

WEB VULNERABILITY SCANNING WITH **NIKTO**



Introduction to Nikto

Nikto is an open-source web vulnerability scanner widely used by cybersecurity professionals to identify security issues in web servers and applications. Created to be both comprehensive and user-friendly, Nikto quickly scans web applications for vulnerabilities, misconfigurations, and outdated components. As it is freely available, it is accessible to professionals, students, and hobbyists alike, providing a hands-on tool for real-world vulnerability assessment.

Key Features of Nikto

- ✔ **Detection of Over 6,700 Vulnerabilities:** Nikto scans for a vast array of issues, including server misconfigurations, insecure files, outdated versions, and more.
- ✔ **Fast Scanning and Reporting:** Nikto is designed to be thorough yet fast, providing detailed results in just a few minutes.
- ✔ **Customizable Scan Options:** Nikto allows custom configurations, such as choosing specific modules, target directories, or user agents, making it adaptable for different scanning needs.

Getting Started with Nikto

To use Nikto effectively, you'll first need to install and configure it. Here is how to set up Nikto on different operating systems.

Installing Nikto

1. **On Linux:** Most Linux distributions allow you to install Nikto through package managers, or you can install it directly from the source.

Install using apt (Debian/Ubuntu)

```
sudo apt update  
sudo apt install nikto
```

Installing from source (for any Linux distribution)

```
git clone https://github.com/sullo/nikto.git  
cd nikto  
sudo chmod +x nikto.pl
```

On macOS: You can use Homebrew to install Nikto

```
brew install nikto
```

Installing from source (for any Linux distribution)

```
git clone https://github.com/sullo/nikto.git
cd nikto
sudo chmod +x nikto.pl
```

2. On Windows: Nikto is a Perl-based application, so you will need to install Perl first. Afterward, you can use Git Bash or any command line to run Nikto.

Step 1: Install Perl for Windows (ActivePerl)

Step 2: Clone the Nikto repository

```
git clone https://github.com/sullo/nikto.git
cd nikto
```

Command to check the current version of Nikto's plugins and database:

```
nikto.pl -Version
```

```
(root@kali)-[/home/kali]
# nikto -Version
Nikto 2.5.0 (LW 2.5)
```

Nikto is now set up, and you're ready to perform your first scan!

Core Functionalities of Nikto

Nikto offers a wide range of scanning capabilities, helping you detect various types of vulnerabilities, including:

- ✓ **Outdated Software:** Identifies outdated versions of software components on the server.
- ✓ **Default Files and Directories:** Checks for files like `phpinfo.php` or `admin` directories left from development.
- ✓ **Configuration Issues:** Detects common misconfigurations, such as HTTP methods (OPTIONS, TRACE), that may increase attack surfaces.
- ✓ **Security Headers:** Checks for missing or misconfigured security headers that could expose vulnerabilities.

Here are commands to use Nikto's core scanning functionalities effectively.

Running Basic Scans with Nikto

Basic Scan Command: The simplest command to scan a website is as follows:

```
nikto -h <URL or IP address>
```

Example

```
nikto -h http://example.com
```

This command initiates a basic scan, which will test the target for known vulnerabilities, misconfigurations, and outdated software.

```
(root@kali)-[/home/kali]
# nikto -h http://192.168.109.131/
- Nikto v2.5.0

+ Target IP: 192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port: 80
+ Start Time: 2025-01-06 16:49:12 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006.
+ /: 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/
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/006000-robots-txt-file
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/006000-robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will
```

Useful Parameters:

- ✔ **-output:** Saves the scan results to a file.
- ✔ **-timeout:** Sets a timeout for the scan.
- ✔ **-ssl:** Specifies SSL if the site doesn't use HTTP.
- ✔ **-C:** Checks for HTTP-related vulnerabilities.

```
nikto -h http://example.com -output example_scan.txt -timeout 10 -C all
```

```
(root@kali)-[/home/kali]
# nikto -h http://192.168.109.131/ -output test_scan.txt -timeout 10 -C all
- Nikto v2.5.0

+ Target IP: 192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port: 80
+ Start Time: 2025-01-06 17:03:15 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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/
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/006000-robots-txt-file
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/006000-robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
```

Scan for Specific Vulnerabilities: Nikto can target specific types of vulnerabilities by using the `-Tuning` option. The Tuning codes allow you to specify the scan focus.

