Fencer

Secure software, **early**.

HONEY CORP

Penetration Test Executive Summary

Version 1.0

honey-corp.com Fencer Agent Penetration Test - Aug 20, 2026: August 20, 2026 - August 20, 2026

Table of Contents

1 Legal Responsibility

The contents of this report are **CONFIDENTIAL** and must not be disclosed or reproduced in any form to third parties, whether in hardcopy or electronic format (softcopy), without the express written consent of both parties. Upon delivery of this report to **Fencer**, the right to reproduce, share with third parties, and distribute it falls under the discretion and responsibility of your institution.

It should be noted, however, that sharing, duplicating, or distributing this report, either internally or externally, could pose significant risks and damage to your cybersecurity and information systems. **Fencer** shall not be held liable for any risks or losses incurred due to the sharing, duplication, and distribution actions taken by your institution, or as a result of these actions.

This report reflects the status of the systems within the defined scope in relation to known vulnerabilities at the time of testing. The testing period was designed to identify and document the maximum number of vulnerabilities. However, attackers with more time, resources, and advanced capabilities might discover and exploit vulnerabilities not identified in this report.

Furthermore, **Fencer** shall not be held accountable for:

- Security vulnerabilities that may arise from changes to the systems after testing or that were not detectable during the test period.
- Despite diligent efforts to ensure the accuracy and completeness of the report's contents, the possibility of undetected flaws exists.
- Any loss resulting from critical information within the report being compromised due to loss or unauthorized acquisition by third parties.
- Implementation of the remediation recommendations within the report is deemed as effective solutions for the identified issues; however, should these implementations result in new issues within the institution's systems, it is advised to consult with support companies or specialist consultants in the field for their perspectives.

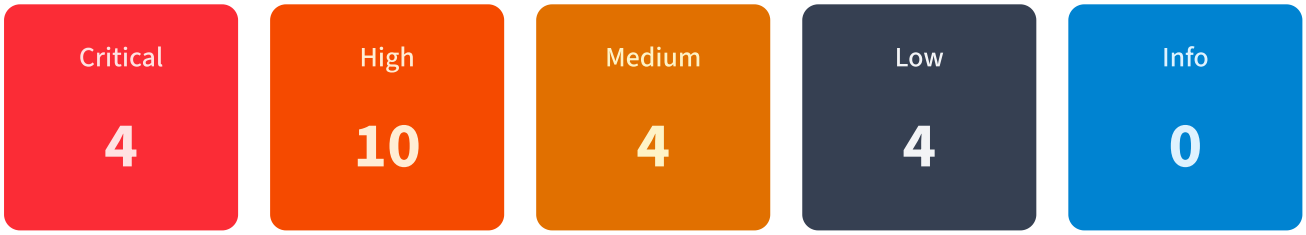
2 Management Summary

2.1 Overview

This executive summary provides a high-level overview of the penetration test conducted for Honey Corp. It presents a comprehensive view of all vulnerabilities identified during the engagement, including their current status and remediation progress.

2.2 Risk Assessment

The following is a count of the total amount of each finding severity.



3 Objectives & Outcomes

Each stated objective is assessed below, with a verdict on whether the simulated attacker reached it.

Read data belonging to another tenant/user (cross-tenant/broken-access read)

Achieved

Kill chain summary

Forged a JWT with alg:none and admin claims. Server accepted the unsigned token. Used it to read GET /rest/basket/2 (Jim's basket: 2x Raspberry Juice) and GET /rest/basket/3 (Bender's basket: 1x Raspberry Juice). Also listed all 41 user accounts via GET /api/Users/.

Escalate from starting position to administrative/higher-privilege role and exercise it

Achieved

Kill chain summary

Three independent paths to admin: (1) JWT alg:none forgery with role:admin, (2) mass assignment via POST /api/Users/ with role:admin, (3) login as admin@juice-sh.op:admin123. All three grant full admin access including user management, configuration, and all basket reads.

Achieve code or command execution on the target (RCE)

Not achieved

Kill chain summary

No RCE primitive identified. XXE reads files but cannot execute commands. SSRF reaches internal HTTP services but no command injection sink was found behind them. The application runs Node.js without any discovered exec/spawn sink reachable from user input.

