# Vulnerability Assessment Partlow

## System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

## Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

**The database server is critical to business operations as it stores customer information, sales data, and other proprietary business intelligence.** The company relies on employees querying this server for potential customer insights, making its security essential. Keeping this database publicly accessible exposes sensitive data to unauthorized access, data theft, or corruption. If the server were compromised or disabled, it could result in significant financial loss, reputational damage, and potential legal repercussions due to data breaches. Conducting this vulnerability analysis helps identify security risks and propose effective solutions to protect business operations.

## Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Source | Threat Event | Likelihood (1-3) | Severity (1-3) | Risk (1-9) |
| Hacker (Outsider) | Obtain sensitive information via exfiltration | 3 | 3 | 9 |
| Competitor | Perform reconnaissance and surveillance | 2 | 2 | 4 |
| Hacktivist | Conduct Denial of Service (DoS) attack | 3 | 3 | 9 |

## Approach

The risks evaluated were chosen based on the system’s exposure as a publicly accessible database server. **The identified threats—data exfiltration, reconnaissance, and DoS attacks**—are among the most common attack vectors targeting internet-facing servers. The likelihood and severity scores were derived from industry best practices, the nature of the threat actors, and the server's open access. Given the lack of stringent access controls, hackers and competitors could easily exploit vulnerabilities. This assessment, however, does not account for physical security risks or other IT systems connected to the server.

## Remediation Strategy

To mitigate the identified risks, the company should **implement stricter access controls using the principle of least privilege**, ensuring only authorized personnel can access the database. **Multi-factor authentication (MFA) should be enforced for all remote access.** To prevent reconnaissance and DoS attacks, the **server should be placed behind a firewall with intrusion detection/prevention systems (IDS/IPS) actively monitoring for suspicious activity. Encrypting stored data and enforcing role-based access control (RBAC)** will further reduce the risk of unauthorized access. These measures will significantly improve the server’s security posture and protect business-critical data.