

PASSIVE RECONNAISSANCE REPORT

Assignment 2 - Cyber Security Internship

Target Domain: vulnweb.com

Date: September 9-10, 2025

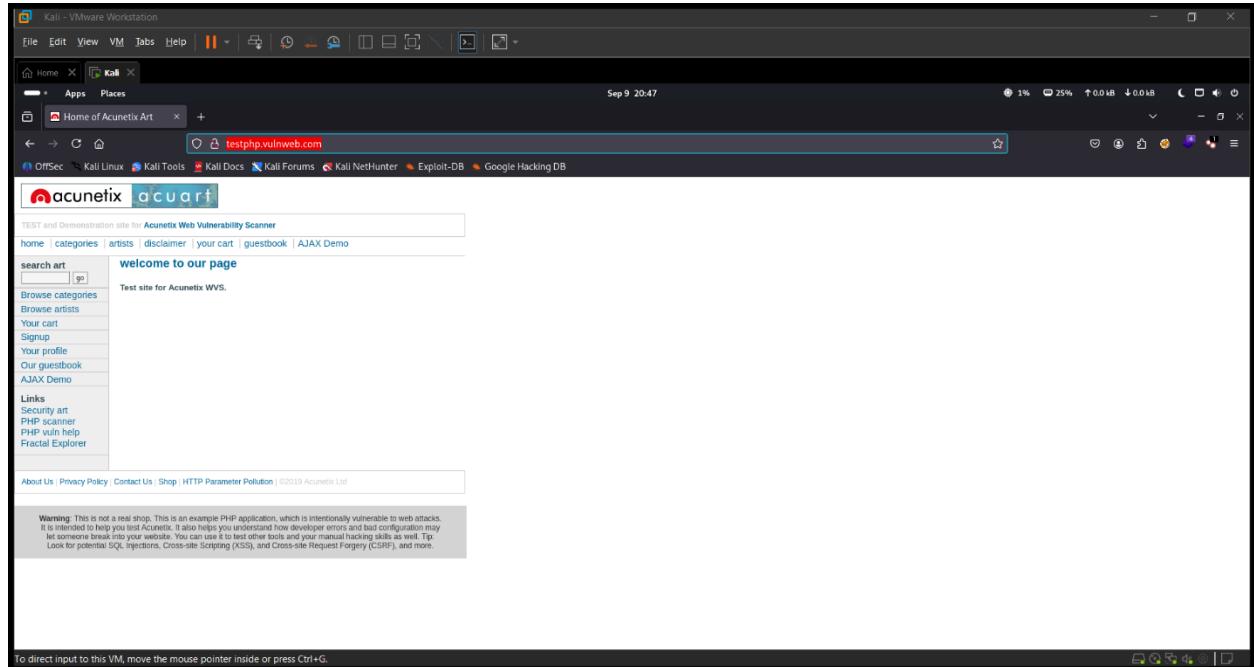
Performed By: Om Barot

Tools Used: Kali Linux

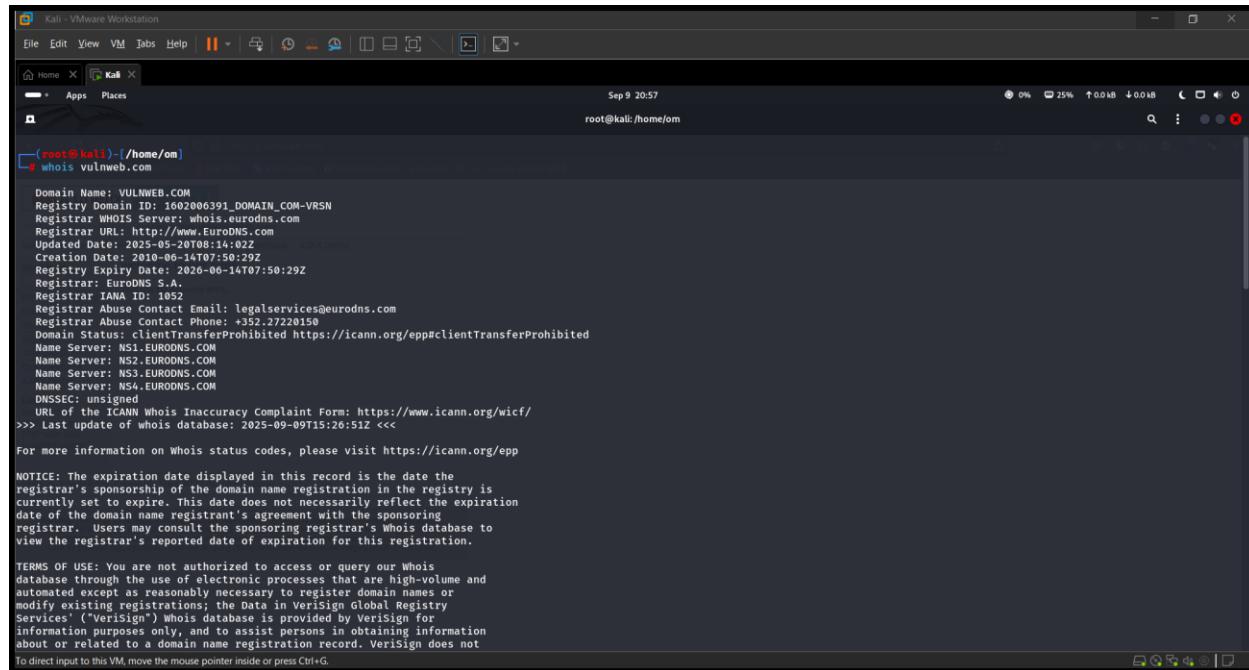
1. Target Domain Selection

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.



