

CybeRaccoon Penetration Test Report

Prepared for XX

Date: XX

Confidentiality Statement

This document contains confidential and proprietary information belonging to CybeRaccoon and XX. It is solely for the use of individuals within the organization for whom it was intended. No part of this document may be disclosed, distributed, or reproduced in any form without the prior written consent of both CybeRaccoon and XX.

Disclaimer

A penetration test is a snapshot of the security posture at the time of testing. The findings and recommendations within this report reflect the state of the assessed systems during the engagement period. Any subsequent changes to the systems, applications, or infrastructure may render the contents of this report obsolete. CybeRaccoon recommends conducting regular security assessments to maintain a strong security posture.

CybeRaccoon Penetration Test Report..... 1
Confidentiality Statement..... 1
Disclaimer.....1
Contact Information.....2
Executive Summary.....2
Key Findings..... 2
Project Overview.....3
Testing Methodology.....3
Findings Severity Rating.....4
Scope.....4
Vulnerability Summary.....5
Summary of report.....7

Contact Information

Name	Contact Information
XX	
XX	XX
CybeRaccoon	
XX	XX

Executive Summary

This report details the findings of a penetration test conducted by CybeRaccoon for XX between DATE and DATE. The objective of this engagement was to identify and exploit security vulnerabilities within the in-scope assets to evaluate the overall security posture and provide actionable remediation guidance.

The assessment was conducted using a methodology aligned with the OWASP Top 10 framework to ensure coverage of the most critical web application security risks. All vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) v4.0 to provide a standardized measure of severity.

The overall security risk of the assessed environment is determined to be XX.

Key Findings

Critical Vulnerabilities

High-Risk Vulnerabilities

Medium-Risk Vulnerabilities

This assessment revealed several vulnerabilities, particularly in the areas of XX and XX. Successful exploitation of these issues could lead to XX. Immediate remediation of the high and critical findings is strongly advised.

Project Overview

Assessment Type: Web Application / External Network / Internal Network / Mobile Application / etc
Timeline: XX to XX

Testing Methodology

CybeRaccoon employs a structured, intelligence-led testing methodology aligned with industry standards such as NIST SP 800-115, the Penetration Testing Execution Standard (PTES), and the OWASP Web Security Testing Guide (WSTG).

Our testing approach is strategically mapped to the OWASP Top 10 to ensure comprehensive coverage of the most prevalent and critical application security risks.

Planning & Scoping: Defined goals, rules of engagement, and scope in collaboration with the client.

Information Gathering & Reconnaissance: Collected publicly available information and performed active scanning to identify potential entry points.

Vulnerability Analysis: Analyzed gathered data to identify potential vulnerabilities, with a focus on OWASP Top 10 categories.

Exploitation: Attempted to exploit identified vulnerabilities to validate their severity and impact.

Post-Exploitation: Determined the value of compromised systems and attempted to pivot to other systems (where within scope).

Reporting: Documented all findings, exploitation paths, and recommendations in this report, utilizing CVSS v4.0 for consistent severity scoring.

Findings Severity Rating

The following table defines the severity levels and corresponding Common Vulnerability Scoring System (CVSS) v4.0 score ranges used to assess vulnerabilities.

Severity	CVSS Score	Definition
🔴**Critical**	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. Form a plan of action and patch it immediately.
🟠**High**	7.0-8.9	Exploitation is more complex but could cause elevated privileges and potentially data loss or downtime. Forming a plan of action and patching as soon as possible is advised.
🟡**Moderate**	4.0-6.9	Vulnerabilities exist, but are not exploitable or require extra steps such as social engineering. Forming a plan of action and patching it after high-priority issues have been resolved is advised.
🔵**Low**	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. Forming a plan of action and patching during the next maintenance window is advised.
⚪**Informational**	N/A	No vulnerability exists, and sensitive data is not exposed. Additional information is provided regarding items noticed during testing.

