NexusPenTest Security Report

Target: scanme.nmap.org

Methodology: OWASP

Date: 2026-02-11 10:09 UTC

Severity Summary

Critical: 5

High: 3

Medium: 8

Low: 9

Info: 2

Findings

theharvester [low]

Command: theharvester --help scanme.nmap.org

??([1;31mMessage from Kali developers [00m)

?

? The command theharvester is deprecated. Please use theHarvester instead.

?

??

whatweb [low]

Command: whatweb --help scanme.nmap.org

[1m [34m

.$$$ $. .$$$ $.

$$$$ $$. .$$$ $$$.$$$$$$. .$$$$$$$$$$. $$$$ $$. .$$$$$$$. .$$$$$$.

$ $$ $$$ $ $$ $$$ $ $$$$$$. $$$$$ $$$$$$ $ $$ $$$ $ $$ $$ $ $$$$$$.

$ `$ $$$ $ `$ $$$ $ `$ $$$ $$' $ `$ `$$ $ `$ $$$ $ `$ $ `$ $$$'

$. $ $$$ $. $$$$$$ $. $$$$$$ `$ $. $:' $. $ $$$ $. $$$$ $. $$$$$.

$::$. $$$ $::$ $$$ $::$ $$$ $::$ $::$. $$$ $::$ $::$ $$$$

$;;$ $$$ $$$ $;;$ $$$ $;;$ $$$ $;;$ $;;$ $$$ $$$ $;;$ $;;$ $$$$

$$$$$$ $$$$$ $$$$ $$$ $$$$ $$$ $$$$ $$$$$$ $$$$$ $$$$$$$$$ $$$$$$$$$'

[0m

WhatWeb - Next generation web scanner version 0.6.3.

Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).

Homepage: https://morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

TARGET SELECTION:

<TARGETs> Enter URLs, hostnames, IP addresses, filenames or
IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
format.

--input-file=FILE, -i Read targets from a file. You can pipe
hostnames or URLs directly with -i /dev/stdin.

```
TARGET MODIFICATION:
  --url-prefix   Add a prefix to target URLs.
  --url-suffix   Add a suffix to target URLs.
  --url-pattern   Insert the targets into a URL.
    e.g. example.com/%insert%/robots.txt

AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
  --aggression, -a=LEVEL Set the aggression level. Default: 1.
  1. Stealthy   Makes one HTTP request per target and also
     follows redirects.
  3. Aggressive   If a level 1 plugin is matched, additional
     requests will be made.
  4. Heavy   Makes a lot of HTTP requests per target. URLs
     from all plugins are attempted.

HTTP OPTIONS:
  --user-agent, -U=AGENT Identify as AGENT instead of WhatWeb/0.6.3.
  --header, -H   Add an HTTP header. eg "Foo:Bar". Specifying a
    default header will replace it. Specifying an
    empty value, e.g. "User-Agent:" will remove it.
  -
```

nmap [medium]

```
Command: nmap --help scanme.nmap.org
Nmap 7.98 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

```
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity
```

dirb [low]

Command: dirb --help scanme.nmap.org

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------


(!) FATAL: Invalid URL format: --help/
    (Use: "http://host/" or "https://host/" for SSL)
```

nikto [medium]

Command: nikto --help scanme.nmap.org

```
   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 errors
      -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
-followredirects Follow 3xx redirects to new location
-Format+ S

nmap [medium]

Command: nmap --help scanme.nmap.org

Nmap 7.98 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity

masscan [low]

Command: masscan --help scanme.nmap.org

MASSCAN is a fast port scanner. The primary input parameters are the
IP addresses/ranges you want to scan, and the port numbers. An example
is the following, which scans the 10.x.x.x network for web servers:
 masscan 10.0.0.0/8 -p80
The program auto-detects network interface/adapter settings. If this
fails, you'll have to set these manually. The following is an
example of all the parameters that are needed:
 --adapter-ip 192.168.10.123
 --adapter-mac 00-11-22-33-44-55
 --router-mac 66-55-44-33-22-11
Parameters can be set either via the command-line or config-file. The
names are the same for both. Thus, the above adapter settings would
appear as follows in a configuration file:
 adapter-ip = 192.168.10.123
 adapter-mac = 00-11-22-33-44-55
 router-mac = 66-55-44-33-22-11
All single-dash parameters have a spelled out double-dash equivalent,
so '-p80' is the same as '--ports 80' (or 'ports = 80' in config file).
To use the config file, type:
 masscan -c <filename>
To generate a config-file from the current settings, use the --echo
option. This stops the program from actually running, and just echoes
the current configuration instead. This is a useful way to generate
your first config file, or see a list of parameters you didn't know
about. I suggest you try it now:
 masscan -p1234 --echo

nikto [medium]

Command: nikto --help scanme.nmap.org

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 errors
-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
-followredirects Follow 3xx redirects to new location
-Format+ S

whatweb [low]

Command: whatweb --help scanme.nmap.org

```
 [1m [34m
.$$$    $.                          .$$$    $.
$$$$    $$. .$$$  $$$ .$$$$$$.  .$$$$$$$$$$. $$$$    $$. .$$$$$$$. .$$$$$$.
$ $$    $$$ $ $$  $$$ $ $$$$$$. $$$$$ $$$$$$ $ $$    $$$ $ $$   $$ $ $$$$$$.
$ `$    $$$ $ `$  $$$ $ `$  $$$ $$' $ `$ `$$ $ `$    $$$ $ `$     $ `$  $$$'
$. $    $$$ $. $$$$$$ $. $$$$$$ `$  $. $  :' $. $    $$$ $. $$$$   $. $$$$$.
$::$  .  $$$ $::$  $$$ $::$  $$$    $::$    $::$  .  $$$ $::$     $::$  $$$$
$;;$ $$$ $$$ $;;$  $$$ $;;$  $$$    $;;$    $;;$ $$$ $$$ $;;$     $;;$  $$$$
$$$$$$ $$$$$ $$$$  $$$ $$$$  $$$    $$$$    $$$$$$ $$$$$ $$$$$$$$$ $$$$$$$$$'

 [0m
WhatWeb - Next generation web scanner version 0.6.3.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).
Homepage: https://morningstarsecurity.com/research/whatweb

Usage: whatweb [options] <URLs>

TARGET SELECTION:
  <TARGETs>   Enter URLs, hostnames, IP addresses, filenames or
      IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
      format.
  --input-file=FILE, -i  Read targets from a file. You can pipe
    hostnames or URLs directly with -i /dev/stdin.

TARGET MODIFICATION:
  --url-prefix   Add a prefix to target URLs.
  --url-suffix   Add a suffix to target URLs.
  --url-pattern   Insert the targets into a URL.
    e.g. example.com/%insert%/robots.txt

AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
  --aggression, -a=LEVEL Set the aggression level. Default: 1.
  1. Stealthy   Makes one HTTP request per target and also
      follows redirects.
  3. Aggressive   If a level 1 plugin is matched, additional
      requests will be made.
  4. Heavy   Makes a lot of HTTP requests per target. URLs
      from all plugins are attempted.
```

HTTP OPTIONS:
  --user-agent, -U=AGENT Identify as AGENT instead of WhatWeb/0.6.3.
  --header, -H   Add an HTTP header. eg "Foo:Bar". Specifying a
    default header will replace it. Specifying an
    empty value, e.g. "User-Agent:" will remove it.
  -

dirb [low]

Command: dirb --help scanme.nmap.org

DIRB v2.22
By The Dark Raver

(!) FATAL: Invalid URL format: --help/
    (Use: "http://host/" or "https://host/" for SSL)

hydra [medium]

Command: hydra --help scanme.nmap.org

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

sslscan [critical]

Command: sslscan --help scanme.nmap.org

Version: [32m2.1.5 [0m
OpenSSL 3.5.4 30 Sep 2025
 [0m

hydra [medium]

Command: hydra --help scanme.nmap.org

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

nikto [critical]

Command: nikto --help scanme.nmap.org

  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 errors
    -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
    -followredirects  Follow 3xx redirects to new location
    -Format+          S
```

sqlmap [high]

