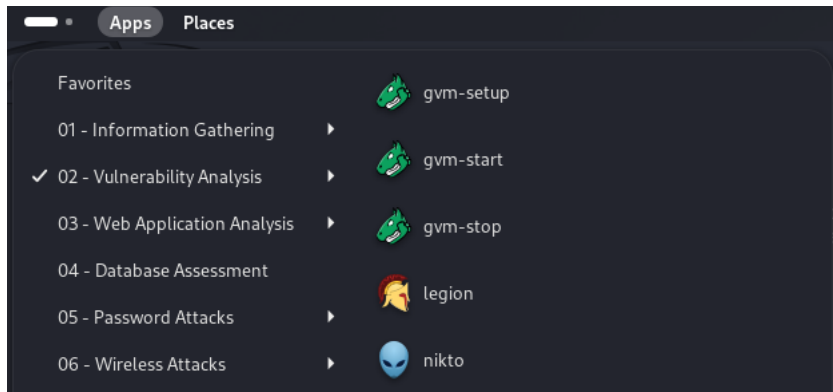


Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Here we are using Kali Linux

Open Kali Linux > **Apps**>Vulnerability analysis >nikto



```
-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)
-Userdb+     Load only user databases, not the standard databases
              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 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

-(kali@kali)-[~]
```

Type nikto -h

```
(kali@kali)-[~]
└─$ nikto -h
Option host requires an argument

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 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+             Save file (-o) format:
                        csv   Comma-separated-value
                        json  JSON Format
                        htm   HTML Format
                        nbe   Nessus NBE format
```

The result appears, displaying various available options in Nikto. We will use the Tuning option to do a deeper and more comprehensive scan on the target web server

In the terminal window, type **nikto-h (Target Website) -Tuning x** (here, the target web site is <https://www.certifiedhacker.com>) and press Enter. Nikto starts scanning with all the tuning options enabled.

nikto -h https://www.certifiedhacker.com -Tuning x

```
(kali@kali)-[~]
└─$ nikto -h https://www.certifiedhacker.com -Tuning x
- Nikto v2.5.0

-----
+ Target IP:      162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port:    443
-----
+ SSL Info:      Subject: /CN=webdisk.certifiedhacker.com
                  Ciphers: TLS_AES_256_GCM_SHA384
                  Issuer: /C=US/O=Let's Encrypt/CN=R10
+ Start Time:    2025-04-12 12:57:47 (GMT+4)
-----
+ Server: nginx/1.25.5
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ /: Uncommon header 'x-server-cache' found, with contents: true.
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkbmJsdWVob3N0LmNvbQ==.
+ /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ : Server banner changed from 'nginx/1.25.5' to 'Apache'.
```

The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

Here, we will check for cgi directories with the **-Cgидirs** option. In this option, search for specific directories or use all options to search for all the available directories.

In the terminal window, type `nikto -h (TargetWebsite) -Cgirdirs all`, (here, the target website is <https://www.certifiedhacker.com>) and hit Enter

The target web site does not have any CGI directory; therefore, the same result as the previous scan was obtained.

nikto -h https://www.certifiedhacker.com -Cgirdirs all

```
(kali@kali)~$ nikto -h https://www.certifiedhacker.com -Cgirdirs all
Nikto v2.5.0
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 443
+ SSL Info: Subject: /CN=webdisk.certifiedhacker.com
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=Let's Encrypt/CN=R10
+ Start Time: 2025-04-12 13:41:01 (GMT-4)
-----
+ Server: nginx/1.25.5
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LmNvbQ==.
+ /: Uncommon header 'x-server-cache' found, with contents: true.
+ /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ : Server banner changed from 'nginx/1.25.5' to 'Apache'.
```

Now, we will save the scan results in the form of a text file on Desktop. To do so, type `cd` and press Enter to jump to the root directory.

nikto -h https://www.certifiedhacker.com -Cgirdirs all -o /home/kali/Desktop/nikto_scan_results.txt -Format txt

```
(kali@kali)~/Desktop$ nikto -h https://www.certifiedhacker.com -Cgirdirs all -o /home/kali/Desktop/nikto_scan_results.txt -Format txt
Nikto v2.5.0
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 443
+ SSL Info: Subject: /CN=webdisk.certifiedhacker.com
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=Let's Encrypt/CN=R10
+ Start Time: 2025-04-12 14:09:01 (GMT-4)
-----
+ Server: nginx/1.25.5
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LmNvbQ==.
+ /: Uncommon header 'x-server-cache' found, with contents: true.
+ /: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ : Server banner changed from 'nginx/1.25.5' to 'Apache'.
[[B"c

(kali@kali)~/Desktop$ ls
nikto_scan_results.txt  test_nikto.txt

(kali@kali)~/Desktop$ cat nikto_scan_results.txt
Nikto v2.5.0/
+ Target Host: www.certifiedhacker.com
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ GET /: Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LmNvbQ==.
```