



SECURITY ASSESSMENT REPORT

Authorized Security Report

Prepared for the authorized owner of

example-customer.com

OVERALL RISK SCORE

35 /100



Safe, authorized simulation results

RISK LEVEL

Medium

PACKAGE

Api Security

STATUS

Completed

FINDINGS

2

SCAN DATE

01 Aug 2026

REPORT TYPE

Client Evidence

Confidential security evidence

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

Generated by BreakMesh

Contents

Executive Summary	3
Executive Actions	3
Checks Performed	3
Scope & Confidence	3
SOC 2 Evidence Mapping	4
PCI-DSS v4.0 Control Mapping	4
ISO/IEC 27001:2022 Control Mapping	5
HIPAA Security Rule Control Mapping	5
DPDP Act 2023 (India) Control Mapping	6
Severity Distribution	6
Master Findings Table	6
Detailed Findings	6
Appendix A — Scope & Methodology	8
Appendix B — Check Register	9
Appendix C — Glossary	10

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

Checks Performed

The **Api Security** package included **16** checks in scope. **0** completed without producing findings. Effectively tested 0 of 16 checks. 14 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	- JWT Weakness Detection - Shadow API Discovery
Inconclusive	14	- API Documentation Exposure (No execution record is available for this check) - HTTP Method Exposure (No execution record is available for this check) - Versioned Endpoint Discovery (No execution record is available for this check) - Endpoint Auth Indicators (No execution record is available for this check) - Excessive API CORS Checks (No execution record is available for this check) - Sensitive Response Pattern Detection (No execution record is available for this check) - API Rate-Limit Readiness (No execution record is available for this check) - API Third-Party Dependency Inventory (No execution record is available for this check) + 6 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	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	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	2
A.8.28	31	
A.8.3	19	
A.8.5	19	
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)	37	
164.312(c)(1)	37	
164.312(d)	19	
164.312(e)(1)	22	2
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	
Rule 6(b)	19	
Rule 6(d)	4	
Sec 11-14	3	
Sec 6	3	
Sec 8(4)	3	
Sec 8(5)	88	
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
	JWT Accepts "alg: none"	HIGH
	Undocumented Internal API Endpoint	MEDIUM

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
VERIFICATION	Indicative
REVIEW	Legacy verification requires review
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
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.8.26 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.

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
JWT Weakness Detection	Needs review	Finding raised - see Detailed Findings
Shadow API Discovery	Needs review	Finding raised - see Detailed Findings
API Documentation Exposure	Inconclusive	No execution record is available for this check
HTTP Method Exposure	Inconclusive	No execution record is available for this check
Versioned Endpoint Discovery	Inconclusive	No execution record is available for this check
Endpoint Auth Indicators	Inconclusive	No execution record is available for this check
Excessive API CORS Checks	Inconclusive	No execution record is available for this check
Sensitive Response Pattern Detection	Inconclusive	No execution record is available for this check
API Rate-Limit Readiness	Inconclusive	No execution record is available for this check
API Third-Party Dependency Inventory	Inconclusive	No execution record is available for this check
GraphQL Introspection Exposure	Inconclusive	No execution record is available for this check
GraphQL DoS Readiness (Batching / Alias / Depth)	Inconclusive	No execution record is available for this check
WebSocket Security Check	Inconclusive	No execution record is available for this check
Subresource Integrity (SRI) Missing	Inconclusive	No execution record is available for this check
Dependency CVE Matching (SBOM)	Inconclusive	No execution record is available for this check
Drive-by Download / Malicious Redirect Chain	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
CVE	Common Vulnerabilities and Exposures. A public reference number for one specific known flaw in a specific piece of software.
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.
JWT	JSON Web Token. A signed ticket proving who a user is. If the signature is not checked properly, anyone can forge one and become any user.
GraphQL introspection	A built-in query that returns the API's entire schema. Left open, it hands an attacker a complete map of your data and operations.
SBOM	Software Bill of Materials. The list of third-party components your application is built from, used to tell whether a newly announced flaw affects you.

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.