ASSIGNMENT - 1

K. Naveen Abhiram

21BCE7357

WEB APPLICATIONS SECURITY RISKS

1) OWASP: A01: 2021 – Broken Access Control
CWE: CWE-284: Improper Access Control

Description:

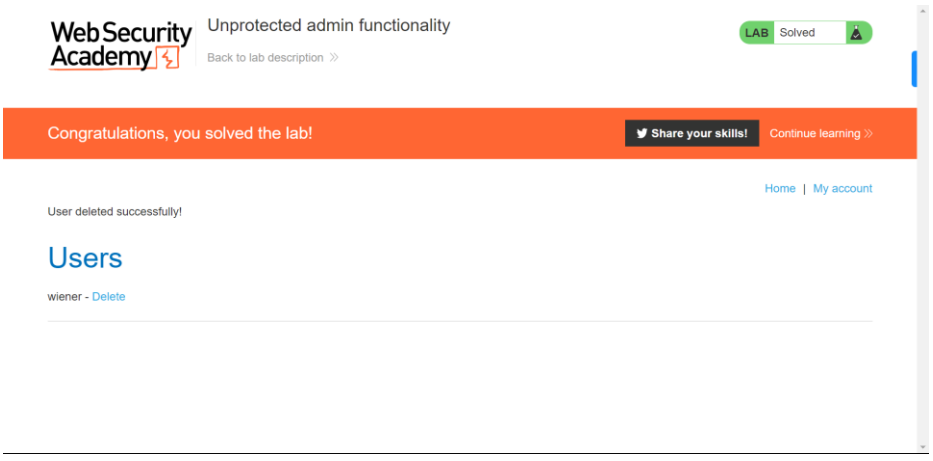
The product either doesn't restrict access to a resource from an unauthorized actor or restricts access to it wrongly.

Business Impact:

Based on the user's rights and any permissions or other access-control requirements that apply to the resource, authorisation is the process of deciding whether a user with a certain identity can access a specific resource. Users are able to access data or carry out actions that they shouldn't be able to carry out when access control checks are not executed consistently, or at all.

Numerous issues, such as information exposes, denial of service attacks, and arbitrary code execution, may result from this.

Lab Practice:



2) OWASP: A02: 2021 – Cryptographic Failures
CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Description:
The product uses a broken or risky cryptographic algorithm or protocol.

Business Impact:
By accepting an incoming password, computing its hash, and then comparing it to the previously saved hash, authentication is accomplished in this approach. An attacker is always able to brute force hashes offline once they have obtained saved password hashes. The only way a defender can sluggish offline attacks is by using hash algorithms that are as resource-intensive as feasible.

3) OWASP: A03: 2021 – Injection
CWE: CWE-564: SQL Injection: Hibernate

Description:
Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

Business Impact:
SQL injection attacks are used by hackers to get access to critical business or personally identifiable information (PII), which ultimately exposes more sensitive data. Attackers can retrieve and modify data using SQL injection, putting the sensitive firm data kept on the SQL server at risk of exposure. Privacy of Users Is Vulnerable: Private user information, including credit card details, may be exposed by an attack, depending on the data kept on the SQL server.

Lab Practice:

4) OWASP: A04: 2021 – Insecure Design
CWE: CWE-657: Violation of Secure Design Principles

Description:
The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centred around design, it can be resource-intensive to fix design problems.

Business Impact:
Insecure system configuration risks are caused by weaknesses in the security configuration, hardening, and settings of the many systems used in the pipeline. This frequently produces "low hanging fruits" for attackers attempting to increase their foothold in the environment. Due to the possibility of resulting in vulnerabilities and inadequate security architecture, it has significant business ramifications. This may result in data leaks, financial losses, reputational harm, and legal repercussions.

5) OWASP: A05: 2021 – Security Misconfiguration
CWE: CWE-319: Cleartext Transmission of Sensitive Information

Description:
The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact:
Security Misconfiguration is the fifth-most serious AppSec vulnerability. According to the research, with an average occurrence rate of 4%, over 90% of apps reported misconfiguration. It can hurt organizations by disclosing private information as it is being transmitted, which could result in data breaches, weakened customer confidence, regulatory infractions, and possible legal repercussions. Attackers can access networks, systems, and data without authorization thanks to security configuration errors, which can seriously harm your company's finances and reputation.