



# CHRIST

(DEEMED TO BE UNIVERSITY)

BANGALORE | DELHI NCR | PUNE

# DISCOVER HIDDEN DIRECTORIES

Submitted by: Joy Aanchal Rose

Register No.: 2460481

# INDEX

S.I.No	Contents	Pg. No.
1.	Methodology	1
2.	Findings	1
3.	Code	2
4.	Screenshots(Proof)	2
5.	Conclusion	6

# DISCOVER HIDDEN DIRECTORIES

## METHODOLOGY

To identify hidden or unlinked directories on the target website (<http://testphp.vulnweb.com/>), I used **Gobuster**, a directory and file brute-forcing tool. The enumeration was performed using a common wordlist (`common.txt`) provided by the SecLists project.

### COMMAND USED:

```
gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt -t 40 -o gobuster-results.txt
```

- `-u` specifies the target URL.
- `-w` points to the wordlist used for brute-forcing.
- `-t` sets the number of concurrent threads.
- `-o` specifies the output file for storing results.

This allowed me to discover directories and files by sending HTTP requests and analyzing status codes returned by the server

## FINDINGS

The scan revealed the following directories and files of interest:

Directory / File	Status Code	Description
/admin/	301	Redirects to admin panel – potentially sensitive
/cgi-bin/	403	Forbidden – commonly contains scripts; possible entry point
/CVS/	200	Exposed version control system directory – misconfigured
/CVS/Entries	200	VCS metadata – could reveal file structure
/CVS/Root	200	CVS root config – may leak repository info
/CVS/Repository	200	May show internal repository names
/crossdomain.xml	200	Flash cross-domain policy file – inspect for misconfigurations
/images/	200	Publicly accessible – may host media or leak metadata
/pictures/	301	Redirect – similar to /images/
/secured/	301	Redirects to restricted resource – inspect for auth bypass
/vendor/	301	May expose package manager files (e.g., PHP Composer)

