

```

File Actions Edit View Help
(kali@kali)-[~]
$ nikto -h www.saveetha.com -tuning x
Unknown option: tuning

Options:
  -ask+                Whether to ask about submitting updates
                        yes   Ask about each (default)
                        no   Don't ask, don't send
                        auto Don't ask, just send
  -check6              Check if IPv6 is working (connects to ipv6.google.
                        com or value set in nikto.conf)
  -Cgидirs+            Scan these CGI dirs: "none", "all", or values like
                        "/cgi/" /cgi-a/"
  -config+             Use this config file
  -Display+            Turn on/off display outputs:
                        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
  -dbcheck             Check database and other key files for syntax error
  -evasion+            Encoding technique:
                        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
                        B     Use binary value 0x0b as a request space
  -followredirects     Follow 3xx redirects to new location
  -Format+             Save file (-o) format:
                        csv   Comma-separated-value
                        json  JSON Format
                        htm   HTML Format
                        nbe   Nessus NBE format
                        sql   Generic SQL (see docs for schema)
                        txt   Plain text
                        xml   XML Format
                        (if not specified the format will be taken from
                        the file extension passed to -output)
  -Help               This help information
  -host+              Target host/URL

```

```
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
(kali@kali)-[~]
$ nikto -h www.saveetha.com -tuning x
Unknown option: tuning

Options:
  -ask+                Whether to ask about submitting updates
                        yes  Ask about each (default)
                        no   Don't ask, don't send
                        auto Don't ask, just send
  -check6              Check if IPV6 is working (connects to ipv6.google.
                        com or value set in nikto.conf)
  -Cgidirs+            Scan these CGI dirs: "none", "all", or values like
                        "/cgi/ /cgi-a/"
  -config+             Use this config file
  -Display+            Turn on/off display outputs:
                        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
  -dbcheck             Check database and other key files for syntax error
  -evasion+            Encoding technique:
                        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
                        B    Use binary value 0x0b as a request space
  -followredirects     Follow 3xx redirects to new location
  -Format+             Save file (-o) format:
                        csv  Comma-separated-value
                        json JSON Format
                        htm  HTML Format
                        nbe  Nessus NBE format
                        sql  Generic SQL (see docs for schema)
                        txt  Plain text
                        xml  XML Format
                        (if not specified the format will be taken from
                        the file extension passed to -output)
  -Help               This help information
  -host+              Target host/URL
```

```
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
-host+ Target host/URL
-id+ Host authentication to use, format is id:pass or id
:pass:realm
-ipv4 IPv4 Only
-ipv6 IPv6 Only
-key+ Client certificate key file
-list-plugins List all available plugins, perform no testing
-maxtime+ Maximum testing time per host (e.g., 1h, 60m, 3600s)
) File System
-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-b
in/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 th
e supplied dictionary file
-mutate-options Provide information for mutates
-nointeractive Disables interactive features
-nolookup Disables DNS lookups
-nossl Disables the use of SSL
-noslash Strip trailing slash from URL (e.g., '/admin/' to '
/admin')
-no404 Disables nikto attempting to guess a 404 page
-Option Over-ride an option in nikto.conf, can be issued mu
ltiple times
-output+ Write output to this file ('.' for auto-name)
-Pause+ Pause between tests (seconds)
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-RSAcert+ Client certificate file
-root+ Prepend root value to all requests, format is /dire
ctory
-Save Save positive responses to this directory ('.' for
auto-name)
-ssl Force ssl mode on port
-Tuning+ 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
```



```

File Actions Edit View Help

Trash

l except specified)
  -timeout+ Timeout for requests (default 10 seconds)
  -Userdbs Load only user databases, not the standard database
s File System
  all Disable standard dbs and load only user
dbs
  tests Disable only db_tests and load udb_tests
  -useragent Over-rides the default useragent
  -until Run until the specified time or duration
  -url+ Target host/URL (alias of -host)
  -usecookies Use cookies from responses in future requests
  -useproxy Use the proxy defined in nikto.conf, or argument ht
tp://server:port
  -Version Print plugin and database versions
  -vhost+ Virtual host (for Host header)
  -404code Ignore these HTTP codes as negative responses (alwa
ys). Format is "302,301".
  -404string Ignore this string in response body content as nega
tive response (always). Can be a regular expression.
    + requires a value

(kali㉿kali)-[~]
$ nikto -h www.saveetha.com -tuning x
Unknown option: tuning

Options:
  -ask+ Whether to ask about submitting updates
        yes Ask about each (default)
        no Don't ask, don't send
        auto Don't ask, just send
  -check6 Check if IPv6 is working (connects to ipv6.google.
com or value set in nikto.conf)
  -Cgidirs+ Scan these CGI dirs: "none", "all", or values like
"/cgi/ /cgi-a/"
  -config+ Use this config file
  -Display+ Turn on/off display outputs:
        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
  -dbcheck Check database and other key files for syntax error

```

```
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
- dbcheck Check database and other key files for syntax error
s - evasion+ Encoding technique:
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
r - followredirects Follow 3xx redirects to new location
- Format+ Save file (-o) format:
csv Comma-separated-value
json JSON Format
htm HTML Format
nbe Nessus NBE format
sql Generic SQL (see docs for schema)
txt Plain text
xml XML Format
(if not specified the format will be taken from the file extension passed to -output)
- Help This help information
- host+ Target host/URL
- id+ Host authentication to use, format is id:pass or id:pass:realm
- ipv4 IPv4 Only
- ipv6 IPv6 Only
- key+ Client certificate key file
- list-plugins List all available plugins, perform no testing
- maxtime+ Maximum testing time per host (e.g., 1h, 60m, 3600s)
)
- 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-options Provide information for mutates
- nointeractive Disables interactive features
- nolookup Disables DNS lookups
- nossl Disables the use of SSL
- noslash Strip trailing slash from URL (e.g., '/admin/' to 'admin')
```

```
Kali Linux - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
-noslash Strip trailing slash from URL (e.g., '/admin/' to '/admin')
-no404 Disables nikto attempting to guess a 404 page
-Option Over-ride an option in nikto.conf, can be issued multiple times
-output+ Write output to this file ('.' for auto-name)
-Pause+ Pause between tests (seconds)
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-RSAcert+ Client certificate file
-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
-Tuning+ 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
d Webservice
e Administrative Console
x Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdbs Load only user databases, not the standard database
s all Disable standard dbs and load only user tests
dbs tests Disable only db_tests and load udb_tests
-useragent Over-rides the default useragent
-until Run until the specified time or duration
-url+ Target host/URL (alias of -host)
-usecookies Use cookies from responses in future requests
-useproxy Use the proxy defined in nikto.conf, or argument http://server:port
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
-404code Ignore these HTTP codes as negative responses (always). Format is "302,301".
-404string Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value
```