

DL-vScanly

Security Assessment Report

Automated Vulnerability Analysis

Project: Illustrative report example
Target URL: https://example.com/
Scan ID: 00000000-0000-4000-8000-000000000001
Generated: 2026-10-12T03:00:00Z
Report Type: Full report

Overall Risk Score

2.0 /100

Risk Level

PARTIALLY ASSESSED

2 finding(s) lack a valid CVSS score. Scored portion: no scored risk signal. Review severity and evidence alongside this partial score.

Total Findings

2

Critical + High

0

Pages Crawled

1

URL Risk Rows

1

Severity Distribution



Critical	0 (0.0%)
High	0 (0.0%)
Medium	1 (50.0%)
Low	1 (50.0%)
Info	0 (0.0%)

Summary · Executive Summary

This fictional example illustrates the report format and is not an assessment of a real site. It shows two security-header signals and remediation guidance. Review service configuration and compatibility before making production changes.

Assessment scope and limitations

Scan type: Quick scan · Status: Completed

Scan window: 2026-10-12T02:59:50Z to 2026-10-12T03:00:00Z

Findings are automated signals pending verification. Detection confidence differs from severity. Absence of findings does not prove security; inaccessible pages and checks outside the configured scope remain unassessed.

Risk scores are product indicators, not CVSS scores. Standards mapping and percentages do not certify compliance. All explanations require review against the evidence. Sensitive headers and credential fields are masked in exports; review remaining evidence before sharing.

Executive Summary

2 automated finding(s) are included. None are rated critical or high. 2 finding(s) lack a valid CVSS score, so the overall assessment is partial. Validate evidence before planning a change. Test the fix and key user flows in staging, then repeat the relevant check.

Priority Actions (Top 2)

Address these first — ordered by severity and impact. Each item links to the detailed finding below.

#1

[MEDIUM] Content-Security-Policy

Inventory required resources and validate Content-Security-Policy-Report-Only in staging. Test login, checkout and third-party scripts before gradual enforcement and a follow-up check.

#2

[LOW] Strict-Transport-Security

Confirm HTTPS support across required services and validate with a short max-age. Do not enable includeSubDomains or preload before checking HTTPS readiness across all subdomains.

Detailed Findings

2 findings form 2 evidence groups. This PDF includes 2 groups ordered by severity. See the JSON report for all findings.

MEDIUM**#1 Content-Security-Policy****Affected URL****example.com**

- <https://example.com/>

Parameter

Content-Security-Policy

Automated signal; verification required · Detection confidence: 0.8

1. Summary

The collected response did not include a CSP header. Review the browser resource execution policy.

2. Impact**Business Impact: MEDIUM**

An additional defense against some script injection attacks may be absent. This finding alone does not confirm an XSS vulnerability or successful exploitation.

3. What to do next

Inventory required resources and validate Content-Security-Policy-Report-Only in staging. Test login, checkout and third-party scripts before gradual enforcement and a follow-up check.

4. Technical details**Detection / scan method**

Configuration check of collected response headers

5. Evidence & verification**Source / Evidence Excerpt**

```
[response-header] Content-Security-Policy: absent
```

LOW**#2 Strict-Transport-Security****Affected URL****example.com**

- <https://example.com/>

Parameter

Strict-Transport-Security

Automated signal; verification required · Detection confidence: 0.8

1. Summary

The collected HTTPS response did not include an HSTS header.

2. Impact**Business Impact: LOW**

An additional browser HTTPS policy may be absent. Actual impact depends on redirects, domain configuration and client conditions.

3. What to do next

Confirm HTTPS support across required services and validate with a short max-age. Do not enable includeSubDomains or preload before checking HTTPS readiness across all subdomains.

4. Technical details

Detection / scan method

Configuration check of collected response headers

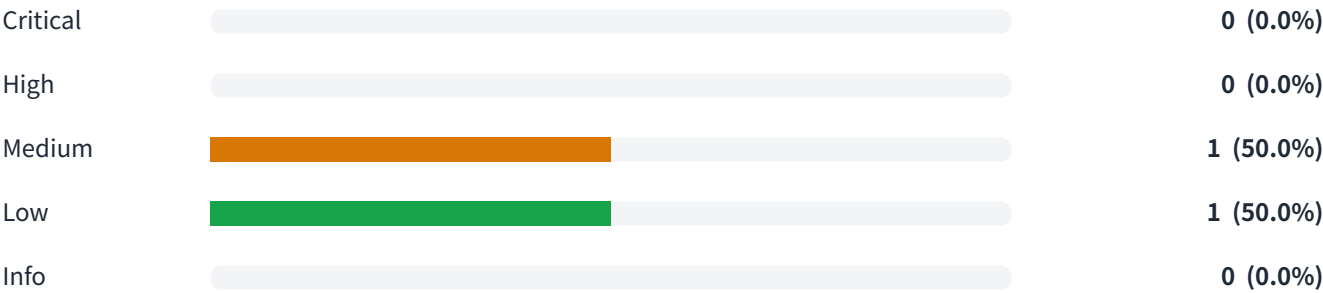
5. Evidence & verification

Source / Evidence Excerpt

[response-header] Strict-Transport-Security: absent

Appendix

Severity Distribution



URL Risk Summary

URL	Risk %	Findings
https://example.com/	—	2

Showing 1 of 1 URL rows. A dash means the score is not recorded. Consult the JSON report for all rows.

How this report is organised

Each finding follows: summary / risk / what to do next / (appendix) technical details and evidence. This export uses your selected report language.

- 1. Summary — what it is and why it matters
- 2. Risk — business impact
- 3. Actions — what to do next (priority list first)
- 4. Technical details — for engineering review
- 5. Evidence — how we verified it
- 6. Appendix — charts, URL risk, compliance