

Information Gathering Report

Target: testphp.vulnweb.com

Performed on Kali Linux

December 2025

1 Introduction

This report documents the passive and active legal information gathering performed on the target **testphp.vulnweb.com**, a publicly accessible and intentionally vulnerable web application hosted by Acunetix for cybersecurity testing and research. No intrusive or unauthorized exploitation was attempted.

2 Objective

The objectives of this assignment were:

- Gather publicly available information about the target.
- Enumerate DNS records, hosting provider, subdomains, technologies, directories, and ports.
- Document results with screenshots.
- Follow ethical hacking rules and avoid intrusive techniques.

3 Target Details

Target Subdomain: testphp.vulnweb.com

Parent Domain: vulnweb.com

4 Basic Information Gathering

4.1 WHOIS Lookup

WHOIS entries apply only to the root domain. Command used:

```
whois vulnweb.com
```

Screenshot:

```
(root㉿kali)-[~/home/kali/Desktop]
# whois vulnhub.com
Domain Name: VULNHUB.COM
Registry Domain ID: 1744580017_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2025-08-12T20:39:50Z
Creation Date: 2012-09-12T23:36:17Z
Registry Expiry Date: 2026-09-12T23:36:17Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ERIC.NS.CLOUDFLARE.COM
Name Server: JEAN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>> Last update of whois database: 2025-12-07T05:33:16Z <<

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.
```

4.2 DNS Enumeration

Commands executed:

```
dig vulnweb.com
dig ANY vulnweb.com
dig MX vulnweb.com
dig NS vulnweb.com
nslookup vulnweb.com
```

Screenshots:

```
(root㉿kali)-[~/home/kali/Desktop]
# dig testphp.vulnhub.com

<<>> DiG 9.20.11-4+b1-Debian <<>> testphp.vulnhub.com
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NOERROR, id: 63971
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; QUESTION SECTION:
testphp.vulnhub.com.           IN      A

; AUTHORITY SECTION:
vulnhub.com.          1800    IN      SOA     eric.ns.cloudflare.com. dns.cloudflare.com. 2390450717
10000 2400 604800 1800

; Query time: 319 msec
; SERVER: 10.139.49.25#53(10.139.49.25) (UDP)
; WHEN: Sun Dec 07 11:10:07 UTC 2025
; MSG SIZE  rcvd: 107
```

```
[root@kali]-[~/home/kali/Desktop]
└# dig testphp.vulnhub.com ANY

; <>> DiG 9.20.11-4+b1-Debian <>> testphp.vulnhub.com ANY
;; global options: +cmd
;; Got answer:
;; →HEADER<— opcode: QUERY, status: NOERROR, id: 33647
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;testphp.vulnhub.com.      IN      ANY

;; ANSWER SECTION:
testphp.vulnhub.com.    3600    IN      HINFO   "RFC8482" ""
testphp.vulnhub.com.    3600    IN      RRSIG   HINFO 13 3 3600 20251208065640 20251206045640 34505 vulnhub.com. rAV
Q39zT1z1Rh8oWzL29hVYA0/gksXGUvOWTLDFeSiSPkcAkqSB15NJ pNbLz9LVz3DPj0VXANW3lMSc5/5gAg==

;; Query time: 551 msec
;; SERVER: 10.139.49.25#53(10.139.49.25) (TCP)
;; WHEN: Sun Dec 07 11:27:30 UTC 2025
;; MSG SIZE rcvd: 176

[root@kali]-[~/home/kali/Desktop]
└# dig NS vulnhub.com

; <>> DiG 9.20.11-4+b1-Debian <>> NS vulnhub.com
;; global options: +cmd
;; Got answer:
;; →HEADER<— opcode: QUERY, status: NOERROR, id: 53139
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;vulnhub.com.          IN      NS

;; ANSWER SECTION:
vulnhub.com.        86400   IN      NS      eric.ns.cloudflare.com.
vulnhub.com.        86400   IN      NS      jean.ns.cloudflare.com.

;; Query time: 155 msec
;; SERVER: 10.139.49.25#53(10.139.49.25) (UDP)
;; WHEN: Sun Dec 07 11:30:55 UTC 2025
;; MSG SIZE rcvd: 92

[root@kali]-[~/home/kali/Desktop]
└# nslookup testphp.vulnhub.com
Server:          10.139.49.25
Address:         10.139.49.25#53

Non-authoritative answer:
*** Can't find testphp.vulnhub.com: No answer
```