✓ Scan for File Upload Vulnerabilities (Code 4)

```
nikto -h <target-domain> -Tuning 4
```

```
# nikto -h http://192.168.109.131/ -Tuning 4
- Nikto v2.5.0

+ Target IP:      192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port:    80
+ Start Time:     2025-01-06 17:15:24 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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/
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.28 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
```

✓ Scan for Injection Vulnerabilities (Code 5)

```
nikto -h <target-domain> -Tuning 5
```

```
# nikto -h http://192.168.109.131/ -Tuning 5
- Nikto v2.5.0

+ Target IP:      192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port:    80
+ Start Time:     2025-01-06 17:15:55 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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/
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.28 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
```

Tuning codes reference

- ✓ 0: File upload
- ✓ 1: Interesting files / Seen in logs
- ✓ 2: Misconfiguration / Default files
- ✓ 3: Information disclosure
- ✓ 4: Injection (XSS/Script/HTML)
- ✓ 5: Remote file retrieval (shells)

Exporting Results to a Report: To export the results to a file, you can use the `-o` (output) option:

```
nikto -h <target-domain> -o output.txt
```

```
# nikto -h http://192.168.109.131/ -output test_scan.txt
- Nikto v2.5.0

+ Target IP:      192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port:    80
+ Start Time:     2025-01-06 17:19:25 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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 user agent. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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 were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 2020.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.28 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ /backup/: This might be interesting.
+ /cgi-bin/test.cgi: This might be interesting.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
```

```
(root@kali)-[/home/kali/rob]
# ls
test_scan.txt
```

Advanced Scanning Options

Nikto also supports various advanced options for custom scans.

- ✔ **Limiting Scan Scope:** Use the `-p` option to specify a particular port (useful if the server runs multiple services):

```
nikto -h <target-domain> -p 443
```

```

$ nikto -h 192.168.109.131 -p 443
- Nikto v2.5.0

+ Target IP:      192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port:    443

+ SSL Info:      Subject:  /C=US/ST=Illinois/L=Grayslake/O=BadStore.net/OU=Crack Development Team/CN=www.badstore.net/emailAddress=root@badstore
                  Ciphers: DHE-RSA-AES256-SHA
                  Issuer:   /C=XY/ST=Snake Desert/L=Snake Town/O=Snake Oil, Ltd/OU=Certificate Authority/CN=Snake Oil CA/emailAddress=ca@snakeoil
+ Start Time:    2025-01-06 17:25:27 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org
+ /: 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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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 f
+ were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Hostname '192.168.109.131' does not match certificate's names: www.badstore.net. See: https://cwe.mitre.org/data/definitions/297.html
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
  
```

- ✔ **Customizing the User-Agent:** A great way to mimic legitimate browser traffic (Google Chrome browser on Windows 10) and avoid detection by simple monitoring tools

```
nikto -h <target-domain> -useragent "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124
Safari/537.36"
```

