Strengthening Digitanotion Defence using OWASP Top 10

## Abdulazeez Uthman

## Cohort 1

## Week 1 Task

Challenge Overview

This challenge aims to strengthen the cybersecurity posture of Digitalnotion Limited by identifying and addressing vulnerabilities that could potentially compromise the organization’s systems and data. The report covers research and analysis of the OWASP Top 10 vulnerabilities, lessons learned from the Equifax 2017 data breach, an action plan to mitigate critical risks, and a conclusion reinforcing proactive cybersecurity measures.

## Research and Analysis

### OWASP Top 10 Vulnerabilities and Their Impact on Digitalnotion Limited

https://owasp.org/www-project-top-ten/

#### Broken Access Control: Weak or improperly enforced access controls can allow unauthorized users to access restricted data or functionality.

#### Impact: Unauthorized data exposure and privilege escalation.

#### Cryptographic Failures: Inadequate encryption practices can expose sensitive data. Impact: Data breaches and non-compliance with data protection regulations.

#### Injection: Unvalidated input may lead to SQL, NoSQL, or command injection.

#### Impact: Data manipulation and server compromise.

#### Insecure Design: Lack of secure software design principles. Impact: Increased vulnerability to attacks.

#### Security Misconfiguration: Unsecured configurations expose systems to attacks. Impact: Unpatched software and exposed sensitive data.

#### Vulnerable and Outdated Components: Using outdated libraries can introduce known vulnerabilities.

#### Impact: Remote code execution and data compromise.

#### Identification and Authentication Failures: Poor authentication practices may allow unauthorized access.

#### Impact: Credential theft and identity impersonation.

#### Software and Data Integrity Failures: Lack of integrity checks can result in unauthorized data modifications.

#### Impact: Tampered data or corrupted software.

#### Security Logging and Monitoring Failures: Inadequate monitoring may delay detection of breaches.

#### Impact: Prolonged exposure to cyberattacks.

#### Server-Side Request Forgery (SSRF): Exploiting server requests to access unintended resources.

#### Impact: Data exfiltration and internal system compromise.

Relevant CVEs

CVE-2021-44228 https://cve.org/CVERecord?id=CVE-2021-44228 (Log4Shell): Remote code execution vulnerability in Apache Log4j 2. Impact: Allows attackers to execute arbitrary code.

CVE-2022-0778 https://cve.org/CVERecord?id=CVE-2022-0778 (OpenSSL): Denial of service vulnerability due to malformed certificates. Impact: Service disruption and downtime.

CVE-2022-1388 https://cve.org/CVERecord?id=CVE-2022-1388 (F5 BIG-IP): Authentication bypass leading to remote code execution. Impact: Unauthorized system control.

### Case Study Reflection

The Equifax 2017 data breach https://www.breachsense.com/blog/equifax-data-breach/ demonstrated the severe consequences of delayed patching and vulnerability management. Attackers exploited a known flaw in Apache Struts (CVE-2017-5638), leading to data exposure of 147 million individuals. Key lessons include the importance of timely patching, robust vulnerability management, and comprehensive monitoring.

If Digitalnotion Limited fails to address similar vulnerabilities, it could face data breaches, financial losses, and reputational damage, similar to Equifax. Implementing timely updates and proactive monitoring is essential to mitigate such risks.

### Action Plan Proposal

Vulnerability 1: Broken Access Control

Priority: High, due to potential unauthorized data access.

Action Plan: Implement role-based access control (RBAC), conduct regular access audits, and enforce least privilege policies.

Vulnerability 2: Vulnerable and Outdated Components

Priority: High, as outdated components are frequently exploited.

Action Plan: Automate patch management, regularly update libraries, and perform vulnerability scanning to identify outdated software.

### Justification

Addressing these vulnerabilities helps prevent unauthorized access and exploitation of outdated components, reducing the risk of catastrophic breaches like the Equifax incident.

### Conclusion

Proactively addressing cybersecurity risks by implementing timely patching, regular monitoring, and robust access control measures is vital to safeguarding Digitalnotion Limited’s assets and reputation.