Topic 4 Discussion 2

In your lab, you identified privilege escalation, as well as multiple other attack types. List a minimum of four other attacks not discussed and provide a brief summary of each.

Hello Class,

While exploring privilege escalation in the lab, I discovered several other critical attack types that pose serious threats to system security. Here are four worth highlighting:

SQL Injection

SQL Injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. By injecting malicious SQL code into input fields, attackers can manipulate the database to reveal sensitive information, modify data, or even execute administrative operations(OWASP, 2024). This type of attack exploits the application's failure to properly sanitize user inputs, making it one of the most common and dangerous vulnerabilities in web applications. Effective mitigation strategies include using prepared statements and parameterized queries to ensure that user input is treated as data, not executable code.

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a type of security vulnerability found in web applications that allows attackers to inject malicious scripts into web pages viewed by other users. When a user visits a compromised page, the injected script can execute in their browser, potentially stealing cookies, session tokens, or other sensitive information. XSS attacks can be categorized into three types: stored, reflected, and DOM-based. To prevent XSS, developers should implement input validation, output encoding, and use security headers like Content Security Policy (CSP) to restrict the execution of scripts(OWASP, 2020).

Denial of Service (DoS)

A Denial of Service (DoS) attack aims to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests. This can lead to service outages, rendering websites or applications inaccessible(Cloudflare, 2019). DoS attacks can be executed using various methods, including flooding the target with traffic or exploiting vulnerabilities to crash the service. Distributed Denial of Service (DDoS) attacks, which involve multiple compromised systems attacking a single target, are particularly challenging to mitigate. Effective defenses include rate limiting, traffic filtering, and employing DDoS protection services.

Man-in-the-Middle (MITM)

A Man-in-the-Middle (MITM) attack occurs when an attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. This type of attack can be executed through various methods, such as eavesdropping on unsecured Wi-Fi networks or using phishing techniques to intercept communications(Lindemulder & Kosinski, 2024). MITM attacks can lead to data theft, session hijacking, and unauthorized access to sensitive information. To protect against MITM attacks, it is essential to use encryption protocols like HTTPS, implement strong authentication mechanisms, and educate users about the risks of unsecured networks.

References:

Cloudflare. (2019). *What is a denial-of-service (DoS) attack?* Cloudflare; Cloudflare. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Lindemulder, G., & Kosinski, M. (2024, June 11). *What Is a Man-in-the-Middle (MITM) Attack? | IBM*. IBM. https://www.ibm.com/think/topics/man-in-the-middle

OWASP. (2020). *Cross Site Scripting (XSS) | OWASP*. Owasp.org; OWASP. https://owasp.org/www-community/attacks/xss/

OWASP. (2024). *SQL Injection*. OWASP. https://owasp.org/www-community/attacks/SQL\_Injection