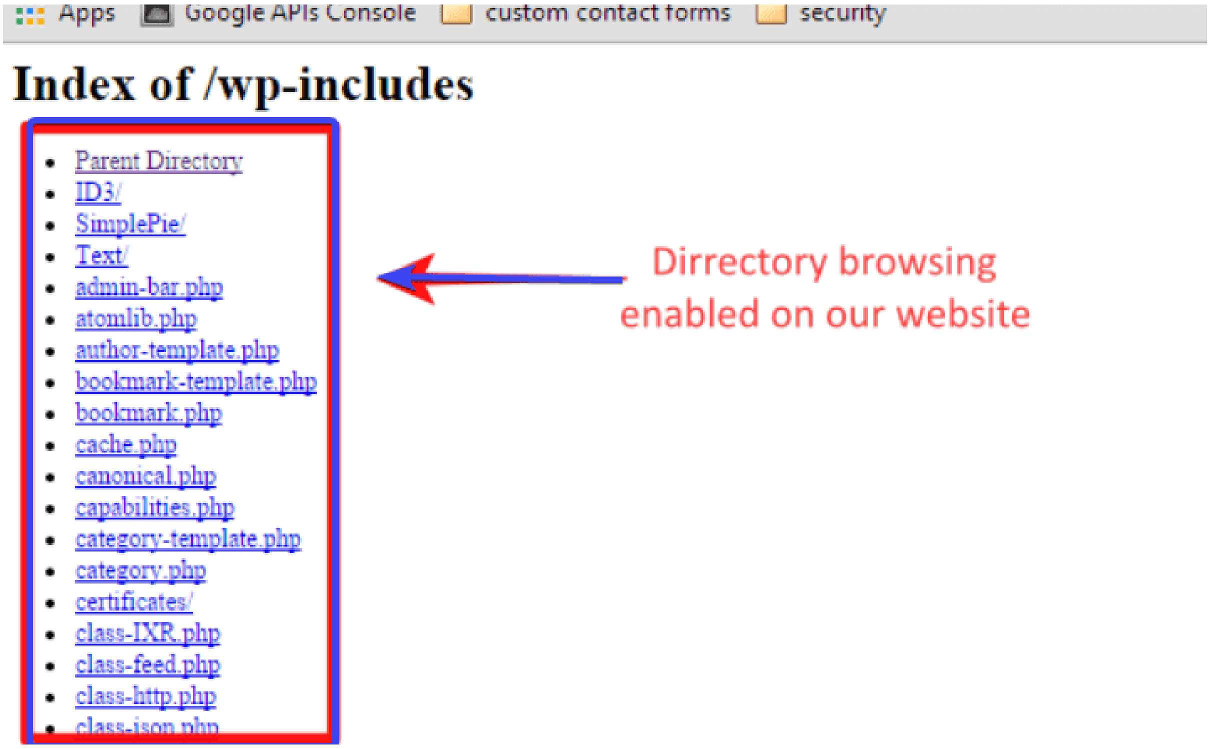
Directory Listing or Open directory

#Session_Task_15 by Sukhveer singh

1. What is Directory Listing or Open directory –



Index of /wp-includes

- Parent Directory
- ID3/
- SimplePie/
- Text/
- admin-bar.php
- atomlib.php
- author-template.php
- bookmark-template.php
- bookmark.php
- cache.php
- canonical.php
- capabilities.php
- category-template.php
- category.php
- certificates/
- class-IXR.php
- class-feed.php
- class-http.php
- class-json.php

Dirrectory browsing enabled on our website

Directory Listing, also known as Open Directory, is a vulnerability in web servers that allows users to view the contents of directories on a website. When Directory Listing is enabled, if a directory does not contain an index file (like index.html or index.php), the web server will display a list of all files and folders within that directory. This can pose a security risk as it may expose sensitive information to attackers, such as configuration files, source code, or other confidential data. Attackers can exploit Directory Listing to gather information about the structure and contents of a website, which could be used for further attacks or exploitation. It's important for website administrators to disable Directory Listing to prevent unauthorized access to directory contents.

2. How do we find it? –

How to find out Directory Listing VULNERABILITY ?

