

# Passive Reconnaissance Report

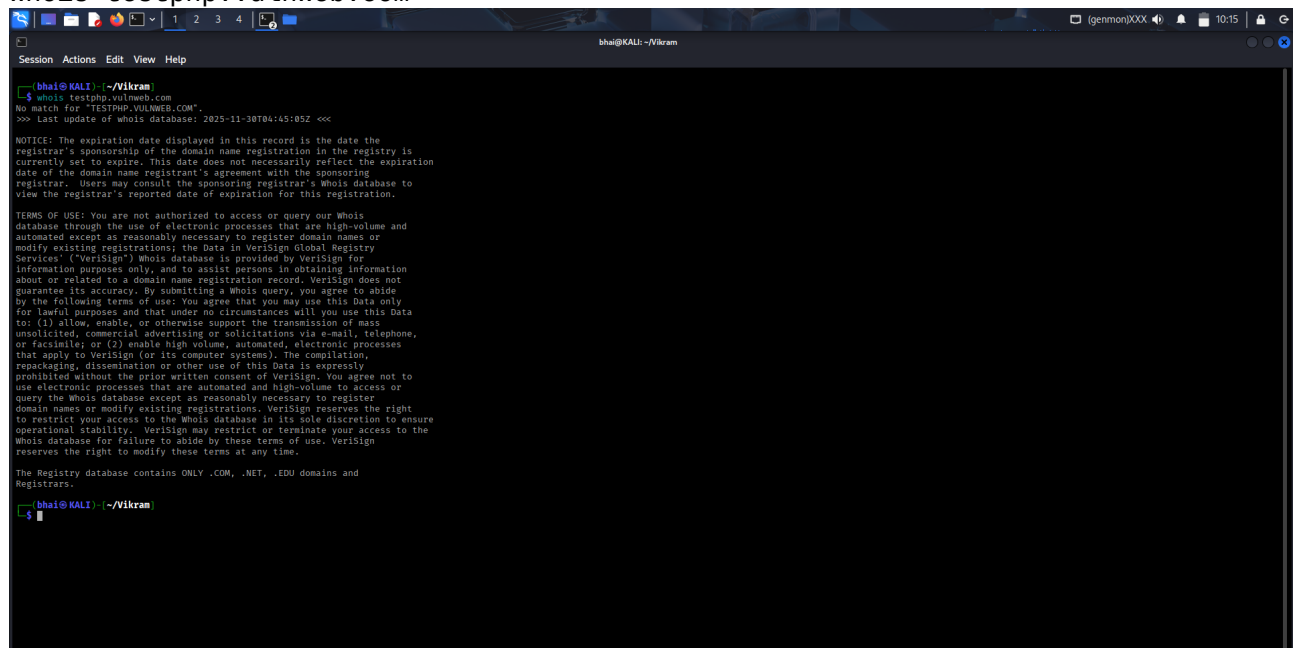
Target Domain: testphp.vulnweb.com and facebook.com

## WHOIS & DNS Findings

- Basic WHOIS and DNS info collected.

### Commands Used:

whois testphp.vulnweb.com



```
bhai@KALI: ~/Vikram
$ whois testphp.vulnweb.com
No match for "TESTPHP.VULNWEB.COM".
>>> Last update of whois database: 2025-11-30T04:45:05Z <<<

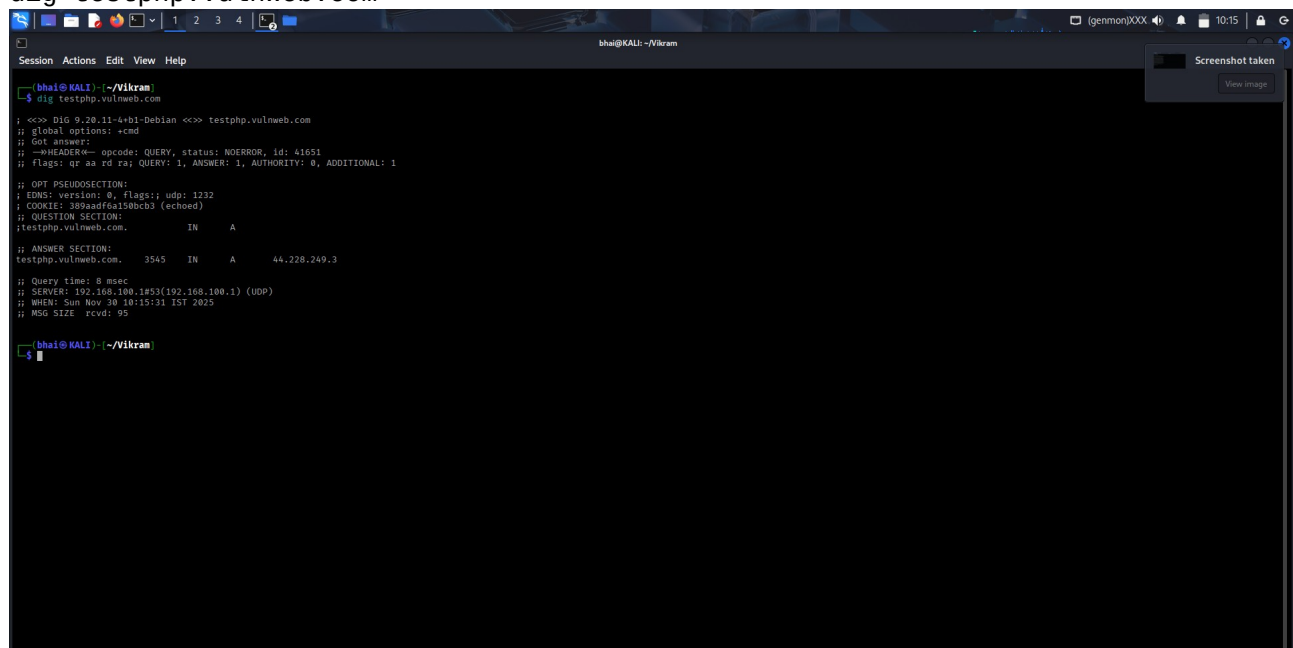
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  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
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may 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, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

bhai@KALI: ~/Vikram
$
```

