Nikto Cheat Sheet

by fool via cheatography.com/218112/cs/48118/

Target Options

Specify host	nikto -h <IP/domain>
Specify port	nikto -h <IP/domain> -p <port>
Multiple ports	nikto -h <IP/domain> -p <port1>,<port2>,etc
Specify port in url	nikto -h http(s)://<IP/domain>:<port>

Tuning Options

Specify tuning	-Tuning <option>
Interesting File / Seen in logs	1
Misconfiguration / Default File	2
Information Disclosure	3
Injection (XSS/Script/HTML)	4
Remote File Retrieval - Inside Web Root	5
Denial of Service	6
Remote File Retrieval - Server Wide	7
Command Execution / Remote Shell	8
SQL Injection	9
File Upload	0
Authentication Bypass	a
Software Identification	b
Remote Source Inclusion	c
WebService	d
Administrative Console	e
Reverse (all but specified)	x

Evasion Options

Specify technique	-evasion <optio-n>
Random URI encoding (non-UTF8)	1
Directory self-reference (/./)	2
Premature URL ending	3
Prepend long random string	4
Fake parameter	5
TAB as request spacer	6
Change the case of the URL	7
Use Windows directory separator (\)	8
Use a carriage return (0x0d) as a request spacer	A
Use binary value 0x0b as a request spacer	B

Display Options

Toggle display outputs	-Display <option>
Show redirects	1
Show cookies received	2
Show all 200/OK responses	3
Show URLs which require authentication	4
Debug output	D
Display all HTTP errors	E
Print progress to STDOUT	P
Scrub output of IPs and hostnames	S
Verbose output	V

File Output Options

Output file	-o <filename or . for auto name>
Specify format	-Format <format>
Available formats	csv
	json
	htm (HTML)
	txt
	xml

If format is left unspecified, it will be determined by the extension used in the output filename. Format can also be specified with plugins.

Plugin Examples

-plugin dictionary	Use a dictionary attack to enumerate directories and files
-plugin robots	Check robots.txt for paths to pass to other scripts
-plugin cgi	Check for CGI vulnerabilities
-plugin sitefiles	look for files based on the sites IP or name

Plugins Usage

List plugins	nikto --list-plugins
Specify plugin	-Plugin <plugin name>