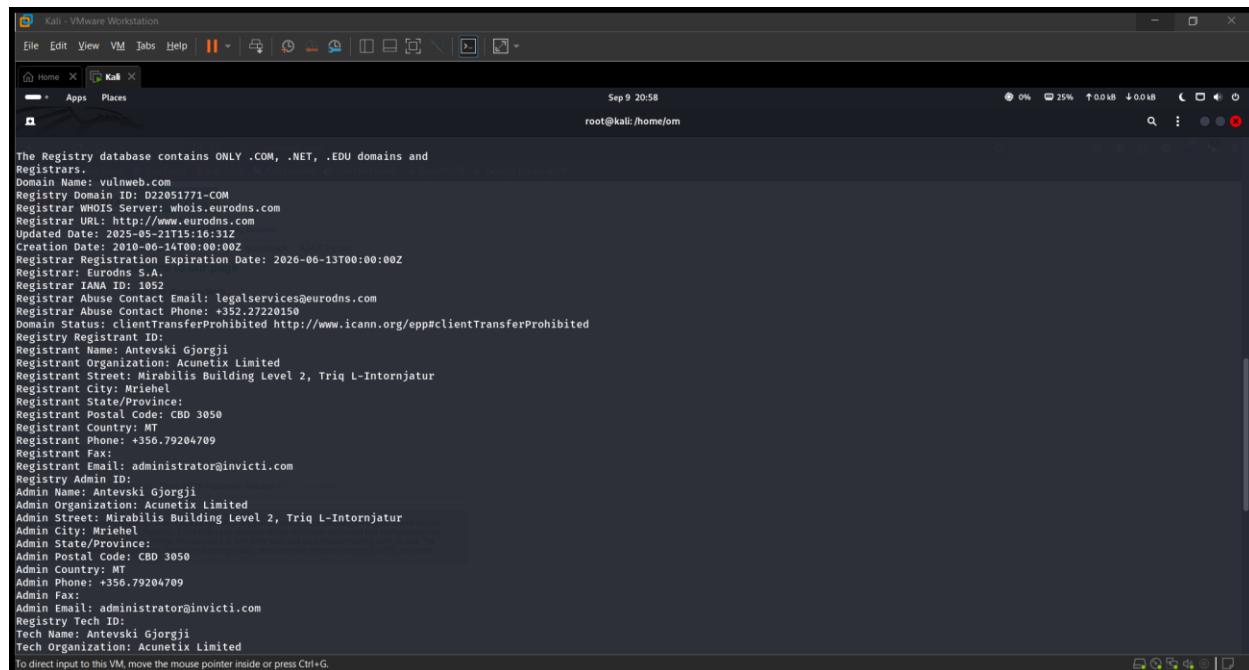
2. WHOIS & DNS Findings



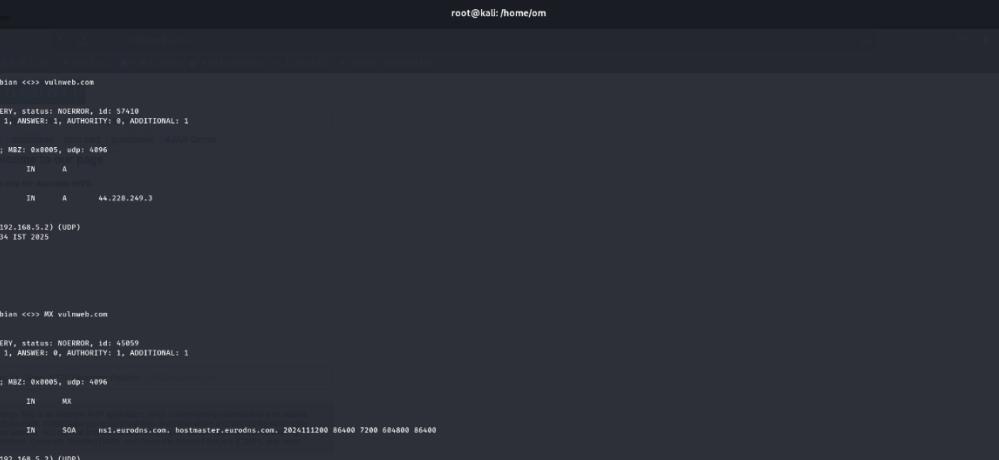
```
root@kali:[/home/om]
# whois vulnweb.com
Domain Name: VULNWEB.COM
Registry Domain ID: 1502006391_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2025-05-20T08:14:02Z
Creation Date: 2010-06-14T07:50:29Z
Registry Expiry Date: 2026-06-14T07:50:29Z
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: 2025-09-09T15:26:51Z <<
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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: vulnweb.com
Registry Domain ID: D22051771-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2025-05-21T15:16:31Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2026-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrar ID:
Registrant Name: Antevski Giorgji
Registrant Organization: Acunetix Limited
Registrant Street: Mirabilis Building Level 2, Triq L-Intornjatur
Registrant City: Mriehel
Registrant State/Province:
Registrant Postal Code: CBD 3050
Registrant Country: MT
Registrant Phone: +356.79204709
Registrant Fax:
Registrant Email: administrator@invicti.com
Registry Admin ID:
Admin Name: Antevski gjorgji
Admin Organization: Acunetix Limited
Admin Street: Mirabilis Building Level 2, Triq L-Intornjatur
Admin City: Mriehel
Admin State/Province:
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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



```
[root@kali:~]# dig vulnweb.com
; <>> DIG 9.20.11-4+deb1-Debian <>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 57418
;; 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: 192.168.5.253(192.168.5.2) (UDP)
;; WHEN: Tue Sep 09 23:00:34 IST 2025
;; MSG SIZE rcvd: 56

[root@kali:~]# dig MX vulnweb.com
; <>> DIG 9.20.11-4+deb1-Debian <>> MX vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 45059
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: MBZ: 0x0005, udp: 4096
; QUESTION SECTION: ;vulnweb.com. IN MX
;; ANSWER SECTION:
vulnweb.com. 5 IN SOA ns1.eurodns.com. hostmaster.eurodns.com. 2026111200 86400 7200 604800 86400
;; Query time: 299 msec
;; SERVER: 192.168.5.253(192.168.5.2) (UDP)
;; WHEN: Tue Sep 09 23:07:01 IST 2025
;; MSG SIZE rcvd: 99
```

```
Kali - VMware Workstation
File Edit View VM Tabs Help ||| 
Home X 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]
#
```

```
Kali - VMware Workstation
File Edit View VM Tabs Help ||| 
Home X 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]
#
```

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

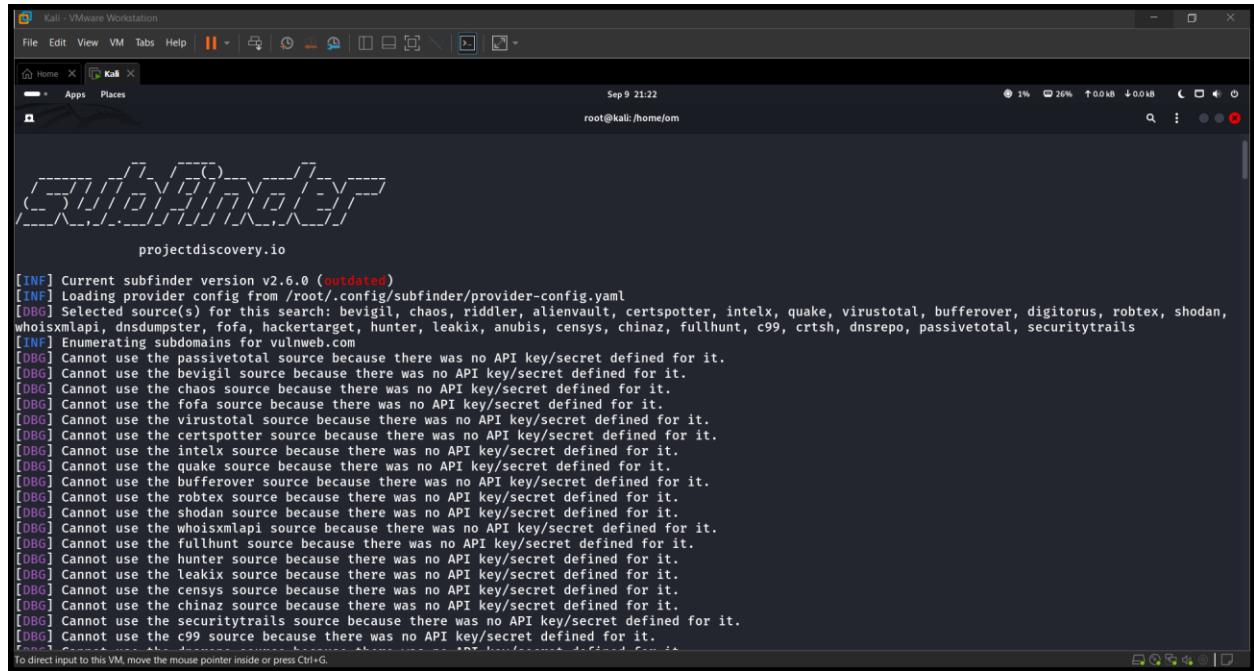
DNS enumeration using dig and nslookup revealed:

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

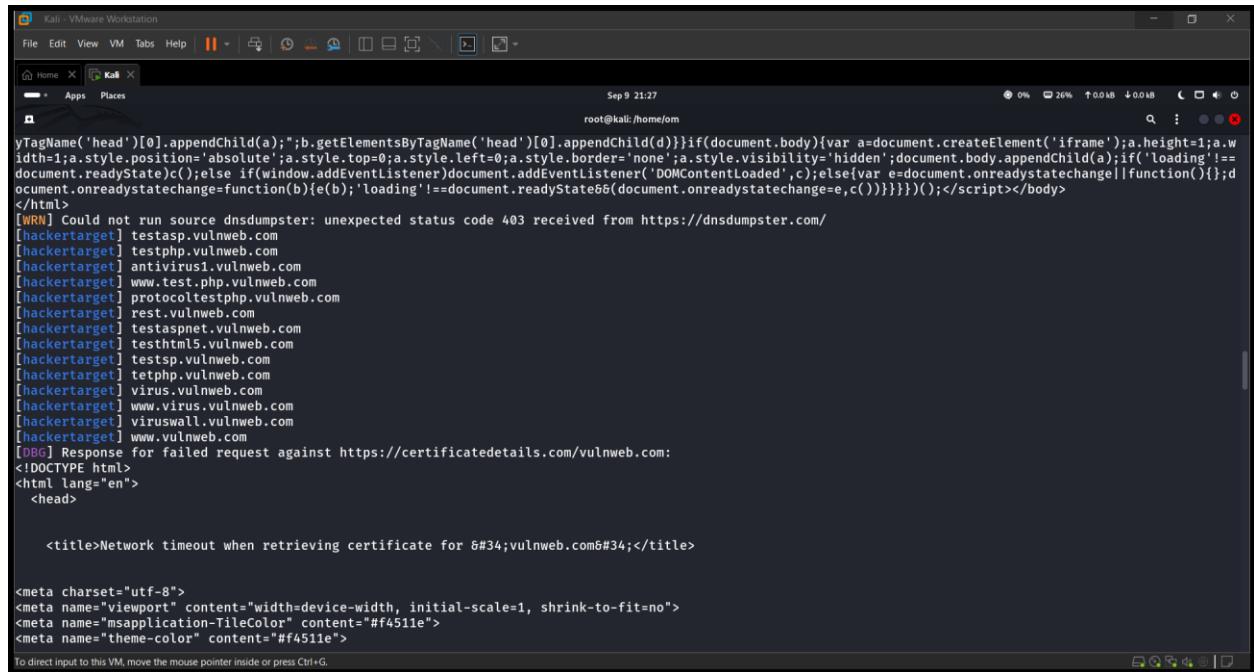
- [ns1.eurodns.com](#)
 - [ns2.eurodns.com](#)
 - [ns3.eurodns.com](#)
 - [ns4.eurodns.com](#)
- **MX Records:** No mail exchange records found
 - **Infrastructure:** Hosted on Amazon AWS (ASN 16509)

3. Subdomains Discovered

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