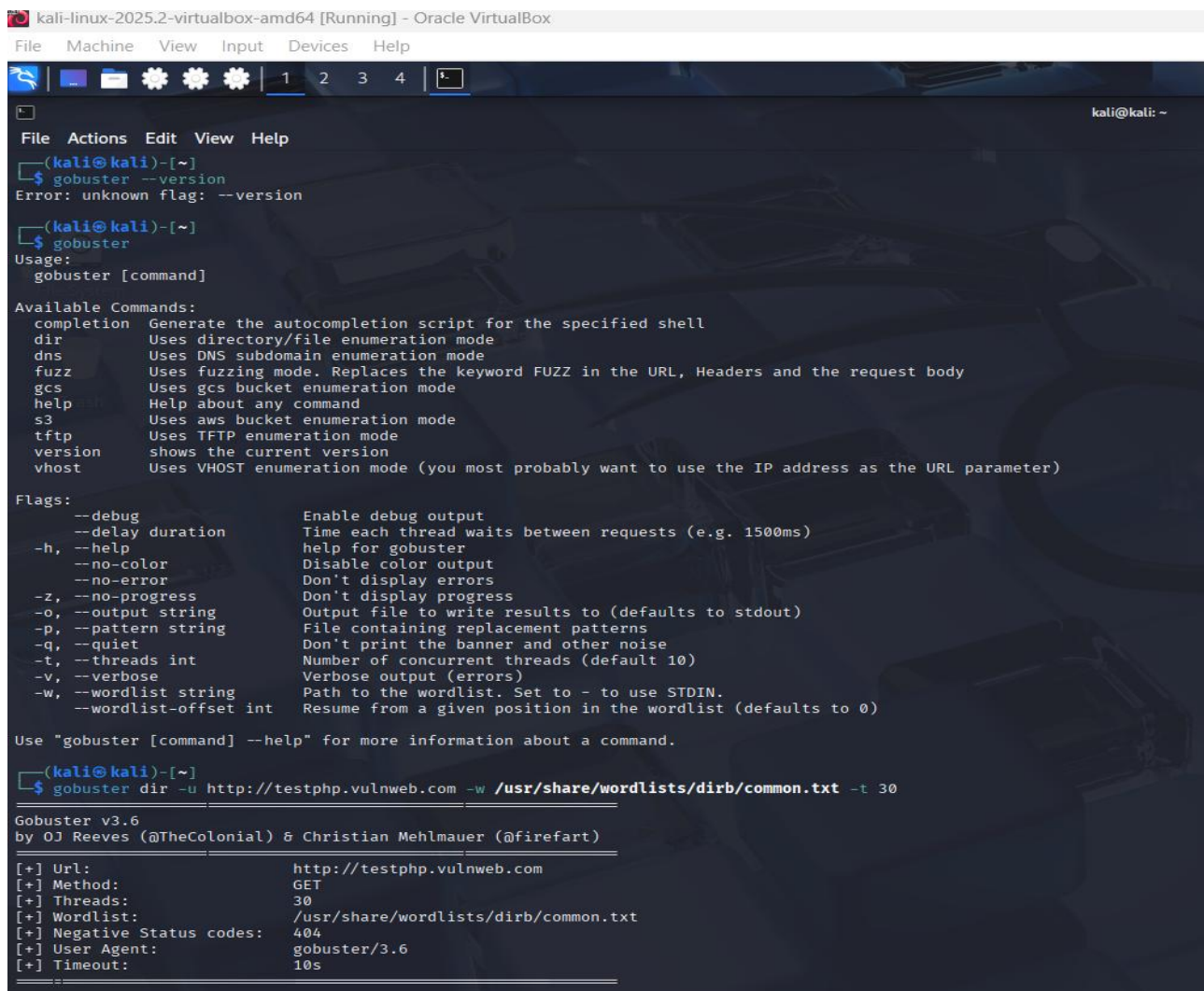
## CODE / SCRIPT USED

### Gobuster Command:

```
gobuster dir \  
-u http://testphp.vulnweb.com/ \  
-w /usr/share/wordlists/dirb/common.txt \  
-t 40 \  
-o gobuster-results.txt
```

Optionally, the -x flag can be used to scan for specific file extensions (e.g., .php, .bak, .txt) if further enumeration is required.

## SCREENSHOTS



```
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
1 2 3 4  
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ gobuster --version  
Error: unknown flag: --version  
(kali@kali)-[~]  
$ gobuster  
Usage:  
gobuster [command]  
  
Available Commands:  
completion  Generate the autocompletion script for the specified shell  
dir          Uses directory/file enumeration mode  
dns          Uses DNS subdomain enumeration mode  
fuzz         Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body  
gcs          Uses gcs bucket enumeration mode  
help         Help about any command  
s3           Uses aws bucket enumeration mode  
tftp         Uses TFTP enumeration mode  
version      shows the current version  
vhost        Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)  
  
Flags:  
--debug          Enable debug output  
--delay duration Time each thread waits between requests (e.g. 1500ms)  
-h, --help       help for gobuster  
--no-color       Disable color output  
--no-error       Don't display errors  
-z, --no-progress Don't display progress  
-o, --output string Output file to write results to (defaults to stdout)  
-p, --pattern string File containing replacement patterns  
-q, --quiet       Don't print the banner and other noise  
-t, --threads int Number of concurrent threads (default 10)  
-v, --verbose     Verbose output (errors)  
-w, --wordlist string Path to the wordlist. Set to - to use STDIN.  
--wordlist-offset int Resume from a given position in the wordlist (defaults to 0)  
  
Use "gobuster [command] --help" for more information about a command.  
(kali@kali)-[~]  
$ gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/common.txt -t 30  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: http://testphp.vulnweb.com  
[+] Method: GET  
[+] Threads: 30  
[+] Wordlist: /usr/share/wordlists/dirb/common.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s
```

