Vulnerability Assessment Report

20th September 2025

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 current access controls of the system. The assessment will cover a period of three months, from June 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this report is to conduct a thorough vulnerability analysis on our DB Server in order to best assess our security weaknesses and strengths. This will allow us to address any pressing security needs, implement resolutions, deploy company-wide training, as well as ensuring a general review of any current standing security controls. The security of our DB Server is crucial to business operations as it contains PII and other sensitive user and consumer data. Our internal users regularly request data and information from the server so it is crucial only authorized users have access to it. Malicious actors, competitors, disgruntled employees, or even a malicious insider threat could misuse this data. Our reputation and integrity is crucial to continuing business operations. It is our job as the Security team to ensure confidentiality, integrity, and accessibility are implemented across our entire security spectrum.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious Actor	*Obtain PII or other sensitive information via exfiltration*	*3*	*3*	*9*

Internal Threat	*Misuse or mishandling of sensitive information*	*2*	*2*	*4*
Software Vulnerabilities	*BSOD or any other software threat that can cause servers to be down or inaccessible*	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. For Human threats we looked at malicious actor, internal, and competitor threats - respectively from highest to lowest risk. Given the findings of the unsecure DB Server, external malicious actors pose the highest risk due to their intent to exploit sensitive data. Next was internal threats - this is including but not limited to disgruntled employees and non-malicious internal user threats. Due to the human nature aspect of security, there is room to believe an internal user could be a security risk whether accidental or on purpose. And lastly, competitor threats are deemed least likely due to legal consequences serving as a deterrent.

Computer Fraud and Abuse Act (CFAA): In the U.S., unauthorized access to computer systems—including databases—can lead to criminal charges under this federal law.

Trade Secret Misappropriation: If the stolen data includes proprietary business information (like customer lists, pricing models, or internal processes), it may be protected under trade secret laws. Violators can be sued civilly and even face criminal charges under the **Economic Espionage Act**.

Civil Lawsuits: Companies can file lawsuits for damages, injunctions, and even punitive measures if a competitor unlawfully obtains or uses their data.

Regulatory Penalties: If the stolen data includes **PII** (personally identifiable information), regulators like the FTC or state attorneys general may impose fines for failing to protect consumer data—even if the breach was caused by a third party.

The final threat was Software Vulnerabilities as part of the Technological Assessment. Third party vulnerabilities can cause issues for us as well. An assessment of our software can help us determine where improvements and upgrades can be made, identify legacy systems in need of decommissioning, etc.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.