```
[INFO] Current subfinder version v2.6.0 (outdated)
[INFO] Loading provider config from /root/.config/subfinder/provider-config.yaml
[DBG] Selected source(s) for this search: bevigil, chaos, riddler, alienvault, certspotter, intelx, quake, virustotal, bufferover, digitorus, robtex, shodan, whoisxmlapi, dnsdumpster, fofa, hackertarget, hunter, leakix, anubis, censys, chinaz, fullhunt, c99, crtsh, dnsrepo, passivetotal, securitytrails
[INF] Enumerating subdomains for vulnweb.com
[DBG] Cannot use the passivetotal source because there was no API key/secret defined for it.
[DBG] Cannot use the bevigil source because there was no API key/secret defined for it.
[DBG] Cannot use the chaos source because there was no API key/secret defined for it.
[DBG] Cannot use the fofa source because there was no API key/secret defined for it.
[DBG] Cannot use the virustotal source because there was no API key/secret defined for it.
[DBG] Cannot use the certspotter source because there was no API key/secret defined for it.
[DBG] Cannot use the intelx source because there was no API key/secret defined for it.
[DBG] Cannot use the quake source because there was no API key/secret defined for it.
[DBG] Cannot use the bufferover source because there was no API key/secret defined for it.
[DBG] Cannot use the robtex source because there was no API key/secret defined for it.
[DBG] Cannot use the shodan source because there was no API key/secret defined for it.
[DBG] Cannot use the whoisxmlapi source because there was no API key/secret defined for it.
[DBG] Cannot use the fullhunt source because there was no API key/secret defined for it.
[DBG] Cannot use the hunter source because there was no API key/secret defined for it.
[DBG] Cannot use the leakix source because there was no API key/secret defined for it.
[DBG] Cannot use the censys source because there was no API key/secret defined for it.
[DBG] Cannot use the chinaz source because there was no API key/secret defined for it.
[DBG] Cannot use the securitytrails source because there was no API key/secret defined for it.
[DBG] Cannot use the c99 source because there was no API key/secret defined for it.
```

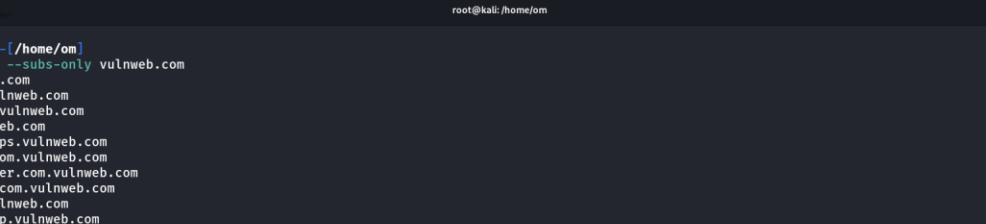


```
yTagName('head')[0].appendChild(a);";b.getElementsByTagName('head')[0].appendChild(d)}if(document.body){var a=document.createElement('iframe');a.height=1;a.width=1;a.style.position='absolute';a.style.top=0;a.style.left=0;a.style.border='none';a.style.visibility='hidden';document.body.appendChild(a);if('loading'!=document.readyState){}else if(window.addEventListener){document.addEventListener('DOMContentLoaded',c);else{var e=document.onreadystatechange||function(){}};document.onreadystatechange=function(b){e(b);'loading'!=document.readyState&&(document.onreadystatechange=e,c())}}})());</script></body>
</html>
[WRN] Could not run source dnsdumpster: unexpected status code 403 received from https://dnsdumpster.com/
[hackertarget] testasp.vulnweb.com
[hackertarget] testphp.vulnweb.com
[hackertarget] antivirus1.vulnweb.com
[hackertarget] www.test.php.vulnweb.com
[hackertarget] protocoltestphp.vulnweb.com
[hackertarget] rest.vulnweb.com
[hackertarget] testaspnet.vulnweb.com
[hackertarget] testhtml5.vulnweb.com
[hackertarget] testsp.vulnweb.com
[hackertarget] tetphp.vulnweb.com
[hackertarget] virus.vulnweb.com
[hackertarget] www.virus.vulnweb.com
[hackertarget] viruswall.vulnweb.com
[hackertarget] www.vulnweb.com
[DBG] Response for failed request against https://certificatedetails.com/vulnweb.com:
<!DOCTYPE html>
<html lang="en">
  <head>
```

<title>Network timeout when retrieving certificate for "vulnweb.com";</title>

```
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<meta name="msapplication-TileColor" content="#f4511e">
<meta name="theme-color" content="#f4511e">
```

```
[Kali - VMware Workstation] File Edit View VM Tabs Help || Home X 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.
```



```
(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.blogspot.com.vulnweb.com
promotion.blogspot.com.vulnweb.com
origin.blogspot.com.vulnweb.com
testasp.blog.vulnweb.com
partner.test.php.vulnweb.com
si.test.vulnweb.com
acc.testsp.vulnweb.com
blogger2.com.vulnweb.com
wwwwp.test.php.vulnweb.com
httpstestaspnet.service.vulnweb.com
testvpn.php.vulnweb.com
test.monitor.vulnweb.com
cms1.blogspot.com.vulnweb.com
virus.vpn.vulnweb.com
httpstestaspnet.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.antivirusi.vulnweb.com
proxy.protocoltestphp.vulnweb.com
www.monitor.vulnweb.com
blogger.docs.com.vulnweb.com
v2.www.test.php.vulnweb.com
```