dig testphp.vulnweb.com



```
bhai@KALI: ~/Vikram
$ dig testphp.vulnweb.com

;<>> DIG 9.28.11-4+b1-Debian <>> testphp.vulnweb.com
;; global options: +cmd
;; Got answer:
;;->HEADER-<- opcode: QUERY, status: NOERROR, id: 41651
;; Flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 389eadf6a150bcb3 (echoed)
;; QUESTION SECTION:
;testphp.vulnweb.com.            IN      A

;; ANSWER SECTION:
testphp.vulnweb.com.    3545    IN      A      44.228.249.3

;; Query time: 8 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Sun Nov 30 10:15:31 IST 2025
;; MSG SIZE rcvd: 95

bhai@KALI: ~/Vikram
$
```

dig testphp.vulnweb.com ANY

```
Session Actions Edit View Help
bhai@KALI: ~/Vikram

(bhai@KALI)~-[~/Vikram]
$ dig testphp.vulnweb.com ANY

; <<>> DiG 9.20.11-4+b1-Debian <<>> testphp.vulnweb.com ANY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOTIMP, id: 41546
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 184fb5bfa032b3dd (echoed)
;; QUESTION SECTION:
;; testphp.vulnweb.com.                IN      ANY

;; Query time: 28 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (TCP)
;; WHEN: Sun Nov 30 10:15:47 IST 2025
;; MSG SIZE rcvd: 60

(bhai@KALI)~-[~/Vikram]
$
```

nslookup testphp.vulnweb.com

```
Session Actions Edit View Help
bhai@KALI: ~/Vikram

(bhai@KALI)~-[~/Vikram]
$ nslookup testphp.vulnweb.com
Server:      192.168.100.1
Address:     192.168.100.1#53

Name:   testphp.vulnweb.com
Address: 44.228.249.3

(bhai@KALI)~-[~/Vikram]
$
```

---

## Subdomains Discovered

- Subdomains gathered using passive tools.

