Name: Aditya Baheti

Roll Number: 22BCE10521

Project Title: Web Vulnerability Scanning

Tools Used: Kali Linux**,** Nikto, Go buster.

Web Vulnerability Scanning

Lab Environment Setup

- To simulate the vulnerability scanning in a controlled environment, the following setup was created:
- **Host Machine:** Windows 11 (Laptop)
- **VM1 – Kali Linux:** Used as the attacker machine with tools like Nikto, Dirb, and What Web installed.
- **Network Mode:** Host-only Adapter (to ensure both VMs could communicate without internet exposure)
- **Key Tools Installed:** Nikto, Go Buster

Step-by-Step Implementation

Step 1: Initial Setup

- Launched Kali Linux and the internal web server VM.

Step 2: Tool Configuration

- Confirmed that Nikto, gobuster were pre-installed on Kali Linux.

Step 3: Execution – Scanning Begins

- Nikto Vulnerability Scan

Using command

```
nikto  -h http://testphp.vulnweb.com/
```

- For Gobuster scan

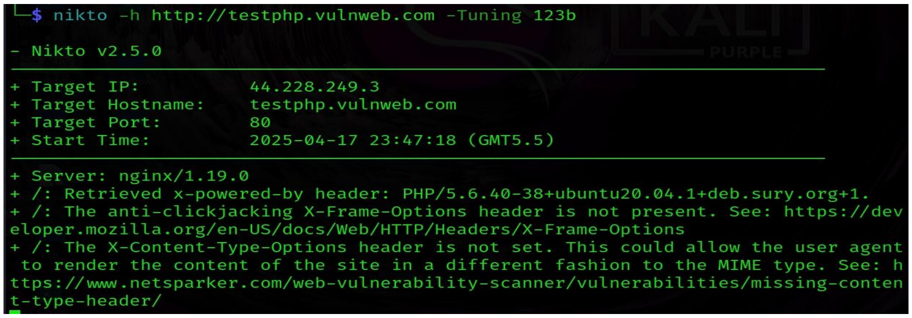
```
gobuster dir -uhttp://testphp.vulnweb.com/
```

-w /user/share/wordlists/dirbuster/directory-list-2.3-medium.txt

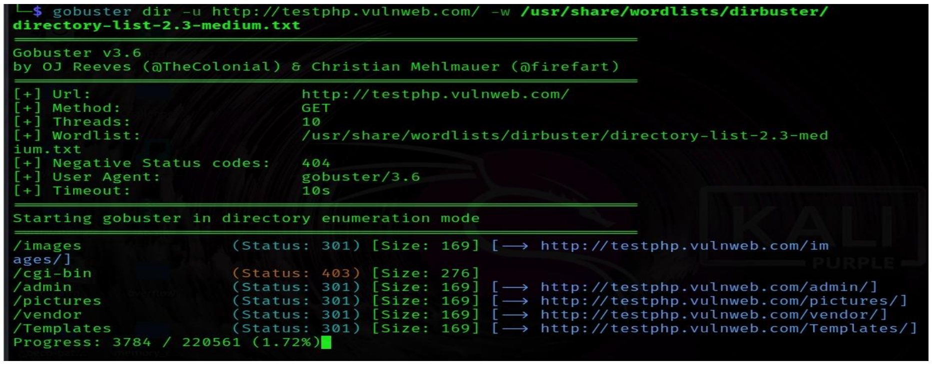
Step 4: Observation & Results

- **Nikto** confirmed the lack of security headers, directory indexing, and outdated software versions.

- GOBUSTER gives all the hidden directories in the given websites.



```
└─$ nikto -h http://testphp.vulnweb.com -Tuning 123b

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-04-17 23:47:18 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
 to render the content of the site in a different fashion to the MIME type. See: h
ttps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
t-type-header/
```



```
└─$ gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-med
ium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/im
ages/]
/cgi-bin              (Status: 403) [Size: 276]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/Templates            (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Templates/]
Progress: 3784 / 220561 (1.72%)
```

Observations & Findings

- The internal web server is running an outdated version of Apache and PHP.
- Several sensitive directories like `/admin` and `/backup` are publicly accessible.
- The server is missing critical security headers like `X-Frame-Options` and `Strict-Transport-Security`.
- Directory indexing is enabled, which exposes the internal file structure.

