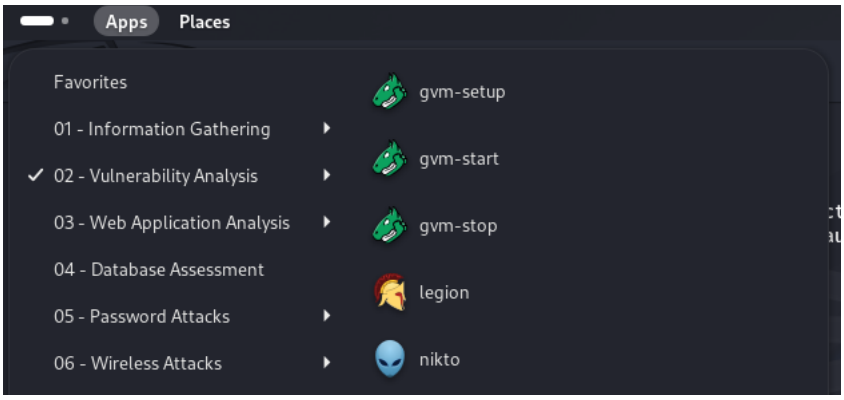
Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

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)
    -Userdbs           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

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

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 -Cgidirs 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) -Cgidirs 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 -Cgidirs all

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 -Cgidirs all -o /home/kali/Desktop/nikto_scan_results.txt -Format txt