

Penetration Test Report

CyberHammer



HACKTHEBOX

Client: ACME Corp
Date: August 6, 2025

Contents

1	Executive Summary	2
2	Findings	2
2.1	High Level Summary	2
2.2	Technical Findings	2

1 Executive Summary

This [2] test was conducted on ACME Corp's network to identify vulnerabilities...

Key findings include[1]:

- High severity SQL injection vulnerability in the customer portal.
- Outdated software versions exposing critical security risks.
- Weak password policies discovered in the internal system.

Recommendations are provided to mitigate these risks.[2]

2 Findings

2.1 High Level Summary

High-Level Summary

This report summarizes the key vulnerabilities identified during the penetration test. A total of 15 issues were discovered, categorized by severity below:

High	Medium	Low	Informational
5	2	3	5

Key observations:

- Outdated plugin enabling remote code execution on core backend server.
- Weak password policy enforcement across external login interfaces.
- Lack of input sanitization on user data entry points.

A detailed breakdown of each finding is available in the following section.

2.2 Technical Findings

Outdated WordPress Plugin

Severity: Medium

CWE: CWE-79

CVSS 3.1 Score: 7.5 (High)

Affected Domain: example.com

Description and Root Cause:

The vulnerable plugin allows unauthenticated users to inject arbitrary JavaScript...

Security Impact:

Attackers may execute JavaScript in the user's browser...

Remediation:

Update the plugin to version $\geq 1.2.4$ or remove it completely...

External References:

- <https://cwe.mitre.org/data/definitions/79.html>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX>

Finding Evidence: Outdated WordPress Plugin

- WPScan Output:

[+] Name: vulnerable-plugin

Version: 1.2.3

References:

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-XXXX>

References

References

- [1] Cve-2023-xxxxx. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-XXXXX>, 2023. Critical RCE vulnerability.
- [2] Gordon Lyon. Nmap network scanning. <https://nmap.org/book/>, 2023. Accessed: 2025-08-04.