Nikto Cheat Sheet

by sinnert via cheatography.com/184781/cs/38587/

Installation & Getting Started

Website	https://github.com/sullo/nikto.git
Install	git clone https://github.com/sullo/nikto.git
Kali	apt install nikto

Commands

nikto -H, -Help	Help options
-ask+	yes Ask about each (default). no Don't ask don't send. auto Don't ask, just send
-Cgidirs+	Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a"
-config+	Use this config file
-Display+ # or letter	Turn on/off display outlets. 1 Show redirects. 3 Show all 200/OK responses 4 Show URLs which require authentication D Debug output E Display all HTTP errors P Print progress to STDOUT S Scrub output of IPs and hostnames V Verbose output
-dbcheck	Check database and other key files for syntax errors
-evasions+ # or letter	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 (\) A Use a carriage return (0x0d) as a request spacer B Use binary value 0x0b as a request spacer

Commands (cont)

-Format+	Save file (-o) format: csv Comma-separated-value htm HTML Format msf+ Log to Metasploit nbe Nessus NBE format txt Plain text xml XML Format (if not specified the format will be taken from the file extension passed to -output)
-host+	Target host
-list--plugins	List all available plugins, perform no testing
-maxtime+	Maximum testing time per host
-mutate-options	Provide information for mutates
-nolookup	Disables DNS lookups
-nossl	Disables the use of SSL
-no404	Disables nikto attempting to guess a 404 page
-output+	Write output to this file ('.' for auto-name)
-port+	Port to use (default 80)
-root+	Prepend root value to all requests, format is /directory
-Save	Save positive responses to this directory ('.' for auto-name)
-ssl	Force ssl mode on port

Commands (cont)

-Tuning+ # or letter	Scan tuning: 1 Interesting File / Seen in logs 2 Misconfiguration / Default File 3 Information Disclosure 4 Injection (XSS/Script/HTML) 5 Remote File Retrieval - Inside Web Root 6 Denial of Service 7 Remote File Retrieval - Server Wide 8 Command Execution / Remote Shell 9 SQL Injection 0 File Upload a Authentication Bypass b Software Identification c Remote Source Inclusion x Reverse Tuning Options (i.e., include all except specified)
-timeout+	Timeout for requests (default 10 seconds)
-until	Run until the specified time or duration
-vhost+	Virtual host (for Host header)