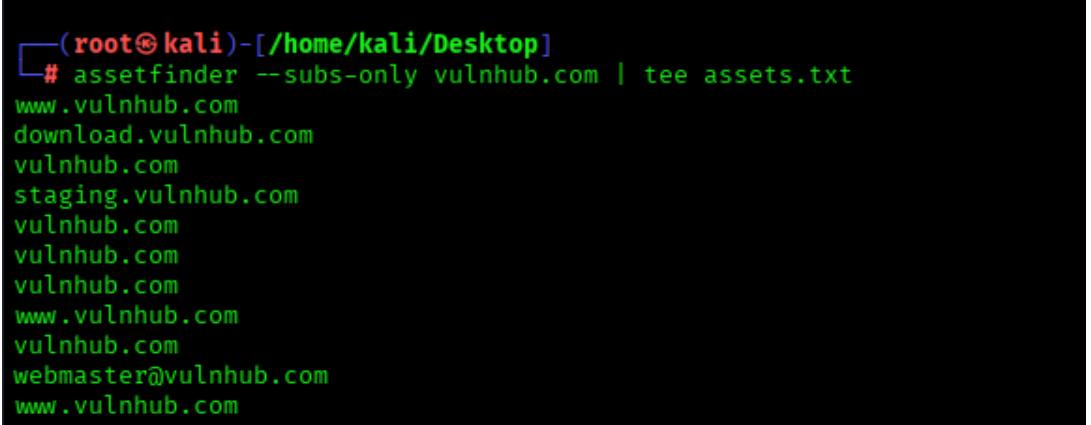
5 Subdomain Enumeration

Tools used: assetfinder, amass

5.1 assetfinder

```
assetfinder --subs-only vulnweb.com
```

Screenshot:



```
(root㉿kali)-[~/home/kali/Desktop]
# assetfinder --subs-only vulnhub.com | tee assets.txt
www.vulnhub.com
download.vulnhub.com
vulnhub.com
staging.vulnhub.com
vulnhub.com
vulnhub.com
vulnhub.com
www.vulnhub.com
vulnhub.com
webmaster@vulnhub.com
www.vulnhub.com
```

