Risk Assessment Report

CYBR 3060

Gregory Stephens

Background

Information about the Asset

The asset in question is the financial web server. It is a Linux-based server that hosts the financial application used by the organization's finance staff to manage financial transactions, reports, and other critical financial operations. This server is integral to the day-to-day functioning of the finance department and supports the organization's financial health.

Location Information

The financial web server is located in the organization’s primary data center, which is housed within the corporate headquarters. The server is accessible internally via the organization's intranet and externally through a public-facing interface for authorized users (e.g., finance staff working remotely). The server resides on a specific subnet within the network, which is segmented from other internal systems for security purposes.

Who Has Access to It?

Access to the financial web server is primarily granted to:

- Finance Staff: Authorized employees within the finance department who use the server-hosted application for financial reporting, transaction processing, and recordkeeping.
- IT Staff: Members of the IT department responsible for maintaining the server, performing updates, troubleshooting, and ensuring its availability.
- External Auditors: Occasionally, external auditors may require access to the server for compliance reviews or audits.

Type of Information Stored

The financial web server stores and processes the following types of sensitive information:

- Financial Data: Transaction records, invoices, payroll details, budget reports, and other financial records.
- Personal Identifiable Information (PII): Employee and client data, including names, addresses, Social Security numbers, and banking information.
- Authentication Credentials: Usernames and passwords for accessing the financial application.
- System Logs: Logs of user activity, system events, and errors.

Criticality of the Asset

The financial web server is classified as a mission-critical asset due to its role in supporting the organization’s financial operations. A compromise of this server could lead to:

- Operational Disruption: Loss of access to financial data and tools, halting critical business processes.
- Data Breach: Exposure of sensitive financial and personal information, leading to reputational damage, regulatory fines, and legal liabilities.
- Financial Losses: Unauthorized transactions, fraud, or theft of funds.

- Compliance Violations: Failure to meet regulatory requirements such as GDPR, PCI-DSS, or SOX, depending on the jurisdiction.

Attack Tree

The attack tree will be a structured diagram that shows how the financial system can be attacked. We are going to represent the diagram starting with an attacker main goal at the top and branches into various methods and sub-technique used to reach the goal. In this evaluation, we are exploring three different methods an attacker might use to attack the financial injection. The use of a vulnerability assessment scanner will provide us with a comprehensive report on the threats.

SQL Injection Attack Tree on the financial system

In SQL injection scenario, the main goal is to compromise the financial system. The branches in Figure 1 show the different options to achieve this goal for the attacker.