Blocker

No command execution primitive (exec, spawn, eval with OS access) identified in the reachable attack surface. File read and SSRF confirmed but neither chains to code execution.

Read server-side file/resource or reach internal-only service unreachable from outside (SSRF/XXE/traversal)

Achieved

Kill chain summary

XXE via /file-upload read /etc/hostname (b9e08a63c357). SSRF via /profile/image/url fetched http://localhost:3000/rest/admin/application-version and stored the response. Null-byte bypass at /ftp/ downloaded restricted files (package.json.bak, incident-support.kdbx, etc.).

Extract sensitive data at scale via injection interpreter (SQL/NoSQL)

Achieved

Kill chain summary

UNION-based SQL injection at /rest/products/search extracted a credit card record (PAN: 481520XXXXXX2754, holder: Bjoern Kimminich, exp 12/2092) from the Cards table. The same technique reads the entire Users table (credentials), Addresses, and all other SQLite tables. NoSQL operator injection at PATCH /rest/products/reviews proved write access to all 31 review documents.

Manipulate a business-logic/workflow flaw for financial or data-integrity impact

Achieved

Kill chain summary

Unauthenticated PUT to /api/Products/1 changed the product price to $0.01 (from $1.99). No authentication or authorization check exists on the Products PUT endpoint. Any product's price, description, or metadata can be arbitrarily modified by an external attacker.

Compromise another user's session or browser context via client-side flaw (XSS/CSRF/CORS)

Achieved

Kill chain summary

DOM XSS confirmed at /#/search?q= with payload <iframe src="javascript:alert('fencerXSS8421')"> — browser_probe verified JavaScript execution in the application's origin. No CSP blocks execution. JWT tokens stored in localStorage are accessible to injected scripts. Combined with wildcard CORS, exfiltration has no cross-origin barrier.

Subvert an AI/LLM feature (prompt injection, tool/agency abuse, system-prompt or data leakage)

Partial

Kill chain summary

The chatbot's full system prompt and tool source code were leaked via GET /snippets/chatbotGreedyInjectionChallenge without authentication. The prompt reveals a confidential 15% discount policy and the tool code reveals a NoSQL $where injection pattern. However, the Ollama LLM backend at 127.0.0.1:11434 is offline, preventing live prompt injection exploitation.

Blocker

LLM backend (Ollama at 127.0.0.1:11434) is offline (ECONNREFUSED). Cannot interact with the chatbot to demonstrate prompt injection or tool abuse.

Take over another user's account by abusing an authentication/session flaw

Achieved

Kill chain summary

SQL injection in POST /rest/user/login with payload {"email":"jim@juice-sh.op'--","password":"x"} authenticates as Jim without knowing his password. The password change endpoint (GET /rest/user/change-password?new=X&repeat=X) requires no current password. Combined with JWT alg:none forgery, any user's password can be changed via their forged token — complete account takeover.

Recover a valid credential via brute-force/spray and reuse it for authenticated access

Achieved

Kill chain summary

Throttle probe confirmed no rate limiting on /rest/user/login (25 consecutive failures with no lockout/CAPTCHA). Credential spray recovered admin@juice-sh.op:admin123. Additionally, credential testing validated jim@juice-sh.op:ncc-1701, demo:demo, and mc.safesearch@juice-sh.op:Mr. N00dles via bounded default-credential checks on leaked hashes.

4 Vulnerability Summary

The following is a summary of all vulnerabilities identified during the assessment.

Vulnerability	Severity	Confirmation	Status	Discovered
Mass assignment allows self-registration as admin	Critical	Confirmed	Open	2026-08-03
Credential leak via /rest/memories exposes all password has…	Critical	Confirmed	Open	2026-08-03
SQL injection in product search and login endpoints	Critical	Confirmed	Open	2026-08-03
JWT algorithm bypass enables token forgery	Critical	Confirmed	Open	2026-08-03
XXE via XML file upload enables arbitrary file read	High	Confirmed	Open	2026-08-20
SSRF via profile image URL fetch	High	Confirmed	Open	2026-08-20
Weak credential on admin account	High	Confirmed	Open	2026-08-12