```

Kali - VMware Workstation
File Edit View VM Tabs Help || Home Apps Places Sep 9 21:52 root@kali:/home/om
# amass enum -passive -d vulnweb.com -o amass.txt
vulnweb.com (FQDN) --> ns_record --> ns2.eurodns.com (FQDN)
vulnweb.com (FQDN) --> ns_record --> ns1.eurodns.com (FQDN)
vulnweb.com (FQDN) --> ns_record --> ns4.eurodns.com (FQDN)
vulnweb.com (FQDN) --> ns_record --> ns3.eurodns.com (FQDN)
testaspnet.vulnweb.com (FQDN) --> a_record --> 44.238.29.244 (IPAddress)
44.224.0.0/16 (Netblock) --> contains --> 44.238.29.244 (IPAddress)
16509 (ASN) --> managed_by --> AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) --> announces --> 44.224.0.0/11 (Netblock)
ns3.eurodns.com (FQDN) --> a_record --> 199.167.66.108 (IPAddress)
ns3.eurodns.com (FQDN) --> aaaa_record --> 2610:1c8:b002::108 (IPAddress)
199.167.64.0/22 (Netblock) --> contains --> 199.167.66.108 (IPAddress)
23393 (ASN) --> managed_by --> NUCDN (RIROrganization)
23393 (ASN) --> announces --> 199.167.64.0/22 (Netblock)
2610:1c8:b002::/48 (Netblock) --> contains --> 2610:1c8:b002::108 (IPAddress)
23393 (ASN) --> managed_by --> NUCDN, US (RIROrganization)
23393 (ASN) --> announces --> 2610:1c8:b002::/48 (Netblock)
ns4.eurodns.com (FQDN) --> a_record --> 104.37.178.108 (IPAddress)
ns4.eurodns.com (FQDN) --> aaaa_record --> 2610:1c8:b001::108 (IPAddress)
testasp.vulnweb.com (FQDN) --> a_record --> 44.238.29.244 (IPAddress)
104.37.176.0/21 (Netblock) --> contains --> 104.37.178.108 (IPAddress)
23393 (ASN) --> announces --> 104.37.176.0/21 (Netblock)
2610:1c8:b001::/48 (Netblock) --> contains --> 2610:1c8:b001::108 (IPAddress)
23393 (ASN) --> announces --> 2610:1c8:b001::/48 (Netblock)

The enumeration has finished

```

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:

```
Kali - VMware Workstation
File Edit View VM Tabs Help ||| 
Sep 9 22:03
root@kali:/home/om

[root@kali ~]# theHarvester -d vulnweb.com -b bing,duckduckgo,crtsh,dnsdumpster,otx -f harvester_vulnweb.html
Read proxies.yaml from /etc/theHarvesterproxies.yaml
*****
* [!] Target: vulnweb.com
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
[!] Missing API key for DNSDumpster.
[*] Searching DuckDuckGo.
    Searching 0 results.
[*] Searching Bing.
[*] Searching CRTSh.
[*] Searching OTX.

[*] IPs Found: 10
-----
176.28.50.165
18.192.172.30
3.126.110.1
35.81.188.86
44.228.249.3
44.238.29.244
5.175.17.140
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
Kali - VMware Workstation
File Edit View VM Tabs Help ||| 
Sep 9 22:03
root@kali:/home/om

176.28.50.165
18.192.172.30
3.126.110.1
35.81.188.86
44.228.249.3
44.238.29.244
5.175.17.140
87.230.29.167
87.230.87.158
89.39.182.167

[*] No emails found.
[*] No people found.

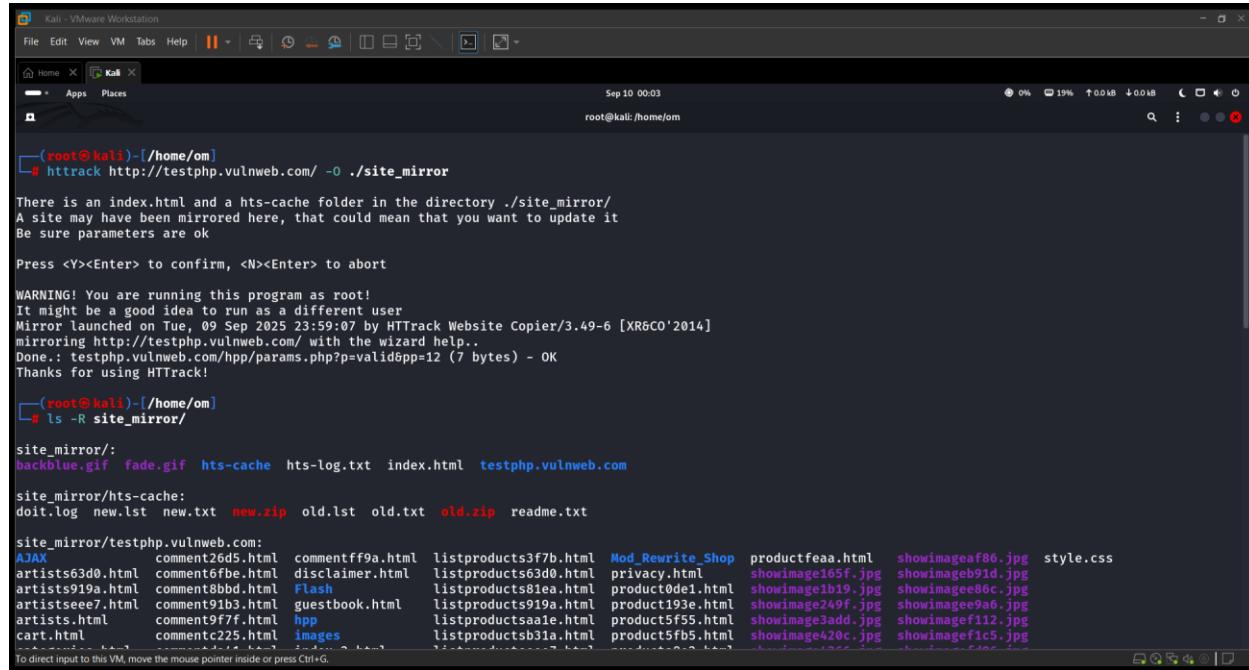
[*] Hosts found: 17
-----
blogger.com.vulnweb.com
httpstestaspnet.vulnweb.com
rest.vulnweb.com
restasp.vulnweb.com
restweb.vulnweb.com
sieb-webtestphp.vulnweb.com
testphp.vulnweb.com
testhttp.vulnweb.com
test.vulnweb.com
testap.vulnweb.com
testaps.vulnweb.com
testaspsnet.vulnweb.com
testasp.vulnweb.com
testaspsnet.vulnweb.com
testaspv.vulnweb.com
testhtml5.vulnweb.com
testphp.vulnweb.com
ttestphp.vulnweb.com

