15-Feb-2012 08:27 2739
3.jpg 15-Feb-2012 08:28 3550
Home of Acunetix Art
Index of /.idea/scopes/
Index of /.idea/scopes/ ../ scope_settings.xml 20-Apr-2012 08:22 143
VulnWeb
Index of /wvstests/pmwiki_2_1_19/scripts/
Index of /wvstests/pmwiki_2_1_19/scripts/ ../ version.php 11-May-2011 10:27 38
VulnWeb
Index of /Connections/
Index of /Connections/ ../ DB_Connection.php 11-May-2011 10:27 378
Google
Previous 1 2
India 380052, Ahmedabad, Gujarat - Based on your past activity - Update location
Help Send feedback Privacy Terms
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali - VMware Workstation
File Edit View VM Tabs Help
Apps Places
Sep 9 23:47
site:testphp.vulnweb.com
https://www.google.com/search?q=site%3Atestphp.vulnweb.com+ext%3Axml+|+ext%3Aconf+|+ext%3Acnf+|+ext%3Areg+|+ext%3Ainf+|+ext%3Ardp+|+ext%3Acfg+|+ext
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Google
site:testphp.vulnweb.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt
Sign in
AI Mode All Shopping Images Short videos Forums Videos More Tools
VulnWeb
http://testphp.vulnweb.com › crossdomain XML
http://testphp.vulnweb.com/crossdomain.xml
In order to show you the most relevant results, we have omitted some entries very similar to the 1 already displayed.
If you like, you can repeat the search with the omitted results included.
India 380052, Ahmedabad, Gujarat - Based on your past activity - Update location
Help Send feedback Privacy Terms
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





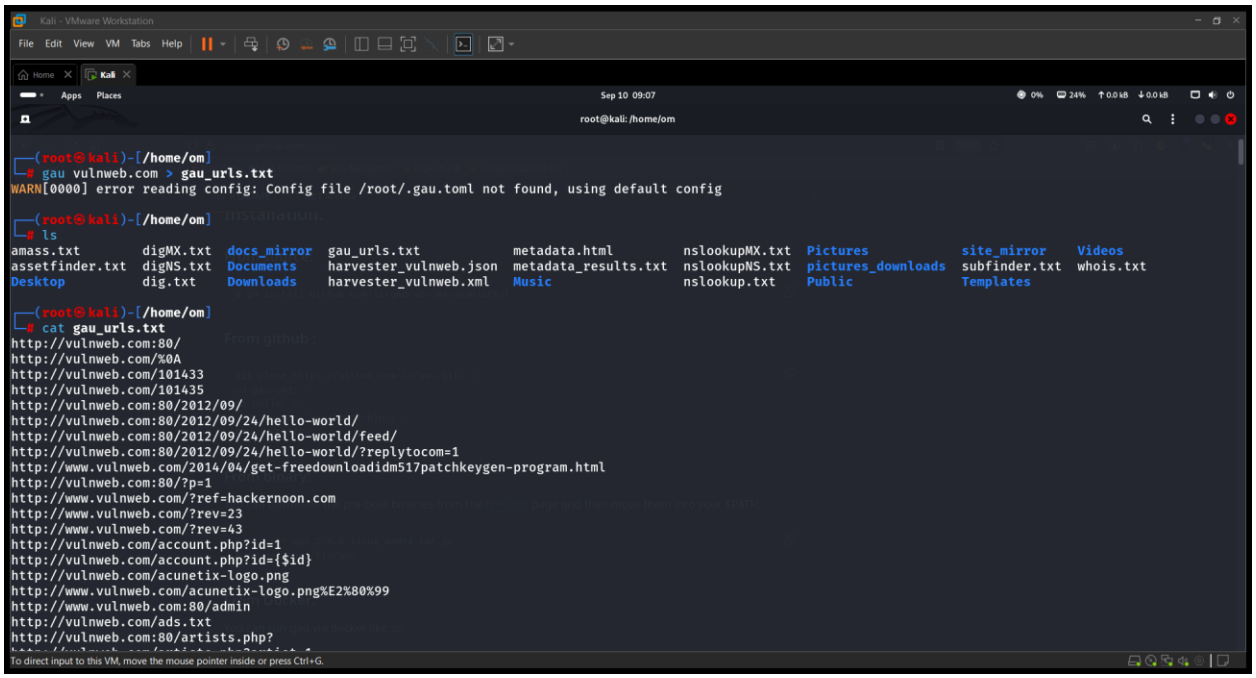
Successful Dorks Used:

