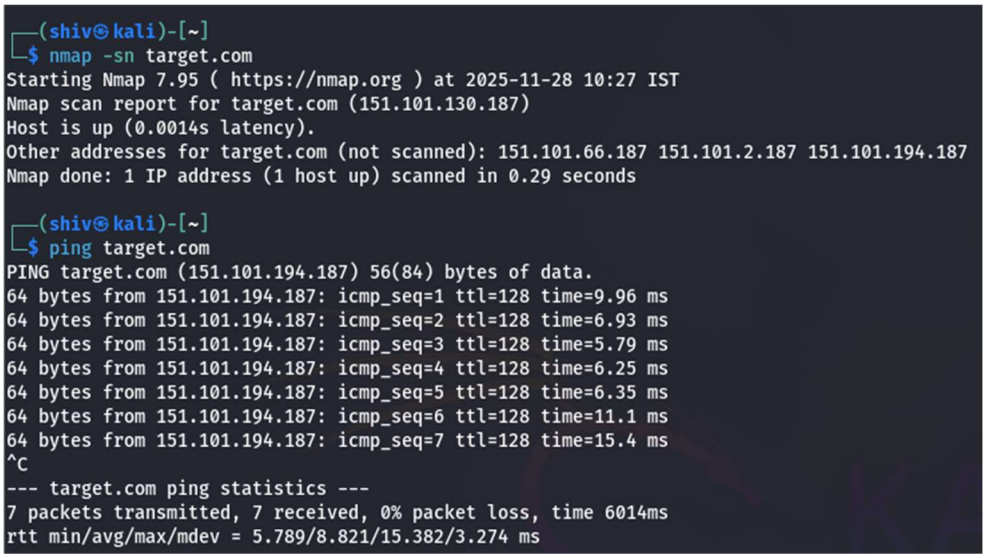
Assignment 4- Active Recon and web enumeration using nmap & directory brute forcers