## Vulnerable directories found

```
(kali@kali)-[~]
$ gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/common.txt -t 30

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://testphp.vulnweb.com
[+] Method: GET
[+] Threads: 30
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] 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/Root (Status: 200) [Size: 1]
/ CVS/Repository (Status: 200) [Size: 8]
/ 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/pictures/]
/ secured (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/secured/]
/ vendor (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)

Finished

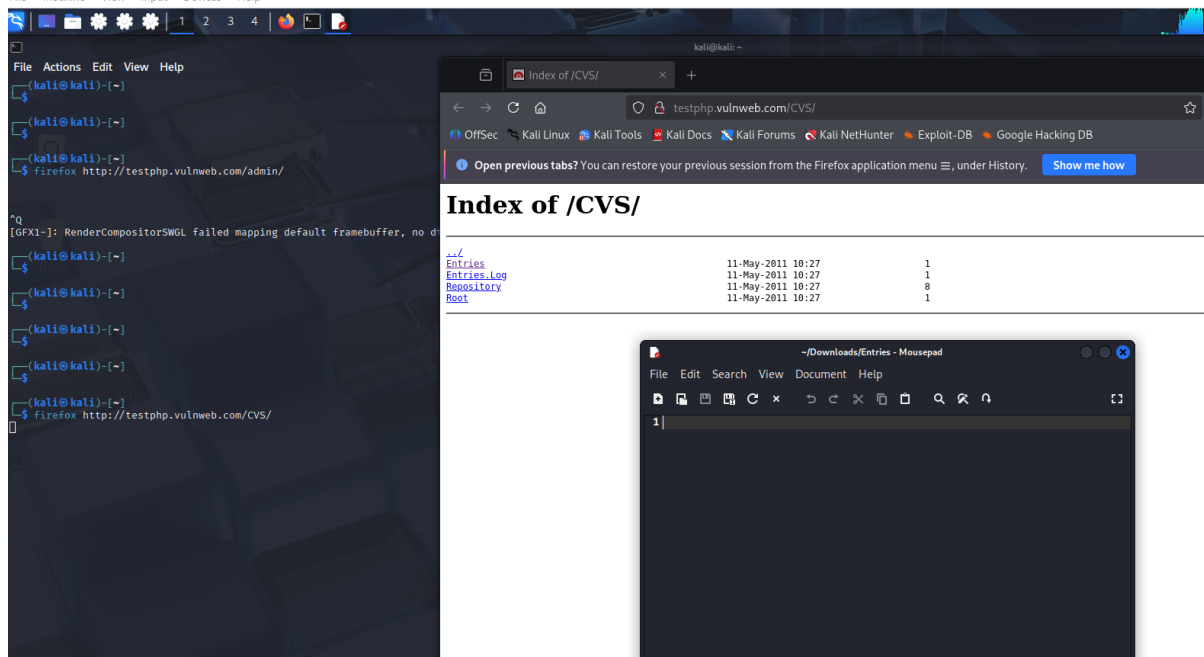
(kali@kali)-[~]
$
```

