SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

28 /100

GRADE
C

Safe, authorized simulation results

RISK LEVEL
Medium

FINDINGS
2

PACKAGE
Owasp Starter

SCAN DATE
01 Aug 2026

STATUS
Completed

REPORT TYPE
Client Evidence

Confidential security evidence

This report is intended for authorized stakeholders and contains safe passive assessment results.

Contents

Executive Summary

This report summarises the findings from an automated security simulation performed by BreakMesh against **https://example-customer.com**. All checks are passive and safe-simulated — no destructive payloads are used. Overall result: grade **C** with a risk score of **28/100** and **Medium** risk.

RISK SCORE	GRADE	RISK LEVEL	TOTAL FINDINGS
28/100	**C**	**Medium**	**2**

SEVERITY	FINDINGS	RECOMMENDED ACTION
HIGH	1	Remediate within days
LOW	1	Schedule remediation in backlog

Executive Actions

What passed: **0** checks completed without findings. What needs action: **2** checks produced findings for review.

Checks Performed

The **Owasp Starter** package included **14** checks in scope. **0** completed without producing findings.
Effectively tested 0 of 14 checks. 12 checks were inconclusive (could not reach the target, or the check has an inherent tooling limitation — see the report for the specific reason) and are not counted as passing.

CHECK OUTCOME	COUNT	CHECKS
Passed	0	- No passing checks recorded
Needs review	2	- CSP Quality Review - Source Map Exposure
Inconclusive	12	- CORS Policy (No execution record is available for this check) - CORS Edge Cases (null origin / preflight) (No execution record is available for this check) - Open Redirect (No execution record is available for this check) - Directory Listing (No execution record is available for this check) - Sensitive Files (No execution record is available for this check) - Secrets in JavaScript Bundles (No execution record is available for this check) - Trusted Types Signal (No execution record is available for this check) - Deprecated Browser APIs (No execution record is available for this check) + 4 more references

Scope & Confidence

Breakmesh is a continuous safeguard, not a guarantee of safety. This scan identifies and prioritises common, detectable weaknesses so they can be fixed before an attacker finds them — it reduces risk but cannot prove the absence of every

vulnerability. No scanner can. Absence of findings means the checks that ran did not surface an issue, not that the target is immune to attack. Use these results as one layer of a defense-in-depth programme alongside secure development, timely patching, monitoring, and periodic human-led penetration testing.

SOC 2 Evidence Mapping

This mapping shows which SOC 2 trust service themes the completed checks can support as audit evidence.

SOC 2 THEME	MAPPED CHECKS	FINDINGS
Security	14	2
Confidentiality	8	2
Privacy	2	
Processing Integrity	2	

PCI-DSS v4.0 Control Mapping

This mapping shows which PCI-DSS v4.0 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
1.2.1	8	
1.3.1	10	
11.3.1	21	
4.2.1	7	
6.2.4	49	2
6.3.1	4	
6.4.1	7	
7.2.1	29	
8.3.1	19	

ISO/IEC 27001:2022 Control Mapping

This mapping shows which ISO/IEC 27001:2022 controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
A.5.18	10	
A.5.24	3	
A.5.34	3	
A.8.14	7	
A.8.20	8	
A.8.24	7	
A.8.26	12	
A.8.28	31	
A.8.3	19	
A.8.5	19	
A.8.8	4	
A.8.9	26	2

HIPAA Security Rule Control Mapping

This mapping shows which HIPAA Security Rule controls the completed checks can support as audit evidence.

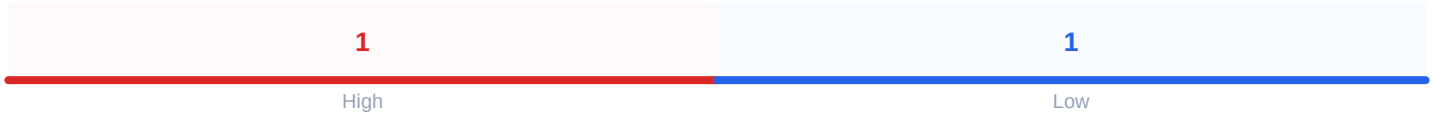
CONTROL	MAPPED CHECKS	FINDINGS
164.308(a)(1)	4	
164.308(a)(6)	3	
164.308(a)(7)	7	
164.312(a)(1)	37	
164.312(c)(1)	37	2
164.312(d)	19	
164.312(e)(1)	22	
164.502	3	

DPDP Act 2023 (India) Control Mapping

This mapping shows which DPDP Act 2023 (India) controls the completed checks can support as audit evidence.

CONTROL	MAPPED CHECKS	FINDINGS
Rule 6(a)	33	2
Rule 6(b)	19	
Rule 6(d)	4	
Sec 11-14	3	
Sec 6	3	
Sec 8(4)	3	
Sec 8(5)	88	2
Sec 8(6)	3	

Severity Distribution



Master Findings Table

Every finding in this report, worst first. Each is written up in full under Detailed Findings, and can be referred to by the ID shown here.