Command: sqlmap --help scanme.nmap.org

```
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.10#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
```

```
  --check-tor         Check to see if Tor is used properly

 Injection:
   These options can be used to specify which parameters to test for,
   provide custom injection payloads and optional tampering scripts

   -p TESTPARAMETER    Testable parameter(s)
   --dbms=DBMS         Force back-end DBMS to provided value

 Detection:
   These options can be used to customize the detection phase

   --level=LEVEL       Level of tests to perform (1-5, default 1)
   --risk=RISK         Risk of tests to perform (1-3, default 1)

 Techniques:
   These options can be used to tweak testing of specific SQL injection
   techniques

   --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

 Enumeration:
   These options can be used to enumerate the back-end database
   management system information, structure and data contained in the
   tables

   -a, --all
```

dirb [low]

Command: dirb --help scanme.nmap.org

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------


(!) FATAL: Invalid URL format: --help/
    (Use: "http://host/" or "https://host/" for SSL)
```

xsser [info]

Command: xsser --help scanme.nmap.org

wireshark [medium]

Command: wireshark --help scanme.nmap.org

```
Wireshark 4.6.3
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: wireshark [options] ... [ <infile> ]

Capture interface:
  -i <interface>, --interface <interface>
```

```
                    name or idx of interface (def: first non-loopback)
  -f <capture filter>       packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                    packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                    don't capture in promiscuous mode
  -I, --monitor-mode        capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                    size of kernel buffer in MiB (def: 2MiB)
  -y <link type>, --linktype <link type>
                    link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces     print list of interfaces and exit
  -L, --list-data-link-types
                    print list of link-layer types of iface and exit
  --list-time-stamp-types   print list of timestamp types for iface and exit

Capture display:
  -k                start capturing immediately (def: do nothing)
  -S                update display when new items are captured
  -l                turn on automatic scrolling while -S is in use
  --update-interval         interval between updates with new items, in milliseconds (def: 100ms)
Capture stop conditions:
  -c <item count>           stop after n items (def: infinite)
  -a <autostop cond.> ..., --autostop <autostop cond.> ...
                    duration:NUM - stop after NUM seconds
                    filesize:NUM - stop this file after NUM KB
                      files:NUM - stop after NUM files
                    packets:NUM - stop after NUM packets
Capture output:
  -b <ringbuffer opt.> ..., --ring-buffer <ringbuffer opt.>
```

xsser [info]

Command: xsser --help scanme.nmap.org

sqlmap [high]

Command: sqlmap --help scanme.nmap.org

```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.10#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)
```

```
Target:
  At least one of these options has to be provided to define the
  target(s)

  -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  -g GOOGLEDORK       Process Google dork results as target URLs

Request:
  These options can be used to specify how to connect to the target URL

  --data=DATA         Data string to be sent through POST (e.g. "id=1")
  --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
  --random-agent      Use randomly selected HTTP User-Agent header value
  --proxy=PROXY       Use a proxy to connect to the target URL
  --tor               Use Tor anonymity network
  --check-tor         Check to see if Tor is used properly

Injection:
  These options can be used to specify which parameters to test for,
  provide custom injection payloads and optional tampering scripts

  -p TESTPARAMETER    Testable parameter(s)
  --dbms=DBMS         Force back-end DBMS to provided value

Detection:
  These options can be used to customize the detection phase

  --level=LEVEL       Level of tests to perform (1-5, default 1)
  --risk=RISK         Risk of tests to perform (1-3, default 1)

Techniques:
  These options can be used to tweak testing of specific SQL injection
  techniques

  --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables

  -a, --all
```

commix [critical]

```
Command: commix --help scanme.nmap.org
Usage: commix [option(s)]

Options:
  -h, --help          Show help and exit.

  [1m [4mGeneral [0m:
  These options relate to general matters.

