## **Part 1: Cyber Attacks Assessment Report**

1. Introduction

Finding potential vulnerabilities in the online application was the goal of the audit. Unauthorized access, problems with configuration management, information leakages, and other flaws were among the web application's vulnerabilities that were tested. Testing on a black box was carried out.

The test only included web applications; it excluded host servers or network-related problems. We have researched cross-site scripting, a practice where malicious data is introduced between reputable websites.

Apart from our standard security assessment practices, we performed general review of applications and the same is provided in our reporting format. Below gives the glance of complete sections of our security assessment, where for this report we are highlighting the findings as below.

2.

|  |  |  |
| --- | --- | --- |
|  | Name of the vulnerability | Reference -CWE |
| 1 | **Broken Access Control** | CWE -284 Improper Access Control |
| 2. | Cryptographic Failures | CWE-327: Use of a Broken or Risky Cryptographic Algorithm |
| 3 | Injection | |  |  | | --- | --- | |  |  | | CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | |
| 4 | Insecure Design | CWE-657:Violation of Secure Design Principles |
| 5 | Security Misconfiguration | CWE-16 **Configuration** |
| 6 | Vulnerable and Outdated Components | CWE-1104: Use of Unmaintained Third Party Components |
| 7 | [Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) | [CWE-287: Improper Authentication](https://cwe.mitre.org/data/definitions/287.html) |
| 8 | Software and Data Integrity Failures | CWE-494 :Download of Code without Integrity Check |
| 9 | Security Logging and Monitoring Failures | **CWE-532** [Insertion of Sensitive Information into Log File](https://cwe.mitre.org/data/definitions/532.html) |
| 10 | Server-Side Request Forgery (SSRF) | **CWE-918**  Request Forgery attack (SSRF) |

3.

1.Vulnerability Name :Broken Access control

CWE : CWE-284 Improper Access Control

OWASP Category: A01:2021

DESCRIPTION: The restriction of access is less it provide easily access without many restrictions

Business Impact: In business its access can be very devastated for the user as it can easily give access to hacker which can change or delete accounts.

2.Vulnerability Name :Cryptographic Failures

CWE : CWE-327 Use of a Broken or Risky Cryptographic Algorithm

OWASP Category: A02:2021

DESCRIPTION:  Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

Bussiness Impact: Attempting to create non-standard and non-tested algorithms, using weak algorithms, or applying algorithms incorrectly will pose a high weakness to data that is meant to be secure.

3.Vulnerability Name: Injection

CWE : CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

OWASP Category: A03:2021

DESCRIPTION:  Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

Bussiness Impact:The unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

4.Vulnerability Name:Insecure Design

CWE : CWE-657:Violation of Secure Design Principles

DESCRIPTION:  It is related to critical design and architectural flaws in web applications that hackers can exploit.

Bussiness Impact: Failing to do so can lead to flaws that threaten your organizational security, compromising sensitive data, granting privileges to individuals who can abuse them, and more.

5.Vulnerability Name: Security Misconfiguration

CWE : CWE-16 Configuration

DESCRIPTION:  A security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access.

Bussiness Impact: Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization.

**6** Vulnerability Name: Vulnerable and Outdated Components

CWE : CWE-1104

OWASP Category: A06:2021

Description: Use of Unmaintained Third Party Components

Business Impact: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Using vulnerable and outdated components is the sixth category in OWASP Top 10 web application security risks and one of the most common and serious mistakes developers and companies make. It can lead to devastating consequences such as data breaches, malware infections, and compromised systems.

* 7.Vulnerability Name:  [Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)

CWE : [CWE-287 Improper Authentication](https://cwe.mitre.org/data/definitions/287.html)

OWASP Category: A06:2021

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

Business Impact: Improper authentication can lead to various security threats, such as: Data breaches: Improper authentication can allow unauthorized users to gain access to sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

# 8. Vulnerability Name: Software and Data Integrity Failures

CWE : CWE-494

OWASP Category: A06:2021

Description: Download of Code without Integrity Check

Business Impact: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

# 9 Vulnerability Name: Security Logging and Monitoring Failures

CWE : CWE-532

OWASP Category: A06:2021

Description:  [Insertion of Sensitive Information into Log File](https://cwe.mitre.org/data/definitions/532.html)

Business Impact: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. Sensitive data exposure can be financially costly to your business and damage your reputation and brand. The type of data at risk of exposure includes financial reports, bank account numbers, credit card numbers, usernames, passwords, customers' personal details, and healthcare information.

# 10. Vulnerability Name: Server-Side Request Forgery (SSRF)

CWE : CWE-918

OWASP Category: A06:2021

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. A Server-Side Request Forgery attack (SSRF) is a security vulnerability in which a hacker tricks a server into accessing unintended resources on his behalf. An SSRF attack can lead to sensitive information being leaked or the attacker gaining control of other systems.

Business Impact: In some situations, the SSRF vulnerability might allow an attacker to perform arbitrary command execution. An SSRF exploit that causes connections to external third-party systems might result in malicious onward attacks that appear to originate from the organization hosting the vulnerable application.