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

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 **Auth Session** 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	- MFA Configuration Indicators - BOLA / IDOR Two-Account Comparison
Inconclusive	14	- Login Surface Controls (No execution record is available for this check) - Session Cookie Scope (No execution record is available for this check) - Login Rate-Limit Simulation (No execution record is available for this check) - Password Reset Flow Checks (No execution record is available for this check) - Account Enumeration Indicators (No execution record is available for this check) - Credentialed Test-Account Checks (No execution record is available for this check) - Weak Password Policy Review (No execution record is available for this check) - Authenticated Deep Crawl (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	1	
Confidentiality	7	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	21	
4.2.1	7	
6.2.4	49	
6.3.1	4	
6.4.1	7	
7.2.1	29	2
8.3.1	19	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	31	
A.8.3	19	2
A.8.5	19	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)	37	2
164.312(c)(1)	37	
164.312(d)	19	2
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	
Rule 6(b)	19	2
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
	BOLA — Cross-Account Order Access	HIGH
	MFA Not Enforced for Admin Accounts	MEDIUM

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
VERIFICATION	Indicative
REVIEW	Legacy verification requires review
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) **DPDP Act 2023 (India)**: Rule 6(b), Sec 8(5)
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
VERIFICATION	Indicative
REVIEW	Legacy verification requires review
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) **DPDP Act 2023 (India)**: Rule 6(b), Sec 8(5)
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.`

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
MFA Configuration Indicators	Needs review	Finding raised - see Detailed Findings
BOLA / IDOR Two-Account Comparison	Needs review	Finding raised - see Detailed Findings
Login Surface Controls	Inconclusive	No execution record is available for this check
Session Cookie Scope	Inconclusive	No execution record is available for this check
Login Rate-Limit Simulation	Inconclusive	No execution record is available for this check
Password Reset Flow Checks	Inconclusive	No execution record is available for this check
Account Enumeration Indicators	Inconclusive	No execution record is available for this check
Credentialed Test-Account Checks	Inconclusive	No execution record is available for this check
Weak Password Policy Review	Inconclusive	No execution record is available for this check
Authenticated Deep Crawl	Inconclusive	No execution record is available for this check
OAuth 2.0 / OIDC Security Checks	Inconclusive	No execution record is available for this check
BFLA Privilege Escalation Probe	Inconclusive	No execution record is available for this check
CSRF Protection Enforcement	Inconclusive	No execution record is available for this check
Session Fixation Check	Inconclusive	No execution record is available for this check
Password Spray Indicator	Inconclusive	No execution record is available for this check
Default Credentials Check	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
IDOR / BOLA	Changing an identifier in a request — an order number, a user id — and getting back someone else's record, because the site checks who you are but not what you may see.
BFLA	Broken Function Level Authorization. An ordinary user can reach an administrative action simply by calling it directly, because the check only hid the button.
Cross-site request forgery (CSRF)	A visitor who is logged in to your site is tricked into submitting an action they did not intend, because their browser sends their session automatically.
Session fixation	An attacker sets a visitor's session identifier before they log in, then reuses that same identifier afterwards to act as them.