### Commands Used:

subfinder -d facebook.com

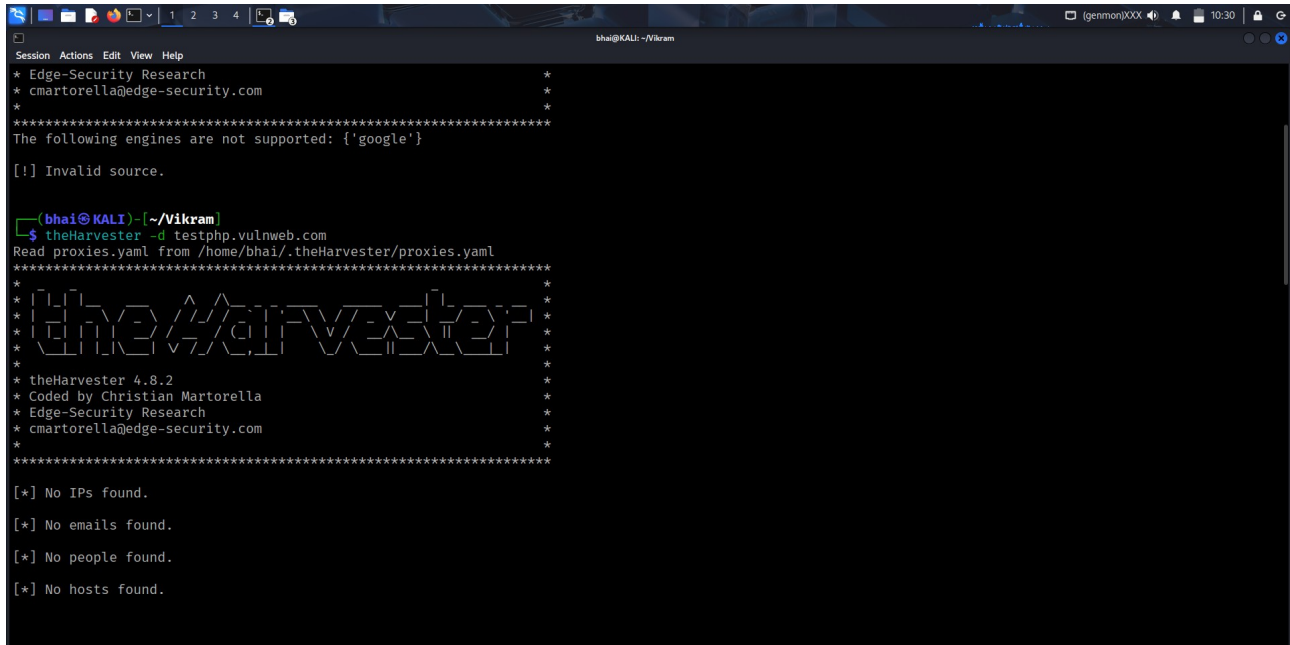


# Email / Employee Information

- Email and related info collected using theHarvester.

## Command Used:

theHarvester -d testphp.vulnweb.com -b google,bing,linkedin

A screenshot of a Kali Linux terminal window. The terminal shows the execution of theHarvester. It starts with a header for Edge-Security Research and cmartorella@edge-security.com. It then displays an error message: "The following engines are not supported: {'google'}" and "[!] Invalid source." The user then runs theHarvester -d testphp.vulnweb.com. The terminal shows the command, the path to the proxies.yaml file, and a large ASCII art logo for theHarvester. Below the logo, it shows the version (4.8.2), the coder (Christian Martorella), and the research organization (Edge-Security Research). Finally, it displays four status messages: "[\*] No IPs found.", "[\*] No emails found.", "[\*] No people found.", and "[\*] No hosts found."

```

Session Actions Edit View Help
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
The following engines are not supported: {'google'}
[!] Invalid source.

(bhai@KALI)-[~/Vikram]
$ theHarvester -d testphp.vulnweb.com
Read proxies.yaml from /home/bhai/.theHarvester/proxies.yaml
*****
*
* theHarvester
*
* theHarvester 4.8.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] No hosts found.

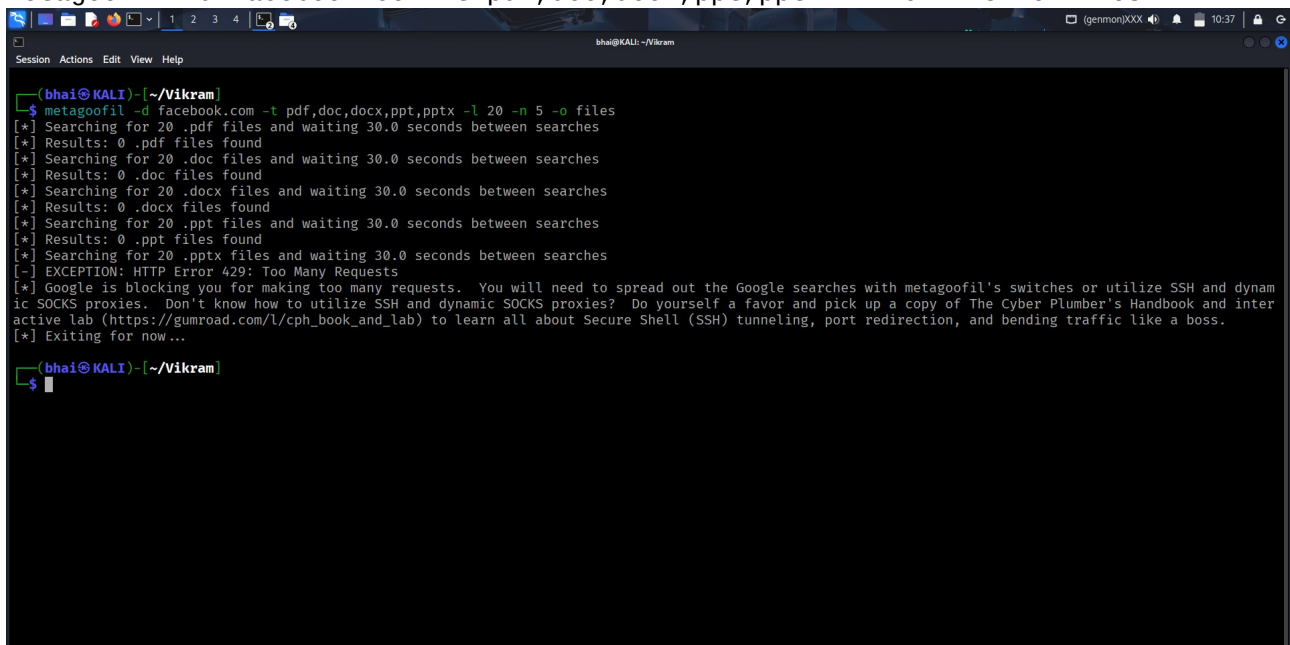
```

