GINRŌ GUARD

CapsuleCorp

Vulnerability Assessment and Penetration Testing Report

Date: August 26, 2025
Project: CCorp-2025-08-A
Security Analyst: Baptiste Bellecour
Version: 1.0

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to CapsuleCorp or facilitate attacks against CapsuleCorp. GINRŌ GUARD shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on CapsuleCorp’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

GINRŌ GUARD performed a security assessment of the internal corporate network of CapsuleCorp from 16/08/2025 to 28/08/2025. GINRŌ GUARD's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the CapsuleCorp corporate network. The purpose of this assessment was to discover and identify vulnerabilities in CapsuleCorp's infrastructure and suggest methods to remediate the vulnerabilities. GINRŌ GUARD identified a total of 5 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRIT	HIGH	MEDIUM	LOW	INFO
1	1	1	1	1

The highest severity vulnerabilities give potential attackers the opportunity to take over customer accounts. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn't a technical vulnerability but still should be brought to the attention of the executive team.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

GINRŌ GUARD identified the following strengths in CapsuleCorp's network which greatly increases the security of the network. CapsuleCorp should continue to monitor these controls to ensure they remain effective.

- CapsuleCorp Request Rate limit is on point.

Areas for Improvement

GINRŌ GUARD recommends CapsuleCorp to take the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack CapsuleCorp's information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

GINRŌ GUARD recommends CapsuleCorp take the following actions as soon as possible to minimize business risk.

- Use parameterized queries to prevent SQL injection.
- Sanitize and encode all untrusted input before inserting into the DOM.

Long Term Recommendations

GINRŌ GUARD recommends the following actions be taken over the next 6 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

- Adopt a Web Application Firewall
- Implement backend checks to enforce payment business logic security

SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Networks

NETWORK	NOTE
10.0.1.0/24	Network for CapsuleCorp HQ
10.0.2.0/24	Tokyo, Japan, CapsuleCorp branch site

Web Application

NAME	SYSTEM TYPE	URL
CapsuleCorp website	Web App	https://www.capsule.web

Provided Credentials

CapsuleCorp provided GINRŌ GUARD with the following credentials and access to facilitate the security assessment listed below.

ITEM	NOTE
Test Accounts	(devbobtest@capsule.web) A fake customer account in the capsule.web application for testing functionality that requires authentication.

TESTING METHODOLOGY

GINRŌ GUARD's testing methodology was split into three phases: Reconnaissance, Target Assessment, and Execution of Vulnerabilities. During reconnaissance, we gathered information about CapsuleCorp's network systems. GINRŌ GUARD used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. GINRŌ GUARD simulated an attacker exploiting vulnerabilities in the CapsuleCorp network. GINRŌ GUARD gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations. The image on the next page is a graphical representation of this methodology.


1
PLANNING
Establish scope
Research assets
Confirm targets
TARGET ACQUISITION
Network scanning
OS Fingerprint
Banner grabbing
2
3
PRE-EXPLOITATION
Assess vulnerabilities
Customize attack tools
Confirm targets
EXPLOITATION
Leverage vulnerabilities
Execute payloads
Establish system access
4
5
POST-EXPLOITATION
Escalate privileges
Lateral movement
Network Pivoting
REPORTING
Evidence collection
Findings write-down
Risk assessment
6

CLASSIFICATION DEFINITIONS

Risk Classifications

SEVERITY	CVSS SCORE	DESCRIPTION
CRIT	9-10	The vulnerability poses an immediate and severe threat to the organization, with urgent remediation required. Exploitation could cause catastrophic business, financial, or reputational damage.
HIGH	7-10	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
MEDIUM	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
LOW	2-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
INFO	1	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Risk Matrix

	IMPACT		
LIKELIHOOD	MINOR	MODERATE	MAJOR
UNLIKELY	Info	Low	Medium
POSSIBLE	Low	Medium	High
LIKELY	Medium	High	Crit

Exploitation Likelihood Classifications

LIKELIHOOD	DESCRIPTION
LIKELY	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
POSSIBLE	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
UNLIKELY	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

IMPACT	DESCRIPTION
MAJOR	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
MODERATE	Successful exploitation may cause noticeable disruption to some business operations, with limited financial or operational impact.
MINOR	Successful exploitation may affect few users, without causing much disruption to routine business functions.

ASSESSMENT FINDINGS

#	FINDING	SCORE	Risk
1	Authentication Bypass	10	CRIT
2	DOM Cross Site Scripting	8	HIGH
3	Access Control Misconfiguration	6	MEDIUM
4	Robots.txt Exposing Sensitive Data	3	LOW
5	Server Version disclosure	1	INFO

Sorting by descending risk score

1 - Authentication Bypass

RISK	CRIT
CVSS V3.1 SCORE	10
TARGET URL	http://capsule.web/#/login

Security Implications

The login form on CapsuleWeb is vulnerable to an authentication bypass due to improper input handling and lack of server-side validation. By injecting SQL logic into the email field, attackers can alter the underlying query to always return true, thereby bypassing the password check entirely.

