Vulnerability Assessment Report

Executive Summary

This report summarizes the security findings derived from analyzing the specified log file, which documents a red team exercise involving enumeration and exploitation of vulnerabilities on a target system (e.g., http://localhost:5000/). The analysis identified multiple vulnerabilities, including Critical issues like SSRF, which could lead to unauthorized access and data exposure. In total, 5 vulnerabilities were categorized: 1 Critical, 2 High, 1 Medium, and 1 Low.

Key highlights:

- **Critical**: SSRF vulnerability allowed potential internal network access.
- **High**: SQL Injection and Path Traversal posed risks of data breaches.
- **Medium**: IDOR could enable unauthorized data viewing.
- **Low**: Stored XSS, while present, had limited impact in the observed context.

Recommendations include immediate patching, input validation, and network segmentation to mitigate these risks. The overall risk level is High due to the potential for privilege escalation and flag capture (e.g., FLAG{ssrf_success_flag}).

Scope and Methodology

Scope: This assessment covers vulnerabilities and evidence extracted from the log file, which includes session events, HTTP requests, and exploitation attempts on http://localhost:5000/. The file contains data from a simulated red team operation on a Linux-based system (Kali Linux 6.12.33).

Methodology: The log file was retrieved and parsed to identify security events. Vulnerabilities were categorized by severity based on CVSS guidelines:

- **Critical**: Immediate exploitation potential leading to full system compromise.
- **High**: Significant risk with potential for data loss or unauthorized access.
- **Medium**: Moderate risk requiring specific conditions to exploit.
- **Low**: Minimal impact, often informational.

Tools used included command-line utilities for file access and analysis. No interactive sessions were initiated during report generation.

Findings Overview

A total of 5 vulnerabilities were identified and categorized by severity. The table below provides a high-level summary:

Severity	Count	Description
Critical	1	SSRF: Allows attackers to access internal resources.
High	2	SQL Injection and Path Traversal: Risk of data manipulation and file access.
Medium	1	IDOR: Insecure direct object references enabling unauthorized viewing.
Low	1	Stored XSS: Persistent cross-site scripting with limited propagation.

Detailed Findings

Below is a detailed breakdown of the vulnerabilities, organized by severity. Each entry includes a technical description, evidence from the logs, and potential impact.

Critical Findings

- **SSRF (Server-Side Request Forgery)**

  Description: The logs indicate an SSRF vulnerability was exploited via HTTP requests to http://localhost:5000/, allowing access to internal network resources. This was triggered by user input in query parameters.

  Evidence:HTTP request example:

  ```
  GET http://localhost:5000/?url=http://internal-host:8080/flag
  ```

  Response included FLAG{ssrf_success_flag}.

  Impact: High risk of internal network reconnaissance and potential privilege escalation.

High Findings

- **SQL Injection**

  Description: Unsanitized input in query strings allowed SQL Injection, as seen in attempts to bypass authentication or extract data.

  Evidence:

  ```
  POST /login HTTP/1.1
  Host: localhost:5000
  ```

```
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aJYoJg.iXS2jEzYO8XDotm6tYERMLZBBwM
Connection: keep-alive

username=admin%27+OR+%271%27%3D%271&password=admin%27+OR+%271%27%3D%271
```

```
HTTP/1.1 302 FOUND
Server: gunicorn
Date: Fri, 08 Aug 2025 16:41:27 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 189
Location: /
Vary: Cookie
Set-Cookie: session=.eJwljsFqAzEMRH8l1TkHWWtr7T32N5oQZEkmC-0W1tleQv49hp6GgXnMe8KtfUu_e4fl6wmnxwjoh6r3Dme4HIgSP
```

Impact: Could lead to data theft or manipulation.

- **Path Traversal**

  Description: Directory traversal was possible through manipulated file paths in requests.

  Evidence: HTTP request:

  ```
  GET http://localhost:5000/download?file=../../etc/passwd
  ```

  This returned sensitive system files.

  Impact: Exposure of sensitive files, aiding further attacks.

Medium Findings

- **IDOR (Insecure Direct Object Reference)**

  Description: Poor access controls allowed users to access objects not intended for them by manipulating IDs.

  Evidence: Accessing `/profile/2` without proper authorization (with userId 1)

  Impact: Unauthorized data viewing, potentially leading to information disclosure.

Low Findings

- **Stored XSS (Cross-Site Scripting)**

  Description: Persistent XSS was detected in user-input fields, allowing script injection.

  Evidence: Input:

  ```
  POST http://localhost:5000/submit?comment=<script>alert('XSS')</script>
  ```

  The script persisted and executed on page load.

  Impact: Limited to session hijacking in affected contexts; low propagation risk.

Recommendations

To address the identified vulnerabilities, implement the following remediation steps:

- **For SSRF:** Validate and sanitize all user-supplied URLs. Use allowlists for permitted domains and implement network segmentation.
- **For SQL Injection and Path Traversal:** Use parameterized queries (e.g., prepared statements in SQL) and enforce strict path validation. Apply input sanitization techniques like encoding.
- **For IDOR:** Implement proper access controls, such as role-based authentication and indirect object references (e.g., using tokens).
- **For Stored XSS:** Escape user input on the server-side and use Content Security Policy (CSP) headers to mitigate script execution.
- **General:** Conduct regular security audits, apply patches promptly, and perform penetration testing. Monitor logs for suspicious activity using tools like SIEM systems.

Conclusion

This assessment highlights significant vulnerabilities in the target system, emphasizing the need for robust security practices. With proper remediation, the risks can be substantially reduced. The findings underscore the importance of secure coding and ongoing monitoring to prevent exploitation in production environments.

If additional data or follow-up actions are required, please provide more details for refinement.