- **Using browser developer tools:** Inspect the network requests and responses while navigating through a website. Look for directory paths in the responses that reveal directory listing.

- **Using search engines:** Enter specific search queries in search engines like Google, Bing, or Shodan, targeting known directory listing structures. Websites with Directory Listing enabled may appear in search results, revealing their vulnerable directories.

- **Using online tools:** Several online tools and websites offer directory scanning services. You can input a website URL, and these tools will scan and report any directories that have listing enabled.

- **Analyzing server response headers:** Check the server response headers using tools like curl or browser extensions. Look for headers like "X-Directory-Listing" or "X-Directories-Exposed" which might indicate Directory Listing vulnerability.

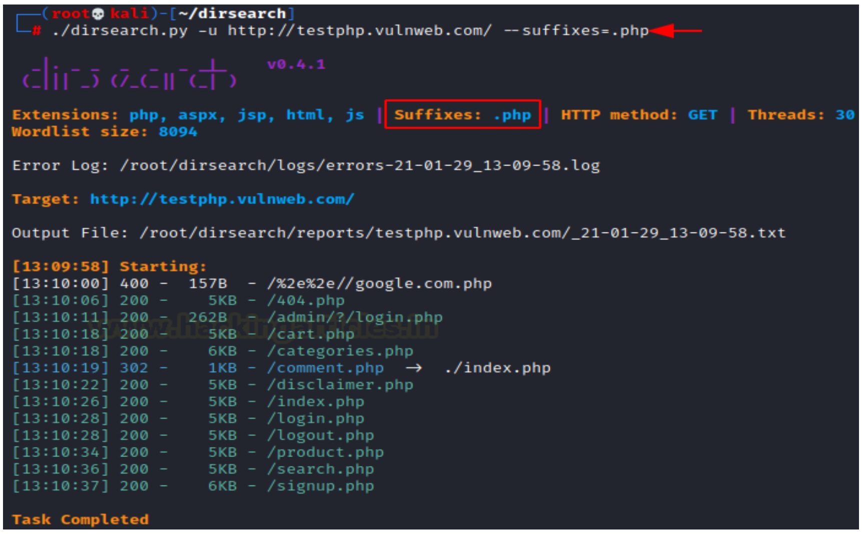
- **Analyzing error messages:** Sometimes, accessing non-existent directories or files may generate error messages that inadvertently reveal directory listings. Analyze these error messages to identify if Directory Listing is enabled.

3. Tools –

i. Kali linux tools –

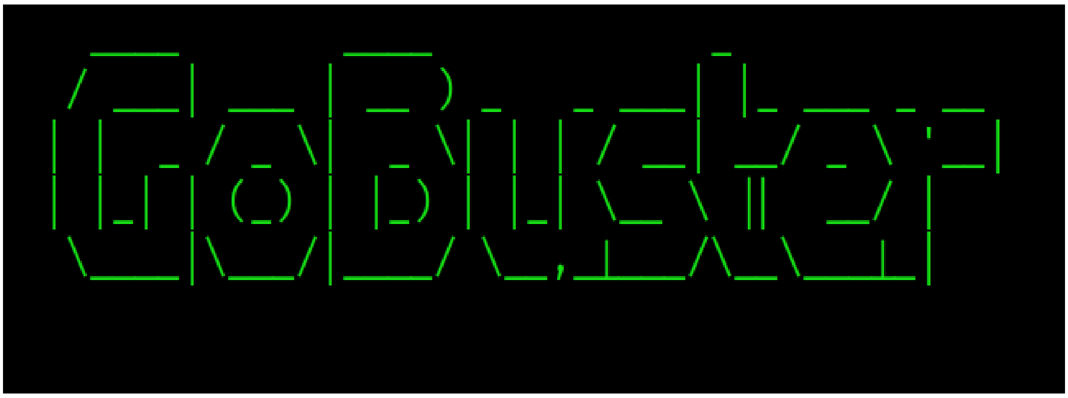
- **DirBuster:** DirBuster is a directory brute-forcing tool that comes pre-installed in Kali Linux. It can be used to discover hidden directories and files on a web server, including those with Directory Listing enabled.

