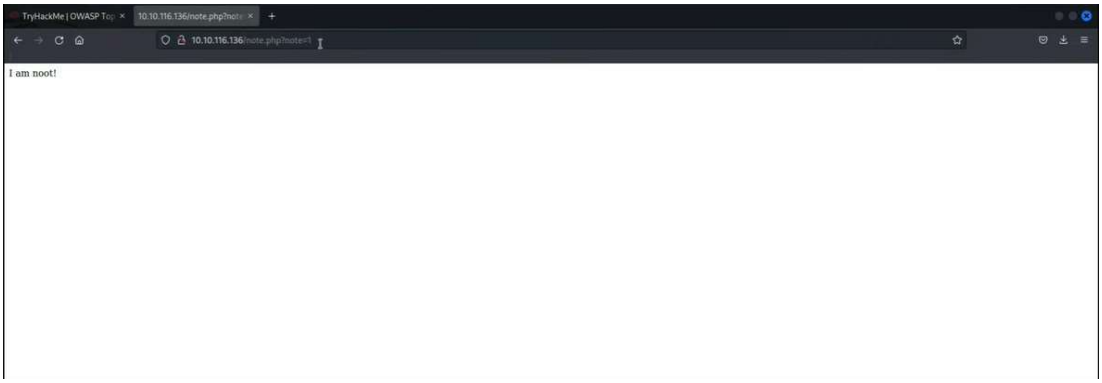
Name- Shashibhushan Das

ASSIGNMENT-1

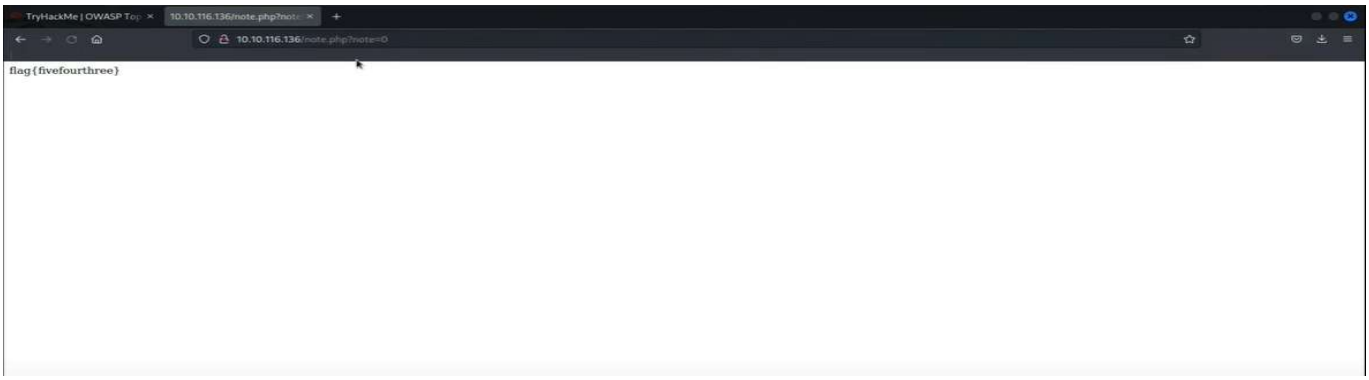
OBJECTIVE -: To write and perform the first 5 vulnerabilities of the OWASP TOP 10

1. A01:2021-BROKEN ACCESS CONTROL -:

Broken access control refers to security vulnerabilities that occur when unauthorized users gain access to restricted resources or functionalities. This breach happens due to improper configuration, weak authentication mechanisms, or flawed permission assignments. Such lapses can lead to data leaks, unauthorized modifications, and system compromise. Effective access control is crucial to maintain the confidentiality and integrity of sensitive information. Organizations must implement proper authentication, authorization protocols, and regular audits to mitigate the risks associated with broken access control. Proactive measures are essential to prevent unauthorized users from exploiting these weaknesses and to ensure a robust and secure system.
For eg:-

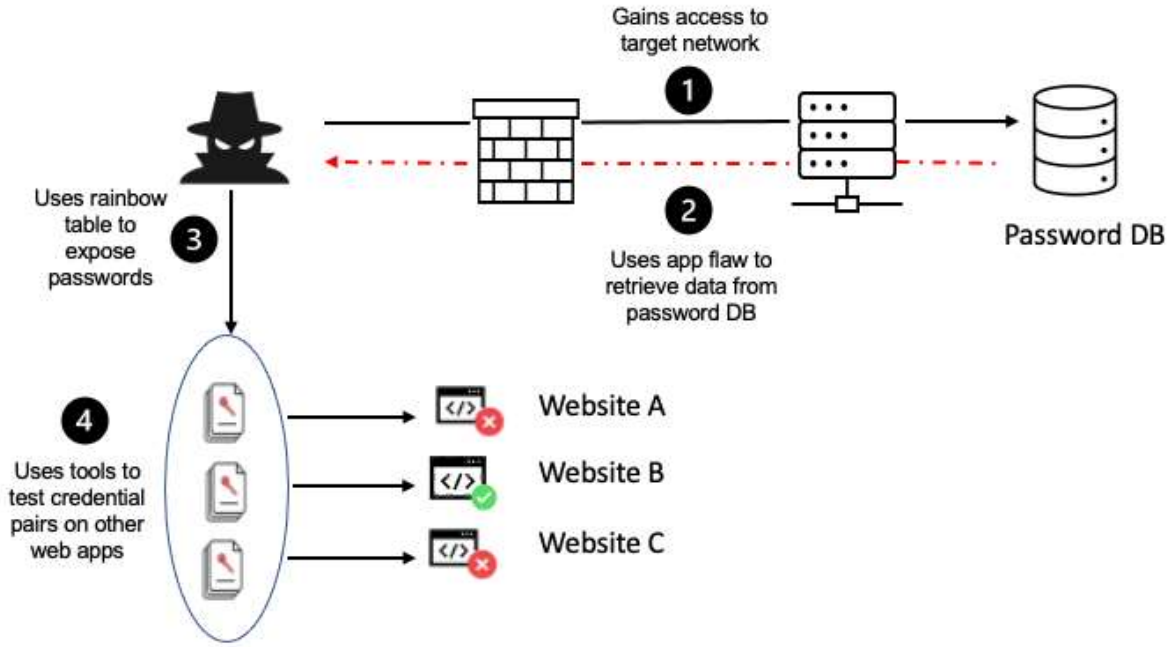


On changing the note=1 to note=0 we are able to view other flags.



2. A02:2021-CRYPTOGRAPHIC FAILURES -:

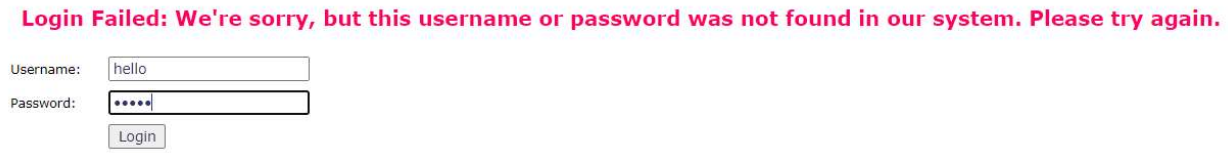
Cryptographic failure denotes the breakdown of security mechanisms that use encryption to protect sensitive information. It can arise from weak algorithms, poorly generated keys, or improper implementation. When cryptographic systems fail, data confidentiality and integrity are compromised, leading to unauthorized access and potential breaches. Historical instances like the "Heartbleed" bug underline the ramifications of cryptographic vulnerabilities. Rigorous algorithm selection, secure key management, and constant scrutiny are paramount to avert cryptographic failures. Regular updates and adherence to best practices ensure the resilience of encryption methods, reinforcing the safeguarding of digital communications and assets.



3. A03:2021-INJECTION -:

Injection refers to a critical cybersecurity threat where malicious code or commands are inserted into a software application. This occurs due to insufficient input validation or improper handling of user-generated data, enabling attackers to manipulate and control the application. Common types include SQL injection, where databases are exploited, and cross-site scripting (XSS), which compromises website integrity. Injection attacks can lead to data leaks, unauthorized access, and system compromise. Mitigation involves thorough input validation, using parameterized queries, and employing security mechanisms to block malicious input. A proactive stance against injection attacks is essential for safeguarding applications and user information.

