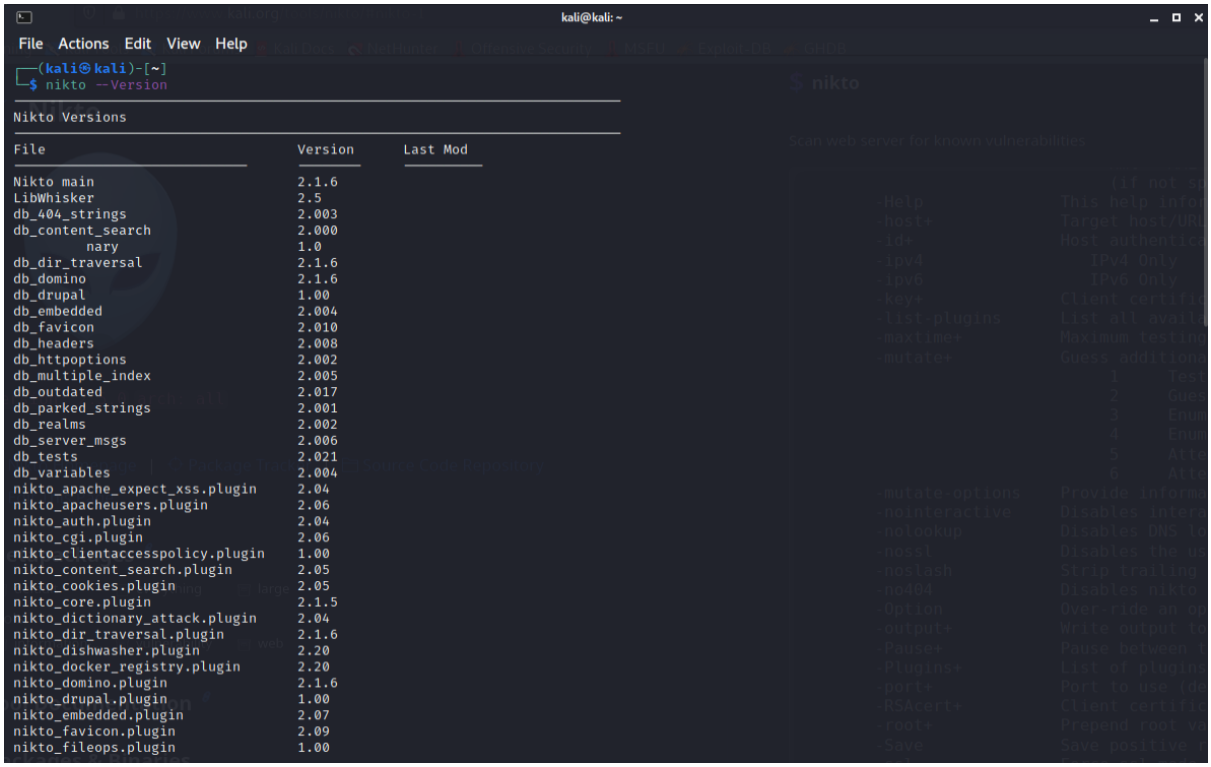
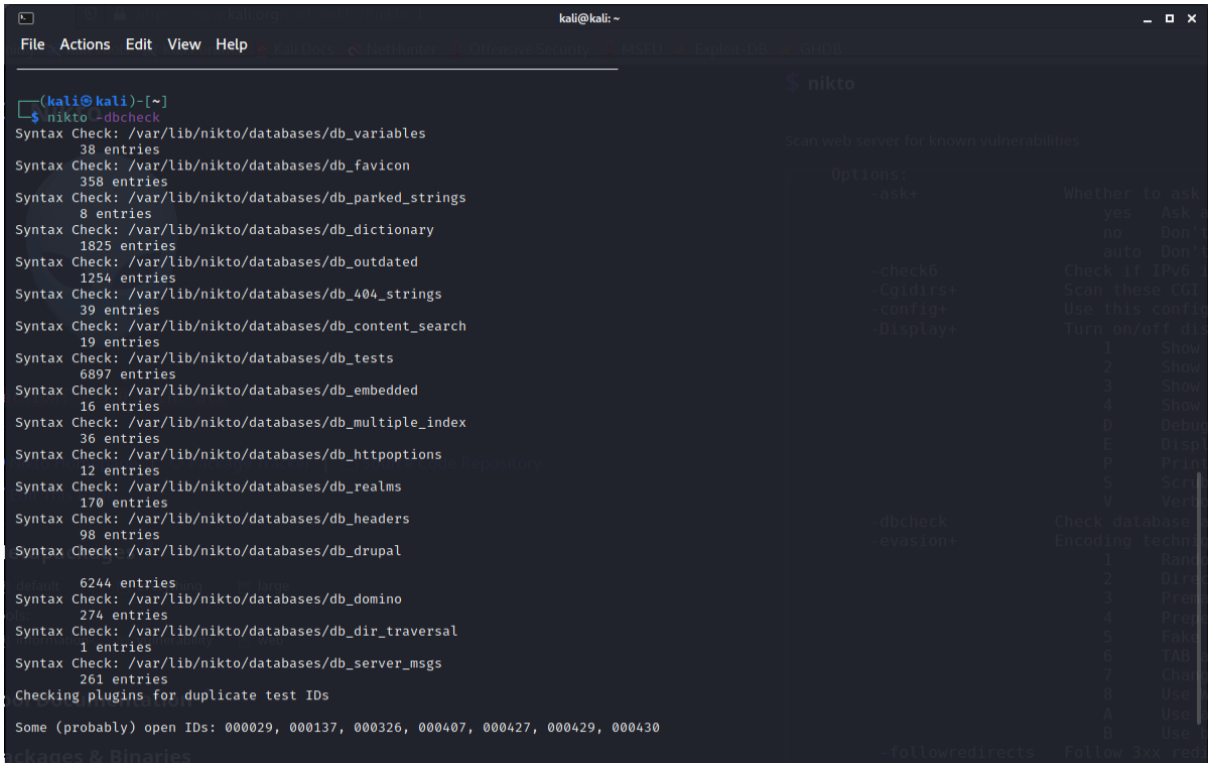