- **DirSearch:** Another directory brute-forcing tool available in Kali Linux. It searches for hidden directories and files by using a predefined wordlist.



```
┌──(root💀 kali)-[~/dirsearch]
└─# ./dirsearch.py -u http://testphp.vulnweb.com/ --suffixes=.php

                                v0.4.1

Extensions: php, aspx, jsp, html, js | Suffixes: .php | HTTP method: GET | Threads: 30
Wordlist size: 8094

Error Log: /root/dirsearch/logs/errors-21-01-29_13-09-58.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_13-09-58.txt

[13:09:58] Starting:
[13:10:00] 400 -  157B  - /%2e%2e//google.com.php
[13:10:06] 200 -    5KB - /404.php
[13:10:11] 200 -  262B  - /admin/?/login.php
[13:10:18] 200 -    5KB - /cart.php
[13:10:18] 200 -    6KB - /categories.php
[13:10:19] 302 -    1KB - /comment.php  →  ./index.php
[13:10:22] 200 -    5KB - /disclaimer.php
[13:10:26] 200 -    5KB - /index.php
[13:10:28] 200 -    5KB - /login.php
[13:10:28] 200 -    5KB - /logout.php
[13:10:34] 200 -    5KB - /product.php
[13:10:36] 200 -    5KB - /search.php
[13:10:37] 200 -    6KB - /signup.php

Task Completed
```

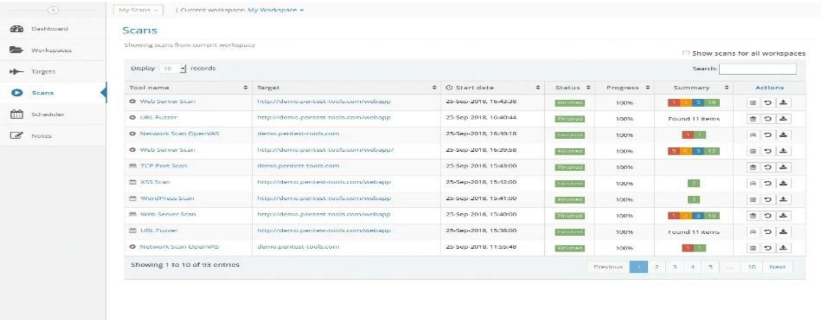
- **Gobuster:** Gobuster is a directory and file brute-forcing tool that comes with Kali Linux. It can be used to discover directories and files on web servers, including those with Directory Listing enabled.



ii. Online tools –

- **Recon-ng:** Recon-ng is a reconnaissance framework that includes various modules for information gathering. It can be used to find Directory Listing vulnerabilities by leveraging its web-based reconnaissance modules.

- **Pentest-Tools.com:** This online platform offers a variety of tools and services for penetration testing. It includes directory scanning tools that can help identify Directory Listing vulnerabilities on websites.



Scans

Showing scans from current workspace

□ Show scans for all workspaces

Display 10 records

Search:

