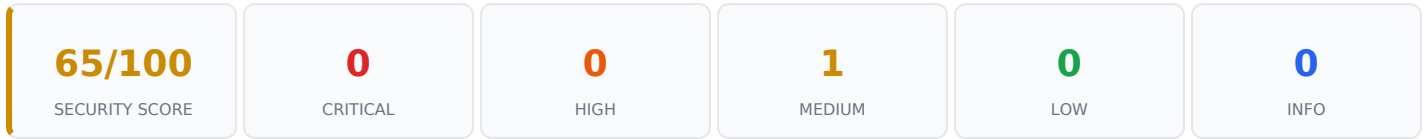


EXECUTIVE SUMMARY

This report covers an automated security assessment of https://app.example.com, run in comprehensive mode on 2026-09-08.

1 verified finding(s) were retained, of which 0 require prompt attention (critical or high).

Confirmation level: 0 confirmed (the exploit was reproduced), 1 observed (the behaviour was seen directly), 0 inconclusive (no replayable proof — leads to triage, not confirmed exploits).



WHAT THIS SCAN COULD NOT TEST

- DEMONSTRATION ONLY. All findings, scores, timestamps and evidence in this report are fictional. No target was scanned to produce this sample.
- This fictional example covers public pages only. Authenticated areas and business logic are outside the illustrated scope.

TARGET	SCAN TYPE	SCAN DATE	RISK LEVEL	TOTAL FINDINGS
https://app.example.com	Comprehensive	2026-09-08	MEDIUM	1

FINDINGS SUMMARY

#	TITLE	SEVERITY	CVSS	CWE	OWASP	STATUS
1	Sample finding: missing frame embedding restriction	MEDIUM	—	CWE-1021	A05:2021	Open

Sample finding: missing frame embedding restriction

MEDIUM

DESCRIPTION

Fictional example: a public account page is served without a frame-ancestors policy or X-Frame-Options header. An unrelated site may be able to embed the page. Actual impact depends on the page and browser behavior.

AFFECTED URL

https://app.example.com/account

REMEDIATION

Define a Content-Security-Policy frame-ancestors directive that matches the application's embedding requirements. Use 'none' when no embedding is required, or an explicit allowlist when it is. Deploy the header and retest the relevant pages.

EVIDENCE / PROOF OF CONCEPT

HTTP_RESPONSE

```
FICTIONAL SAMPLE RESPONSE
GET /account HTTP/1.1
Host: app.example.com

HTTP/1.1 200 OK
Content-Type: text/html
X-Frame-Options: (absent)
Content-Security-Policy: (absent)
```

CWE: CWE-1021

OWASP: A05:2021

Status: Open

Confirmation level: Observed (header_analysis)