



UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 7

Website Directory Bruteforcing Using Dirb or Gobuster:

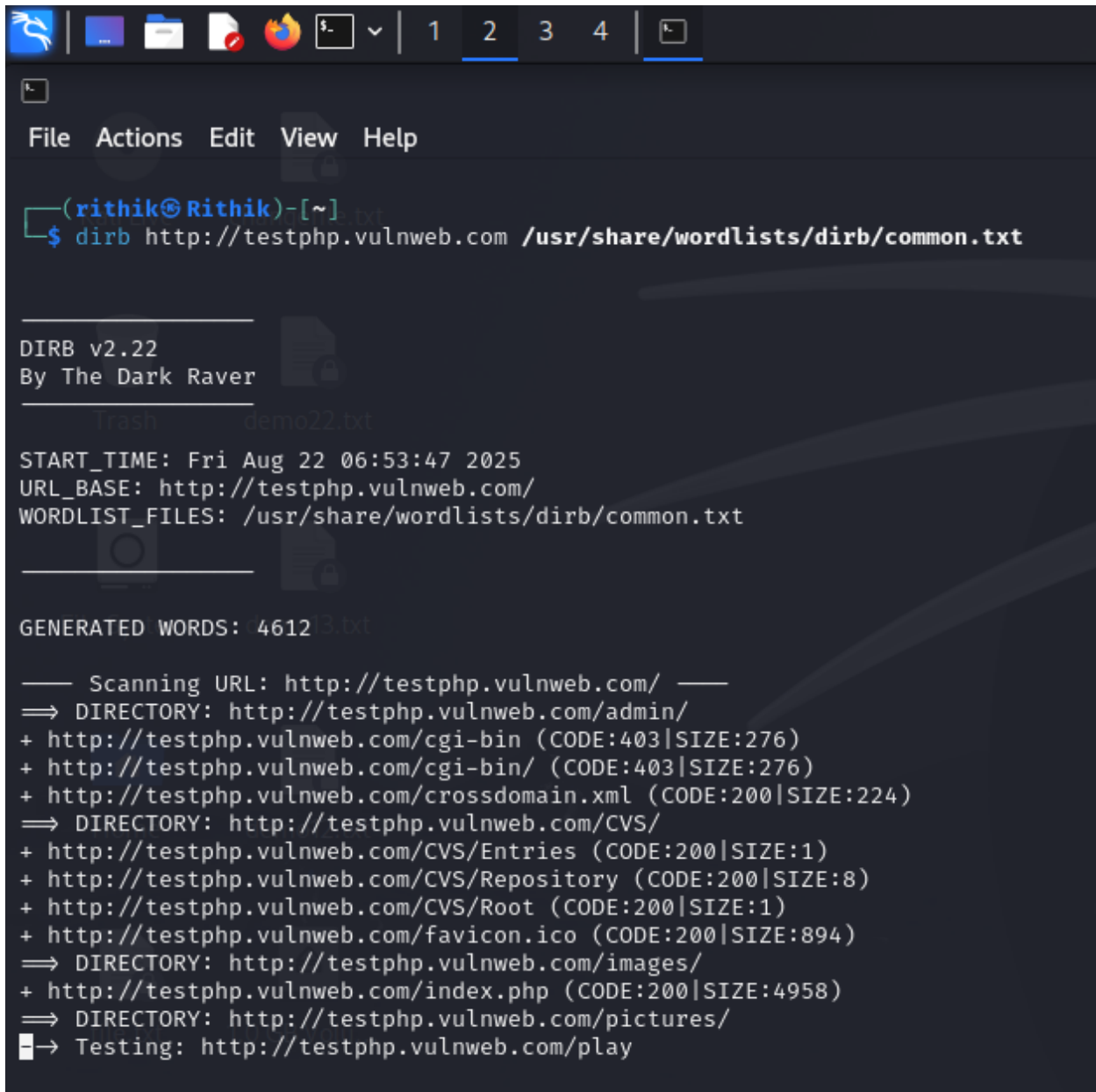
Understand and practically identify by scanning a target website for hidden directories or files using Dirb or Gobuster, which is a key step in web application penetration testing.

PRACTICAL DESCRIPTION

Problem:- *Explore a Linux machine To perform directory and file enumeration on a target website using Dirb or Gobuster, identifying hidden paths, admin panels, or unlisted resources — a key skill in ethical hacking and penetration testing*

Methodology used in *Practical Using Kali Linux* :

1. Using Drib:-

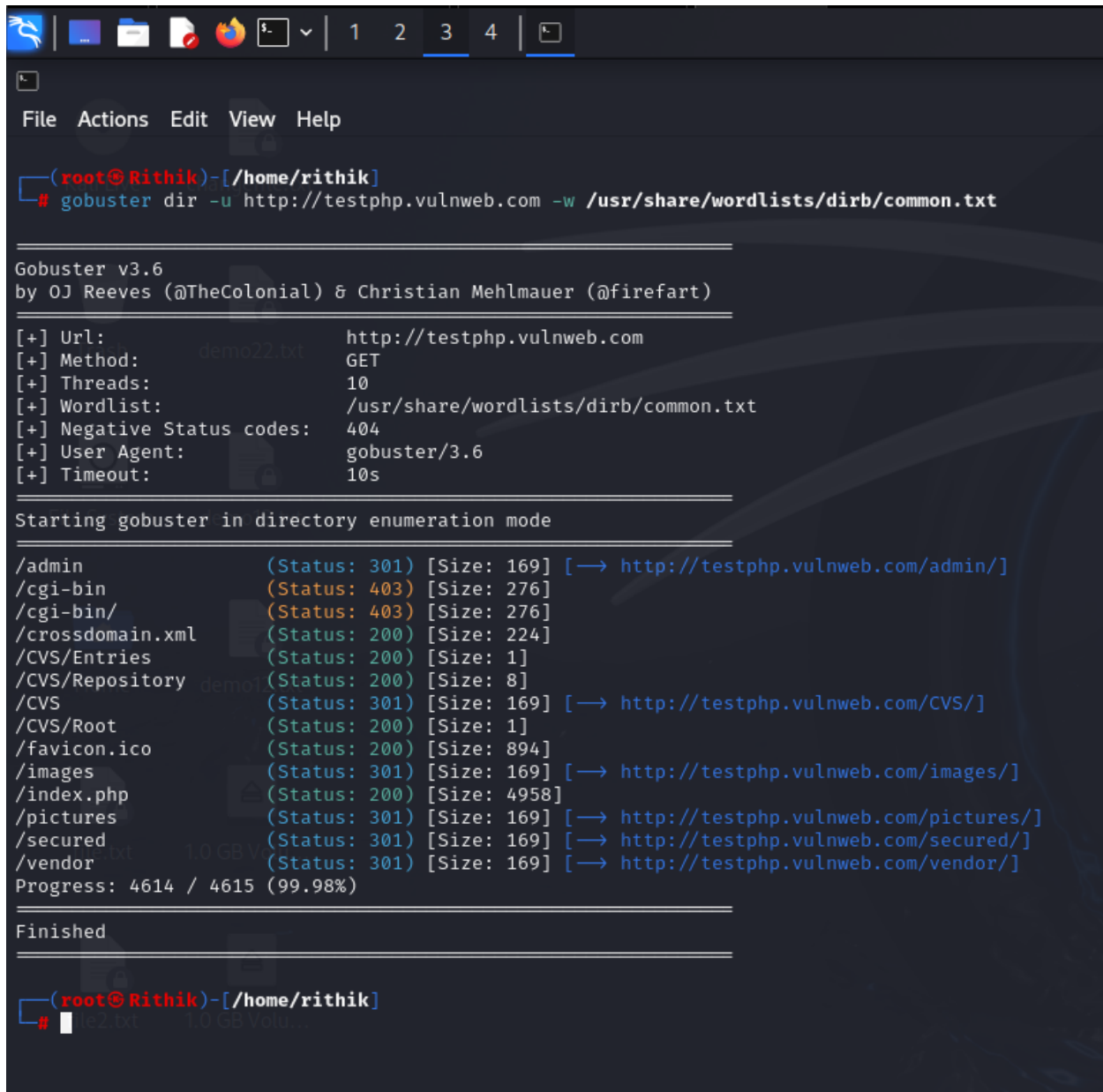


```
(rithik@Rithik)-[~]  
$ dirb http://testphp.vulnweb.com /usr/share/wordlists/dirb/common.txt  
  
_____  
Dirb v2.22  
By The Dark Raver  
_____  
Trash demo22.txt  
  
START_TIME: Fri Aug 22 06:53:47 2025  
URL_BASE: http://testphp.vulnweb.com/  
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt  
  
_____  
GENERATED WORDS: 4612  
  
— Scanning URL: http://testphp.vulnweb.com/ —  
⇒ DIRECTORY: http://testphp.vulnweb.com/admin/  
+ 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)  
⇒ DIRECTORY: http://testphp.vulnweb.com/pictures/  
→ Testing: http://testphp.vulnweb.com/play
```

Function: Dirb scans the website using a predefined wordlist and reports all accessible directories and files.

Dirb is simple and effective but slower compared to Gobuster.

2. Using Gobuster :-



```
(root@Rithik)-[/home/rithik]
# gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
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/3.6
[+] 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/Entries (Status: 200) [Size: 1]
/CVS/Repository (Status: 200) [Size: 8]
/CVS (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CVS/]
/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/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

(root@Rithik)-[/home/rithik]
```

Function: Gobuster performs high-speed directory brute-forcing using multithreading, making it faster than Dirb.

Gobuster is faster due to multithreading and supports different modes (DNS, VHOST, etc.).

Result:-

/admin → Admin panel (sensitive)

/backup → Backup files (may expose code)

/config → Configuration files (secrets)

/uploads → File upload functionality (can be exploited if insecure)

Conclusion :-

Website directory brute-forcing is an essential step in penetration testing. By using Dirb or Gobuster, security professionals can discover hidden resources that may pose security risks. Organizations should secure these directories with proper authentication, authorization, and access controls to prevent unauthorized access