1) Host Discovery

Using option -sn



2)Port and Service scan using nmap

Using option -sS

Using option -p

```
┌──(shiv㉿kali)-[~]
└─$ nmap -sV -sC -p 80,443 target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 11:52 IST
Nmap scan report for target.com (151.101.130.187)
Host is up (0.0040s latency).
Other addresses for target.com (not scanned): 151.101.194.187 151.101.2.187 151.101.66.187

PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy Varnish
|_http-title: Did not follow redirect to https://target.com/
443/tcp open  ssl/https
| ssl-cert: Subject: commonName=sites.target.com/organizationName=Target Corporation/stateOrProvinceName=Minnesota/countryName=US
| Subject Alternative Name: DNS:sites.target.com, DNS:affiliate.target.com, DNS:apollo-metrics.target.com, DNS:assethub.partnersonline.com, DNS:assethub.target.com, DNS:bex.partnersonline.com, DNS:bex.target.com, DNS:cartster.target.com, DNS:cartwheel.target.com, DNS:cartwheelws-secure.target.com, DNS:circle.target.com, DNS:connect.roundel.com, DNS:corporate.target.com, DNS:developer.target.com, DNS:doppler.partnersonline.com, DNS:elevate.target.com, DNS:extgargantua.partnersonline.com, DNS:factorial.partnersonline.com, DNS:finds.target.com, DNS:greenfield.partnersonline.com, DNS:greenfield.target.com, DNS:hrocdocrequest.target.com, DNS:iccon.target.com, DNS:india.target.com, DNS:jira.target.com, DNS:launchpad.partnersonline.com, DNS:launchpad.target.com, DNS:m.target.com, DNS:marketinghub.target.com, DNS:mercury.partnersonline.com, DNS:mickra.target.com, DNS:mickradashboard.target.com, DNS:mvs.partnersonline.com, DNS:mytime.target.com, DNS:nic.target, DNS:openhouse.target.com, DNS:opensource.target.com, DNS:osmosis.partnersonline.com, DNS:partnersonline.com, DNS:pcn.partnersonline.com, DNS:peg.partnersonline.com, DNS:photosubmission.target.com, DNS:pid.partnersonline.com, DNS:plus.target.com, DNS:pmworkorderadmin.partnersonline.com, DNS:poladmin.partnersonline.com, DNS:pop.partnersonline.com, DNS:qr.target.com, DNS:r2d2.target.com, DNS:rdmplus.target.com, DNS:recognize.target.com, DNS:redcard.target.com, DNS:rik.roundel.com, DNS:roundel.com, DNS:rubix.partnersonline.com, DNS:rubix.target.com, DNS:security.target.com, DNS:servicetech.target.com, DNS:sm.partnersonline.com, DNS:spark.partnersonline.com, DNS:spark.target.com, DNS:stylehub.target.com, DNS:synergy.partnersonline.com, DNS:target.com, DNS:targetmedianetwork.target.com, DNS:tepagent.target.com, DNS:tgt-files.target.com, DNS:tgtdriver.partnersonline.com, DNS:tiam.target.com, DNS:tiam.target.com, DNS:tvi.partnersonline.com, DNS:viewpoint.target.com, DNS:weeklyad.target.com, DNS:www.partnersonline.com, DNS:www.target.com
| Not valid before: 2025-09-04T16:25:19
|_Not valid after:  2026-10-06T16:25:18
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21722
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
|   GetRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21722
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
```

```
|   FourOhFourRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21722
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
|   GetRequest:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21733
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
|   HTTPOptions:
|     HTTP/1.1 421 Misdirected Request
|     Connection: close
|     Content-Length: 291
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21729
|     Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|     Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Length: 11
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21743
|     Request
|   tor-versions:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Length: 11
|     content-type: text/plain; charset=utf-8
|     x-served-by: cache-del21727
|_    Request
| tls-alpn:
|   h3
|   h2
|   http/1.1
```

```
| tls-alpn:
|   h3
|   h2
|   http/1.1
|_  http/1.0
|_http-title: Did not follow redirect to https://www.target.com/
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=11/28%Time=69293FA4%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConne
SF:ction:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nx-served-by:\x20cache-del21733\r\n\r\nRequested\
SF:x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Nam
SF:es\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7880c70cd7
SF:6fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20with\x20thi
SF:s\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/documentatio
SF:n/guides/concepts/errors/#routing-errors\x20for\x20more\x20information\
SF:.\r\n\r")%r(HTTPOptions,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request
SF:\r\nConnection:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20
SF:text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-del21729\r\n\r\nR
SF:equested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternati
SF:ve\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7
SF:880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20wi
SF:th\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/doc
SF:umentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20inf
SF:ormation\.\r\n\r")%r(FourOhFourRequest,1B5,"HTTP/1\.1\x20421\x20Misdire
SF:cted\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nco
SF:ntent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-de
SF:l21722\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subje
SF:ct\x20Alternative\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\
SF:[b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20
SF:in\x20use\x20with\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.
SF:fastly\.com/documentation/guides/concepts/errors/#routing-errors\x20for
SF:\x20more\x20information\.\r\n\r")%r(tor-versions,94,"HTTP/1\.1\x20400\x
SF:20Bad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\nco
SF:ntent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-de
SF:l21727\r\n\r\nBad\x20Request")%r(RTSPRequest,94,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\nconten
SF:t-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-del217
SF:43\r\n\r\nBad\x20Request");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.12 seconds
```

Using option -p-

```
┌──(shiv㉿kali)-[~]
└─$ nmap -sV -p- target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:11 IST
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 34.37% done; ETC: 12:18 (0:04:54 remaining)
Stats: 0:07:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.40% done; ETC: 12:25 (0:06:18 remaining)
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.51% done; ETC: 12:27 (0:05:33 remaining)
Nmap scan report for target.com (151.101.130.187)
Host is up (0.00067s latency).
Other addresses for target.com (not scanned): 151.101.2.187 151.101.66.187 151.101.194.187
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy Varnish
443/tcp open  ssl/https  Varnish
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=11/28%Time=692948A2%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConne
SF:ction:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nx-served-by:\x20cache-del21749\r\n\r\nRequested\
SF:x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Nam
SF:es\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7880c70cd7
SF:6fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20with\x20thi
SF:s\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/documentatio
SF:n/guides/concepts/errors/#routing-errors\x20for\x20more\x20information\
SF:.\r\n\r")%r(HTTPOptions,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request
SF:\r\nConnection:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20
SF:text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-del21732\r\n\r\nR
SF:equested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternati
SF:ve\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7
SF:880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20wi
SF:th\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/doc
SF:umentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20inf
SF:ormation\.\r\n\r")%r(FourOhFourRequest,1B5,"HTTP/1\.1\x20421\x20Misdire
SF:cted\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nco
SF:ntent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-de
SF:l21749\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subje
SF:ct\x20Alternative\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\
SF:[b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20
SF:in\x20use\x20with\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.
SF:fastly\.com/documentation/guides/concepts/errors/#routing-errors\x20for
```

```
Host is up (0.00067s latency).
Other addresses for target.com (not scanned): 151.101.2.187 151.101.66.187 151.101.194.187
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy Varnish
443/tcp open  ssl/https  Varnish
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=11/28%Time=692948A2%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConne
SF:ction:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nx-served-by:\x20cache-del21749\r\n\r\nRequested\
SF:x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Nam
SF:es\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7880c70cd7
SF:6fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20with\x20thi
SF:s\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/documentatio
SF:n/guides/concepts/errors/#routing-errors\x20for\x20more\x20information\
SF:.\r\n\r")%r(HTTPOptions,1B5,"HTTP/1\.1\x20421\x20Misdirected\x20Request
SF:\r\nConnection:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20
SF:text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-del21732\r\n\r\nR
SF:equested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternati
SF:ve\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7
SF:880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20wi
SF:th\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/doc
SF:umentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20inf
SF:ormation\.\r\n\r")%r(FourOhFourRequest,1B5,"HTTP/1\.1\x20421\x20Misdire
SF:cted\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nco
SF:ntent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-de
SF:l21749\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subje
SF:ct\x20Alternative\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\
SF:[b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20
SF:in\x20use\x20with\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.
SF:fastly\.com/documentation/guides/concepts/errors/#routing-errors\x20for
SF:\x20more\x20information\.\r\n\r")%r(tor-versions,94,"HTTP/1\.1\x20400\x
SF:20Bad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\nco
SF:ntent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-de
SF:l21749\r\n\r\nBad\x20Request")%r(RTSPRequest,94,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\nconten
SF:t-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-del217
SF:49\r\n\r\nBad\x20Request");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1179.49 seconds
```

