

RedRecon Assessment Report

Automated Pentest Engine v2.0

December 9, 2025

Abstract

This document contains the automated security assessment results for **target-corp.com**. The scan was performed using RedRecon with dynamic proxy rotation to ensure accurate and evasion-resistant enumeration.

Contents

1 Executive Summary

RedRecon identified a total of **21** potential issues. The assessment focused on external attack surface management and automated vulnerability discovery.

- **Target:** target-corp.com
- **Scan Duration:** 0.087s
- **Proxies Rotated:** 12

2 Vulnerability Findings

2.1 High Severity

Issue: SQL Injection (Blind)

Impact: Allows unauthorized access to database contents.

Remediation: Use parameterized queries/prepared statements.

2.2 Medium Severity

Issue: Reflected Cross-Site Scripting (XSS)

Impact: Execution of malicious scripts in user browser.

Remediation: Context-aware output encoding.

3 Detailed Logs

```
[INF] Starting RedRecon...  
[+] Found IP: 104.28.2.14  
[+] VULN: SQLi at /login.php  
[+] VULN: XSS at /search?q=  
[INF] Scan Finished.
```

4 Disclaimer

This report was generated automatically. All findings should be verified manually before taking remediation actions. The data contained herein is strictly confidential.