

Web Vulnerability Scanning with Nikto

Background / Scenario

Nikto is a popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

Objectives

In this lab, you will complete the following objectives:

- Part 1: Launch Nikto and Perform a Basic Scan
- Part 2: Use Nikto to Scan Multiple Web Servers
- Part 3: Investigate Web Site Vulnerabilities
- Part 4: Export Nikto Results to a File

Part 1: Launch Nikto and Perform a Basic Scan

```
(kali㉿Kali)-[~]
$ nikto -h scanme.nmap.org
- Nikto v2.5.0

+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:        45.33.32.156
+ Target Hostname: scanme.nmap.org
+ Target Port:      80
+ Start Time:       2026-01-06 13:16:54 (GMT0)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcm' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.w3sec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 8 item(s) reported on remote host
+ End Time:          2026-01-06 14:23:20 (GMT0) (3986 seconds)

+ 1 host(s) tested
```

Nikto scans for port 80 web services. To scan domains with HTTPS enabled,

you must specify the **-ssl** flag to scan port 443:**Part 2: Use Nikto to Scan**

Multiple Web Servers

```
(kali㉿Kali)-[~]
$ nikto -h https://nmap.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
+ Target IP: 50.116.1.184
+ Target Hostname: nmap.org
+ Target Port: 443
_____
+ SSL Info: Subject: /CN=insecure.com
Ciphers: ECDHE-RSA-AES128-GCM-SHA256
Issuer: /C=US/O=Let's Encrypt/CN=R12
+ Start Time: 2026-01-06 14:47:37 (GMT0)
_____
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Entry '/search.html?*' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/mailman/listinfo/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/search/?*' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-01-06 15:13:55 (GMT0) (1578 seconds)
_____
+ 1 host(s) tested
```

In this part, you will use Nikto to scan servers on the internal virtual networks to look for vulnerable web servers. You will first create a text file to list the IP addresses that you want to scan. In real-life reconnaissance, you can obtain the IP addresses of the servers by doing a DNS lookup of the server name from the URL.

```
(kali㉿Kali)-[~]
$ nikto -h IP_list.txt
- Nikto v2.5.0

+ Target IP: 10.6.6.23
+ Target Hostname: 10.6.6.23
+ Target Port: 80
+ Start Time: 2026-01-06 15:28:53 (GMT0)
_____
+ Server: nginx/1.14.2
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /admin/: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /wp-admin/: Admin login page/section found.
+ /wp-login/: Admin login page/section found.
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8082 Requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2026-01-06 15:30:01 (GMT0) (68 seconds)
```

```
+ Target IP: 10.6.6.13
+ Target Hostname: 10.6.6.13
+ Target Port: 80
+ Start Time: 2026-01-06 15:30:01 (GMT0)
_____
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 16132 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2026-01-06 15:31:25 (GMT0) (84 seconds)
```

```

+ Target IP:      172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port:    80
+ Start Time:    2026-01-06 15:31:25 (GMT0)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.html, /index.php.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d19,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678

```

```

+ Target IP:      10.6.6.14
+ Target Hostname: 10.6.6.14
+ Target Port:    80
+ Start Time:    2026-01-06 15:33:08 (GMT0)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie showhints created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: database-offline.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Multiple index files found: /index.html, /index.php.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

```

Part 3: Investigate Web Site Vulnerabilities

Nikto provides some information about the vulnerabilities that it uncovers during its scans. Some vulnerabilities are associated with an OSVDB number (an older Open Source Vulnerability Database), a CWE ([Common Weakness Enumeration](#)), or a CVE ([Common Vulnerabilities and Exposures](#)). OSVDB was discontinued in 2016. You can use the CVE reference tool to translate the OSVDB identifier to a CVE entry so you can research the vulnerability further.

```

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2026-01-06 15:31:25 (GMT0)  Templates/badfile.txt

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.html, /index.php.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPE0085r2A0~sc92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via ETags_header found with file /nhoMvAdmin/Changelog, inode: 1115138, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to aut

```

CVE-1999-0678 PUBLISHED View JSON | ≡

Collapse all

Required CVE Record Information

CNA: MITRE Corporation —

Published: 2000-03-22 **Updated:** 2005-11-02

Description

A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to /usr/doc, which allows remote users to read documentation files for the entire server.