Using option -O

```
┌──(shiv㉿kali)-[~]
└─$ nmap -O --osscan-guess target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:38 IST
Nmap scan report for target.com (151.101.2.187)
Host is up (0.0051s latency).
Other addresses for target.com (not scanned): 151.101.66.187 151.101.130.187 151.101.194.187
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.08 seconds
```

3)DIRB

```
┌──(shiv㉿kali)-[~]
└─$ dirb http://target.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov 28 12:40:19 2025
URL_BASE: http://target.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://target.com/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')

-----------------
END_TIME: Fri Nov 28 12:40:19 2025
DOWNLOADED: 0 - FOUND: 0
```

4)whatweb

```
┌──(shiv㉿kali)-[~]
└─$ whatweb http://target.com
http://target.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.130.187], RedirectLocation[https://target.com/], UncommonHeaders[retry-after,x-served-by,x-cache-hits,x-timer], Varnish, Via-Proxy[1.1 varnish]
https://target.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.2.187], RedirectLocation[https://www.target.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[retry-after,x-served-by,x-cache-hits,x-timer], Varnish, Via-Proxy[1.1 varnish]
https://www.target.com/ [200 OK] Cookies[GuestLocation,TealeafAkaSid,accessToken,adScriptData,egsSessionId,idToken,onboardingGuest,refreshToken,sapphire,visitorId], Country[UNITED STATES][US], HTML5, HttpOnly[accessToken,egsSessionId,refreshToken], IP[199.232.22.187], Open-Graph-Protocol, OpenSearch[https://assets.targetimg1.com/webui/top-of-funnel/opensearchdescription.xml], Script[application/json,application/ld+json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], UncommonHeaders[referrer-policy,x-content-type-options,content-security-policy], X-Frame-Options[SAMEORIGIN]
```

5)Nikto

```
┌──(shiv㉿kali)-[~]
└─$ nikto -h http://target.com -o nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.130.187, 151.101.66.187, 151.101.2.187, 151.101.194.187
+ Target IP:          151.101.130.187
+ Target Hostname:    target.com
+ Target Port:        80
+ Start Time:         2025-11-28 12:44:34 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-del21746-DEL.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-del21746-DEL.
+ /: 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/
+ Root page / redirects to: https://target.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)

^[[A^[[A^[[-C all

- STATUS: Completed 2650 requests (~38% complete, 16.9 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.78495 sec, 10 requests: 0.8595 sec.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-11-28 13:01:53 (GMT5.5) (1039 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(shiv㉿kali)-[~]
└─$ cat nikto.txt
- Nikto v2.5.0/
+ Target Host: target.com
+ Target Port: 80
+ GET /: Retrieved via header: 1.1 varnish.
+ GET /: Retrieved x-served-by header: cache-del21746-DEL.
+ 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 /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/:
+ GET /: Uncommon header 'x-served-by' found, with contents: cache-del21746-DEL.
+ GET /: 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/:
```