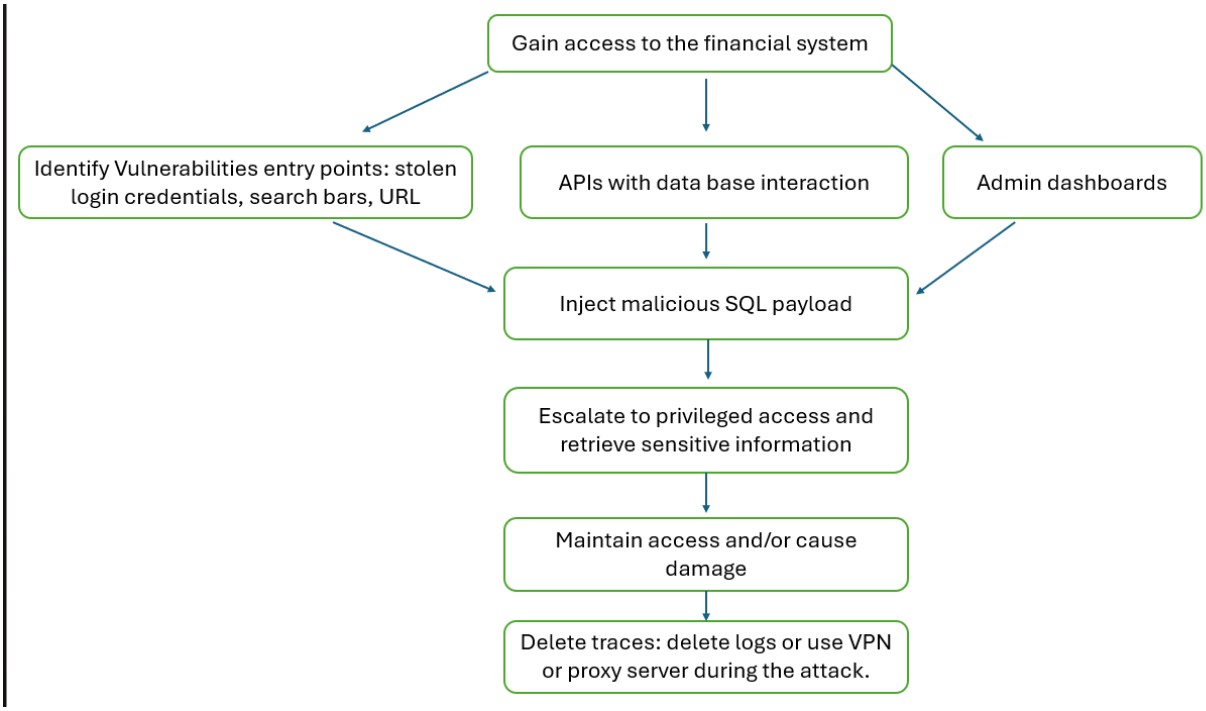

Figure 1: SQL injection attack tree

Buffer Overflow Attack Tree

In this scenario, the attacker will give a computer program more information that it can handle and confuses it and gain full access to the system. Figure 2 shows in a simple way the steps of the process that the attacker can take. The attacker might go from a single weak point to breaking down the system or takin full access to it.

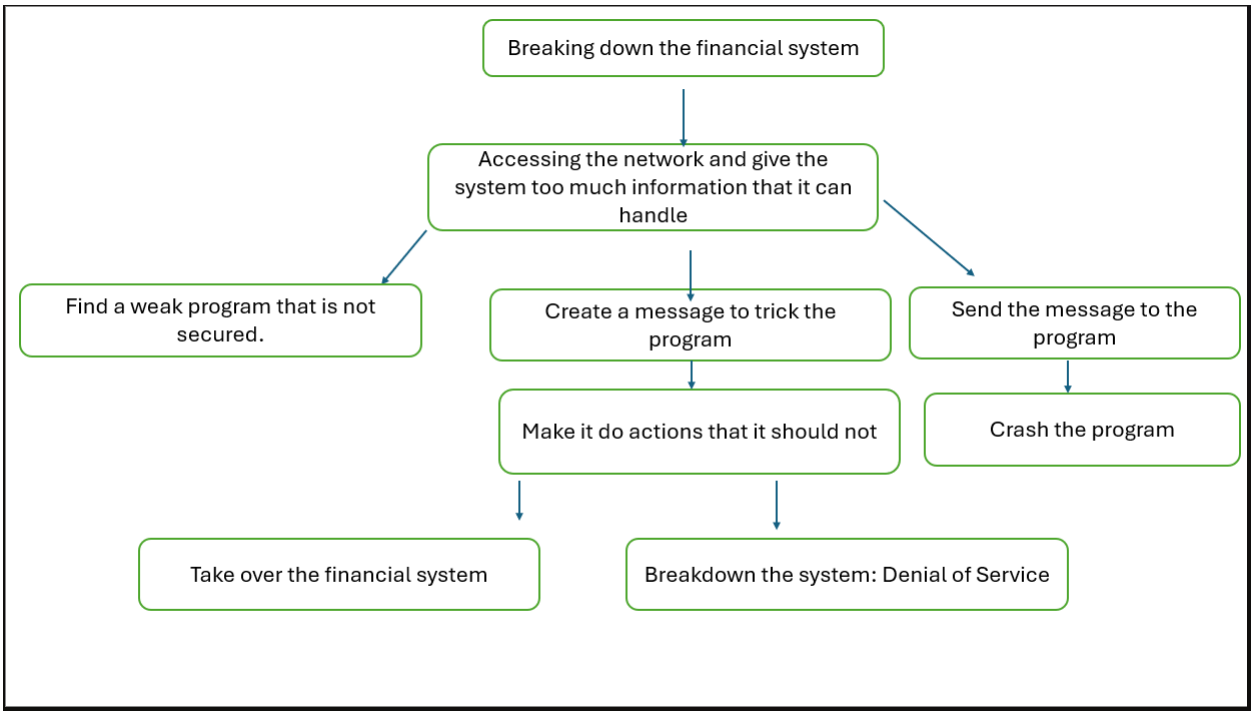

Figure 2: Buffer flow attack tree

Phishing Attack Tree

The phishing email technique is one of the most common techniques used by cyberattacks to gain unauthorized access to a system. It exploits human weaknesses to take advantage of their vulnerabilities. Figure 3 provides insight into a typical phishing attack by exploring the possibilities in an attack tree. Therefore, by understanding the steps involved, users, regardless of their technical background can be aware and will better recognize and avoid these threats.

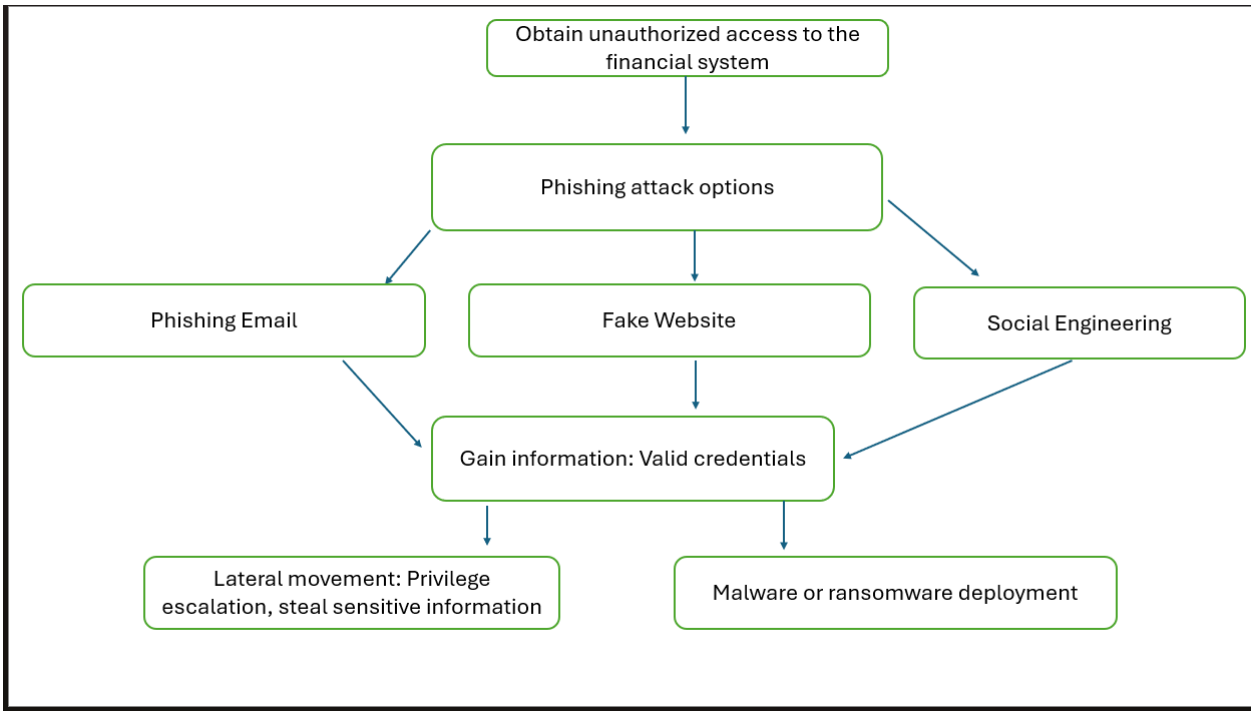

Figure 3: Phishing email attack tree

Risk Analysis

Threat/Attack: SQL Injection

Risk Scenario:
An attacker exploits a weak input field in the web application of the financial system to feed it malicious SQL queries. This allows unauthorized access to sensitive financial information, user data, and possibly administrative functions.

Risk Severity:
High – A successful SQL injection can result in data breaches, unauthorized transactions, or a total system compromise.

Required Controls:

- Implement input validation and prepared statements to prevent injection.
- Regularly test web applications using vulnerability scanners.
- Apply the principle of least privilege for database users.
- Conduct secure coding training for developers.
- Enable web application firewall rules to detect and block SQL injection attempts.

Threat/Attack: Buffer Overflow

Risk Scenario:
The attacker sends excessively long input to a vulnerable application component, leading to memory corruption. This can result in arbitrary code execution, allowing the attacker to take full control of the system or crash critical services.

Risk Severity:
Critical – Can lead to system-level access, denial of service, or complete control of the financial infrastructure.

Required Controls:

- Use secure programming languages or implement bounds checking in C/C++ code.
- Apply regular patching and updates to operating systems and software.
- Enable stack protection mechanisms.
- Conduct regular code reviews and penetration testing.
- Monitor for unusual system behavior and crashes.

Threat/Attack: Phishing Email

Risk Scenario:
An attacker sends a deceptive email to employees in the financial department, tricking them into clicking a malicious link or opening an attachment. This could lead to credential theft or malware installation.

Risk Severity:
Medium to High – Depending on the target and impact, phishing can lead to credential compromise or entry point for broader attacks like ransomware.

Required Controls:

• Give regular security awareness training to everyone.

• Install anti-phishing filters and gateway protection for e-mail.

• Enable multi-factor authentication on every user account.

• Monitor for unusual login activity and enforce strong password policies.

• Simulate phishing attacks periodically to evaluate user awareness.

Recommendations

In addition to the required controls, provide the list of recommendations that must be applied at an enterprise level to address security issues that may occur in other systems as well. For example:

- Access control must be regularly reviewed and approved
- Implement a firewall to block/filter unwanted traffic
- Intrusion detection / Log Management
- Prioritization of control implementation
- Use a cost-benefit analysis method to justify your recommendations for additional technologies.

References

McGladrey, K. (2025, February 28). *IT Risk Assessment | Protect Your Organization*. Hyperproof. Retrieved April 9, 2025, from https://hyperproof.io/resource/it-risk-assessment/

Virgil. (2025, February 2). *Detailed cyber security report examples*. Sprinto. Retrieved April 9, 2025, from https://sprinto.com/blog/cyber-security-report-example/