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://code-builder--kevinbash99.replit.app/**

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:	2
Low:	4
Info:	33

Scan information:

Start time:	Jan 14, 2026 / 15:00:39 UTC+02
Finish time:	Jan 14, 2026 / 15:01:07 UTC+02
Scan duration:	28 sec
Tests performed:	39/39
Scan status:	Finished

Findings

Insecure cookie setting: missing Secure flag

port 443/tcp

CONFIRMED

URL	Cookie Name	Evidence
https://code-builder--kevinbash99.replit.app/	GAESA	Set-Cookie: GAESA=CpoBMDA1ZWI2OTc0YzhiY2M1ZmIzODdmNzM0ZTFhNzQxMDJkYjg4MzhmY2I1YmY0YzExODRiZTZiY2ZlOTJlNzAxM2ZmYWZkODEyYWVlMGQ0MWU4M2RlYzRhZTM5ODVmZjI5OTRmNjAzNGNlYjJlYzQwZDc5MmQ5MDRiM2VhYzU3M2I1Mjk4MDA2OWNmNDY1NTliYTg4ODZjNTlkZBDIreDkuzM Request / Response

⌄ Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

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

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

port 443/tcp

URL	Cookie Name	Evidence
https://code-builder--kevinbash99.replit.app/	GAESA	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: GAESA=CpoBMDA1ZWI2OTc0YzhiY2M1ZmIzODdmNzM0ZTFhNzQxMDJkYjg4MzhmY2I1YmY0YzExODRiZTZiY2ZlOTJlNzAxM2ZmYWZkODEyYWVlMGQ0MWU4M2RlYzRhZTM5ODVmZjI5OTRmNjAzNGNlYjJlYzQwZDc5MmQ5MDRiM2VhYzU3M2I1Mjk4MDA2OWNmNDY1NTliYTg4ODZjNTlkZBDlreDkuzM Request / Response

⌄ Details

Risk description:
The risk is that an attacker who injects malicious JavaScript code on the page (e.g. by using an XSS attack) can access the cookie and can send it to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:
Ensure that the HttpOnly flag is set for all cookies.

References:
https://owasp.org/www-community/HttpOnly

Classification:
CWE : CWE-1004
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://code-builder--kevinbash99.replit.app/	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

Missing security header: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://code-builder--kevinbash99.replit.app/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

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

Missing security header: X-Content-Type-Options

CONFIRMED

port 443/tcp

URL	Evidence
https://code-builder--kevinbash99.replit.app/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693
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 Cloud	IaaS
Google Cloud CDN	CDN

Google Cloud Trace	Performance
Express	Web frameworks, Web servers
Google Font API	Font scripts
HTTP/3	Miscellaneous
Lucide	Font scripts
Node.js	Programming languages
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

CONFIRMED

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Nothing was found for absence of the security.txt file.

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 passwords submitted in URLs.

Nothing was found for domain too loose set for cookies.

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 login interfaces.

Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for unsafe HTTP header Content Security Policy.

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.

Nothing was found for missing HTTP header - Rate Limit.

Scan coverage information

List of tests performed (39/39)

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

Scan parameters

target:	https://code-builder--kevinbash99.replit.app/
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:	175ms