  -v VERBOSE          Verbosity level (0-4, Default: 0).
```

```
  --version           Show version number and exit.
  --output-dir=OUT..  Set custom output directory path.
  -s SESSION_FILE     Load session from a stored (.sqlite) file.
  --flush-session     Flush session files for current target.
  --ignore-session    Ignore results stored in session file.
  -t TRAFFIC_FILE     Log all HTTP traffic into a textual file.
  --time-limit=TIM..  Run with a time limit in seconds (e.g. 3600).
  --batch             Never ask for user input, use the default behaviour.
  --skip-heuristics   Skip heuristic detection for code injection.
  --codec=CODEC       Force codec for character encoding (e.g. 'ascii').
  --charset=CHARSET   Time-related injection charset (e.g.
                      '0123456789abcdef').
  --check-internet    Check internet connection before assessing the target.
  --answers=ANSWERS   Set predefined answers (e.g. 'quit=N,follow=N').

 [1m [4mTarget [0m:
  This options has to be provided, to define the target URL.

  -u URL, --url=URL   Target URL.
  --url-reload        Reload target URL after command execution.
  -l LOGFILE          Parse target from HTTP proxy log file.
  -m BULKFILE         Scan multiple targets given in a textual file.
  -r REQUESTFILE      Load HTTP request from a file.
  --crawl=CRAWLDEPTH  Crawl the website starting from the target URL
                      (Default: 1).
  --crawl-exclude=..  Regexp to exclude pages from crawling (e.g. 'logout').
  -x SITEMAP_URL      Parse target(s) from remote sitemap(.xml) file.
  --method=METHOD     Force usage of given HTTP method (e.g. 'PUT').

 [1m [4mRequest [0m:
  These options can be used to specify how to connect to the target URL.

  -d DATA, --data=..  Data string to be sent through POST.
```

nikto [critical]

Command: nikto --help scanme.nmap.org

```
  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 errors
-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
-followredirects Follow 3xx redirects to new location
-Format+ S

sslscan [medium]

Command: sslscan --help scanme.nmap.org
Version: [32m2.1.5 [0m
OpenSSL 3.5.4 30 Sep 2025
[0m

nmap [high]

Command: nmap --help scanme.nmap.org
Nmap 7.98 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity

wireshark [low]

Command: wireshark --help scanme.nmap.org
Wireshark 4.6.3
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: wireshark [options] ... [<infile>]

Capture interface:
  -i <interface>, --interface <interface>
                        name or idx of interface (def: first non-loopback)
  -f <capture filter>   packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                        packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                        don't capture in promiscuous mode
  -I, --monitor-mode   capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                        size of kernel buffer in MiB (def: 2MiB)
  -y <link type>, --linktype <link type>
                        link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces   print list of interfaces and exit
  -L, --list-data-link-types
                        print list of link-layer types of iface and exit
  --list-time-stamp-types print list of timestamp types for iface and exit

Capture display:
  -k   start capturing immediately (def: do nothing)
  -S   update display when new items are captured
  -l   turn on automatic scrolling while -S is in use
  --update-interval   interval between updates with new items, in milliseconds (def: 100ms)
Capture stop conditions:
  -c <item count>   stop after n items (def: infinite)
  -a <autostop cond.> ..., --autostop <autostop cond.> ...
                        duration:NUM - stop after NUM seconds
                        filesize:NUM - stop this file after NUM KB
                           files:NUM - stop after NUM files
                         packets:NUM - stop after NUM packets
Capture output:
  -b <ringbuffer opt.> ..., --ring-buffer <ringbuffer opt.>

tcpdump [low]

Command: tcpdump --help scanme.nmap.org

tcpdump version 4.99.5
libpcap version 1.10.5 (with TPACKET_V3)
OpenSSL 3.5.4 30 Sep 2025
64-bit build, 64-bit time_t
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [-B size] [-c count] [--count]
[-C file_size] [-E algo:secret] [-F file] [-G seconds]
[-i interface] [--immediate-mode] [-j tstamptype]
[-M secret] [--number] [--print] [-Q in|out|inout]
[-r file] [-s snaplen] [-T type] [--version]
[-V file] [-w file] [-W filecount] [-y datalinktype]
[--time-stamp-precision precision] [--micro] [--nano]
[-z postrotate-command] [-Z user] [expression]

hydra [critical]

Command: hydra --help scanme.nmap.org

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).