5.2 amass

```
amass enum -passive -d vulnweb.com
```

Screenshot:

```

root@kali:[/home/kali/Desktop]
└─# cat final_subdomains.txt
108.162.192.8/20 (Netblock) → contains → 108.162.192.121 (IPAddress)
108.162.192.8/20 (Netblock) → contains → 108.162.193.112 (IPAddress)
15335 (ASN) → announces → 184.21.32.8/20 (Netblock)
15335 (ASN) → announces → 188.162.192.8/20 (Netblock)
15335 (ASN) → announces → 172.64.8.0/16 (Netblock)
15335 (ASN) → announces → 172.67.8.0/16 (Netblock)
15335 (ASN) → announces → 173.249.35.0/23 (Netblock)
15335 (ASN) → announces → 208.64.7000:3030::/48 (Netblock)
15335 (ASN) → announces → 208.64.7000:50::/44 (Netblock)
15335 (ASN) → announces → 208.64.7000:50::/45 (Netblock)
15335 (ASN) → announces → 208.64.9001:50::/48 (Netblock)
15335 (ASN) → managed_by → CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
142.259.8.0/16 (Netblock) → contains → 142.259.4.26 (IPAddress)
15169 (ASN) → announces → 142.259.8.0/16 (Netblock)
15169 (ASN) → announces → 172.217.64.8/16 (Netblock)
15169 (ASN) → announces → 172.253.116.8/24 (Netblock)
15169 (ASN) → announces → 192.178.8.0/16 (Netblock)
15169 (ASN) → announces → 2484:6000:4003::/48 (Netblock)
15169 (ASN) → announces → 2607:ff000:50::/32 (Netblock)
15169 (ASN) → managed_by → AS15169 - Google LLC (RIROrganization)
15169 (ASN) → managed_by → GOOGLE - Google LLC (RIROrganization)
172.217.64.8/16 (Netblock) → contains → 172.217.78.27 (IPAddress)
172.253.116.8/24 (Netblock) → contains → 172.253.116.27 (IPAddress)
172.64.8.0/16 (Netblock) → contains → 172.64.33.121 (IPAddress)
172.64.8.0/16 (Netblock) → contains → 172.64.33.112 (IPAddress)
172.67.8.0/16 (Netblock) → contains → 172.67.162.8 (IPAddress)
173.245.58.0/23 (Netblock) → contains → 173.245.58.121 (IPAddress)
173.245.58.0/23 (Netblock) → contains → 173.245.59.112 (IPAddress)
192.178.8.0/15 (Netblock) → contains → 192.178.223.26 (IPAddress)
2484:6000:4003::/48 (Netblock) → contains → 2484:6000:4003:c01::1a (IPAddress)
208.64.7000:3030::/48 (Netblock) → contains → 208.64.7000:3030::6015:2a7e (IPAddress)
208.64.7000:3030::/48 (Netblock) → contains → 208.64.7000:3030::ac43:a208 (IPAddress)
208.64.7000:50::/44 (Netblock) → contains → 208.64.7000:50::ad75:3b79 (IPAddress)
208.64.7000:50::/32 (Netblock) → contains → 208.64.7000:50::4023:1c05::1a (IPAddress)
208.64.7000:50::/32 (Netblock) → contains → 208.64.7000:50::6ca2:c979 (IPAddress)
208.64.7000:50::/45 (Netblock) → contains → 208.64.7000:50::6ca2:c179 (IPAddress)
208.64.7000:50::/45 (Netblock) → contains → 208.64.7000:50::6ca2:c179 (IPAddress)
208.64.9001:50::/46 (Netblock) → contains → 208.64.9001:50::ac40:2079 (IPAddress)
208.64.9001:50::/46 (Netblock) → contains → 208.64.9001:50::ac40:2170 (IPAddress)
a111.aspx.1.google.com (FQDN) → aaaa_record → 2587:f000:4000::17::1a (IPAddress)
a111.aspx.1.google.com (FQDN) → a_record → 172.253.116.27 (IPAddress)
a112.aspx.1.google.com (FQDN) → aaaa_record → 2607:ff000:4003:1c05::1a (IPAddress)
a112.aspx.1.google.com (FQDN) → a_record → 172.217.78.27 (IPAddress)
aspx02.googlemail.com (FQDN) → aaaa_record → 2607:ff000:4000::17::1a (IPAddress)
aspx02.googlemail.com (FQDN) → a_record → 172.253.116.27 (IPAddress)
aspx03.googlemail.com (FQDN) → aaaa_record → 2607:ff000:4003:c01::1a (IPAddress)
aspx03.googlemail.com (FQDN) → a_record → 192.178.223.26 (IPAddress)
aspx01.google.com (FQDN) → aaaa_record → 2484:6000:4003:c01::1a (IPAddress)
aspx01.google.com (FQDN) → a_record → 142.259.4.26 (IPAddress)
download.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::6015:2a7e (IPAddress)
download.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::ac43:a208 (IPAddress)
download.vulnhub.com (FQDN) → a_record → 104.21.42.126 (IPAddress)
download.vulnhub.com (FQDN) → a_record → 172.67.162.8 (IPAddress)
eric.na.cloudflare.com (FQDN) → aaaa_record → 208.64.7000:50::ad75:3b79 (IPAddress)
eric.na.cloudflare.com (FQDN) → aaaa_record → 208.64.7000:50::6ca2:c179 (IPAddress)
eric.na.cloudflare.com (FQDN) → aaaa_record → 208.64.9001:50::ac40:2170 (IPAddress)
eric.na.cloudflare.com (FQDN) → a_record → 108.162.193.112 (IPAddress)
eric.na.cloudflare.com (FQDN) → a_record → 172.64.33.112 (IPAddress)
eric.na.cloudflare.com (FQDN) → a_record → 173.245.59.112 (IPAddress)
jean.na.cloudflare.com (FQDN) → aaaa_record → 208.64.7000:50::ad75:3b79 (IPAddress)
jean.na.cloudflare.com (FQDN) → aaaa_record → 208.64.7000:50::6ca2:c179 (IPAddress)
jean.na.cloudflare.com (FQDN) → aaaa_record → 208.64.9001:50::ac40:2079 (IPAddress)
jean.na.cloudflare.com (FQDN) → a_record → 108.162.192.121 (IPAddress)
jean.na.cloudflare.com (FQDN) → a_record → 172.64.32.121 (IPAddress)
jean.na.cloudflare.com (FQDN) → a_record → 173.245.56.121 (IPAddress)
staging.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::6015:2a7e (IPAddress)
staging.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::ac43:a208 (IPAddress)
staging.vulnhub.com (FQDN) → a_record → 104.21.42.126 (IPAddress)
staging.vulnhub.com (FQDN) → a_record → 172.67.162.8 (IPAddress)
vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::6015:2a7e (IPAddress)
vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::ac43:a208 (IPAddress)
vulnhub.com (FQDN) → a_record → 104.21.42.126 (IPAddress)
vulnhub.com (FQDN) → a_record → 172.67.162.8 (IPAddress)
vulnhub.com (FQDN) → mx_record → a111.aspx.1.google.com (FQDN)
vulnhub.com (FQDN) → mx_record → a112.aspx.1.google.com (FQDN)
vulnhub.com (FQDN) → mx_record → aspx02.googlemail.com (FQDN)
vulnhub.com (FQDN) → mx_record → aspx03.googlemail.com (FQDN)
vulnhub.com (FQDN) → mx_record → aspx01.google.com (FQDN)
vulnhub.com (FQDN) → mx_record → eric.na.cloudflare.com (FQDN)
vulnhub.com (FQDN) → mx_record → jean.na.cloudflare.com (FQDN)
www.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::6015:2a7e (IPAddress)
www.vulnhub.com (FQDN) → aaaa_record → 208.64.7000:3030::ac43:a208 (IPAddress)
www.vulnhub.com (FQDN) → a_record → 104.21.42.126 (IPAddress)
www.vulnhub.com (FQDN) → a_record → 172.67.162.8 (IPAddress)
download.vulnhub.com
vulnhub.com
submaster@vulnhub.com
www.vulnhub.com

root@kali:[/home/kali/Desktop]

