**Top 10 Web Application Security Risks**

# WebTech

## Vulnerable and Outdated Components

CSE 502: Web Technologies

Submitted by

**Fahim Morshed**

BSSE Roll No. : 1102

**Saad Sakib Noor**

BSSE Roll No. : 1122

Submitter to

**Moumita Asad**

Designation: Lecturer
Institute of Information Technology

Institute of Information Technology
University of Dhaka
16-04-2022

# Vulnerable and Outdated Components

A software component is part of a system or application that extends the functionality of the application, such as a module, software package, or API. Component-based vulnerabilities occur when a software component is unsupported, out of date, or vulnerable to an exploit[1]. We may unknowingly use vulnerable software components in production environments, posing a threat to the web application. For example, someone may download and use a software component, such as OpenSSL, and fail to regularly update or patch the component as flaws are discovered. This could lead to vulnerability in the application itself. Since many software components run with the same privileges as the application itself, any vulnerabilities or flaws in the component can result in a threat to the web application.

If our software components have known vulnerabilities, that exposes the application to attacks in different parts of the application. Component vulnerabilities may result in attacks described below:

- Code injection
- Buffer overflow
- Command injection
- Cross-site scripting (XSS)

## Example of Exploitation:

**1.** Panamanian law firm Mossck Fonseca (MF) was breached in 2015 and many confidential papers of the clients were leaked that became known as infamous Panama Papers. This breach was caused by an unpatched version of WordPress and Drupal used by MF. Those issued had already been fixed already when the breach took place, but MF failed to apply the appropriate security updates.

[1] "Chapter 6: Vulnerable and outdated components (A6) - AskF5." 2 Feb. 2022, https://support.f5.com/csp/article/K17045144. Accessed 11 Apr. 2022.

2. Equifax had faced the same situation in 2017. The company had been breached and personal information of 145 million were stolen. It all was caused by a flaw in its Apache struts system that had already been fixed 6 months before the breach, but not patched by Equifax.

# Prevention

- **Setting Clearly Defined Patch Management Process:** This will help to keep the app developers informed about the components and easy to keep the components up-to-date. The policy should be careful about keeping components up-to-date, set protocols for when a vulnerability is discovered or if no patch is available. This may be done by keeping the whole app down until the vulnerability is fixed or at least keep the effected features down so the vulnerable components can be separated and dealt with.
- **Continuous Monitoring for Vulnerability:** Always looking for vulnerabilities is the best solution. There are many services that help check out for vulnerabilities in applications. For example, “ImmuniWeb Discovery” can help identifying any unapproved or out of date components. “ImmuniWeb SCA” can xray web applications to find out used open source software with known vulnerabilities.