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
Medium

FINDINGS
2

PACKAGE
Auth Session

SCAN DATE
01 Aug 2026

STATUS
Completed

REPORT TYPE
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: **13** checks completed without findings. What needs action: **2** checks produced findings for review.

Checks Performed

The **Auth Session** package ran **15** checks. **13** completed without producing findings.
Effectively tested 15 of 15 checks.

CHECK OUTCOME	COUNT	CHECKS
Passed	13	- Login Surface Controls - Session Cookie Scope - Login Rate-Limit Simulation - Password Reset Flow Checks - Account Enumeration Indicators - Credentialed Test-Account Checks - Weak Password Policy Review - Authenticated Deep Crawl + 5 more references
Needs review	2	- MFA Configuration Indicators - BOLA / IDOR Two-Account Comparison

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	15	2
Availability	1	
Confidentiality	6	1
Privacy	7	1
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	20	
4.2.1	7	
6.2.4	48	
6.3.1	4	
6.4.1	7	
7.2.1	28	2
8.3.1	18	2

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	30	
A.8.3	18	2
A.8.5	18	2
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	2
164.312(c)(1)	36	
164.312(d)	18	2
164.312(e)(1)	22	
164.502	3	

Detailed Findings

BOLA — Cross-Account Order Access

HIGH

A second test account was able to retrieve another account's order details by changing the numeric ID in the request, with no ownership check.

AFFECTED URL	https://example-customer.com/api/v1/orders/{id}
CONFIDENCE	High
COMPLIANCE IMPACT	**SOC 2**: Confidentiality, Privacy, Security **PCI-DSS v4.0**: 7.2.1, 8.3.1 **ISO/IEC 27001:2022**: A.8.3, A.8.5 **HIPAA Security Rule**: 164.312(a)(1), 164.312(d)
REMEDIATION	Add an object-level authorization check on every order endpoint confirming the resource belongs to the authenticated user.
EVIDENCE	`observed: A second test account was able to retrieve another account's order details by changing the numeric ID in the request, with no ownership check.`
REFERENCES	- OWASP API3:2023 Broken Object Property Level Authorization

MFA Not Enforced for Admin Accounts

MEDIUM

Administrator accounts can sign in with a password only; multi-factor authentication is available but not required.

AFFECTED URL	https://example-customer.com/admin/login
CONFIDENCE	Medium
COMPLIANCE IMPACT	**SOC 2**: Security **PCI-DSS v4.0**: 7.2.1, 8.3.1 **ISO/IEC 27001:2022**: A.8.3, A.8.5 **HIPAA Security Rule**: 164.312(a)(1), 164.312(d)
REMEDIATION	Require MFA enrollment for all administrator and privileged accounts before granting access.
EVIDENCE	`observed: Administrator accounts can sign in with a password only; multi-factor authentication is available but not required.`