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nikto -Version
Nikto Versions
File Version Last Mod
Nikto main 2.1.6
LibWhisker 2.5
db_404_strings 2.003
db_content_search 2.000
nary 1.0
db_dir_traversal 2.1.6
db_domino 2.1.6
db_drupal 1.00
db_embedded 2.004
db_favicon 2.010
db_headers 2.008
db_httpoptions 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


kali@kali: ~
File Actions Edit View Help
(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_httpoptions
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

Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 2

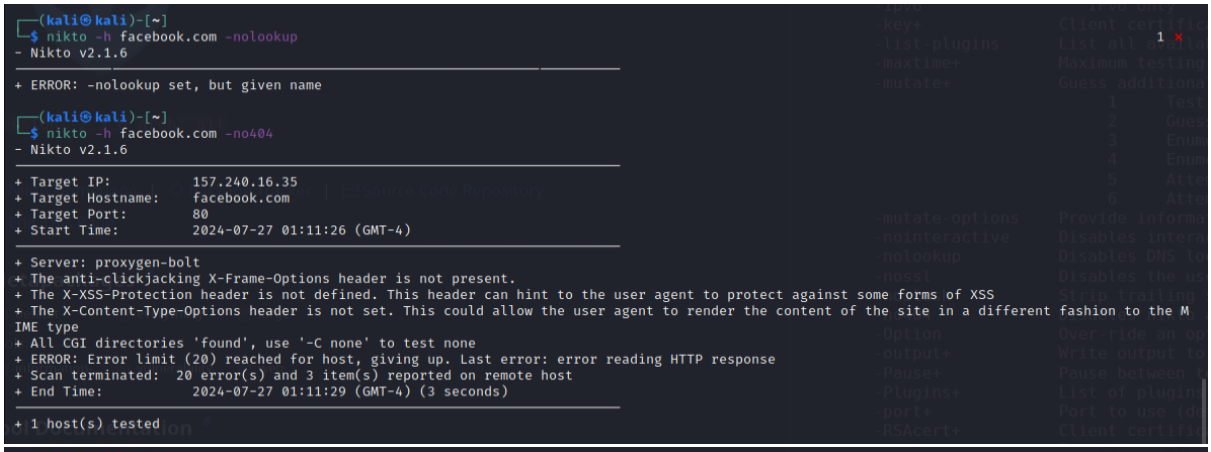
```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -Display 1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          157.240.16.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:07:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:07:39 (GMT-4) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          157.240.16.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:08:13 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:08:23 (GMT-4) (10 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          163.70.143.35
+ Target Hostname:    facebook.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Menlo Park/O=Meta Platforms, Inc./CN=*.facebook.com
                   Ciphers:  TLS_CHACHA20_POLY1305_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time:         2024-07-27 01:09:33 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 'x-fb-connection-quality' found, with contents: EXCELLENT; q=0.9, rtt=7, rtx=0, c=10, mss=1392, tbw=3402, tp=-1, tpl=-1, uplat=
143, ullat=0
+ Uncommon header 'x-fb-server-load' found, with contents: 46
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'x-fb-debug' found, with contents: 0ZSOzbngM9yIG7L8qNe+7HFRLLcZ7SfpuJahkzk/d0HdZVrE/wFVxOnpXKqhzcwp7Yf8ZqEyaklxikwOPUgGZQ==
+ The site uses SSL and Expect-CT header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://www.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'document-policy' found, with contents: force-load-at-top
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin-allow-popups;report-to="coop_report"
+ Uncommon header 'report-to' found, with contents: {"max_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser_reporting\/coop\/
?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":21600,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser_
error_reports\/"}],"group":"permissions_policy"}
+ Uncommon header 'cross-origin-resource-policy' found, with contents: same-origin
+ Uncommon header 'permissions-policy' found, with contents: accelerometer=(), attribution-reporting=(self), autoplay=(), battery=(self), bluetoo
th=(), browsing-topics=(self), camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(
), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=()
, display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), inte
rest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-pict
ure=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-
select-url=(), private-state-token-redemption=(), usb=(), usb-unrestricted=(), unload=(self), window-management=(), xr-spatial-tracking=(self);re
port-to="permissions_policy"
+ Uncommon header 'reporting-endpoints' found, with contents: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0", permissi
```

