TASK 3

A01:2021-Broken Access Control

DESCRIPTION

Users cannot act outside of their intended permissions.Leads to unauthorized data disclosure ,modification and destruction outside the user's limits.

BUSINESS IMPACT

Giving any user authorization to perform such a task which they are not supposed to will result in information exposure, dos(denial of service) and arbitrary code execution.

A02:2021-Cryptographic Failures

DESCRIPTION

Passwords,credit card numbers,health records,personal information and business secrets all require extra protection.

BUSINESS IMPACT

After acquiring password hashes,the attacker can apply various brute force hashes offline.

We can prevent this by including resources which are as intensive as possible

A03:2021-Injection

DESCRIPTION

Using dynamic sql queries and commands to perform data breaches and modification.

BUSINESS IMPACT

These risks involve display of malicious content on the page which is visible to the user.

The attacker can perform privileged tasks of the user to gain access to the personal information.For eg: injecting an XSS(cross site scripting-security vulnerability) log in message which cannot be handled by the user at that time.

A04:2021-Insecure Design

DESCRIPTION

Missing or ineffective control design.An insecure design cannot be fixed with a perfect implementation.

BUSINESS IMPACT

Flaws in security settings,configurations and hardening of different systems across the pipelines.Giving the hackers an opportunity to expand their footprints.

A05:2021-Security Misconfiguration

DESCRIPTION

Makes users send unwanted cookies in an HTML session

BUSINESS IMPACT

Hackers can gain unauthorized access to the networks,systems and data,which can in turn cause monetary and reputational damage to your organization.