ID	FINDING	SEVERITY
	Content Security Policy Not Enforced	HIGH
	Source Map Exposure	LOW

Detailed Findings

Content Security Policy Not Enforced

HIGH

No Content-Security-Policy header is enforced, or it is set in report-only mode only.

AFFECTED URL	https://example-customer.com/
CONFIDENCE	High
VERIFICATION	Indicative
REVIEW	Legacy verification requires review
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Security **PCI-DSS v4.0**: 6.2.4 **ISO/IEC 27001:2022**: A.8.9 **HIPAA Security Rule**: 164.312(c)(1) **DPDP Act 2023 (India)**: Rule 6(a), Sec 8(5)
REMEDIATION	Deploy a restrictive, enforced CSP starting from default-src 'self' and tighten it based on actual script/style sources.
EVIDENCE	`observed: No Content-Security-Policy header is enforced, or it is set in report-only mode only.`
REFERENCES	- OWASP Secure Headers Project

Source Map Exposure

LOW

A JavaScript source map is publicly accessible, revealing original (unminified) source structure.

AFFECTED URL	https://example-customer.com/static/app.js.map
CONFIDENCE	High
VERIFICATION	Indicative
REVIEW	Legacy verification requires review
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Security **PCI-DSS v4.0**: 6.2.4 **ISO/IEC 27001:2022**: A.8.9 **HIPAA Security Rule**: 164.312(c)(1) **DPDP Act 2023 (India)**: Rule 6(a), Sec 8(5)
REMEDIATION	Remove source maps from production deploys or restrict them to authenticated internal access.
EVIDENCE	`observed: A JavaScript source map is publicly accessible, revealing original (unminified) source structure.`

Appendix A — Scope & Methodology

This assessment combines automated checks from the BreakMesh catalogue with the industry methodologies below. Checks are mapped onto these standards; the standards are not run in place of them.

METHODOLOGY	APPLIED AS
OWASP Testing Guide v4.2	The web application testing methodology our check catalogue is structured against.
OWASP ASVS	Application Security Verification Standard - the control set our packages map to.
OWASP API Security Top 10	Used for the API Security package, including BOLA/BFLA and mass assignment.
PTES	Penetration Testing Execution Standard - the engagement structure for Active Pentest.
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment.
BreakMesh safe-simulation model	Passive checks observe only. Active probes are consent-gated, scope-locked, request-budgeted and never carry a destructive payload.
Race conditions / TOCTOU	Business-logic race conditions are assessed during human-led Active Pentest engagements, not automated scanning: confirming one means causing it, and it needs knowledge of the specific application flow.

On proof of exploitation: this report records the request and response that demonstrate each finding. It deliberately does not include runnable exploit code. A security report is forwarded widely, and a working attack script reaches everyone it is forwarded to.

Tests that can change data: not allowed for this scan, which is the default. Every check here observed only, or sent crafted requests that change nothing. Checks that can find a problem only by causing it were skipped and are marked as not run in the Check Register.

Appendix B — Check Register

Every check in this package and what it produced, including those that ran and found nothing. The summary earlier in this report gives counts; this is the evidence behind them, so a question of the form "was X tested?" can be answered directly.

CHECK	OUTCOME	DETAIL
CSP Quality Review	Needs review	Finding raised - see Detailed Findings
Source Map Exposure	Needs review	Finding raised - see Detailed Findings
CORS Policy	Inconclusive	No execution record is available for this check
CORS Edge Cases (null origin / preflight)	Inconclusive	No execution record is available for this check
Open Redirect	Inconclusive	No execution record is available for this check
Directory Listing	Inconclusive	No execution record is available for this check
Sensitive Files	Inconclusive	No execution record is available for this check
Secrets in JavaScript Bundles	Inconclusive	No execution record is available for this check
Trusted Types Signal	Inconclusive	No execution record is available for this check
Deprecated Browser APIs	Inconclusive	No execution record is available for this check
Harmless Reflected XSS Indicators	Inconclusive	No execution record is available for this check
Safe SQL Injection Indicators	Inconclusive	No execution record is available for this check
SSTI Template Injection Indicator	Inconclusive	No execution record is available for this check
Error Disclosure Expansion	Inconclusive	No execution record is available for this check

Appendix C — Glossary

Plain-English definitions for the specialist terms used in this report. Only the terms this report actually uses are listed.

TERM	WHAT IT MEANS
SQL injection	An attacker types database commands into an ordinary input box. If the site passes that text to its database unchecked, they can read or change data they should never see.
Cross-site scripting (XSS)	An attacker gets their own code to run inside another visitor's browser on your site. That code can steal the visitor's session and act as them.
Server-side template injection (SSTI)	An attacker's input is treated as part of the page template rather than as text, which can let them run code on the server.
Open redirect	Your site forwards visitors to any address supplied in the URL. Attackers borrow your domain's good name to make a phishing link look trustworthy.
CORS	Cross-Origin Resource Sharing. The browser rule deciding which other websites may read your site's responses. Set too loosely, any site can read your data.
Content Security Policy (CSP)	A header listing where a page is allowed to load code from. It is the main defence that limits the damage of cross-site scripting.