## 1]ADMIN

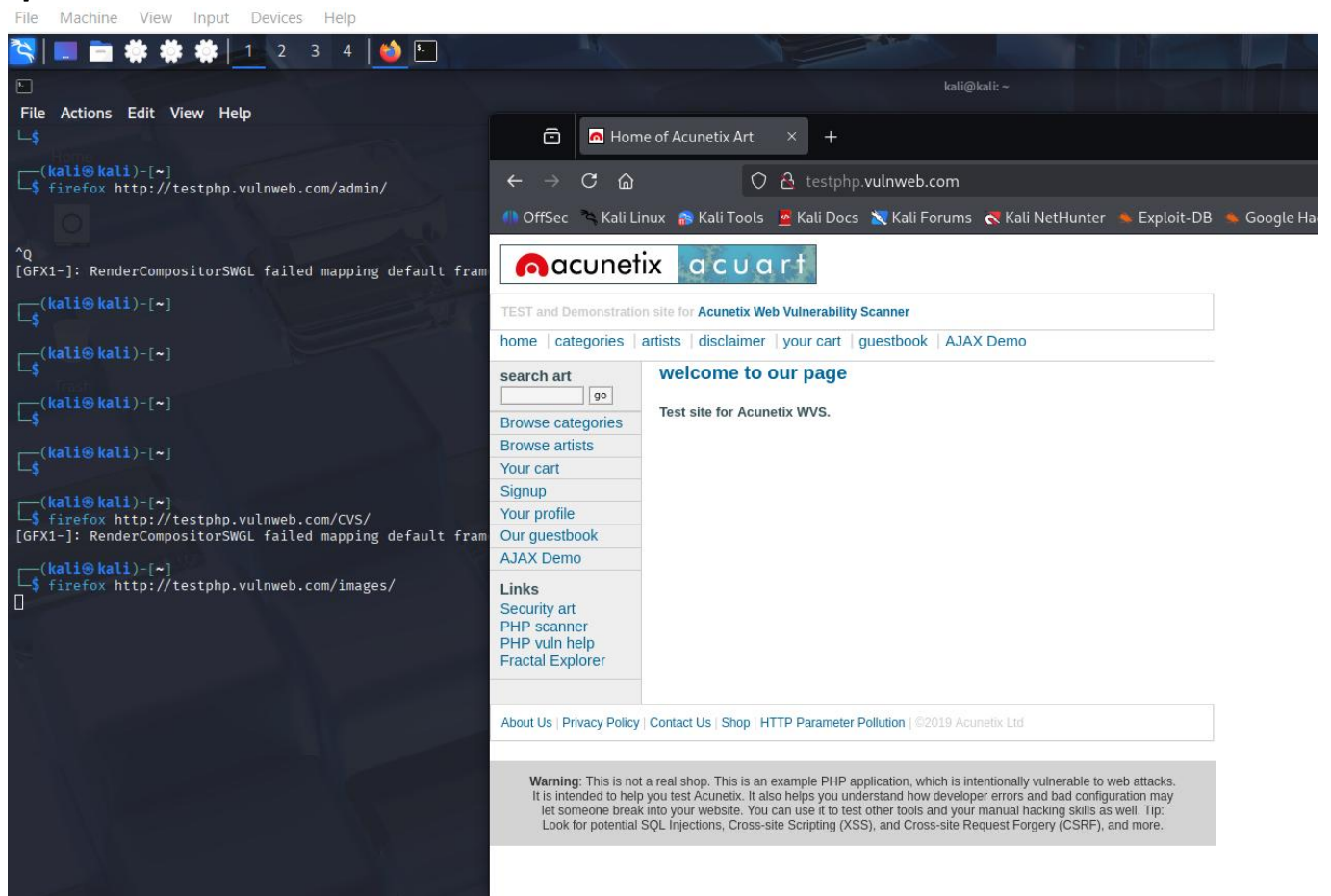
The screenshot shows a Kali Linux desktop environment. On the left, a terminal window displays the output of the `gobuster` command, which has successfully enumerated the `/admin/` directory. In the center, a web browser window shows the `Index of /admin/` page, which is a directory listing. On the right, a text editor window displays a SQL script named `create.sql` that creates a database named `waspart` and defines several tables: `forum`, `artists`, `categ`, and `pictures`.

```
1 create database waspart;
2 use waspart;
3
4 CREATE TABLE IF NOT EXISTS forum(
5     sender CHAR(150),
6     mesaj TEXT,
7     senttime INTEGER(32));
8
9 CREATE TABLE IF NOT EXISTS artists(
10    artist_id INTEGER(5) PRIMARY KEY AUTO_INCREMENT,
11    aname CHAR(50),
12    adesc BLOB);
13
14 CREATE TABLE IF NOT EXISTS categ(
15    cat_id INTEGER(5) PRIMARY KEY AUTO_INCREMENT,
16    cname CHAR(50),
17    cdesc BLOB);
18
19 CREATE TABLE IF NOT EXISTS pictures(
20    pic_id INTEGER(5) PRIMARY KEY AUTO_INCREMENT,
21    pshort BLOB,
22    plong TEXT,
23    orice INTEGER.
```