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

- **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



```
(root@kali)-[~/home/om]
# htrtrack http://testphp.vulnweb.com/ -o ./site_mirror

There is an index.html and a hts-cache folder in the directory ./site_mirror/
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 09 Sep 2025 23:59:07 by HTTrack Website Copier/3.49-6 [XR&CO'2014]
mirroring http://testphp.vulnweb.com/ with the wizard help...
Done.: testphp.vulnweb.com/hpp/params.php?p=valid&pp=12 (7 bytes) - OK
Thanks for using HTTrack!

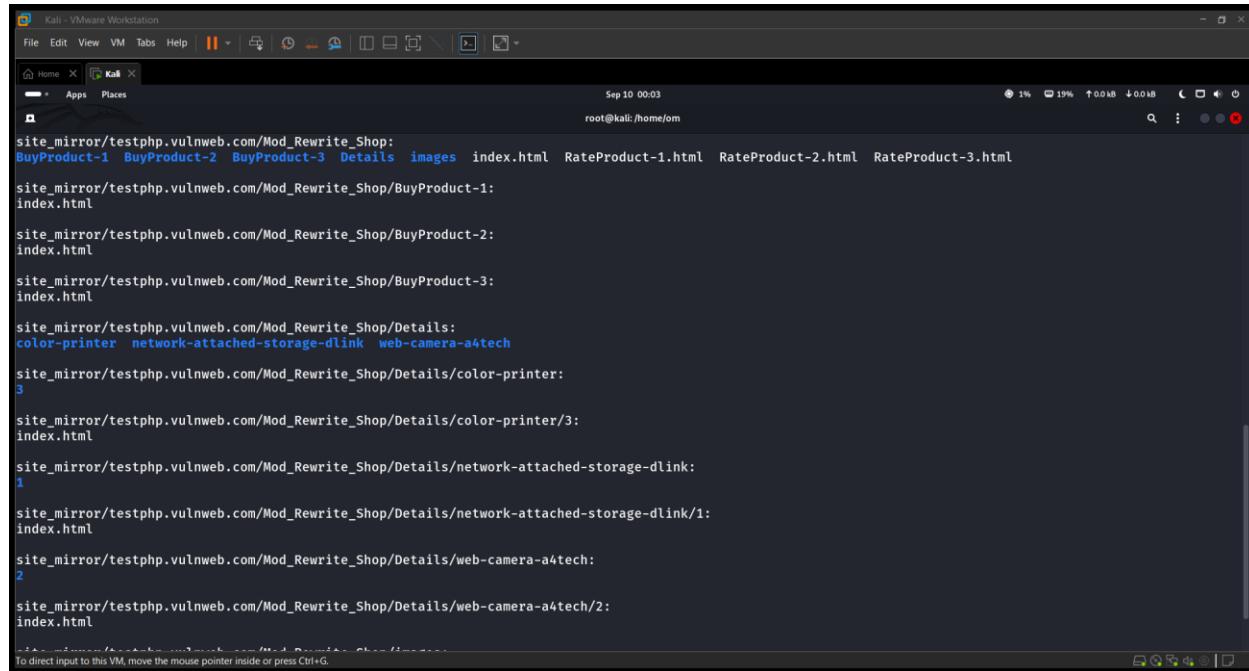
[root@kali)-[~/home/om]
# ls -R site_mirror/

site_mirror/:
backblue.gif fade.gif hts-cache hts-log.txt index.html testphp.vulnweb.com

site_mirror/hts-cache:
doit.log new.lst new.txt new.zip old.lst old.txt old.zip readme.txt

site_mirror/testphp.vulnweb.com:
AJAX comment26d5.html commentff9a.html listproducts3f7b.html Mod_Rewrite_Shop productfeaa.html showimageaf86.jpg style.css
artists63d0.html comment6fbe.html disclaimer.html listproducts63d0.html privacy.html showimageb91d.jpg
artists919a.html comment8bbd.html Flash listproducts81ea.html product0de1.html showimageb1b9.jpg showimagee80c.jpg
artistssee7.html comment91b3.html guestbook.html listproducts919a.html product193e.html showimage249f.jpg showimagee9a6.jpg
artists.html comment9f7f.html hpp listproductsaae.html product5f55.html showimage3add.jpg showimageef112.jpg
cart.html commentc225.html images listproductsb31a.html product5fb5.html showimage420c.jpg showimagefic5.jpg

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



```
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop:
BuyProduct-1 BuyProduct-2 BuyProduct-3 Details images index.html RateProduct-1.html RateProduct-2.html RateProduct-3.html

site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1:
index.html

site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2:
index.html

site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3:
index.html

site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details:
color-printer network-attached-storage-dlink web-camera-a4tech
site_mirror/testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer:
3

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

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 Apps Places Sep 10 00:07
root@kali:/home/om

[root@kali ~]# 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.
HTTP request sent, awaiting response... 200 OK
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
(root@kali)-[~/home/om]
# exiftool pictures_downloads/*.jpg

===== pictures_downloads/1.jpg
ExifTool Version Number : 13.25
File Name : 1.jpg
Directory : pictures_downloads
File Size : 12 kB
File Modification Date/Time : 2011:05:11 15:57:45+05:30
File Access Date/Time : 2025:09:10 00:07:38+05:30
File Inode Change Date/Time : 2025:09:10 00:07:38+05:30
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Image Width : 320
Image Height : 200
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 320x200
Megapixels : 0.064
===== pictures_downloads/2.jpg
ExifTool Version Number : 13.25
File Name : 2.jpg
Directory : pictures_downloads
File Size : 3.3 kB
File Modification Date/Time : 2011:05:11 15:57:45+05:30
File Access Date/Time : 2025:09:10 00:07:38+05:30
File Inode Change Date/Time : 2025:09:10 00:07:38+05:30
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Image Width : 320
Image Height : 200
Encoding Process : Progressive DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 320x200
Megapixels : 0.064
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
(root@kali)-[~/home/om]
# strings pictures_downloads/*.txt
strings pictures_downloads/*.bak

username=test
password=something
sasasasas 192.168.0.26 asasas
asasas
<php
/* MySQL settings */
define('DB_NAME', 'wp265as'); // The name of the database
define('DB_USER', 'root'); // Your MySQL username
define('DB_PASSWORD', ''); // ...and password
define('DB_HOST', 'localhost'); // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
// Change each KEY to a different unique phrase. You won't have to remember the phrases later,
// so make them long and complicated. You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up. Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
// You can have multiple installations in one database if you give each a unique prefix
$table_prefix = 'wp_'; // Only numbers, letters, and underscores please!
// Change this to localize WordPress. A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define('WPLANG', '');
/* That's all, stop editing! Happy blogging. */
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');

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

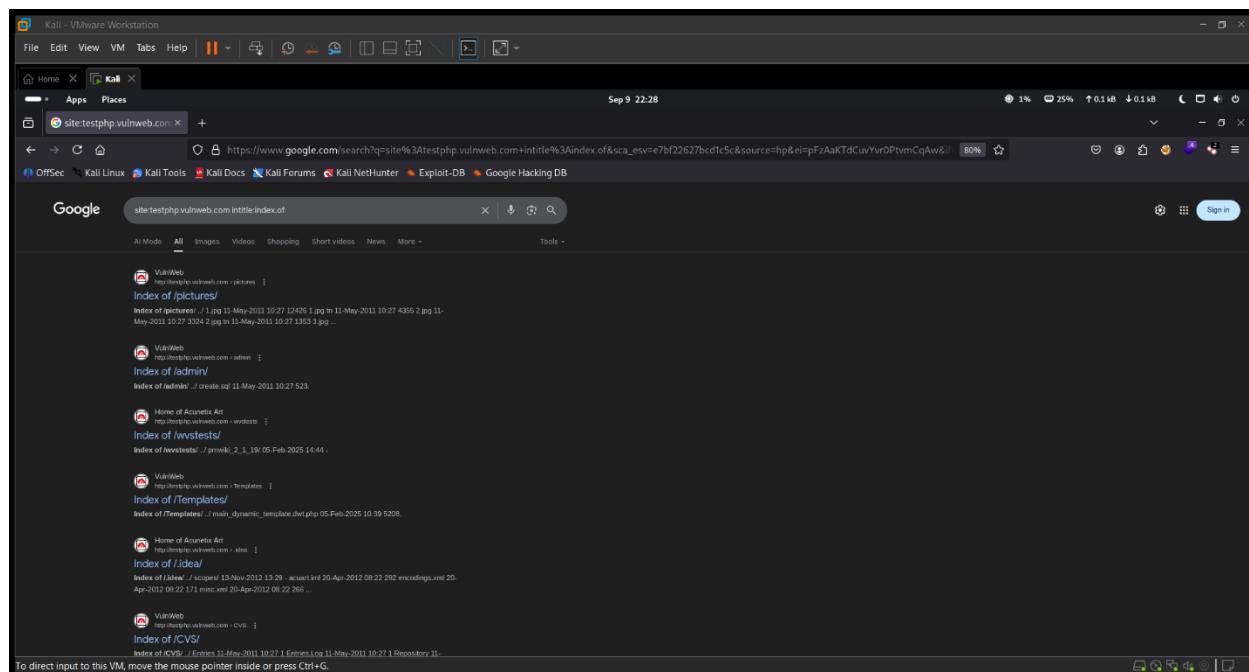
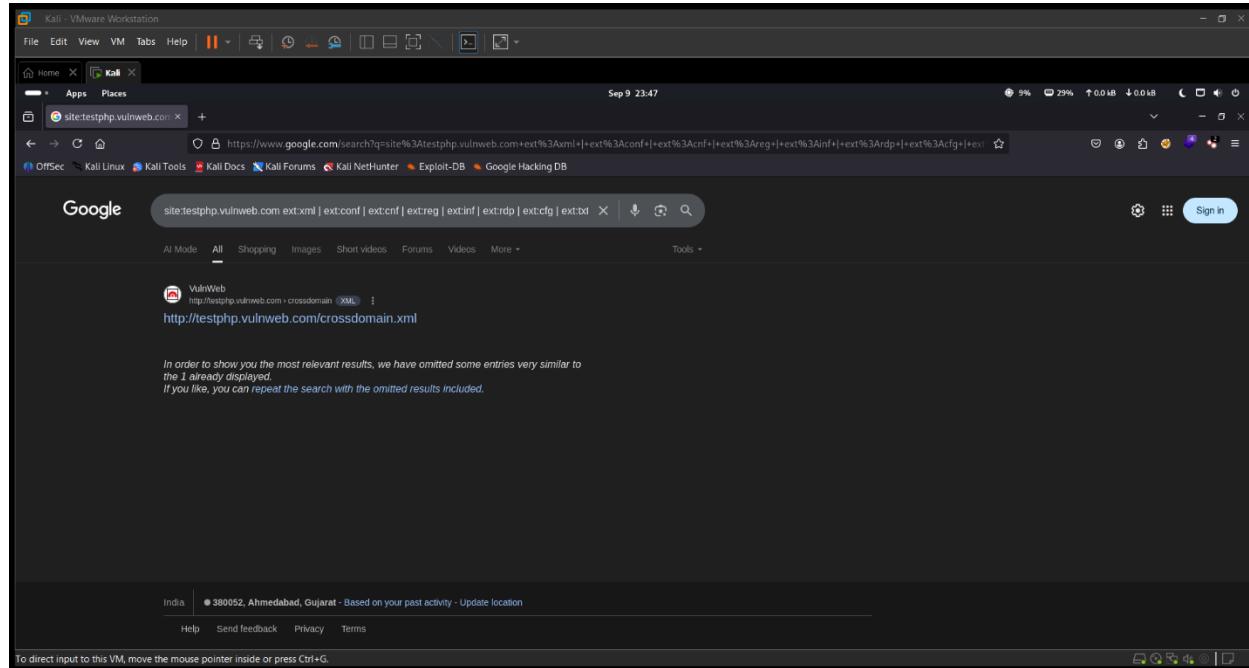
Sensitive Files Discovered:

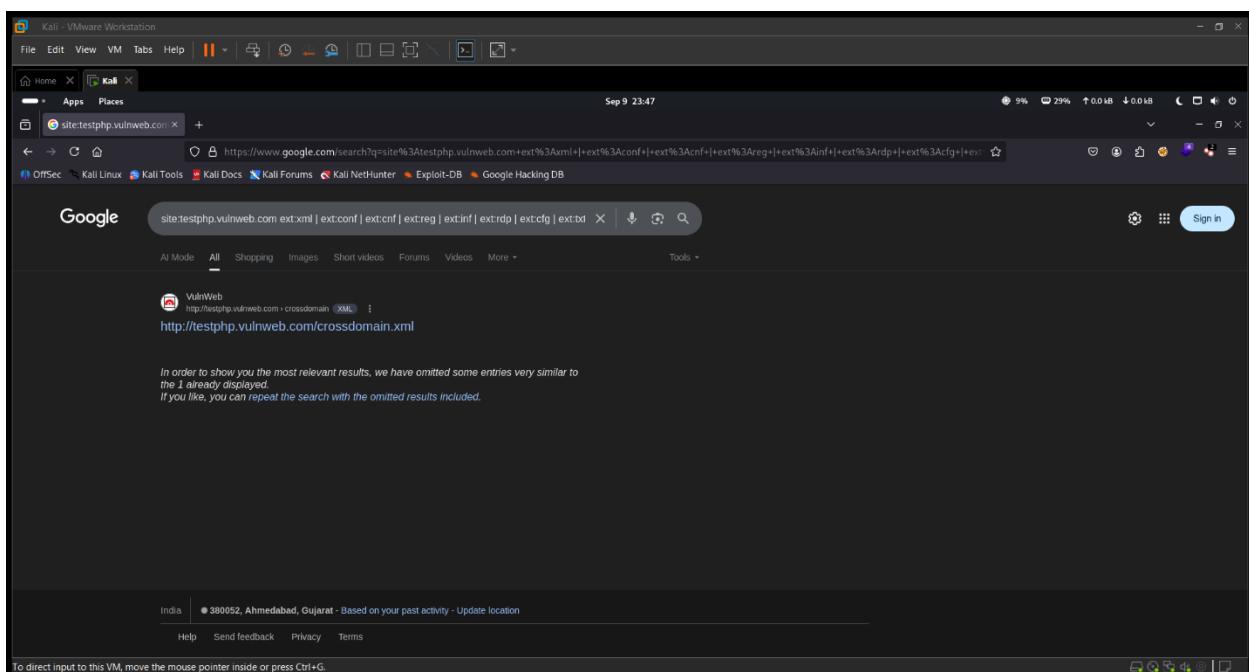
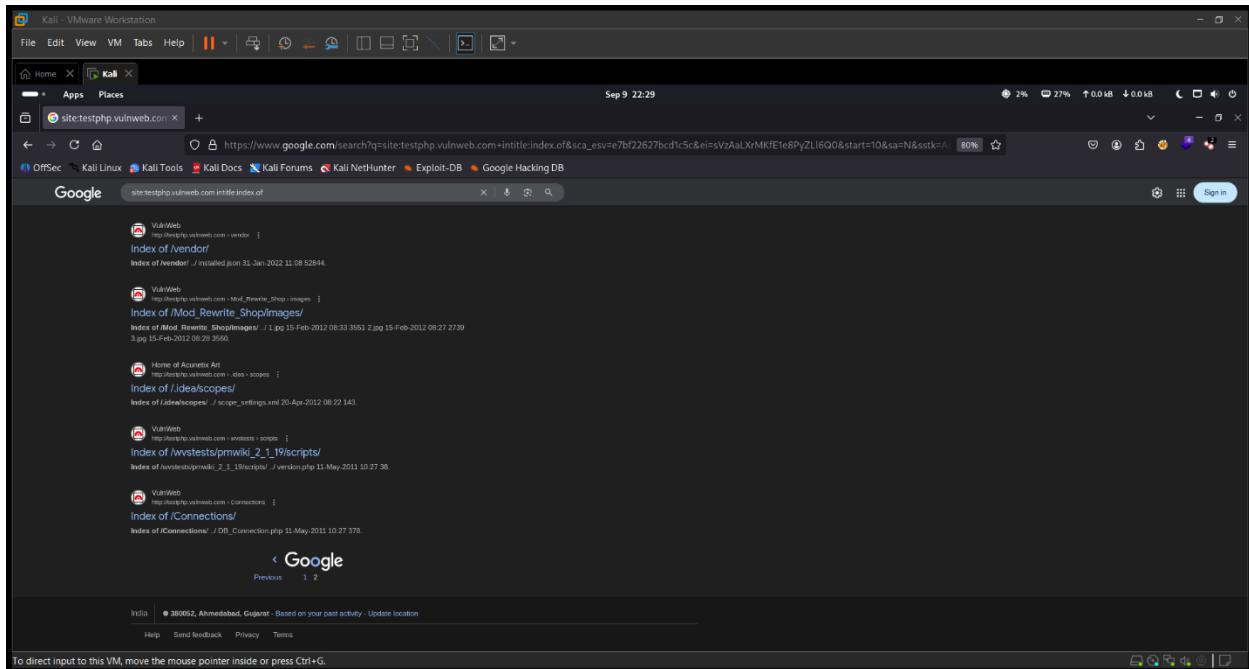
- **credentials.txt** - 33 bytes, potential credential storage
- **wp-config.bak** - WordPress configuration backup (1,535 bytes)
- **ipaddresses.txt** - IP address listing (52 bytes)
- **WS_FTP.LOG** - FTP transfer logs (771 bytes)
- **path-disclosure-unix.html** - System path disclosure examples
-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