# Metadata Extraction

- Public documents checked for metadata (if available).

## Commands Used:

metagoofil -d facebook.com -t pdf,doc,docx,ppt,pptx -l 20 -n 5 -o files

A screenshot of a Kali Linux terminal window. The terminal shows the execution of metagoofil. It starts with a header for Edge-Security Research and cmartorella@edge-security.com. The user then runs metagoofil -d facebook.com -t pdf,doc,docx,ppt,pptx -l 20 -n 5 -o files. The terminal shows the command, the path to the proxies.yaml file, and a large ASCII art logo for metagoofil. Below the logo, it shows the version (4.8.2), the coder (Christian Martorella), and the research organization (Edge-Security Research). Finally, it displays four status messages: "[\*] No IPs found.", "[\*] No emails found.", "[\*] No people found.", and "[\*] No hosts found."

```

Session Actions Edit View Help
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
The following engines are not supported: {'google'}
[!] Invalid source.

(bhai@KALI)-[~/Vikram]
$ metagoofil -d facebook.com -t pdf,doc,docx,ppt,pptx -l 20 -n 5 -o files
[*] Searching for 20 .pdf files and waiting 30.0 seconds between searches
[*] Results: 0 .pdf files found
[*] Searching for 20 .doc files and waiting 30.0 seconds between searches
[*] Results: 0 .doc files found
[*] Searching for 20 .docx files and waiting 30.0 seconds between searches
[*] Results: 0 .docx files found
[*] Searching for 20 .ppt files and waiting 30.0 seconds between searches
[*] Results: 0 .ppt files found
[*] Searching for 20 .pptx files and waiting 30.0 seconds between searches
[*] Results: 0 .pptx files found
[*] EXCEPTION: HTTP Error 429: Too Many Requests
[*] Google is blocking you for making too many requests. You will need to spread out the Google searches with metagoofil's switches or utilize SSH and dynamic SOCKS proxies. Don't know how to utilize SSH and dynamic SOCKS proxies? Do yourself a favor and pick up a copy of The Cyber Plumber's Handbook and interactive lab (https://gumroad.com/l/cph_book_and_lab) to learn all about Secure Shell (SSH) tunneling, port redirection, and bending traffic like a boss.
[*] Exiting for now...

(bhai@KALI)-[~/Vikram]
$

```

exiftool file.pdf

```
bhai@KALI: ~/Desktop
$ exiftool Sample.pdf
ExifTool Version Number      : 13.25
File Name                    : Sample.pdf
Directory                    : .
File Size                     : 38 kB
File Modification Date/Time   : 2025:11:30 10:39:39+05:30
File Access Date/Time        : 2025:11:30 10:39:40+05:30
File Inode Change Date/Time   : 2025:11:30 10:39:39+05:30
File Permissions              : -rw-rw-r--
File Type                     : PDF
File Type Extension          : pdf
MIME Type                     : application/pdf
PDF Version                  : 1.5
Linearized                   : Yes
Author                       : Nigel Maddocks
Comments                      :
Company                       :
Create Date                  : 2015:08:21 09:42:21+01:00
Keywords                     : 12345678
Modify Date                  : 2015:08:21 09:45:31+01:00
Language                     : EN-GB
Tagged PDF                   : Yes
XMP Toolkit                  : Adobe XMP Core 5.6-c015 81.157285, 2014/12-00:43:15
Metadata Date                : 2015:08:21 09:45:31+01:00
Creator Tool                  : Acrobat PDFMaker 15 for Word
Document ID                  : uuid:32f55d7c-7ef1-46ca-85c0-b5b91509ff82
Instance ID                  : uuid:4da38cf4-2b42-417c-b34e-f529c34ac6cc
Format                       : application/pdf
Title                        : PDF Metadata Sample
Description                   : Test Document
Creator                      : Nigel Maddocks
Subject                      : 12345678
Producer                     : Adobe PDF Library 15.0
```

