

### Testing

Single Port	Host/IP	nikto -h 192.168.0.1
	Specify Port	nikto -h 192.168.0.1 -p 443
	URL/PORT	nikto -h <a href="https://192.168.0.1:443/">https://192.168.0.1:443/</a>
	SSL	nikto -h 192.168.0.1 -p 443 -ssl
Multiple Ports	Same Host	nikto -h 192.168.0.1 -p 80,88,443
	Multiple Host via .txt	192.168.0.1:80
		<a href="http://192.168.0.1:8080/">http://192.168.0.1:8080/</a>
		192.168.0.3

### Annotated Option List

#### -Display+

- |                             |  |
|-----------------------------|--|
| 1 Show redirects            | 2 Show cookies received                  |
| 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            |  |

#### -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 (\\)      |
| A Use a carriage return (0x0d) as a request spacer | B Use binary value 0x0b as a request spacer |

#### -Help Help File

-list-- plugins List all available plugins, perform no testing

#### -mutate+

- Guess additional file names:
- |   |   |
|---|---|
| 1 Test all files with all root directories  | 2 Guess for password file names   |
| 3 Enumerate user names via Apache (/~user type requests)                                  | 4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests) |
| 5 Attempt to brute force sub-domain names, assume that the host name is the parent domain | 6 Attempt to guess directory names from the supplied dictionary file      |

#### -mutate-o-ptions

Provide information for mutates

#### -port+

Port to use (default 80)

#### -Tuning+

Scan tuning:

- |                                   |                                   |
|-----------------------------------|-----------------------------------|
| 1 Interesting File / Seen in logs | 2 Misconfiguration / Default File |
|-----------------------------------|-----------------------------------|



### Annotated Option List (cont)

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	d Webservice
e Administrative Console	x Reverse Tuning Options (i.e., include all except specified)

### Scan Tuning

-Tuning	0 File Upload	1 Interesting File/ Seen in Logs
	2 Misconfiguration/Default File	3 Information Disclosure
	4 Injection	5 Remote File Retrieval - Web
	6 Denial of Service	7 Remote File Retrieval - Server
	8 Command Execution / Remote Shell	9 SQL Injection
	a Auth Bypass	b Software ID
	c Remote Source	x Reverse Tuning

## Using a Proxy

Via Command Line	Via nikto.conf
./nikto.pl -h localhost -useproxy http://localhost:8080/	PROXYHOST= PROXYPORT= PROXYUSER= PROXYPASS=  perl nikto.pl -h localhost -p 80 -useproxy

## Debugging & Updating

Debugging -Display v (verbose) d (debug)  
Updating git pull

## Interactive Features

SPACE - Report current scan status  
v - Turn verbose mode on/off  
d - Turn debug mode on/off  
e - Turn error reporting on/off  
p - Turn progress reporting on/off  
r - Turn 3xx/redirect display on/off  
c - Turn cookie display on/off  
o - Turn 200/OK display on/off  
a - Turn auth display on/off  
q - Quit (gracefully)  
N - Next host/post  
P - Pause



By [r.taylor27](https://cheatography.com/r-taylor27/)  
[cheatography.com/r-taylor27/](https://cheatography.com/r-taylor27/)

Published 6th May, 2024.  
Last updated 6th May, 2024.  
Page 3 of 3.

Sponsored by [Readable.com](https://readable.com)  
Measure your website readability!  
<https://readable.com>