ePortfolio NIST Cyber Security  
  
**Vulnerability Assessment Report**

**26th January 2024**

**System Description**

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of 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 system's network security and software integrity. The assessment will cover a period of three months, from June 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

**Purpose**

The database server is a critical asset for XYZ Financial Services, storing sensitive customer data and financial records. Ensuring its security is vital to protect against data breaches, maintain customer trust, and comply with regulatory standards. A compromise of the server could disrupt business operations, lead to financial loss, and damage the company's reputation.

**Risk Assessment**

| **Threat Source** | **Threat Event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Hacker | Exploit unpatched vulnerabilities | 2 | 3 | 6 |
| Insider | Misuse access privileges | 2 | 2 | 4 |
| Malware | Infect server systems | 3 | 3 | 9 |
| Natural Event | Server downtime due to power outage | 1 | 3 | 3 |

**Approach**

The assessment considered network security, software vulnerabilities, and the potential impact of internal and external threats on the operational capability of the business.

**Remediation Strategy**

* **Patch Management:** Implement a robust patch management process to address software vulnerabilities promptly.
* **Access Monitoring:** Enhance monitoring and logging of user activities to detect and prevent misuse.
* **Anti-Malware Measures:** Deploy advanced anti-malware solutions to protect against malicious software attacks.
* **Power Redundancy:** Install uninterruptible power supplies (UPS) to mitigate the risk of server downtime due to power outages.