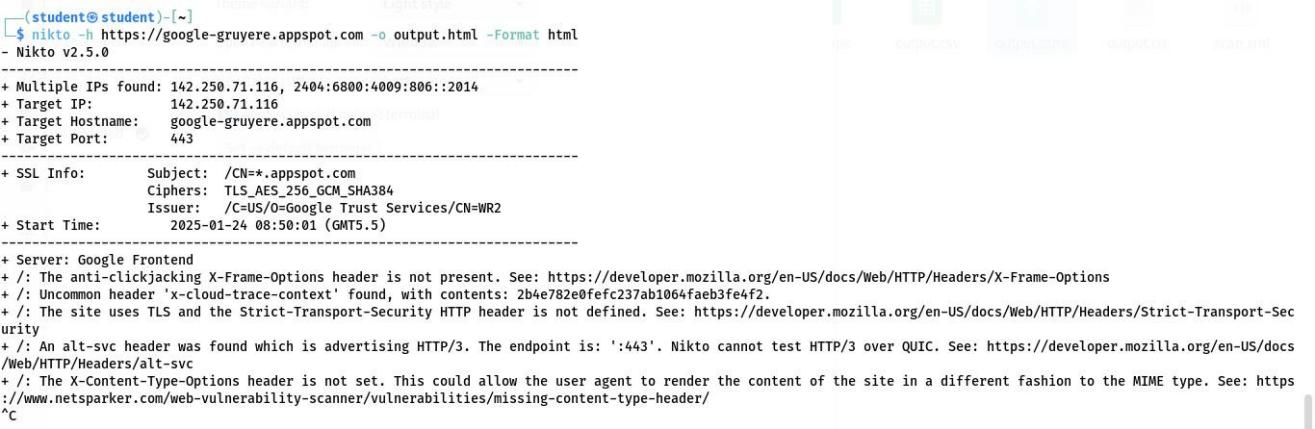
**LabPractical-9:**

# Web site: google-gruyere.appspot.com

IPAddress:142.250.71.116



## 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.

## 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

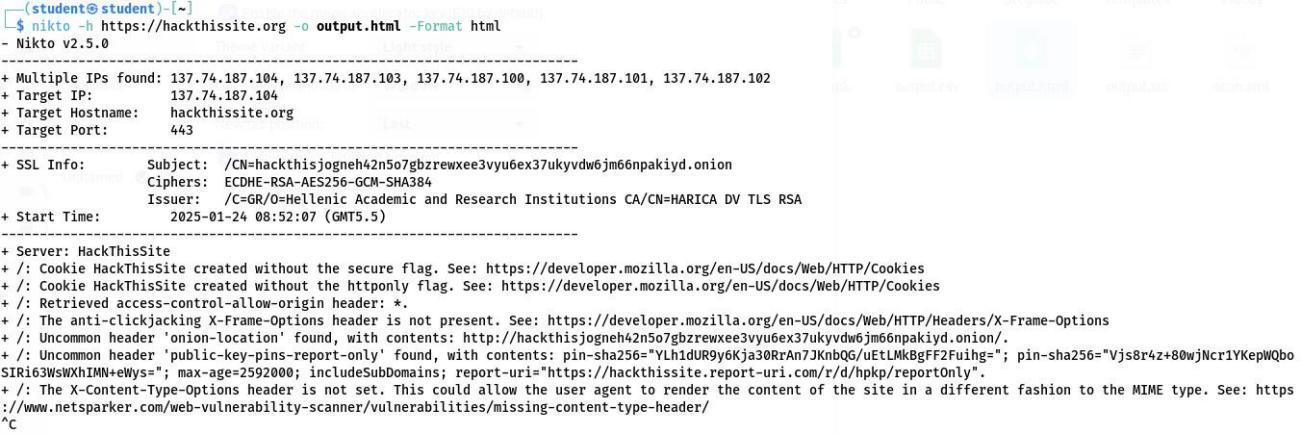
## The X-Content-Type-Options header is not set.

**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/>

# Web site: hack this site.org :

IPAddress:137.74.187.104



## 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>

## 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.

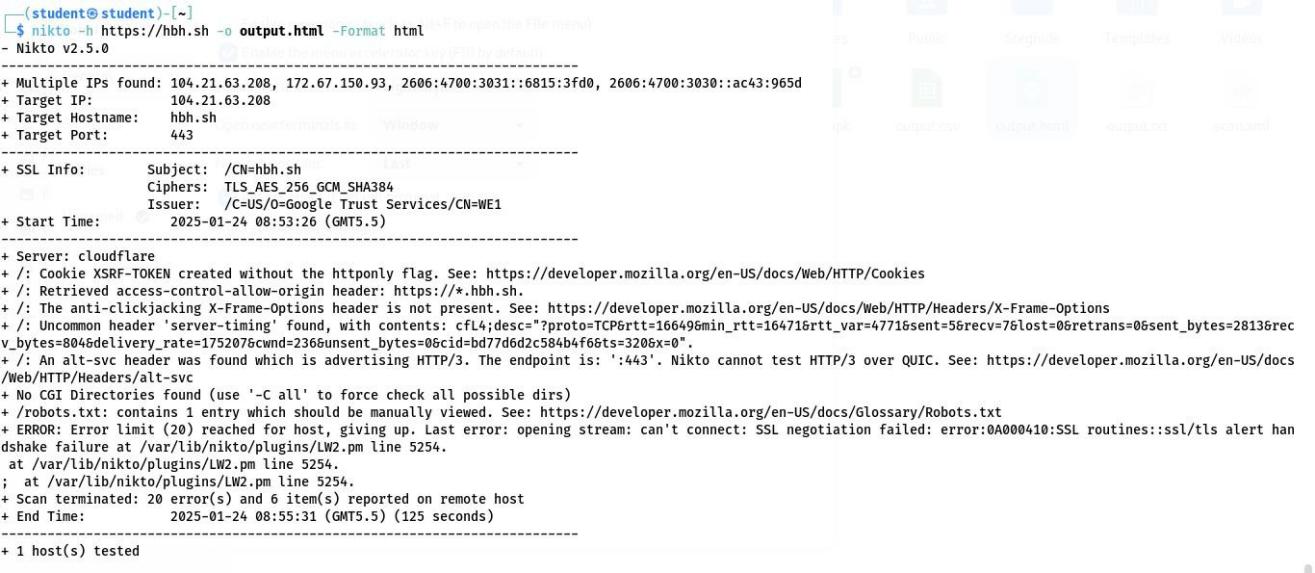
**Solution**: Add the X-Content-Type-Options header to prevent MIME type sniffing. Use: 'X- Content-Type-Options: no sniff'.

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

# Website: hbh.sh

IP Address:

104.21.63.208



## 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.

**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>