Challenges Faced

- Initial networking issues between the two VMs (fixed by switching to host-only adapter).
- Some scans took longer than expected due to low system resources.
- Output filtering in Dirb was initially overwhelming until I understood how to interpret status codes and sizes.

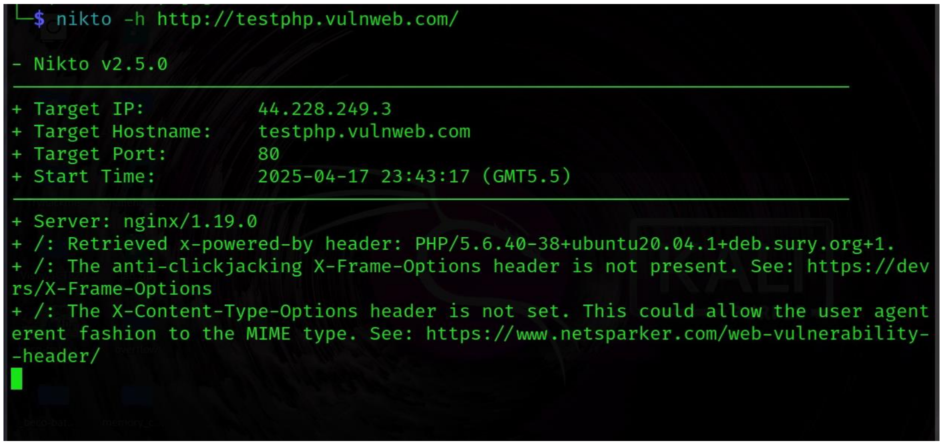
Security Recommendations

- Restrict access to sensitive directories through `.htaccess` or firewall rules.
- Update Apache and PHP to their latest stable versions.
- Implement HTTP security headers (`X-Frame-Options`, `Content-Security-Policy`, etc.).
- Disable directory listing on the web server.
- Conduct regular vulnerability scans before and after any major deployment.

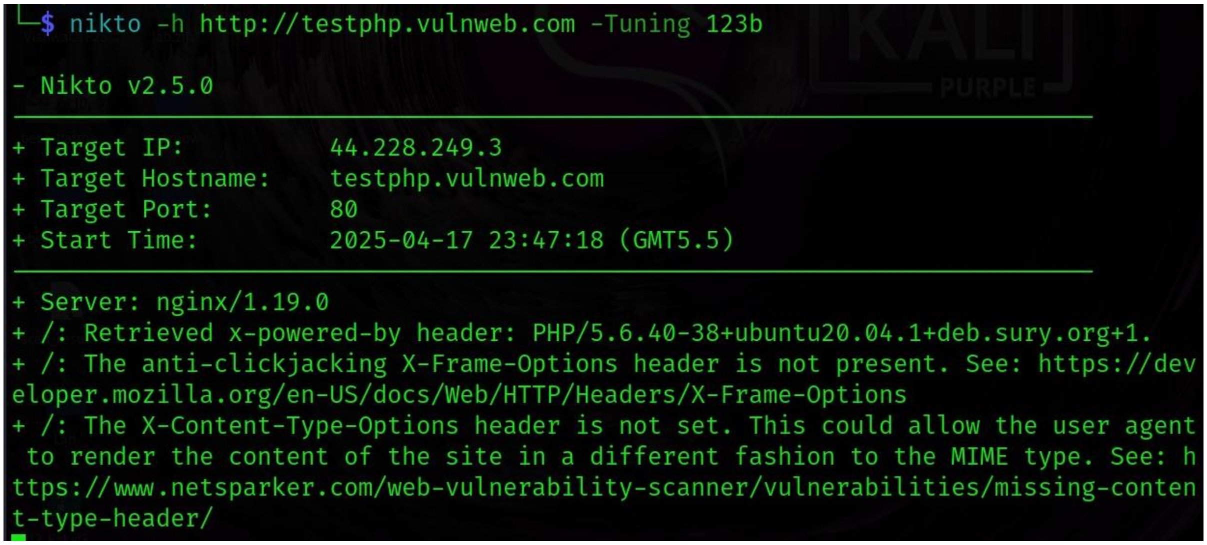
Final Deliverables

http://testphp.vulnweb.com/ is the website which is scanned .

