

Practical 2: Vulnerability Scanning using Nikto in Kali Linux

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nikto -Version  
Nikto Versions  
File Version Last Mod  
Nikto main 2.1.6  
LibWhisker 2.5  
db_404_strings 2.003  
db_content_search 2.000  
db_dir_traversal 1.0  
db_dir_traversal 2.1.6  
db_domino 2.1.6  
db_drupal 1.00  
db_embedded 2.004  
db_favicon 2.010  
db_headers 2.008  
db_httppoptions 2.002  
db_multiple_index 2.005  
db_outdated 2.017  
db_parked_strings 2.001  
db_realms 2.002  
db_server_msgs 2.006  
db_tests 2.021  
db_variables 2.004  
nikto_apache_expect_xss.plugin 2.04  
nikto_apacheusers.plugin 2.06  
nikto_auth.plugin 2.04  
nikto_cgi.plugin 2.06  
nikto_clientaccesspolicy.plugin 1.00  
nikto_content_search.plugin 2.05  
nikto_cookies.plugin 2.05  
nikto_core.plugin 2.1.5  
nikto_dictionary_attack.plugin 2.04  
nikto_dir_traversal.plugin 2.1.6  
nikto_dishwasher.plugin 2.20  
nikto_docker_registry.plugin 2.20  
nikto_domino.plugin 2.1.6  
nikto_drupal.plugin 1.00  
nikto_embedded.plugin 2.07  
nikto_favicon.plugin 2.09  
nikto_fileops.plugin 1.00  
nikto_headers.plugin 2.11  
nikto_httppoptions.plugin 2.10  
nikto_ms10_070.plugin 1.00  
nikto_msgs.plugin 2.07  
nikto_multiple_index.plugin 2.03  
nikto_negotiate.plugin 2.00  
nikto_server_reflection.plugin 2.03
```

```

(kali@kali)-[~]
$ nikto -dbcheck
Syntax Check: /var/lib/nikto/databases/db_variables
    38 entries
Syntax Check: /var/lib/nikto/databases/db_favicon
    358 entries
Syntax Check: /var/lib/nikto/databases/db_parked_strings
    8 entries
Syntax Check: /var/lib/nikto/databases/db_dictionary
    1825 entries
Syntax Check: /var/lib/nikto/databases/db_outdated
    1254 entries
Syntax Check: /var/lib/nikto/databases/db_404_strings
    39 entries
Syntax Check: /var/lib/nikto/databases/db_content_search
    19 entries
Syntax Check: /var/lib/nikto/databases/db_tests
    6897 entries
Syntax Check: /var/lib/nikto/databases/db_embedded
    16 entries
Syntax Check: /var/lib/nikto/databases/db_multiple_index
    36 entries
Syntax Check: /var/lib/nikto/databases/db_httptoptions
    12 entries
Syntax Check: /var/lib/nikto/databases/db_realms
    170 entries
Syntax Check: /var/lib/nikto/databases/db_headers
    98 entries
Syntax Check: /var/lib/nikto/databases/db_drupal
    6244 entries
Syntax Check: /var/lib/nikto/databases/db_domino
    274 entries
Syntax Check: /var/lib/nikto/databases/db_dir_traversal
    1 entries
Syntax Check: /var/lib/nikto/databases/db_server_msgs
    261 entries
Checking plugins for duplicate test IDs

Some (probably) open IDs: 000029, 000137, 000326, 000407, 000427, 000429, 000430

```

```

(kali@kali)-[~]
$ nikto --host 162.159.152.4
- Nikto v2.1.6

+ Target IP:      162.159.152.4
+ Target Hostname: 162.159.152.4
+ Target Port:    80
+ Start Time:     2024-07-27 01:06:20 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time:       2024-07-27 01:06:31 (GMT-4) (11 seconds)

+ 1 host(s) tested

```

```

(kali@kali)-[~]
└─$ nikto -h medium.com -ssl
- Nikto v2.1.6

+ Target IP:          162.159.153.4
+ Target Hostname:    medium.com
+ Target Port:        443

+ SSL Info:          Subject: /C=US/ST=California/L=San Francisco/O=Cloudflare, Inc./CN=medium.com
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer: /C=IN/CN=svkm.ac.in
+ Message:           Multiple IP addresses found: 162.159.153.4, 162.159.152.4
+ Start Time:        2024-07-27 01:08:57 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ The site uses SSL and Expect-CT header is not present.
+ All CGI directories 'found', use '-C none' to test none
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 18 error(s) and 4 item(s) reported on remote host
+ End Time:         2024-07-27 01:09:19 (GMT-4) (22 seconds)

+ 1 host(s) tested

```

```

(kali@kali)-[~]
└─$ nikto -h 162.159.152.4 --port 80
- Nikto v2.1.6

+ Target IP:          162.159.152.4
+ Target Hostname:    162.159.152.4
+ Target Port:        80
+ Start Time:        2024-07-27 01:13:59 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site i
n a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time:         2024-07-27 01:14:09 (GMT-4) (10 seconds)

+ 1 host(s) tested

```