NAME: NANDIGAM KAMALI HARIPRIYA
REG NO: 21BCE2746
AI for Cyber Security with IBM Qradar (AI for Web Security)

Assignment - 1
Study and make a Report on OWASP Top-10 with description and Business Impact with a CWE Vulnerability. How it using a real web application like a portswigger etc.

OWASP Top-10
The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring
10. Server Side Request Forgery

1. CWE-284: Improper Access Control
OWASP CATEGORY: A01:2021-Broken Access Control

DESCRIPTION: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

BUSINESS IMPACT: Access control requires using a number of security measures, including authentication, authorization, and accountability.For example, configuring a password file to be world-writable or granting administrator rights to a guest account are examples of inappropriate privileges, permissions, ownership, etc. that are expressly stated for the person or the resource. Data breaches, financial losses, and intellectual property theft might result from allowing unauthorized access to critical systems and data. Such violations might impair services, raise compliance concerns, and harm an organization's brand, which could lead to consumer mistrust and possible legal repercussions.

2. CWE-916: Use of Password Hash with Insufficient Computational Effort
OWASP CATEGORY: A02:2021-Cryptographic Failures

DESCRIPTION: The product generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.

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.Due to the usage of insecure password hashing techniques that are simple for

attackers to crack, user credentials are compromised, possibly allowing unauthorized access to networks and sensitive data. Passwords that haven't been correctly hashed can result in unauthorized access, data leaks, financial losses from fines, and reputational harm to the company. Such events might lead to regulatory non-compliance, a decline in consumer confidence, and expensive recovery efforts.

3. CWE-94: Improper Control of Generation of Code ('Code Injection')
OWASP CATEGORY: A03:2021-Injection

DESCRIPTION: The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behaviour of the intended code segment.

BUSINESS IMPACT: This weakness is caused during implementation of an architectural security tactic. When a product accepts code syntax as user input, it's feasible for an attacker to write the code in a way that alters the product's intended control flow. Any arbitrary code might be executed as a result of such a change. This vulnerability includes the incorrect processing of user inputs, which permits the injection of malicious code and may result in unauthorized access, data breaches, and system compromise. Information theft, service interruption, monetary loss, legal action, and reputational injury can all come from this. When injectable code manages authentication, a remote vulnerability may result. Resources that the attacker is explicitly prohibited from accessing can be accessed by infected programmes. Since the control-plane data injected during a code injection attack is almost always incidental to data recall or writing, they almost always result in loss of data integrity.

4. CWE-653: Improper Isolation or Compartmentalization
OWASP CATEGORY: A04:2021-Insecure Design

DESCRIPTION: The product does not properly compartmentalize or isolate functionality, processes, or resources that require different privilege levels, rights, or permissions.
BUSINESS IMPACT: The vulnerability concerns a system's failure to adequately separate its resources or data, which might lead to unauthorised access and data leakage. Confidential information cross-contamination, unauthorised privilege escalation, and system breach can all result from insufficient isolation. Without solid boundaries, an attack might cause more damage to higher-privileged users if a vulnerability exists in functionality that is accessible by less privileged users.

5. CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
OWASP CATEGORY: A05:2021-Security Misconfiguration

DESCRIPTION: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.

BUSINESS IMPACT: In this vulnerability, attackers may be able to intercept cookies containing sensitive information across insecure connections since the 'Secure' feature is not set for such cookies. This might lead to identity theft, unauthorized access, and the disclosure

of private user information. Insufficient security might lead to hacked user accounts, legal and regulatory repercussions, monetary losses, and brand harm for the company.

**Sir, I have tried to work on the web application but couldn’t do the other technical part as I’m not familiar with it. I couldn’t further process it as I’m connected to a firewall and didn’t have proper applications on my PC.