Using Nikto the website is scanned for the vulnerability and security auditing below the website is scanned and some screenshots are there:

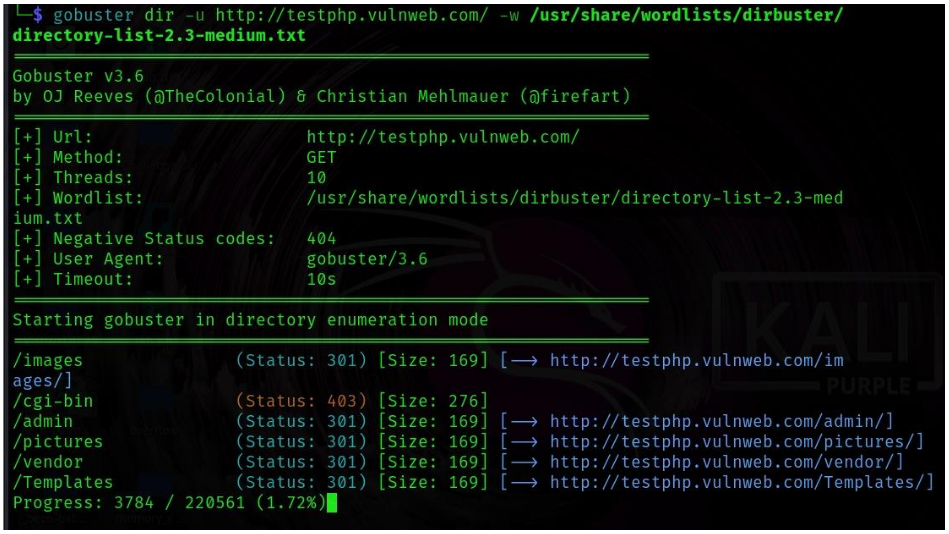


```
└─$ nikto -h http://testphp.vulnweb.com/

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-04-17 23:43:17 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
rs/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
-header/
```

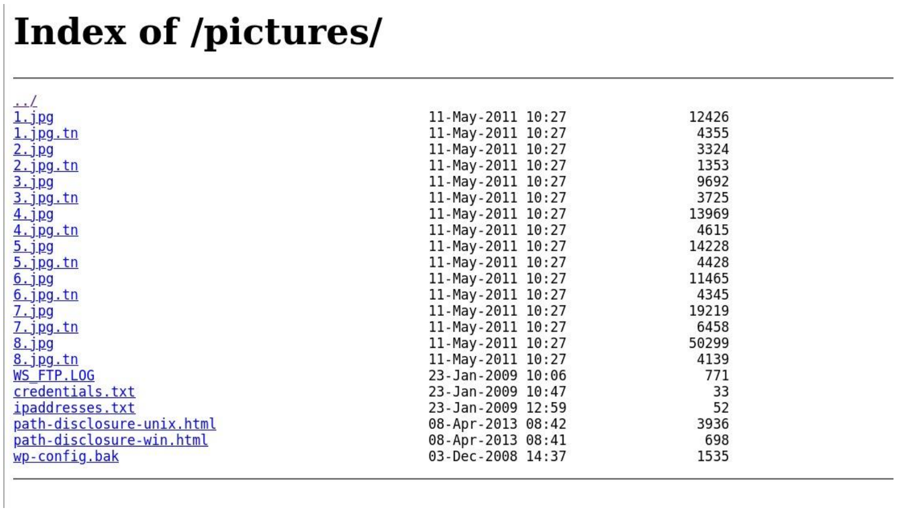


```
└─$ nikto -h http://testphp.vulnweb.com -Tuning 123b

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-04-17 23:47:18 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent
 to render the content of the site in a different fashion to the MIME type. See: h
ttps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
t-type-header/
```

Using the gobuster we got to know about the hidden directories of the web site below:

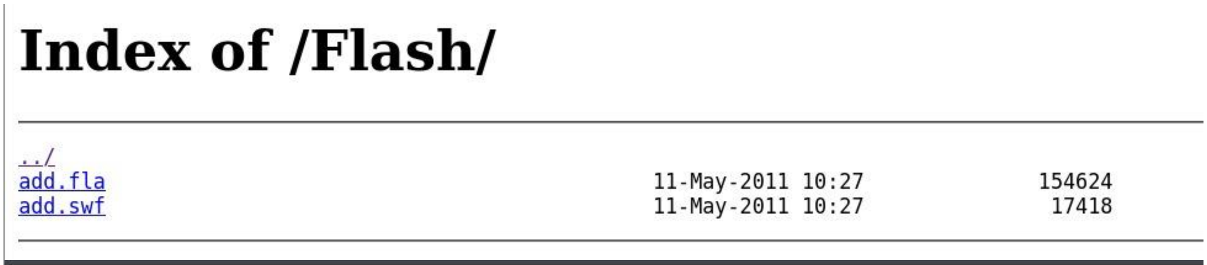


```
└─$ gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-med
ium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/im
ages/]
/cgi-bin              (Status: 403) [Size: 276]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/Templates            (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/Templates/]
Progress: 3784 / 220561 (1.72%)
```



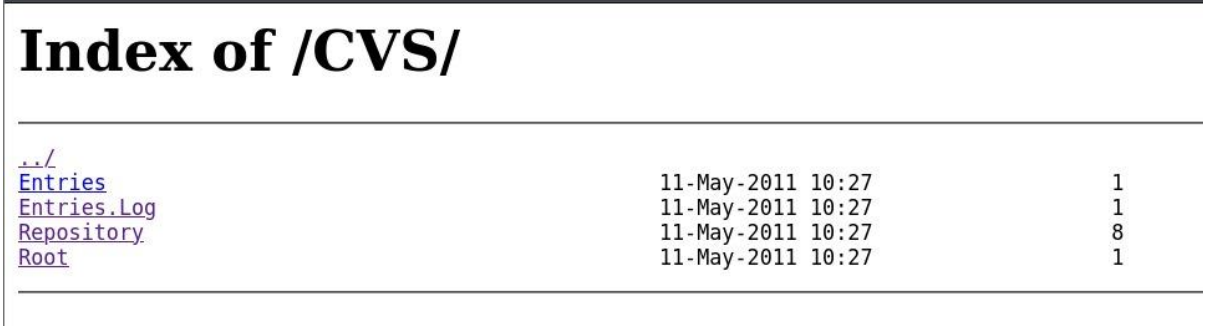
Index of /pictures/

```
../
1.jpg                                              11-May-2011 10:27               12426
1.jpg.tn                                           11-May-2011 10:27                4355
2.jpg                                              11-May-2011 10:27                3324
2.jpg.tn                                           11-May-2011 10:27                1353
3.jpg                                              11-May-2011 10:27                9692
3.jpg.tn                                           11-May-2011 10:27                3725
4.jpg                                              11-May-2011 10:27               13969
4.jpg.tn                                           11-May-2011 10:27                4615
5.jpg                                              11-May-2011 10:27               14228
5.jpg.tn                                           11-May-2011 10:27                4428
6.jpg                                              11-May-2011 10:27               11465
6.jpg.tn                                           11-May-2011 10:27                4345
7.jpg                                              11-May-2011 10:27               19219
7.jpg.tn                                           11-May-2011 10:27                6458
8.jpg                                              11-May-2011 10:27               50299
8.jpg.tn                                           11-May-2011 10:27                4139
WS_FTP.LOG                                         23-Jan-2009 10:06                 771
credentials.txt                                    23-Jan-2009 10:47                  33
ipaddresses.txt                                    23-Jan-2009 12:59                  52
path-disclosure-unix.html                          08-Apr-2013 08:42                3936
path-disclosure-win.html                           08-Apr-2013 08:41                 698
wp-config.bak                                      03-Dec-2008 14:37                1535
```



Index of /Flash/

```
../
add.fla                                            11-May-2011 10:27              154624
add.swf                                            11-May-2011 10:27               17418
```



Index of /CVS/

```
../
Entries                                            11-May-2011 10:27                   1
Entries.Log                                        11-May-2011 10:27                   1
Repository                                         11-May-2011 10:27                   8
Root                                               11-May-2011 10:27                   1
```

Conclusion

This project gave me hands-on experience in performing basic vulnerability assessments of a web application. I learned how simple tools can reveal critical weaknesses even in internal apps. It emphasized the importance of proactive scanning and secure configuration. These skills are directly applicable to real-world cybersecurity practices, ethical hacking.