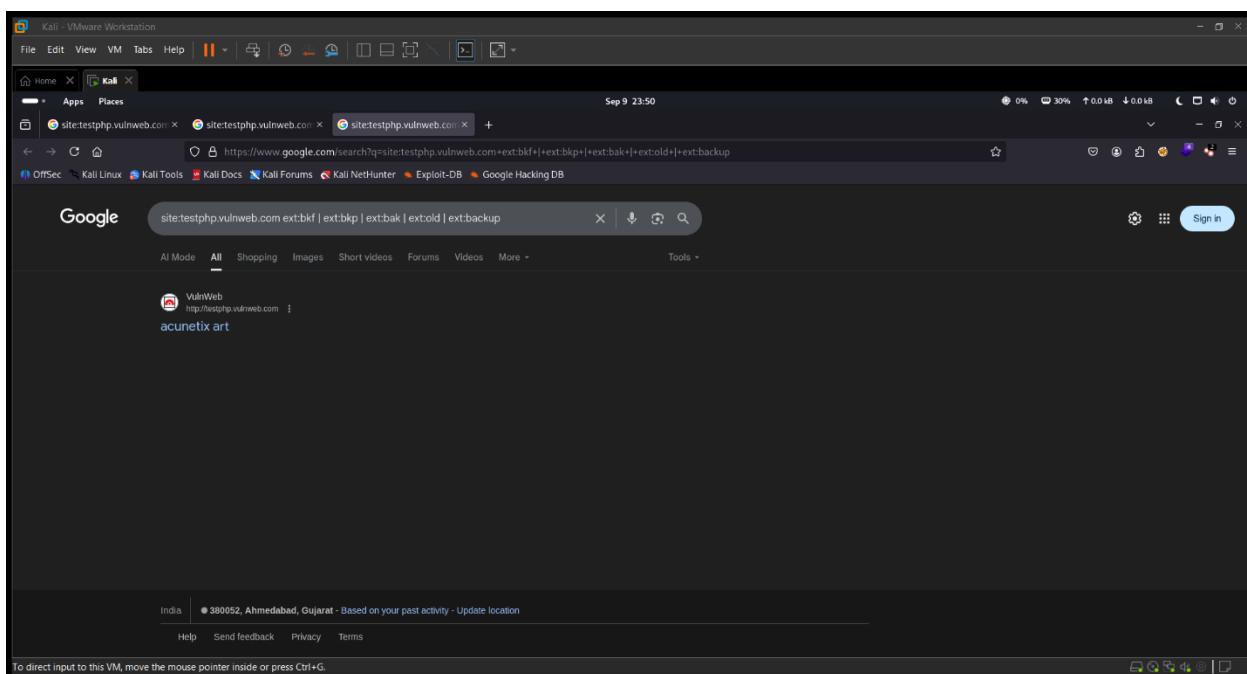
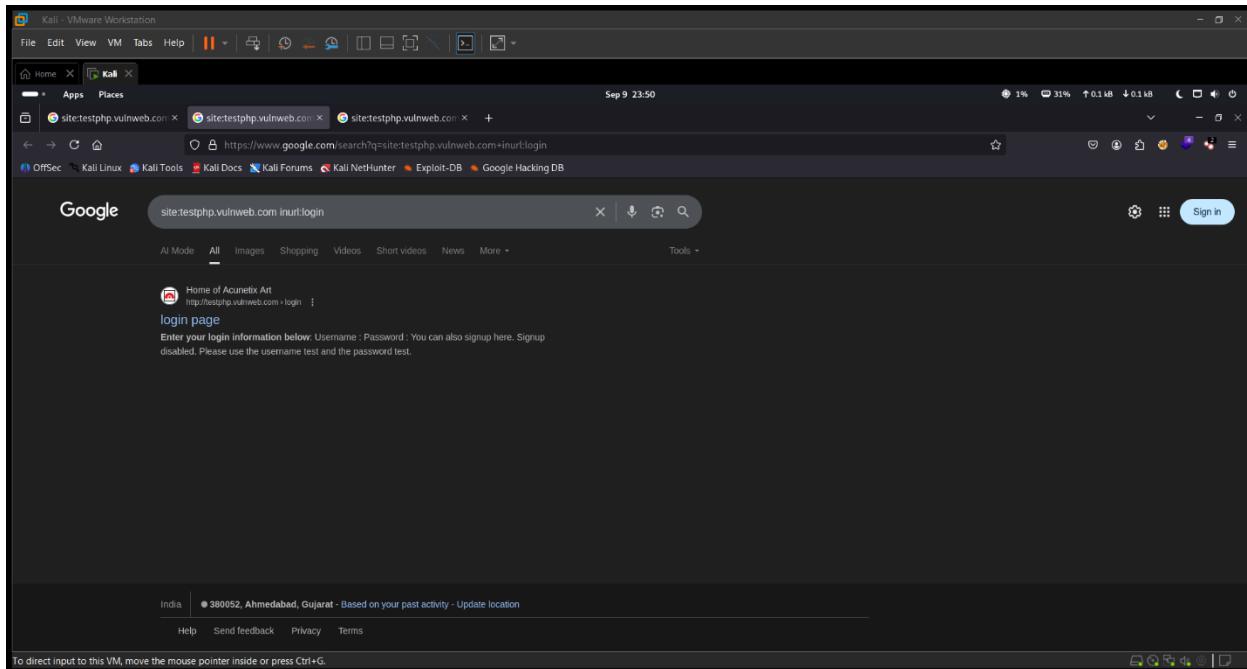
Key Metadata Findings:

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

6. Google Dorks Attempted







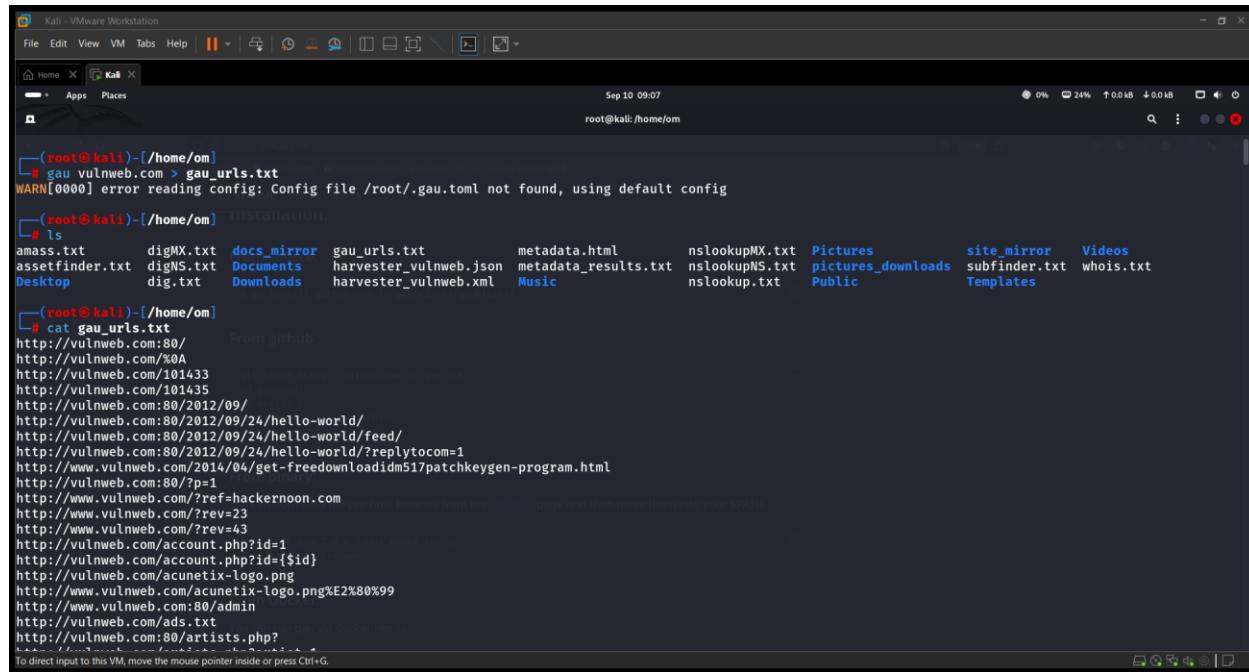
Successful Dorks Used:

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

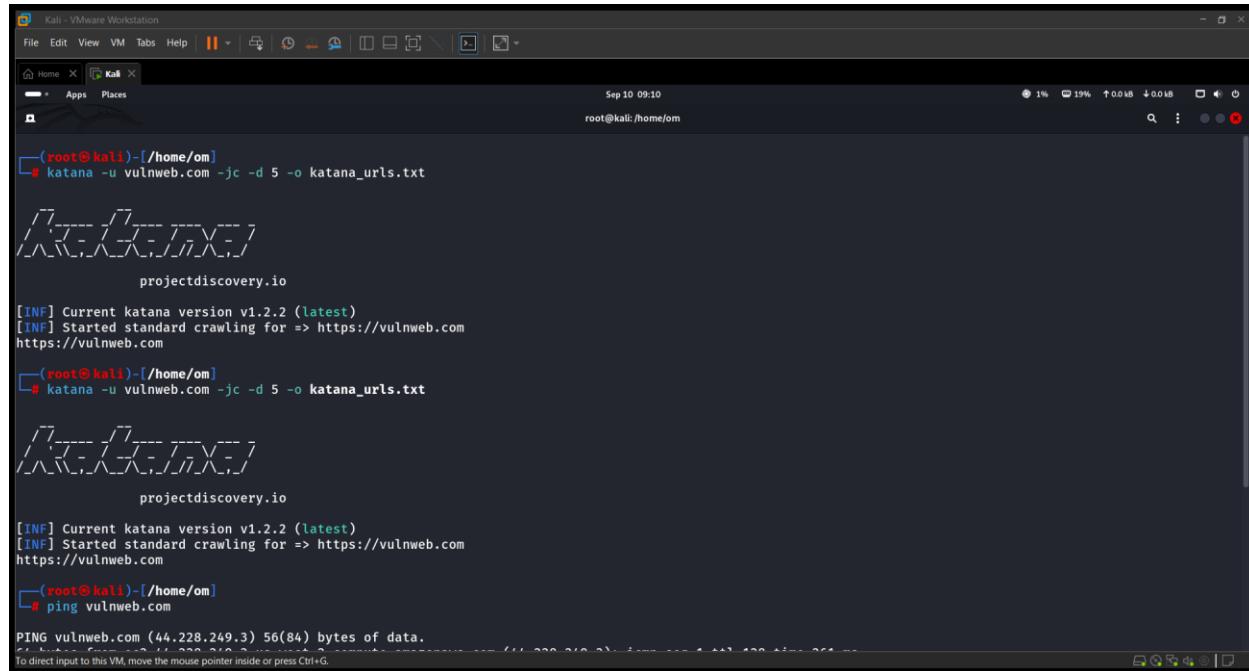
Results Found:

- 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



```
(root㉿kali)-[~/home/om]
# gau vulnweb.com > gau_urls.txt
WARN[0000] error reading config: Config file /root/.gau.toml not found, using default config
(root㉿kali)-[~/home/om] 
# ls
amass.txt      digMX.txt  docs_mirror  gau_urls.txt      metadata.html      nslookupMX.txt  Pictures      site_mirror  Videos
assetfinder.txt  digNS.txt  Documents    harvester_vulnweb.json  metadata_results.txt  nslookupNS.txt  pictures_downloads  subfinder.txt  whois.txt
Desktop          dig.txt   Downloads    harvester_vulnweb.xml   Music           nslookup.txt   Public        Templates
# cat gau_urls.txt
From github:
http://vulnweb.com:80/
http://vulnweb.com/%0A
http://vulnweb.com/101433
http://vulnweb.com/101435
http://vulnweb.com:80/2012/09/
http://vulnweb.com:80/2012/09/24/hello-world/
http://vulnweb.com:80/2012/09/24/hello-world/feed/
http://vulnweb.com:80/2012/09/24/hello-world/?replaytocom=1
http://www.vulnweb.com/2014/04/get-freeownloadidm517patchkeygen-program.html
http://vulnweb.com:80/?p=1
http://www.vulnweb.com/?ref=hackernoon.com
http://www.vulnweb.com/?rev=23
http://www.vulnweb.com/?rev=43
http://vulnweb.com/account.php?id=1
http://vulnweb.com/account.php?id={$id}
http://vulnweb.com/acunetix-logo.png
http://www.vulnweb.com:80%admin
http://vulnweb.com/ads.txt
http://vulnweb.com:80/artists.php?
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



```
(root㉿kali)-[~/home/om]
# katana -u vulnweb.com -jc -d 5 -o katana_urls.txt

projectdiscovery.io

[INF] Current katana version v1.2.2 (latest)
[INF] Started standard crawling for => https://vulnweb.com
https://vulnweb.com

(projectdiscovery.io)

[INF] Current katana version v1.2.2 (latest)
[INF] Started standard crawling for => https://vulnweb.com
https://vulnweb.com

(root㉿kali)-[~/home/om]
# ping vulnweb.com
PING vulnweb.com (44.228.249.3) 56(84) bytes of data.
```

```

ls -la all_js_files.txt
# Now run LinkFinder with correct path
cat all_js_files.txt | xargs -n 1 python3 ./LinkFinder/linkfinder.py -i --o cli

-rw-r--r-- 1 root root 127023 Sep 10 09:17 all_js_files.txt
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://331828.testphp.vulnweb.com
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://55bebe.testphp.vulnweb.com
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://biboyulekaizhu.testphp.vulnweb.com
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/974nnEYY.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/Aq2Yu0Ub.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/B7cySHm.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/BASV0qs6.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/Bnz1EkD.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/d8GM7p8r.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/F53XrZ5W.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/iCXEdWtq.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/IYx4wRAO.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]
linkfinder.py: error: unrecognized arguments: http://blogger.com.vulnweb.com/KjP91sei.php
usage: linkfinder.py [-h] [-d] -i INPUT [-o OUTPUT] [-r REGEX] [-b] [-c COOKIES] [-t <seconds>]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

# echo "http://vulnweb.com" | jsleak -s > jsleak.txt
(root@kali)-[~/home/om]
# echo "http://vulnweb.com" | jsleak -l -s > jsleak.txt
(root@kali)-[~/home/om]
# echo "http://vulnweb.com" | jsleak -s
(root@kali)-[~/home/om]
# cat jsleak.txt
[+] Found link: [http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd] in [http://vulnweb.com]
[+] Found link: [http://www.w3.org/1999/xhtml] in [http://vulnweb.com]
[+] Found link: [text/css] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/] in [http://vulnweb.com]
[+] Found link: [https://testhtml5.vulnweb.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/html5-website-security/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/crawling-html5-javascript-websites/] in [http://vulnweb.com]
[+] Found link: [http://testphp.vulnweb.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/php-security-scanner/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/] in [http://vulnweb.com]
[+] Found link: [http://testasp.vulnweb.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/sql-injection/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/websitesecurity/sql-injection/] in [http://vulnweb.com]
[+] Found link: [https://testaspnet.vulnweb.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/vulnerability-scanner/network-vulnerability-scanner/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/blog/articles/network-vulnerability-assessment-gotchas-avoid/] in [http://vulnweb.com]
[+] Found link: [http://rest.vulnweb.com/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/blog/articles/rest-api-security-testing-acunetix/] in [http://vulnweb.com]
[+] Found link: [https://www.acunetix.com/blog/articles/rest-api-security-testing-acunetix/] in [http://vulnweb.com]

(root@kali)-[~/home/om]
# 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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