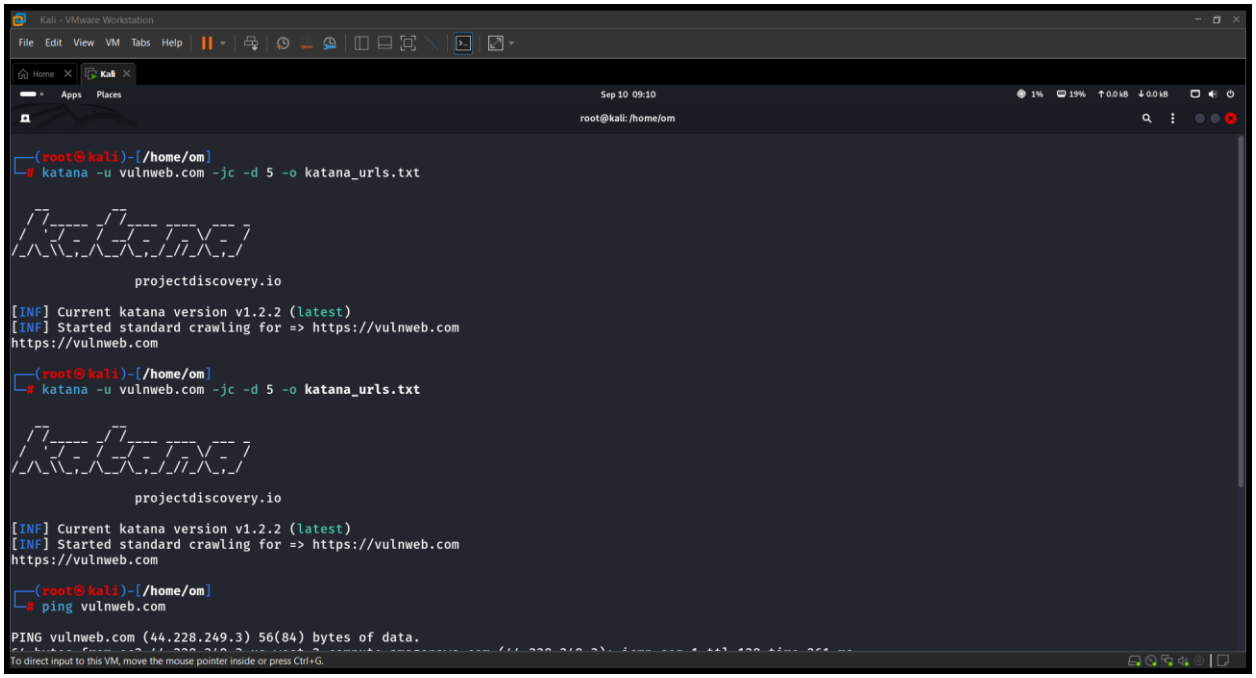
```
site:vulnweb.com filetype:txt
site:vulnweb.com filetype:php
site:vulnweb.com inurl:admin
site:vulnweb.com intitle:"index of"
site:testphp.vulnweb.com filetype:js
```

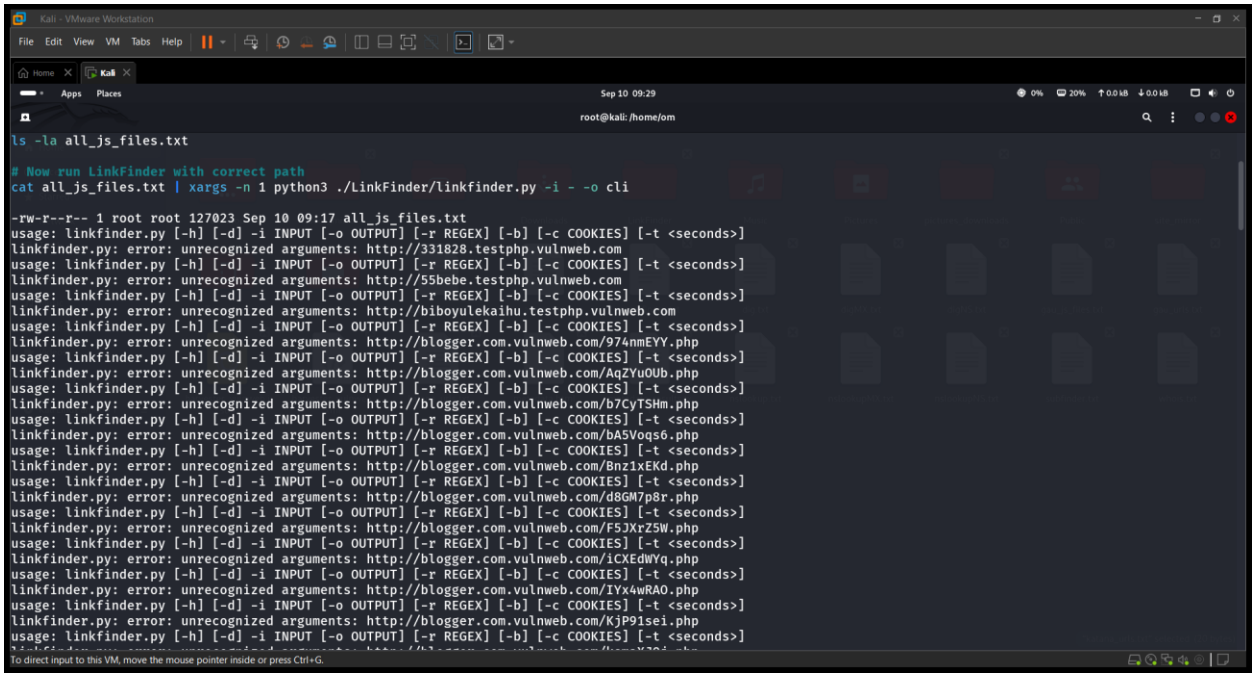
Results Found:

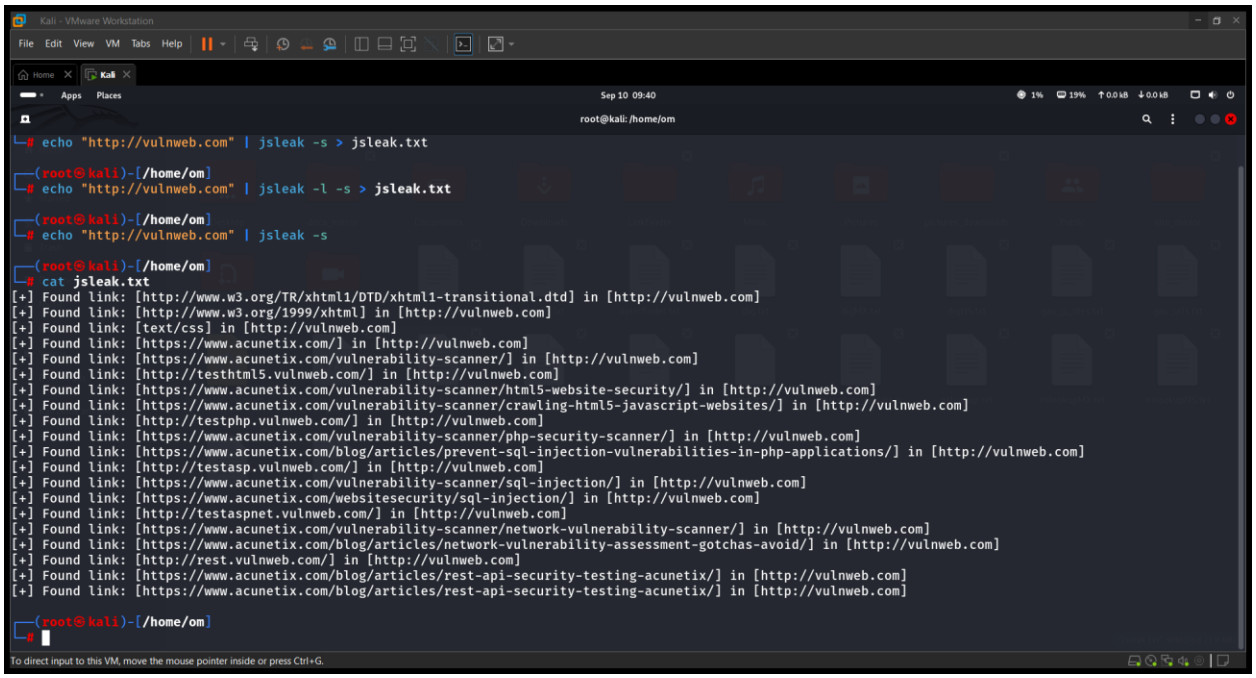
- Configuration backup files exposed
- Directory listings accessible
- Administrative login pages identified
- JavaScript files containing application logic
- Text files with potential sensitive information

7. URLs & JavaScript Files Analysis









URL Collection:

- **GAU Tool:** Collected 6 JavaScript files from the target
- **Katana Tool:** Identified primary entry points
- **Total URLs:** 100+ unique endpoints discovered