This vulnerability allows unauthenticated users to gain administrative access to the application, exposing sensitive data such as registered user accounts

Exploitation Likelihood: Likely

Exploitation is straightforward and does not require advanced knowledge. A single crafted input string can bypass the login mechanism, making this vulnerability highly exploitable.

Business Impact: Major

Successful exploitation grants attackers full access to administrative functionality without valid credentials. This includes viewing or modifying user accounts and potentially escalating further into the system. Such a flaw completely undermines the authentication layer, leading to total loss of confidentiality and integrity of the application.

References:

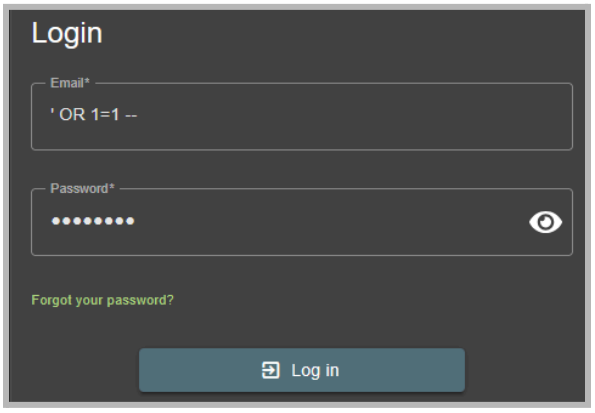
- OWASP Top 10: Injection (A03:2021)
- CWE-89: SQL Injection

Remediation Advice

- Use parameterized queries to prevent SQL injection.
- Add server-side input validation for login fields.
- Restrict DB account privileges to least privilege.
- Suppress detailed error messages from users.

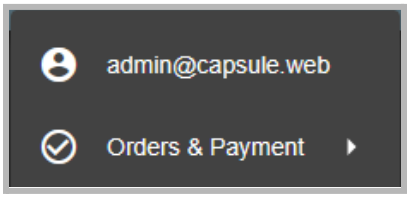
Proof of Concept

1 - Navigate to the login page: http://capsule.web/#/login

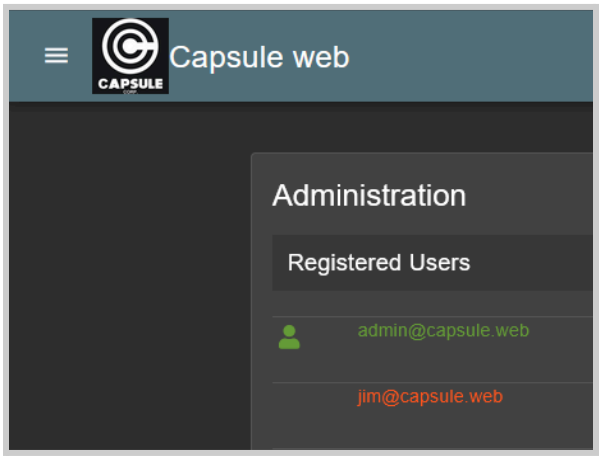


- In the Email field, input the following payload: ' OR 1=1 –
- Enter any password (it will be ignored).
- Submit the form.

2 - The login is successful, the application authenticates the attacker as the admin user.



3 - The /administration page is now accessible, exposing sensitive data and granting attackers full admin rights.



2 - DOM Cross Site Scripting

RISK	**HIGH**
CVSS V3.1 SCORE	8.1
TARGET URL	http://capsule.web/#/search?q=

Security Implications

The search functionality on CapsuleWeb is vulnerable to a DOM-based Cross-Site Scripting (XSS) attack due to improper handling of user-supplied input within client-side JavaScript. The application reflects unsanitized query parameters directly into the DOM using functions such as innerHTML, allowing attackers to inject arbitrary JavaScript.

This vulnerability enables attackers to execute malicious scripts in the victim's browser, potentially stealing session cookies, hijacking accounts, or performing actions on behalf of authenticated users without their knowledge.

Exploitation Likelihood: Possible

Requires tricking a logged in user into visiting a crafted URL. No advanced knowledge is needed. Because the payload executes automatically in the victim's browser, this vulnerability exploitation is possible.

Business Impact: Major

Successful exploitation compromises the confidentiality and integrity of the application by enabling full session hijacking. Attackers can impersonate users (including admin), exfiltrate sensitive data, and perform privileged operations. In environments with reused credentials or shared sessions, this could further lead to system-wide compromise.

