Pentest Tools

Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	–	✓
Cross-Site Scripting	–	✓
Local/Remote File Inclusion	–	✓
Remote command execution	–	✓
Discovery of sensitive files	–	✓

✓ **https://workspace.google.com/intl/en-US/gmail/**

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:

Critical:	0
High:	0
Medium:	1
Low:	4
Info:	34

Scan information:

Start time:	May 02, 2025 / 08:02:22 UTC+03
Finish time:	May 02, 2025 / 08:03:47 UTC+03
Scan duration:	1 min, 25 sec
Tests performed:	39/39
Scan status:	Finished

Findings

Insecure cookie setting: domain too loose

port 443/tcp

CONFIRMED

URL	Cookie Name	Evidence
https://workspace.google.com/intl/en-US/gmail/	NID	Set-Cookie: .google.com Request / Response

Details

Risk description:

The risk is that a cookie set for example.com may be sent along with the requests sent to dev.example.com, calendar.example.com, hostedsite.example.com. Potentially risky websites under your main domain may access those cookies and use the victim session from the main site.

Recommendation:
The `Domain` attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to `Domain=app.mysite.com`

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://workspace.google.com/intl/en-US/gmail/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Unsafe security header: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence

https://workspace.google.com/intl/en-US/gmail/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`report-uri:  report-uri is deprecated in CSP3. Please use the report-to directive instead.`
	`script-src:  https: URI in script-src allows the execution of unsafe scripts.`
	`script-src:  http: URI in script-src allows the execution of unsafe scripts.`
	`default-src:  The default-src directive should be set as a fall-back when other restrictions ha`
	`ve not been specified.`
	Request / Response

Details

Risk description:
For example, if the unsafe-inline directive is present in the CSP header, the execution of inline scripts and event handlers is allowed. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

Recommendation:
Remove the unsafe values from the directives, adopt nonces or hashes for safer inclusion of inline scripts if they are needed, and explicitly define the sources from which scripts, styles, images or other resources can be loaded.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:

CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Robots.txt file found

CONFIRMED

port 443/tcp

URL
https://workspace.google.com/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

port 443/tcp

Software / Version	Category
Google Analytics	Analytics
Google Font API	Font scripts
HTTP/3	Miscellaneous
Open Graph	Miscellaneous
Google Tag Manager	Tag managers
HSTS	Security

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

port 443/tcp

URL

Missing: https://workspace.google.com/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for error messages.

Nothing was found for debug messages.

Nothing was found for code comments.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for missing HTTP header - Content Security Policy.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for missing HTTP header - Feature.

Nothing was found for passwords submitted in URLs.

Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for cross domain file inclusion.

Nothing was found for internal error code.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for login interfaces.

Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Nothing was found for SQL statement in request parameter.

Nothing was found for password returned in later response.

Nothing was found for Path Disclosure.

Nothing was found for Session Token in URL.

Nothing was found for API endpoints.

Nothing was found for emails.

Scan coverage information

List of tests performed (39/39)

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for passwords submitted unencrypted...
- ✓ Checking for error messages...
- ✓ Checking for debug messages...
- ✓ Checking for code comments...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Feature...
- ✓ Checking for passwords submitted in URLs...
- ✓ Checking for mixed content between HTTP and HTTPS...
- ✓ Checking for cross domain file inclusion...
- ✓ Checking for internal error code...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for login interfaces...
- ✓ Checking for secure password submission...
- ✓ Checking for sensitive data...
- ✓ Checking for OpenAPI files...
- ✓ Checking for file upload...
- ✓ Checking for SQL statement in request parameter...
- ✓ Checking for password returned in later response...
- ✓ Checking for Path Disclosure...
- ✓ Checking for Session Token in URL...
- ✓ Checking for API endpoints...
- ✓ Checking for emails...

Scan parameters

target:	https://workspace.google.com/intl/en-US/gmail/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	10
Average time until a response was received:	37ms