strings file.pdf | head

```
bhai@KALI: ~/Desktop
$ strings Sample.pdf | head
%PDF-1.5
19 0 obj
<</Linearized 1/L 37545/O 21/E 32148/N 1/T 37241/H [ 482 170]>>
endobj

34 0 obj
<</DecodeParms<</Columns 4/Predictor 12>>/Filter/FlateDecode/ID[<3CD047149679B641B35FCB2CB4A380AC><35E6FCC49927BE448F99B12AE6BBD75E>]/Index[19 20]/Info 18 0
R/Length 78/Prev 37242/Root 20 0 R/Size 39/Type/XRef/W[1 2 1]>>stream
b
endstream
endobj

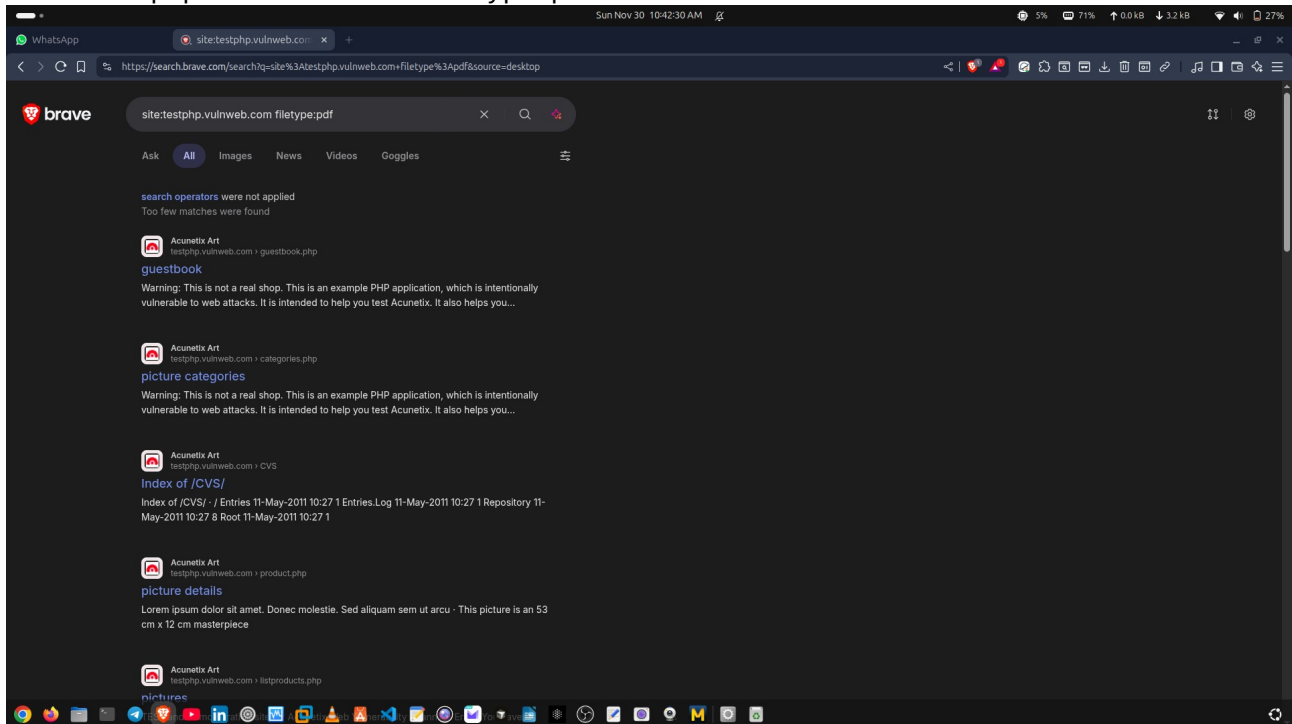
bhai@KALI: ~/Desktop
$
```

# Google Dorks Used

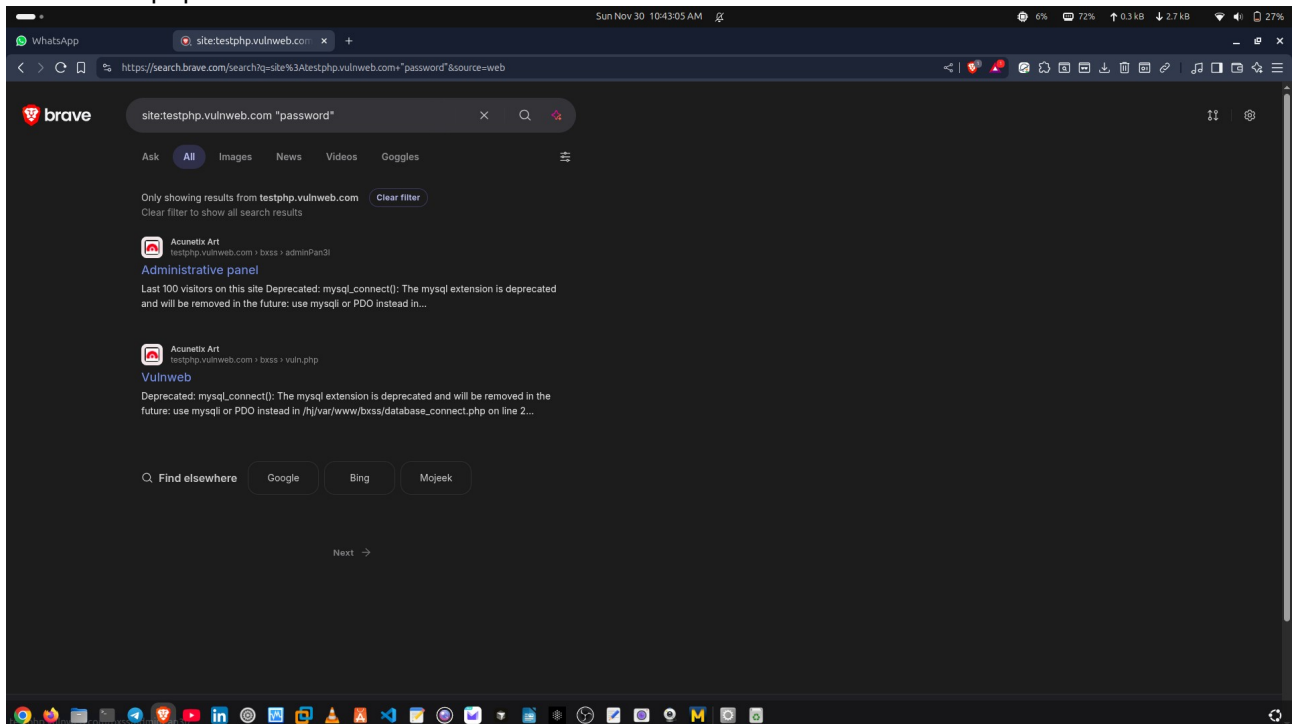
- Dorks applied for passive info.