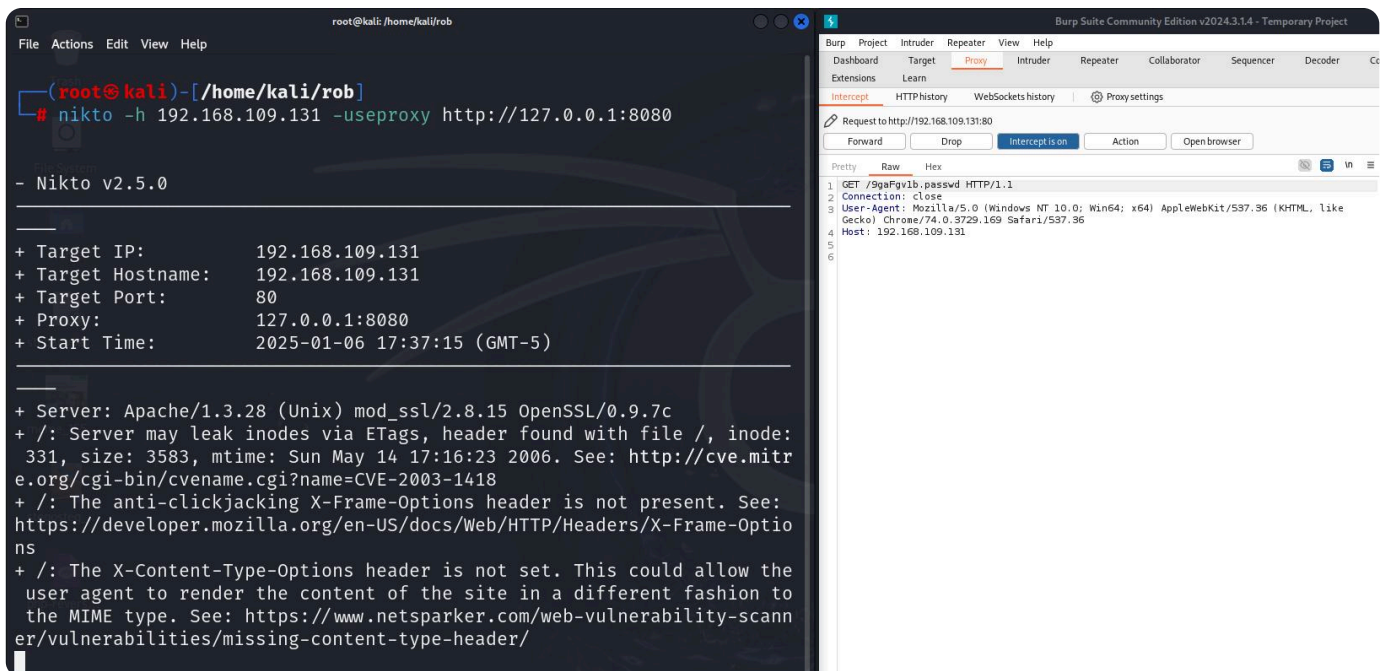
```
(root@kali)-[/home/kali/rob]
# nikto -h 192.168.109.131 -useragent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"
- Nikto v2.5.0

+ Target IP: 192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port: 80
+ Start Time: 2025-01-06 17:29:20 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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/
+ /backup/: Directory indexing found.
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /supplier/: Directory indexing found.
+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /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.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ mod_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported
```

✔ **Using Nikto with Burp Suite:** You can proxy Nikto through Burp Suite for enhanced interception:

`nikto -h <target-domain> -useproxy http://127.0.0.1:8080`



- ✔ **Rate Limiting (Pause):** The `-Pause` parameter adds a delay between requests during scans, minimizing server impact and reducing detection by IDS/IPS.

```
nikto -h 192.168.109.131 -Pause 3
```

```
(root@kali)-[/home/kali/rob]
# nikto -h 192.168.109.131 -Pause 3
-***** Pausing 3 second(s) per request
- Nikto v2.5.0

+ Target IP:      192.168.109.131
+ Target Hostname: 192.168.109.131
+ Target Port:    80
+ Start Time:     2025-01-06 17:41:39 (GMT-5)

+ Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://www.apache.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

-h 192.168.109.131: Specifies the target server's IP address.

-Pause 3: Introduces a 3-second delay between each request sent during the scan.

Best Practices for Web Vulnerability Scanning with Nikto

- ✔ **Schedule Regular Scans:** Automate scans to ensure continuous monitoring.
- ✔ **Avoid Scanning Critical Environments without Permission:** Nikto is an intrusive tool that can generate a lot of traffic. Make sure you have authorization to avoid network disruptions or detection alerts.
- ✔ **Use Scan Results to Guide Mitigation:** Regularly update software, implement recommended security headers, and close access to exposed directories based on Nikto's findings.

In Conclusion

Nikto is an excellent tool for identifying common vulnerabilities and misconfigurations in web applications. By understanding its features and limitations, you can incorporate it effectively into your cybersecurity toolkit.

CEH v13 AI with InfosecTrain

Join InfosecTrain's CEH v13 AI certification training to master tools like Nikto and other critical cybersecurity techniques. This hands-on course combines practical insights with real-world applications, empowering you to identify web vulnerabilities, strengthen security defenses, and tackle cyber threats effectively. Gain in-depth expertise, sharpen your ethical hacking skills, and become job-ready in the fast-evolving cybersecurity landscape. Take the next step in your career with InfosecTrain!

KEEP LEARNING WITH



Contact us

✉ sales@infosectrain.com

🌐 www.infosectrain.com

Follow us on