```

6 Technology Fingerprinting

6.1 What Web

```
whatweb http://testphp.vulnweb.com
```

Screenshot:

```
[root@kali]-[~/home/kali/Desktop]
# whatweb http://testphp.vulnweb.com/
http://testphp.vulnweb.com/ [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab?version=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

7 Directory and File Discovery

7.1 Gobuster

```
gobuster dir -u http://testphp.vulnweb.com \
-w /usr/share/wordlists/dirb/common.txt
```

Screenshot:

```
[root@kali]-[~/home/kali/Desktop]
# gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://testphp.vulnweb.com/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/admin           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/admin/]
/cgi-bin/         (Status: 403) [Size: 276]
/cgi-bin          (Status: 403) [Size: 276]
/crossdomain.xml (Status: 200) [Size: 224]
/CVS             (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CVS/]
/CVS/Entries      (Status: 200) [Size: 1]
/CVS/Repository   (Status: 200) [Size: 8]
/CVS/Root         (Status: 200) [Size: 1]
/favicon.ico      (Status: 200) [Size: 894]
/images           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/images/]
/index.php        (Status: 200) [Size: 4958]
/pictures          (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/picture]
/secured           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/secured]
/vendor            (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]

Progress: 4613 / 4613 (100.00%)
=====

Finished
```

7.2 Dirb

```
dirb http://testphp.vulnweb.com
```

Screenshot:

```
[root@kali]-[/home/kali/Desktop]
# dirb http://testphp.vulnweb.com/

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Sun Dec 7 11:41:10 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612

_____
Scanning URL: http://testphp.vulnweb.com/
==> DIRECTORY: http://testphp.vulnweb.com/admin/
--> Testing: http://testphp.vulnweb.com/bl
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)

(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT CONNECT)

_____
END_TIME: Sun Dec 7 12:03:17 2025
DOWNLOADED: 2488 - FOUND: 8
```

8 Open Ports and Service Enumeration

8.1 Nmap Scan

```
nmap -sV -sC testphp.vulnweb.com
```

Screenshot:

```
[root@kali]-[/home/kali]
# nmap -sV -sC testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 11:59 UTC
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.059s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.0
|_http-title: Home of Acunetix Art

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.84 seconds
```

9 Public OSINT Information

Manual Google queries:

```
site:vulnweb.com contact  
vulnweb.com security  
"vulnweb" linkedin
```

Findings:

- Vulnweb belongs to Acunetix (Invicti Security).
- Public documentation indicates intentionally vulnerable labs.
- No sensitive leaks or unauthorized information found.

10 Summary of Findings

- WHOIS: Valid root domain information for vulnweb.com
- DNS: Standard MX, NS, A records, no zone transfer allowed
- Subdomains: Several discovered, no sensitive ones
- Ports: Only port 80 open running Apache/PHP
- Directories: PHP info, admin pages, test pages discovered
- Technologies: PHP, Apache (from WhatWeb)
- Emails: Limited emails harvested

11 Challenges Faced

- Subdomain WHOIS lookup failed (expected)
- AXFR zone transfer blocked
- Rate limiting slowed directory enumeration

12 Conclusion

The target **testphp.vulnweb.com** behaves as an intentionally vulnerable environment for cybersecurity testing. Information-gathering results align with standard testbed configurations. No exploitation or unauthorized access was performed. Results may be used for academic and security research purposes under ethical guidelines.