Run a search on <https://www.cve.org/>

CVE-2003-1418

PUBLISHED

[View JSON](#)



[Collapse all](#)

Required CVE Record Information

CNA: MITRE Corporation

Published: 2007-10-20 **Updated:** 2017-10-19

Description

Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

Did a cross reference on NIST NVD <https://nvd.nist.gov/vuln/detail/CVE-2003-1418>

CVE-2003-1418 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

QUICK INFO

CVE Dictionary Entry:
CVE-2003-1418

NVD Published Date:
12/31/2003

NVD Last Modified:
04/02/2025
Source:
MITRE

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 2.0 Severity and Vector Strings:



NIST: NVD

Base Score: 4.3 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N)

Have a look at the advisory and solutions.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
http://www.openbsd.org/errata32.html	CVE, MITRE	
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	CVE, MITRE	
http://www.securityfocus.com/bid/6939	CVE, MITRE	
http://www.securityfocus.com/bid/6943	CVE, MITRE	Patch
https://exchange.xforce.ibmcloud.com/vulnerabilities/11438	CVE, MITRE	

Part 4: Export Nikto Results to a File

Nikto can output the results of a scan in various formats including CSV, HTML, SQL, txt, and XML. In addition, Nikto can be paired with Metasploit to launch exploits against the vulnerabilities that you uncover.

```
(kali㉿Kali)-[~]
$ nikto -h 172.17.0.2 -o scan_results.htm
- Nikto v2.5.0
_____
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2026-01-06 18:42:04 (GMT0)
_____
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcm' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wi sec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
```

Locate the file in the /home/kali directory and open it in your browser to view the report format.

172.17.0.2 / 172.17.0.2 port
80
Target IP 172.17.0.2 Target hostname 172.17.0.2 Target Port 80 HTTP Server Apache/2.2.8 (Ubuntu) DAV/2 Site Link (Name) http://172.17.0.2:80/ Site Link (IP) http://172.17.0.2:80/
URI / HTTP Method GET Description /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10. Test Links http://172.17.0.2:80/ References
URI / HTTP Method GET Description /: The anti-clickjacking X-Frame-Options header is not present. Test Links http://172.17.0.2:80/ References https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI / HTTP Method GET Description /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. Test Links http://172.17.0.2:80/ References https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI /index HTTP Method GET Description /index: Uncommon header 'tcn' found, with contents: list. Test Links http://172.17.0.2:80/index References http://172.17.0.2:80/index

Host Summary
Start Time 2026-01-06 18:42:04 End Time 2026-01-06 18:42:35 Elapsed Time 31 seconds Statistics 8910 requests, 0 errors, 27 findings
Scan Summary
Software Details Nikto 2.5.0 CLI Options -h 172.17.0.2 -o scan_results.htm Hosts Tested 1 Start Time Tue Jan 6 18:42:02 2026 End Time Tue Jan 6 18:42:35 2026 Elapsed Time 33 seconds

To specify a text file output format that is independent of the file extension, use the **-Format** flag. Use the **-Format csv** option to save the file in .csv format to import into other analysis applications.

```
(kali㉿Kali)-[~]
$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
- Nikto v2.5.0

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2026-01-06 18:55:45 (GMT0)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wi sec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
```

Use the **cat** command to view the saved **scan_results.txt** file.

```
(kali㉿Kali)-[~]
$ cat scan_results.txt
"nikto - v2.5.0"
"172.17.0.2","172.17.0.2","80","","","","","Apache/2.2.8 (Ubuntu) DAV/2"
"172.17.0.2","172.17.0.2","80","","","GET","/","Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10."
"172.17.0.2","172.17.0.2","80","https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options","GET","/","The anti-clickjacking X-Frame-Options header is not present."
"172.17.0.2","172.17.0.2","80","https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/","GET","/","The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type."
"172.17.0.2","172.17.0.2","80","","GET","/index","Uncommon header 'tcn' found, with contents: list.
"
"172.17.0.2","172.17.0.2","80","http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275","GET","/index","Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php."
"172.17.0.2","172.17.0.2","80","","HEAD","/","Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch."
"172.17.0.2","172.17.0.2","80","","VKRRLEFD","/","Web Server returns a valid response with junk HTTP methods which may cause false positives."
"172.17.0.2","172.17.0.2","80","https://owasp.org/www-community/attacks/Cross_Site_Tracing","TRACE","/","HTTP TRACE method is active which suggests the host is vulnerable to XSS."
"172.17.0.2","172.17.0.2","80","","GET","/phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>
","/phpinfo.php: Output from the phpinfo() function was found."
```