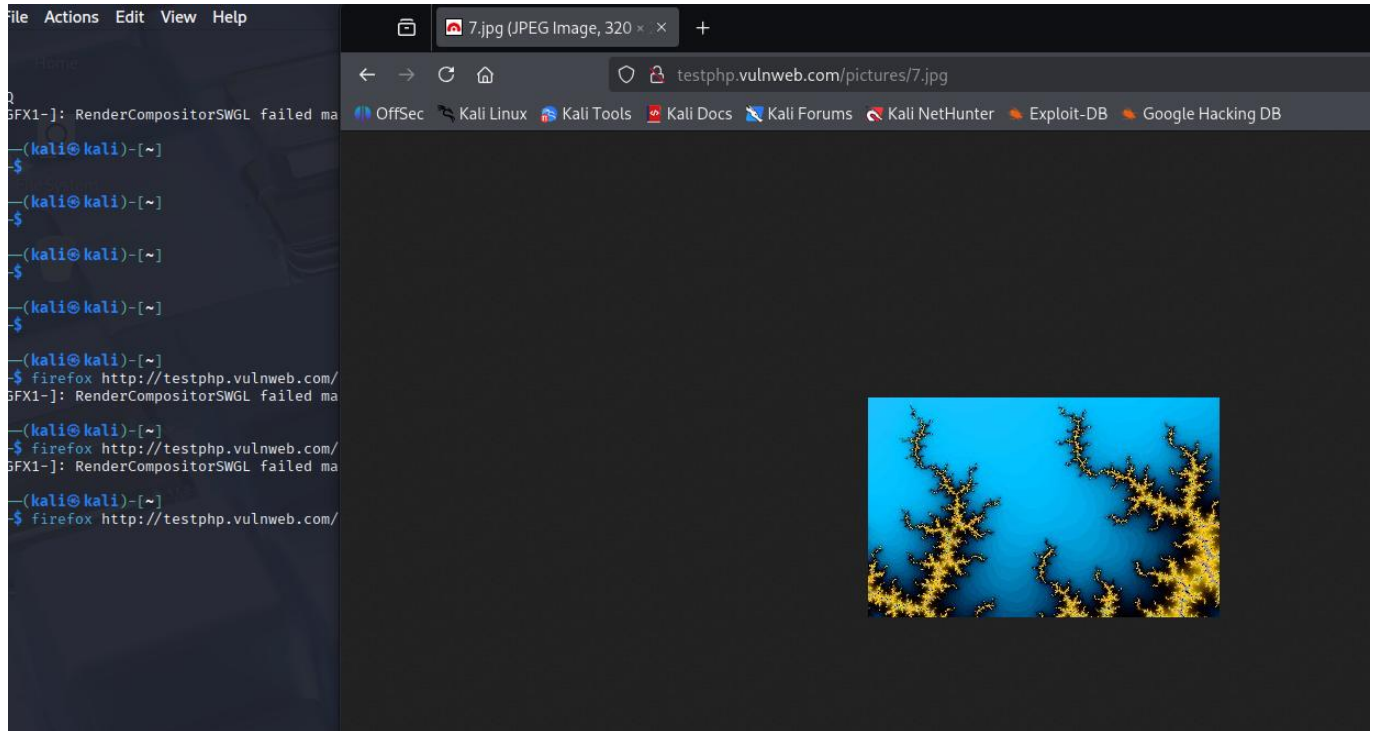
## 2]CVS



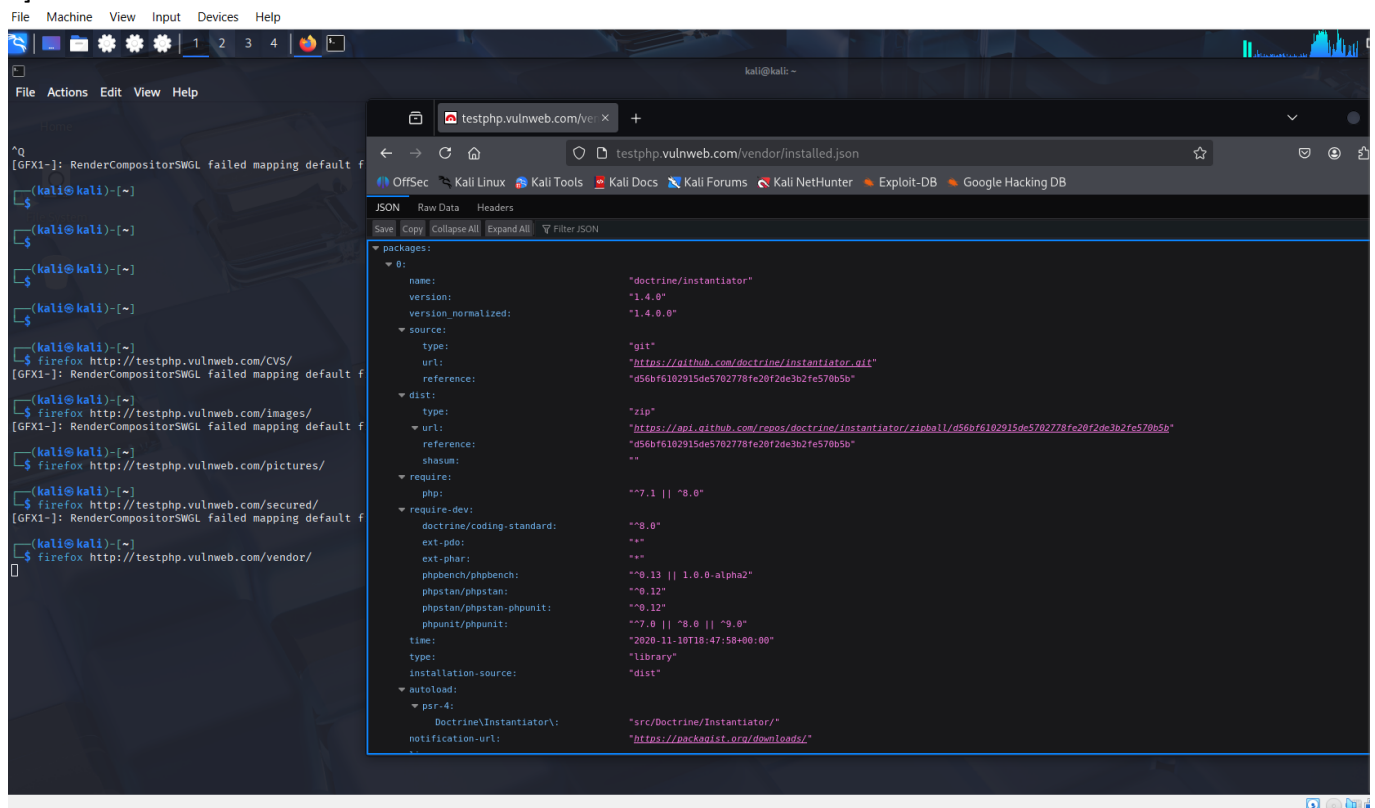
## 3]IMAGES



## 4] PICTURES



## 5] VENDOR





## CONCLUSIONS

- Sensitive and misconfigured directories like /admin, /secured, and /CVS were discovered, which could potentially be leveraged for further exploitation.
- 403 responses such as /cgi-bin/ suggest access control is in place, but these paths still exist and could be brute-forced or fuzzed further.
- Exposure of CVS version control files is a misconfiguration and may leak source code or file structure of the application.
- Crossdomain.xml should be examined to ensure it doesn't allow excessive cross-origin access.

This enumeration step is crucial for identifying attack surfaces and misconfigurations during web application assessments.