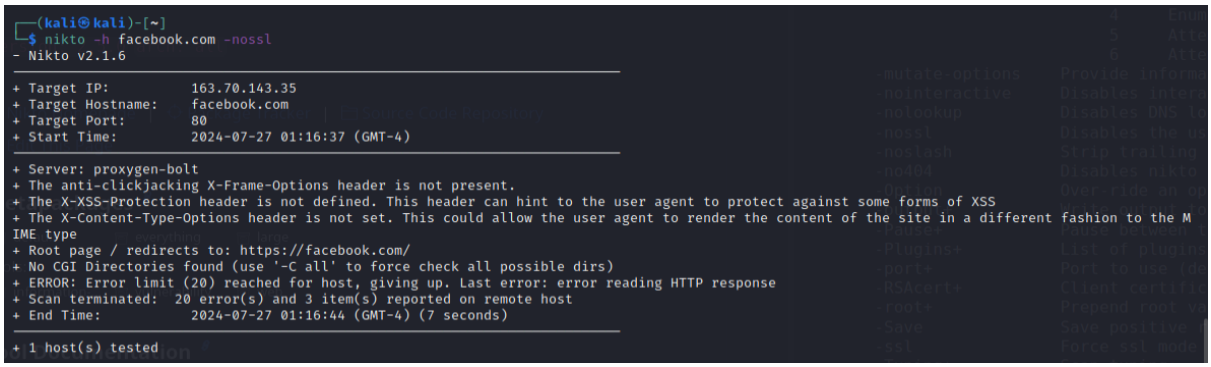
Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 2