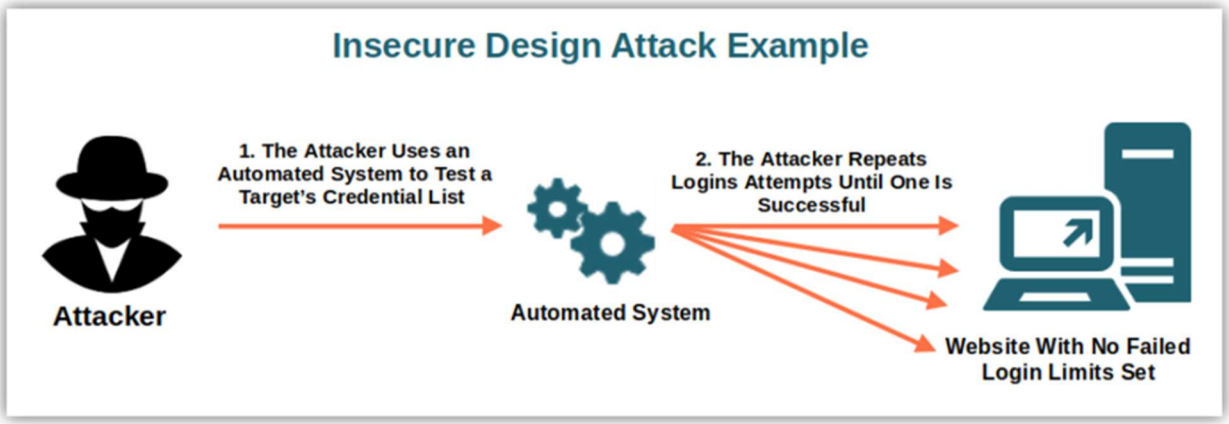
Eg-: When we put a random username and password in the login credentials we could not bypass the login



But when we put the username and password as admin in both the fields we can bypass the login. This is a type of sql injection.

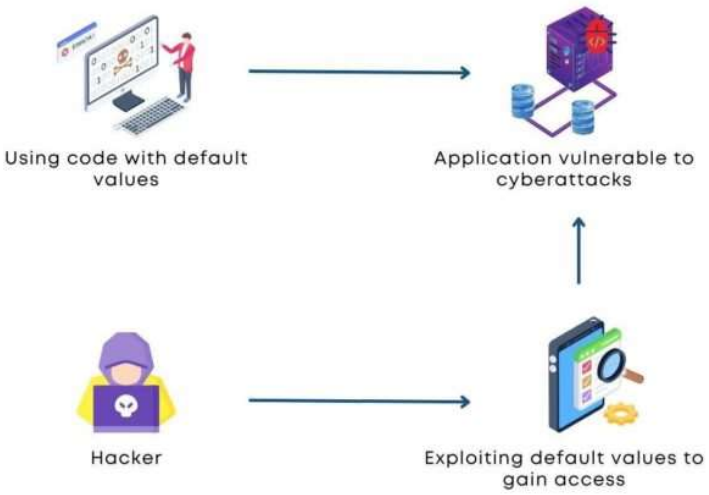
4. A04:2021-INSECURE DESIGN -:

Insecure design refers to the creation of software, systems, or products with inherent vulnerabilities that compromise their security. It stems from a lack of consideration for potential threats during the design phase. Poorly thought-out architectures, weak authentication, and inadequate data handling are common aspects of insecure design. This can result in exploitable weaknesses, leading to data breaches, unauthorized access, and system failures. Addressing insecure design necessitates a security-first approach during development, incorporating threat modeling, risk assessments, and adherence to best practices. By prioritizing security from the outset, organizations can mitigate risks and build more resilient and trustworthy solutions.



5. A05:2021-SECURITY MISCONFIGURATION-:

Security misconfiguration refers to the improper setup and configuration of software, systems, or networks, leading to vulnerabilities and potential breaches. It occurs when default settings, unnecessary features, or weak permissions are left exposed, inadvertently granting attackers access. Examples include open database ports, default passwords, and overly permissive access controls. Such misconfigurations can result in data leaks, unauthorized access, and system compromise. Regular security audits, adherence to hardening guidelines, and ongoing monitoring are essential to prevent security misconfigurations. Ensuring systems are properly configured helps fortify defenses and minimizes the risk of exploitation.



SECURITY MISCONFIGURATION