SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

35 /100

GRADE
C

Safe, authorized simulation results

RISK LEVEL	FINDINGS
Medium	2
PACKAGE	SCAN DATE
Api Security	01 Aug 2026
STATUS	REPORT TYPE
Completed	Client Evidence

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 **35/100** and **Medium** risk.

RISK SCORE	GRADE	RISK LEVEL	TOTAL FINDINGS
35/100	**C**	**Medium**	**2**

SEVERITY	FINDINGS	RECOMMENDED ACTION
HIGH	1	Remediate within days
MEDIUM	1	Remediate within current sprint

Executive Actions

What passed: **14** checks completed without findings. What needs action: **2** checks produced findings for review.

Checks Performed

The **Api Security** package ran **16** checks. **14** completed without producing findings.
Effectively tested 16 of 16 checks.

CHECK OUTCOME	COUNT	CHECKS
Passed	14	- API Documentation Exposure - HTTP Method Exposure - Versioned Endpoint Discovery - Endpoint Auth Indicators - Excessive API CORS Checks - Sensitive Response Pattern Detection - API Rate-Limit Readiness - API Third-Party Dependency Inventory + 6 more references
Needs review	2	- JWT Weakness Detection - Shadow API Discovery

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	16	2
Availability	3	
Confidentiality	5	2
Privacy	3	
Processing Integrity	8	1

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	20	
4.2.1	7	
6.2.4	48	2
6.3.1	4	
6.4.1	7	
7.2.1	28	
8.3.1	18	

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	2
A.8.28	30	
A.8.3	18	
A.8.5	18	
A.8.8	4	
A.8.9	26	

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)	36	
164.312(c)(1)	36	
164.312(d)	18	
164.312(e)(1)	22	2
164.502	3	

Detailed Findings

JWT Accepts "alg: none"

HIGH

The API's JWT validation accepted a token with the alg header set to none, bypassing signature verification.

AFFECTED URL	https://example-customer.com/api/v1/token
CONFIDENCE	High
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Processing Integrity, Security **PCI-DSS v4.0**: 6.2.4 **ISO/IEC 27001:2022**: A.8.26 **HIPAA Security Rule**: 164.312(e)(1)
REMEDIATION	Explicitly allow-list accepted signing algorithms server-side and reject unsigned/none-alg tokens.
EVIDENCE	`observed: The API's JWT validation accepted a token with the alg header set to none, bypassing signature verification.`
REFERENCES	- OWASP API2:2023 Broken Authentication

Undocumented Internal API Endpoint

MEDIUM

An undocumented API path outside the published API surface responded to requests without rate limiting.

AFFECTED URL	https://example-customer.com/api/v2/internal
CONFIDENCE	Medium
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Security **PCI-DSS v4.0**: 6.2.4 **ISO/IEC 27001:2022**: A.8.26 **HIPAA Security Rule**: 164.312(e)(1)
REMEDIATION	Inventory all live API routes against documented ones and either publish, protect, or remove undocumented endpoints.
EVIDENCE	`observed: An undocumented API path outside the published API surface responded to requests without rate limiting.`

Scan ID: d76f55c4-63d9-53e2-8cca-ec4be9f8c38b · This report is confidential and intended solely for the authorised owner of example-customer.com. Breakmesh performs passive simulation only. All findings should be validated by a qualified security professional prior to remediation.