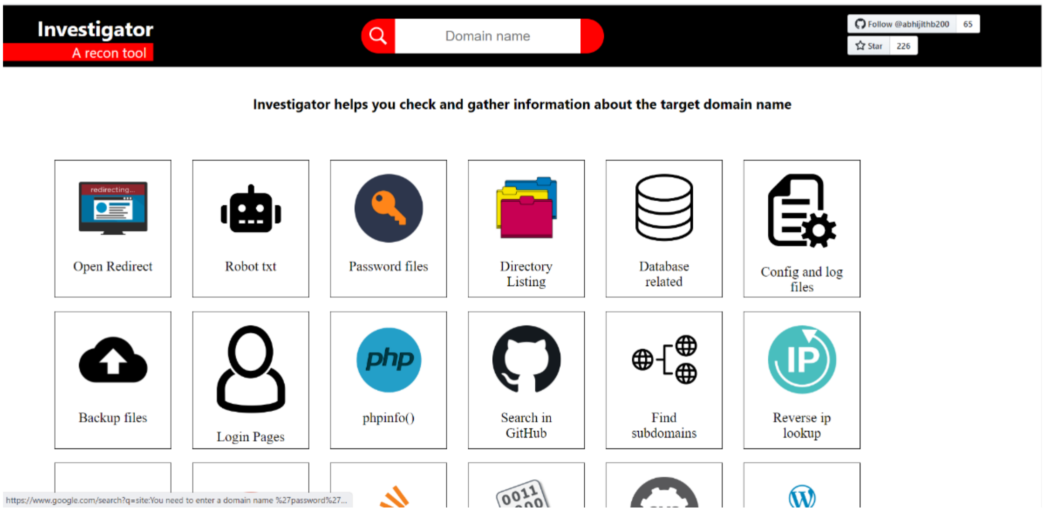
Tool name	Target	Start date	Status	Progress	Summary	Actions
Web Server Scan	http://demo.pentest-tools.com/webapp	25-Sep-2018, 16:43:38	Finished	100%	1 1 3 19	
URL Fuzzer	http://demo.pentest-tools.com/webapp	25-Sep-2018, 16:40:44	Finished	100%	Found 11 items	
Network Scan OpenVAS	demo.pentest-tools.com	25-Sep-2018, 16:40:18	Finished	100%	1 1	
Web Server Scan	http://demo.pentest-tools.com/webapp/	25-Sep-2018, 16:39:58	Finished	100%	5 6 3 12	
TCP Port Scan	demo.pentest-tools.com	25-Sep-2018, 15:43:00	Finished	100%		
XSS Scan	http://demo.pentest-tools.com/webapp	25-Sep-2018, 15:42:00	Finished	100%	2	
WordPress Scan	http://demo.pentest-tools.com/webapp	25-Sep-2018, 15:41:00	Finished	100%	1	
Web Server Scan	http://demo.pentest-tools.com/webapp	25-Sep-2018, 15:40:00	Finished	100%	1 2 3 10	
URL Fuzzer	http://demo.pentest-tools.com/webapp	25-Sep-2018, 15:38:00	Finished	100%	Found 11 items	
Network Scan OpenVAS	demo.pentest-tools.com	25-Sep-2018, 11:55:48	Finished	100%	1 1	

Showing 1 to 10 of 93 entries

- **PunkSPIDER:** PunkSPIDER is a global web application vulnerability search engine that can scan websites for various vulnerabilities, including Directory Listing. Users can search for vulnerable sites and directories through its interface.

- **Nikto:** Nikto is an open-source web server scanner that can detect various vulnerabilities, including Directory Listing. While it's not solely focused on this vulnerability, it can still help identify it among other issues.

- **Investigator Tool:** The Investigator is a web-based tool designed for website reconnaissance and vulnerability scanning. It includes features for discovering various vulnerabilities, including Directory Listing. Users can input website URLs into the tool to scan for vulnerabilities and identify Directory Listing issues.



Investigator helps you check and gather information about the target domain name

4. Mitigations –

- **Disable Directory Listing:** The most effective mitigation is to disable Directory Listing on the web server. This can typically be done by configuring the server to return a 403 Forbidden error or by configuring default index files for directories.

- **Configure Index Files:** Ensure that each directory on the web server contains an index file (e.g., index.html, index.php) to prevent the server from listing directory contents when no index file is present.

- **Review Web Server Configuration:** Regularly review and update the configuration of the web server to ensure that Directory Listing is disabled by default and that new directories are properly configured to prevent listing.

- **Implement Access Controls:** Utilize access controls, such as .htaccess files (for Apache servers) or web.config files (for IIS servers), to restrict access to sensitive directories and files, even if Directory Listing is enabled.

- **Regular Security Audits:** Conduct regular security audits and vulnerability scans to identify any instances of Directory Listing and promptly address them. This can help ensure that the vulnerability is mitigated across all web servers and applications.

- **Educate Developers and Administrators:** Provide training and guidance to developers and administrators on the risks associated with Directory Listing and the importance of properly configuring web servers to prevent it

5. References –

- ✓ https://www.invicti.com/learn/directory-listing/
- ✓ https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/
- ✓ https://sapt.medium.com/directory-listing-vulnerability-cyber-sapiens-internship-task-16-fca5c9a4bb8a
- ✓ https://probely.com/vulnerabilities/directory-listing
- ✓ https://abhijithb200.github.io/investigator/