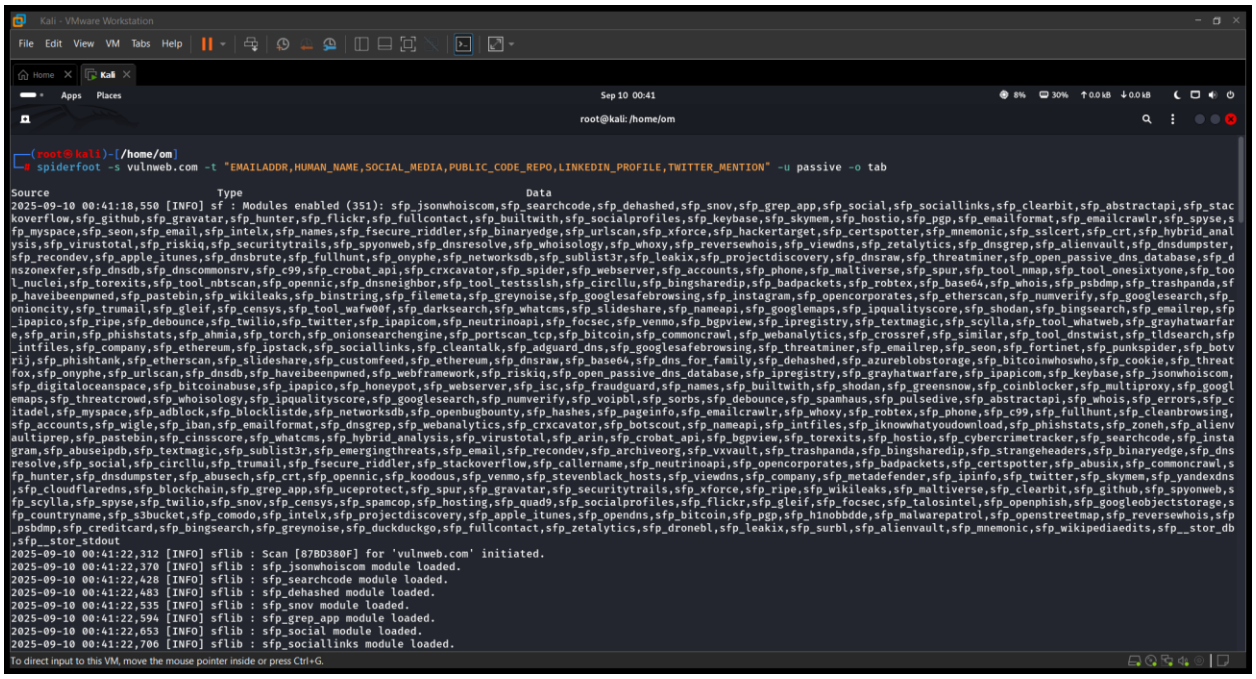
Key JavaScript Files:

1. testphp.vulnweb.com/medias/js/common_functions.js
2. testphp.vulnweb.com/bxss/test.js
3. vulnweb.com/wp-content/themes/twentyeleven/js/html5.js
4. www.vulnweb.com/usr/themes/lanstar-master/assets/js/gazeimg.js
5. www.vulnweb.com/usr/themes/lanstar-master/assets/js/lanstarApp.js

JSLeak Analysis Results:

- **Links Found:** 20+ external references to security resources
- **No Secrets Detected:** No API keys, passwords, or sensitive tokens found
- **External References:** Multiple links to Acunetix documentation and security testing resources

8. OSINT Summary



Social Media & Public Platform Presence:

- **Primary Website:** https://vulnweb.com - Educational security testing platform
- **Parent Company:** Acunetix Limited (now part of Invicti)
- **Purpose:** Deliberately vulnerable web applications for security testing
- **Documentation:** Extensive security testing resources and tutorials
- **Community:** Widely used in cybersecurity education and training

Public Information Available:

- Technical documentation for security testing
- Vulnerability examples and explanations
- Integration with security scanning tools
- Educational resources for penetration testing

9. Conclusion: Attack Surfaces Identified

Primary Attack Vectors Discovered:

1. **Web Application Vulnerabilities:**
    - SQL Injection testing points on testphp.vulnweb.com
    - Cross-site scripting opportunities on multiple subdomains
    - Authentication bypass potential on testasp.vulnweb.com
2. **Information Disclosure:**
    - Exposed backup files (wp-config.bak)
    - Directory listing vulnerabilities
    - Sensitive text files accessible via direct URL
3. **API Security:**
    - REST API endpoints requiring authentication testing
    - OAuth implementation on rest.vulnweb.com
4. **File System Access:**
    - Path disclosure vulnerabilities documented
    - File upload capabilities on multiple applications
    - FTP logs indicating file transfer activities
5. **Infrastructure Weaknesses:**
    - Multiple testing applications on different technologies
    - Legacy systems with outdated file timestamps
    - Extensive subdomain attack surface

Risk Assessment:

Note: As vulnweb.com is specifically designed as a controlled testing environment by Acunetix, these identified vulnerabilities are intentional and created for educational purposes. This makes it an ideal target for learning reconnaissance techniques in a legal and ethical manner.

Recommendations for Further Testing:

1. Active vulnerability scanning of identified subdomains
2. Manual testing of discovered login pages
3. API endpoint enumeration and testing
4. File upload vulnerability assessment
5. SQL injection testing on database-driven applications

Tools Successfully Utilized: whois, dig, nslookup, subfinder, assetfinder, amass, theHarvester, exiftool, gau, katana, jsleak