Scope

Domains	Timeline

Vulnerability Summary

🔴Critical	🟠High	🟡Moderate	🔵Low	⚪Informational
0	0	1	0	0

The following tables illustrate the vulnerabilities found by their risk assessments:

Severity	Finding
🔴**Critical**	001 -
🟠**High**	002 -
🟡**Moderate**	003 - Unrestricted File Upload
🔵**Low**	004 -
⚪**Informational**	005 -

Vulnerability 001:

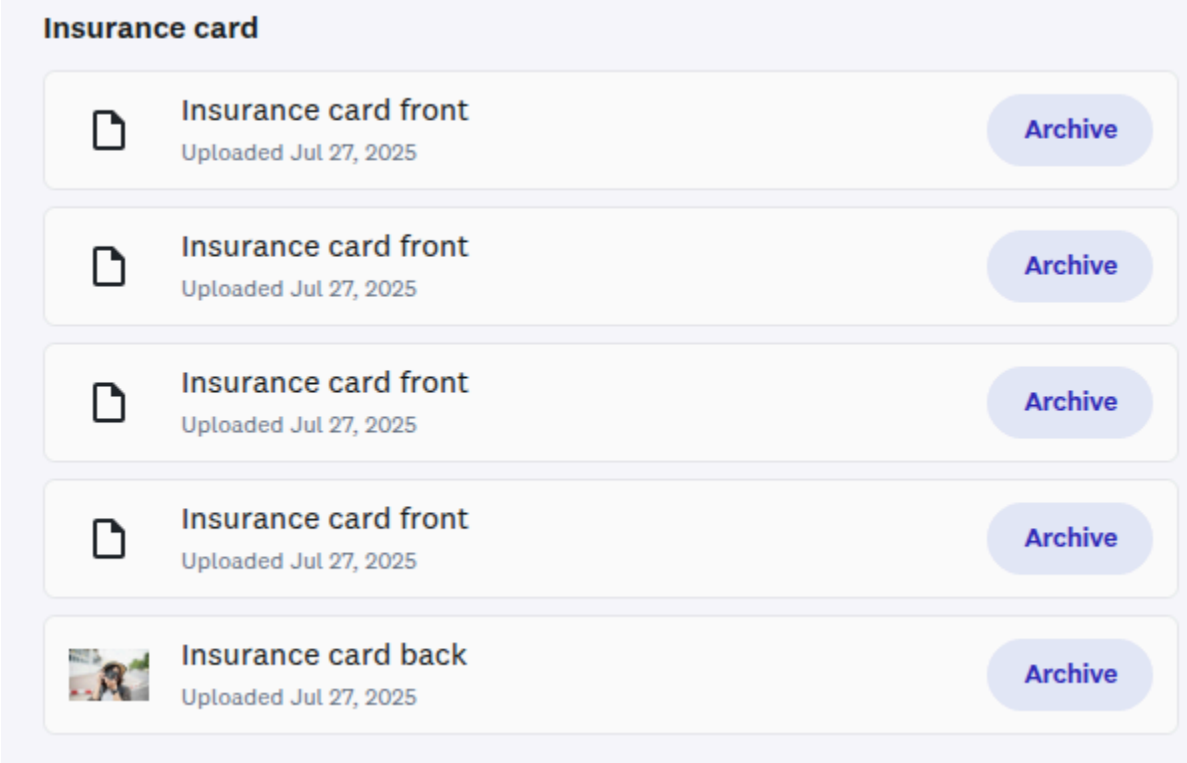
Risk factor :

🟡**Moderate** | CVSS Base Score : 6.0
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:L/SC:H/SI:N/SA:N)

Description :
The web application allows users to upload files without proper validation (e.g checking file type, extension, content or size).

Proof of Concept :

Uploaded php file :




```
<!DOCTYPE html>
<html>
<body>
<?php
echo "testing";
?>
</body>
</html>
```

Remediation :
To prevent file upload exploits, implement layered defenses: validate file contents (not just extensions), store uploads outside webroots with random names, disable execution in upload directories, restrict file permissions, scan for malware, and monitor upload activity.

Summary of report

The web application's overall security risk is High. Our penetration test uncovered multiple high-severity vulnerabilities that threaten unauthorized access, data exposure, and system compromise. While some security controls are effective, critical weaknesses in access control, input validation, and session management require remediation to prevent a possible attack. Prioritizing remediation of the vulnerabilities we found is essential to reduce risk and align with industry best practices.

CybeRaccoon.
Expert Cybersecurity That Protects.

https://cyberaccoon.io