References:

- OWASP Top 10: Cross-Site Scripting (A03:2021)
- CWE-79: Improper Neutralization of Input During Web Page Generation

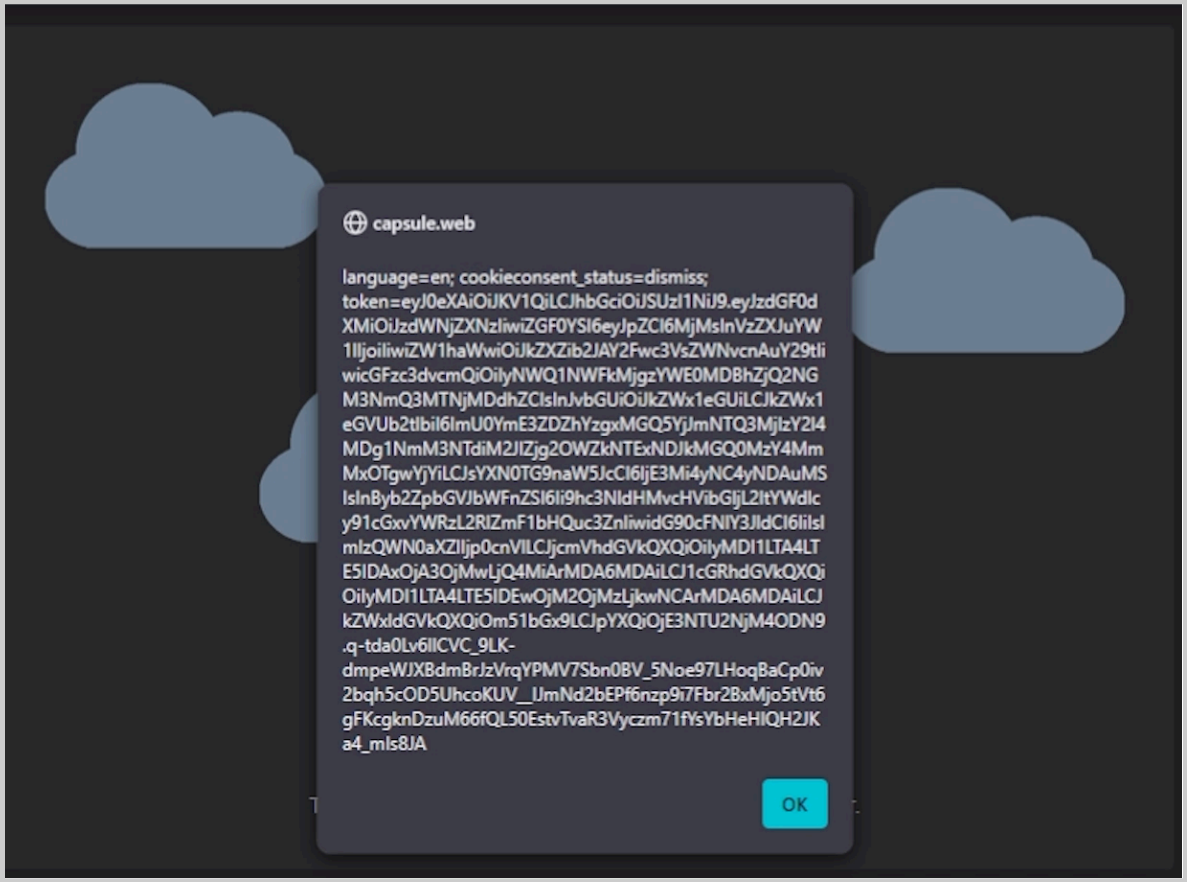
Remediation Advice

- Sanitize and encode all untrusted input before inserting into the DOM.
- Avoid using insecure functions such as innerHTML, document.write, and eval.
- Use safe DOM APIs like textContent or setAttribute when rendering user input.

Proof of Concept

1 - Navigate to the search page:
http://capsule.web/#/search?q=<img src=1 onerror=alert(document.cookie)>

2 - The payload is reflected unsanitized into the DOM. A real-world attacker could replace the alert() with malicious code that would exfiltrate the victim's session token, allowing account takeover.



APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
BurpSuite	Used for testing of web applications.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
Nuclei templates	Used for detecting vulnerabilities, misconfigurations, and exposed data.
Sublist3r	Used for discovering subdomains of a given domain
Amass	Used for network mapping, asset discovery, and subdomain enumeration.

Table A.1: Tools used during assessment

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	CapsuleCorp
Primary Contact	Devbob, CTO
Email	devbob@capsulecorp.com
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement • CapsuleCorp - Dev Bob • GINRO GUARD - Baptiste Bellecour

Contact Information

Name	Baptiste Bellecour
Address	<redacted>Tokyo Japan
Phone	070-3450<redacted>
Email	baptiste@ginro-guard.com