Vulnerability	Severity	Confirmation	Status	Discovered
Unauthenticated PUT on Products enables price manipulation	High	Confirmed	Open	2026-08-12
Password change without current password verification	High	Confirmed	Open	2026-08-12
JWT payload contains password hashes	High	Confirmed	Open	2026-08-03
DOM XSS via search parameter	High	Confirmed	Open	2026-08-03
Encryption keys publicly accessible	High	Confirmed	Open	2026-08-03
IDOR on user baskets allows cross-tenant data read	High	Confirmed	Open	2026-08-03
Null-byte file extension bypass on /ftp/	High	Confirmed	Open	2026-08-03
NoSQL operator injection in product reviews	Medium	Confirmed	Open	2026-08-20
Missing brute-force protection on login	Medium	Confirmed	Open	2026-08-12

Vulnerability	Severity	Confirmation	Status	Discovered
LLM system prompt and tool code leaked	Medium	Confirmed	Open	2026-08-03
Application configuration disclosure without authentication	Medium	Confirmed	Open	2026-08-03
Exposed Swagger/OpenAPI documentation for B2B API	Low	Confirmed	Open	2026-08-20
Wildcard CORS enables cross-origin data theft	Low	Confirmed	Open	2026-08-12
Unauthenticated metrics exposure leaks operational intellig…	Low	Confirmed	Open	2026-08-03
Open redirect via whitelist substring bypass	Low	Confirmed	Open	2026-08-03

5 Scope

The scope of this penetration test was defined to assess the security posture of the following application surfaces belonging to Honey Corp.

Primary target	https://honeyapp.honey-corp.com/
Engagement objective	Perform a full penetration test of honeyapp.honey-corp.com across the entire web and API surface plus any AI/LLM features: recon and enumeration first, then validate and bounded-exploit vulnerabilities across every class. Chain confirmed findings into attack paths, and deliver the consolidated report.
Goal	pentest

5.1 In-Scope hosts

- `https://honeyapp.honey-corp.com/`

5.2 Out-of-Scope

The following activities and systems were explicitly excluded from this testing engagement:

- Social engineering attacks against personnel
- Physical security assessments
- Denial of service (DoS) attacks
- Production data manipulation or deletion

6 Methodology

The test was done according to penetration testing best practices. The flow from start to finish is listed below.

This penetration test was performed by an AI agent using automated tools and analysis throughout the engagement.

6.1 Pre Engagement

- Scoping
- Customer documentation
- Information discovery

6.2 Penetration Testing

- Tool assisted assessment
- Manual assessment
- Exploitation
- Risk analysis
- Reporting

6.3 Post Engagement

- Prioritized remediation*
- Best practice support*
- Retesting*

7 Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7.1 Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems, and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

7.2 Severity Definitions

When our pentesters find vulnerabilities, they use the standard OWASP Risk Rating Methodology, and then classify them into one of the following risk levels, based on their business impact and likelihood:

```
Risk = Impact * Likelihood
```

Critical: Includes vulnerabilities that require immediate attention. Risk score of 25.

High: Impacts the security of your application/platform/hardware, including supported systems. Includes high probability vulnerabilities with a high business impact. Risk score range: 16 through 24.

Medium: Includes vulnerabilities that are: medium risk, medium impact; low risk, high impact; high risk, low impact. Risk score range: 5 through 15.

Low: Specifies common vulnerabilities with minimal impact. Risk score range: 2 through 4.

Informational: Notes vulnerabilities of minimal risk to your business. Risk score of 1.

8 Recommendations

8.1 Immediate Actions Required

- **Critical Vulnerabilities:** Address all 4 critical vulnerabilities immediately. These pose significant risk to the organization.
- **High Severity Vulnerabilities:** Remediate 10 high severity vulnerabilities within 30 days.

8.2 General Security Recommendations

- Implement a regular vulnerability scanning schedule
- Establish a vulnerability management process
- Provide security training to development teams
- Implement secure coding practices
- Regular security assessments and penetration testing

9 Appendix

9.1 Test Summary

Metric	Count
Total Vulnerabilities	22
Critical Severity	4
High Severity	10
Medium Severity	4
Low Severity	4
Informational	0