## Queries Used (browser):

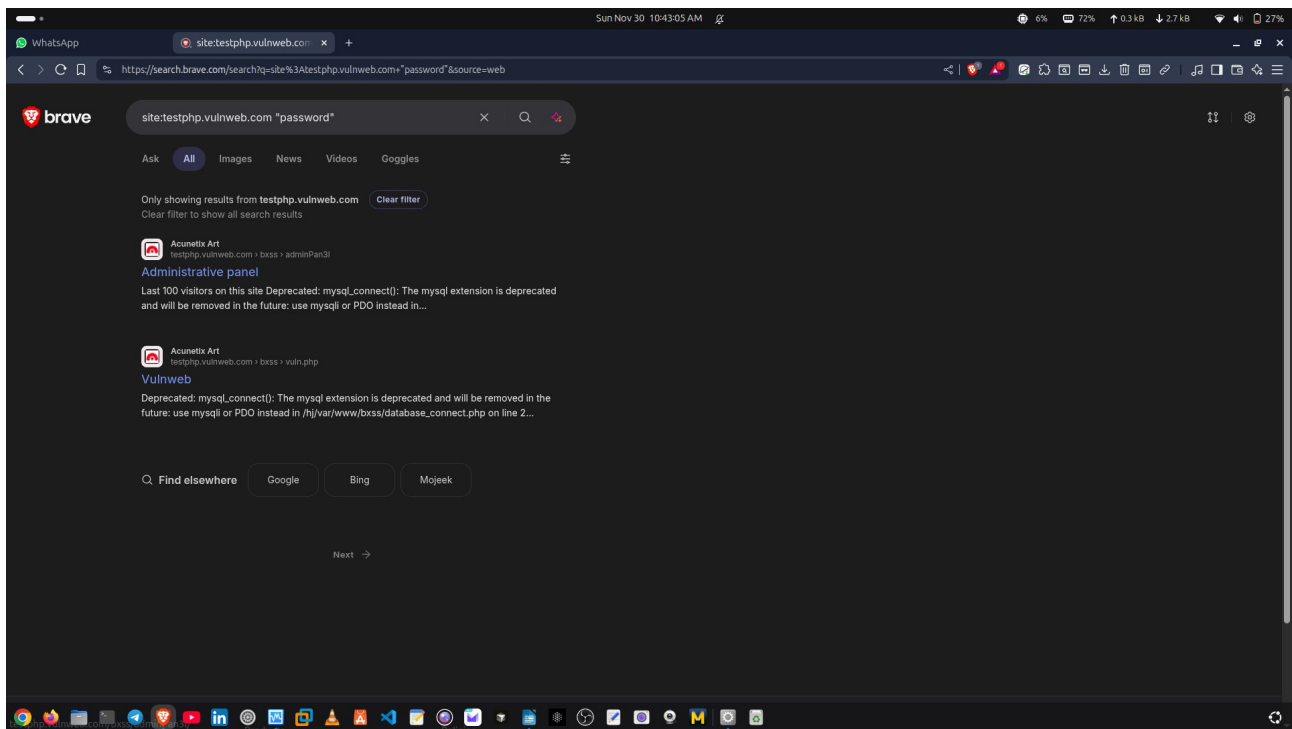
site:testphp.vulnweb.com filetype:pdf



site:testphp.vulnweb.com intitle:"index of"



site:testphp.vulnweb.com "password"

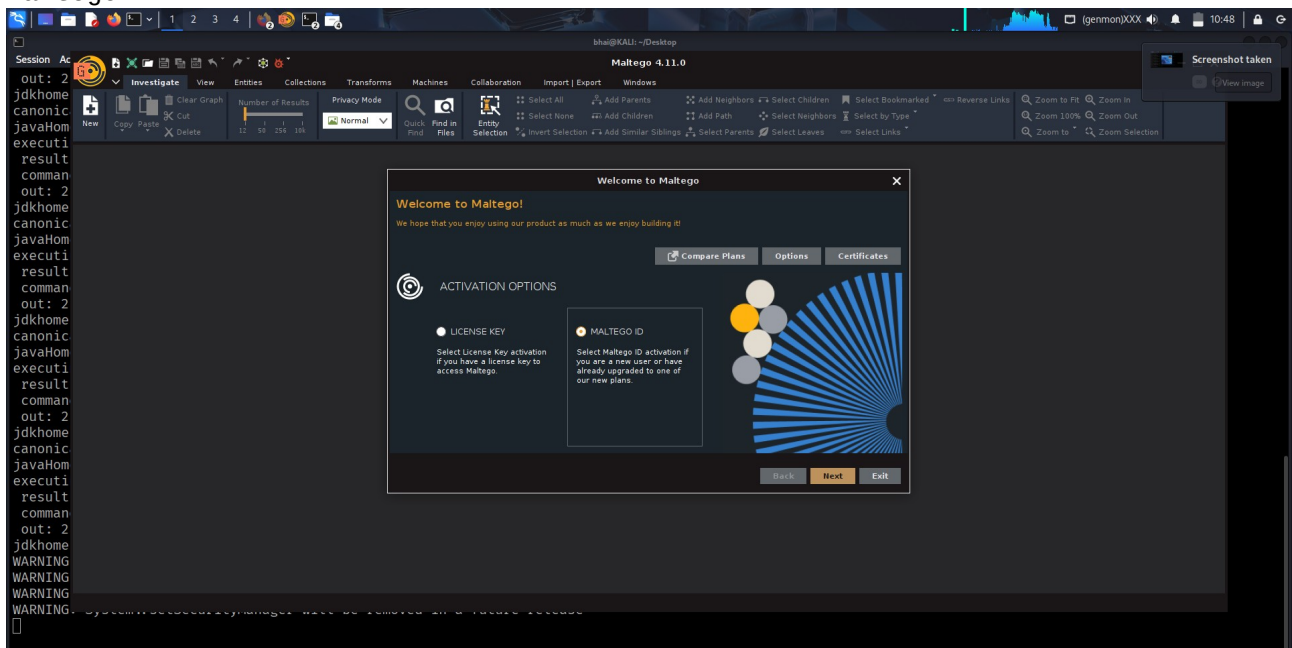


## OSINT Summary

- Checked public OSINT sources.