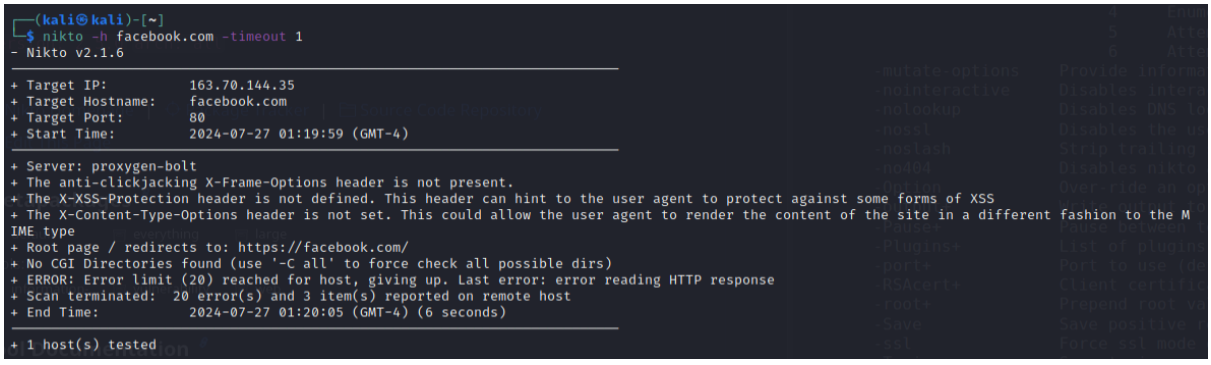
```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -nolookup
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: -nolookup set, but given name

┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -no404
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          157.240.16.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:11:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME 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 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:11:29 (GMT-4) (3 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

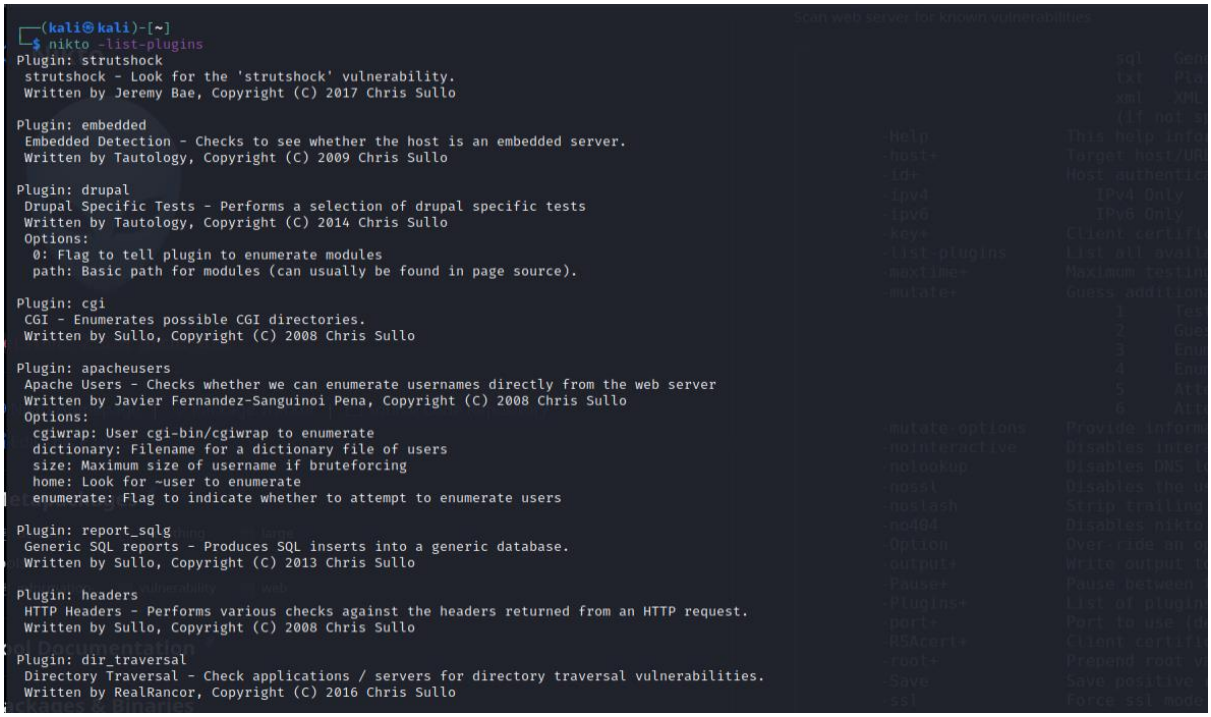
```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -maxtime 1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          163.70.144.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:14:06 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://facebook.com/
+ ERROR: Host maximum execution time of 1 seconds reached
+ Scan terminated:  0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:14:08 (GMT-4) (2 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -nossl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          163.70.143.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:16:37 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:16:44 (GMT-4) (7 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h facebook.com -timeout 1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          163.70.144.35
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2024-07-27 01:19:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: proxygen-bolt
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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 M
IME type
+ Root page / redirects to: https://facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-07-27 01:20:05 (GMT-4) (6 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -list-plugins
Plugin: strutshock
 strutshock - Look for the 'strutshock' vulnerability.
 Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: embedded
 Embedded Detection - Checks to see whether the host is an embedded server.
 Written by Tautology, Copyright (C) 2009 Chris Sullo

Plugin: drupal
 Drupal Specific Tests - Performs a selection of drupal specific tests
 Written by Tautology, Copyright (C) 2014 Chris Sullo
 Options:
  0: Flag to tell plugin to enumerate modules
  path: Basic path for modules (can usually be found in page source).

Plugin: cgi
 CGI - Enumerates possible CGI directories.
 Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: apacheusers
 Apache Users - Checks whether we can enumerate usernames directly from the web server
 Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 Chris Sullo
 Options:
  cgiwrap: User cgi-bin/cgiwrap to enumerate
  dictionary: Filename for a dictionary file of users
  size: Maximum size of username if bruteforcing
  home: Look for ~user to enumerate
  enumerate: Flag to indicate whether to attempt to enumerate users

Plugin: report_sqlg
 Generic SQL reports - Produces SQL inserts into a generic database.
 Written by Sullo, Copyright (C) 2013 Chris Sullo

Plugin: headers
 HTTP Headers - Performs various checks against the headers returned from an HTTP request.
 Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: dir_traversal
 Directory Traversal - Check applications / servers for directory traversal vulnerabilities.
 Written by RealRancor, Copyright (C) 2016 Chris Sullo
```