Cheatography

Nikto Cheat Sheet

by milo.skoro via cheatography.com/203406/cs/43318/

Scan options

–host	Scan host
-port	Scan host targeting specific ports
-maxtime	Define maximum scan time
-until	Scan duration
-vhost	Define host header
-ssl	to use SSL
-dbcheck	Check database
-output	output results into specified file
-ipv4	Ipv4 only
-ipv6	Ipv6 only
-list--plugins	List all available plugins
-nolookup	Disables DNS lookups
-nossl	Disables the use of ssl

Mutate Options

-mutate<#>	1 - Test all files with all root directories
	2 - Guess for password file names
	3 - Enumerate usernames via Apache
	4 - Enumerate usernames via cgiwrap
	5 - Attempt to brute force sub-domain names
	6 - Attempt to guess directory names form the supplied dictionary file

-mutate4 > assumes that the host name is the parent domain

Display Options

-Display<#>	1 - Display redirects
	2 - Display cookies
	3 - Display 200 ok response
	4 - Display Web URLs requiring authentication
-Display<letter>	D - Display debug output
	E - Show HTTP errors
	P - Print to STDOUT
	V - Verbose output display

Output Options

-Format	csv - Comma Separated Value
	htm - HTML Format
	txt - Plain text
	xml - XML Format

Evasion Options

-evasion<#>	1 - Random URI encoding (non-UTF8)
	2 - Directory self-reference
	3 - Premature URL ending
	4 - Prepend long random string
	5 - Fake parameter
	6 - TAB as request spacer
	7 - Change the case of the URL
	8 - Use Windows directory separator (\)

Tuning Options

-tuning<#>	0 - Upload files
	1 - View specific file in log
	2 - Default file misconfiguration
	3 - Display information disclosure
	4 - Injection (XSS/Script/-HTML)
	5 - Remote File Retrieval
	6 - Denial of Service
	7 - Remote File Retrieval - Server Wide
	8 - Remote Shell
	9 - SQL Injection
-tuning<letter>	a - Authentication Bypass
	b - Software Identification
	c - Remote Source Inclusion
	x - Reverse Tuning Options

By **milo.skoro**
cheatography.com/milo-skoro/

Published 6th May, 2024.
Last updated 6th May, 2024.