## Commands Used:

maltego



spiderfoot -l 127.0.0.1:5001



```
Session Actions Edit View Help

(bhai@KALI)-[~/Desktop]
$ spiderfoot -l 127.0.0.1:5001
/usr/lib/python3/dist-packages/adblockparser/parser.py:247: SyntaxWarning: invalid escape sequence '\w'
  rule = rule.replace("^" "(?:[^\w\d \-.%]|$)")
/usr/lib/python3/dist-packages/adblockparser/parser.py:272: SyntaxWarning: invalid escape sequence '\l'
  rule = re.sub("(\\l)[$]", r"\l", rule)
2025-11-30 10:49:17,528 [INFO] sf : Starting web server at 127.0.0.1:5001 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****

2025-11-30 10:49:17,547 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

## URL Collection & JS Filtering

- URLs extracted and JS files filtered.

### Commands Used:

gau testphp.vulnweb.com

```
Terminal

http://testphp.vulnweb.com/udir.php?r=http://indonesianormal23.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal24.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal25.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal26.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal27.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal28.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal29.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal30.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal31.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal32.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal33.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal34.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal35.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal36.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal37.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal38.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal39.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal40.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal41.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal42.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal43.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal44.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal45.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal46.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal47.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal48.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal49.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal50.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal51.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal52.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal53.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal54.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal55.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal56.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal57.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal58.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal59.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal60.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal61.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal62.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal63.weebly.com/
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal64.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal65.weebly.com
http://testphp.vulnweb.com/udir.php?r=http://indonesianormal66.weebly.com
```

gau testphp.vulnweb.com | grep ".js"



```
(vikram@VIKRAM:~)$ gau testphp.vulnweb.com | grep ".js"
WARN[0000] error reading config: Config file /home/vikram/.gau.toni not found, using default config
http://testphp.vulnweb.com/_well-known/robots.txt
http://testphp.vulnweb.com/_well-known/assetlinks.json
http://testphp.vulnweb.com/_well-known/gpc.json
http://testphp.vulnweb.com/bxss/test.js
http://testphp.vulnweb.com/login.phphttps://modcom.pythonanywhere.com/http://www.altoromutual.com:8080/login.jsp
http://testphp.vulnweb.com/login.phphttps://modcom.pythonanywhere.com/http://www.altoromutual.com:8080/login.jsphttps://juice-shop.herokuapp.com/
http://testphp.vulnweb.com/medias/js/
http://testphp.vulnweb.com/medias/js/common_functions.js
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/323/submission/323-13-860-1-2-20220704.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/325/submission/325-13-862-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/327/submission/327-13-864-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/329/submission/329-13-866-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/331/submission/331-13-868-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/333/submission/333-13-870-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/335/submission/335-13-872-1-2-20220705.html
http://testphp.vulnweb.com/redirect.php?r=http://jst.ntt.edu.vn/files/journals/2/articles/399/submission/399-13-952-2-2-20220809.html
http://testphp.vulnweb.com/redirect.php?r=http://nationalfostercaremonth.org/_media_/js/netsoltrademark.php?id=fleetautorepairshop.com2Fpromaster-van-conversion-shop-near-me2F/
http://testphp.vulnweb.com/redirect.php?r=http://ojs.experttel.com.ar/files/journals/2/articles/427/submission/original/427-525-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://thedesigndebureau.net/_media_/js/netsoltrademark.php?id=fleetautorepairshop.com2Fsprinter-van-wrap-shop-near-me2F/
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1180/submission/original/1180-3511-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1182/submission/original/1182-3513-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1184/submission/original/1184-3515-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1186/submission/original/1186-3517-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1188/submission/original/1188-3519-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=http://www.gestionpolitica publica.cide.edu/ojs/cide/files/journals/2/articles/1190/submission/original/1190-3521-1-SM.html
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata10.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata11.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata11.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata12.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata12.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata13.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata13.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata22.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata23.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata39.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata40.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata9.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://cjstrata9.blogspot.com/
http://testphp.vulnweb.com/redirect.php?r=https://garden-ip.com/_media_/js/netsoltrademark.php?id=5-th-frio-card.thai-shop.store
http://testphp.vulnweb.com/redirect.php?r=https://ojs.experttel.com.ar/files/journals/2/articles/1192/submission/original/1192-3523-1-SM.html
```

katana -u <https://testphp.vulnweb.com>

```
(vikram@VIKRAM:~)$ katana -u https://testphp.vulnweb.com

projectdiscovery.io

[INF] Current katana version v1.2.1 (outdated)
[INF] Started standard crawling for => https://testphp.vulnweb.com
https://testphp.vulnweb.com
(vikram@VIKRAM:~)$ katana -u facebook.com

projectdiscovery.io

[INF] Current katana version v1.2.1 (outdated)
[INF] Started standard crawling for => https://facebook.com
https://facebook.com
(vikram@VIKRAM:~)$
```