Date:09/02/2025

LabPractical-9:

Web site: google-gruyere.appspot.com

IPAddress:142.250.71.116

```
┌──(student㉿student)-[~]
└─$ nikto -h https://google-gruyere.appspot.com -o output.html -Format html
Nikto v2.5.0
---------------------------------------------------------------------------
Multiple IPs found: 142.250.71.116, 2404:6800:4009:806::2014
Target IP:          142.250.71.116
Target Hostname:    google-gruyere.appspot.com
Target Port:        443
---------------------------------------------------------------------------
SSL Info:        Subject:  /CN=*.appspot.com
                 Ciphers:  TLS_AES_256_GCM_SHA384
                 Issuer:   /C=US/O=Google Trust Services/CN=WR2
Start Time:         2025-01-24 08:50:01 (GMT5.5)
---------------------------------------------------------------------------
Server: Google Frontend
/: 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-cloud-trace-context' found, with contents: 2b4e782e0fefc237ab1064faeb3fe4f2.
/: 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-Sec
rity
/: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs
Web/HTTP/Headers/alt-svc
/: 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/
```

The anti-click jacking X-Frame-Options header is not present.

Solution: Configure the server to include the X-Frame-Options header in HTTP responses to prevent click jacking attacks. Use the directive: 'X-Frame-Options: SAMEORIGIN' in the server's configuration file.

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Uncommon header's x-cloud-trace-context found.

Solution: Monitor and audit the usage of uncommon headers to ensure they do not leak sensitive information or introduce vulnerabilities.

Date:09/02/2025

The Strict-Transport-Security(HSTS)header is not defined.

Solution: Add the Strict-Transport-Security header to enforce secure connections. Use: 'Strict- Transport-Security: max-age=31536000; include Sub Domain's.

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport- Security

An alt-svc header was found advertising HTTP/3, which Nikto cannot test over QUIC.

Solution: Ensure HTTP/3 endpoints are tested with tools that support the protocol to identify any vulnerabilities.

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc

The X-Content-Type-Options header is not set.

Solution: Add the X-Content-Type-Options header to prevent browsers from interpreting files as a different MIME type. Use: 'X-Content-Type-Options: no sniff'.

Reference:https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Date:09/02/2025

Web site: hack this site.org :

IPAddress:137.74.187.104

```
┌──(student㉿student)-[~]
└─$ nikto -h https://hackthissite.org -o output.html -Format html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 137.74.187.104, 137.74.187.103, 137.74.187.100, 137.74.187.101, 137.74.187.102
+ Target IP:          137.74.187.104
+ Target Hostname:    hackthissite.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=GR/O=Hellenic Academic and Research Institutions CA/CN=HARICA DV TLS RSA
+ Start Time:         2025-01-24 08:52:07 (GMT5.5)
---------------------------------------------------------------------------
+ Server: HackThisSite
+ /: Cookie HackThisSite created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie HackThisSite created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved access-control-allow-origin header: *.
+ /: 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 'onion-location' found, with contents: http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/.
+ /: Uncommon header 'public-key-pins-report-only' found, with contents: pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-sha256="Vjs8r4z+80wjNcr1YKepWQbo
SIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains; report-uri="https://hackthissite.report-uri.com/r/d/hpkp/reportOnly".
+ /: 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/
```

Cookie Hack This Site created without the secure flag.

Solution: Ensure cookies are sent only over HTTP Sby enabling the 'Secure' flag.
Use: 'Set- Cookie: name=value; Secure'.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Cookie Hack This Site created without the http only flag.

Solution: Set the 'Http Only' flag for cookie store strict access to client-side scripts. Use: 'Set-Cookie: name=value; Http Only.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Date:09/02/2025

Access-Control-Allow-Origin header is set to'*'.

Solution: Avoid using wild cards(*) in the Access-Control-Allow-Origin header. Specify trusted domains explicitly.

The anti-click jacking X-Frame-Options header is not present.

Solution: Include the X-Frame-Options header to prevent click jacking. Use: 'X-Frame-Options: SAMEORIGIN'.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Uncommon header onion-location found.

Solution: Review the use of onion-location headers to ensure they do not expose sensitive data.

Uncommon header's public-key-pins-report-only found.

Solution: Validate the configuration of HPKP(HTTP Public Key Pinning)headers to ensure they meet security requirements.

The X-Content-Type-Options header is not set.

Solution: Add the X-Content-Type-Options header to prevent MIME type sniffing. Use: 'X- Content-Type-Options: no sniff'.

Reference:https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Date:09/02/2025

Website: hbh.sh

IP Address:
104.21.63.208

```
┌──(student㉿student)-[~]
└─$ nikto -h https://hbh.sh -o output.html -Format html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.21.63.208, 172.67.150.93, 2606:4700:3031::6815:3fd0, 2606:4700:3030::ac43:965d
+ Target IP:          104.21.63.208
+ Target Hostname:    hbh.sh
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=hbh.sh
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services/CN=WE1
+ Start Time:         2025-01-24 08:53:26 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved access-control-allow-origin header: https://*.hbh.sh.
+ /: 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 'server-timing' found, with contents: cfL4;desc="?proto=TCP&rtt=166496&min_rtt=164716&rtt_var=47716&sent=5&recv=7&lost=0&retrans=0&sent_bytes=2813&rec
v_bytes=8046&delivery_rate=1752076&cwnd=236&unsent_bytes=0&cid=bd77d6d2c584b4f6&ts=3206&x=0".
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs
/Web/HTTP/Headers/alt-svc
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl/tls alert han
dshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-01-24 08:55:31 (GMT5.5) (125 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Cookie XSRF-TOKEN created without the http only flag.

Solution: Set the 'Http Only' flag for cookies to improve security.
Use: 'Set-Cookie: name=value; Http Only.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Access-Control-Allow-Origin header includes a wild card.

Solution: Restrict the Access-Control-Allow-Origin header to trusted origin stop prevent unauthorized access.

The anti-click jacking X-Frame-Options header is not present.

Date:09/02/2025

Solution:AddtheX-Frame-Optionsheadertopreventclickjacking.Use:'X-Frame-Options: SAMEORIGIN'.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Uncommon header server-timing found.

Solution: Analyze the server-timing header to ensure it does not expose sensitive server performance metrics.

An alt-svc header was found advertising HTTP/3, which Nikto cannot test over QUIC.

Solution: Test HTTP/3 end points with tools that support the protocol to identify any vulnerabilities.

Reference:https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc

robots.txt contains one entry that should be manually reviewed.

Solution: Review the/robots.txt file to ensure it does not disclose sensitive information. Reference: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt