SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

23CAT704 – CYBER SECURITY

II YEAR III SEM

UNIT II – CYBER SECURITY VULNERABILITIES AND CYBER SECURITY SAFEGUARDS

TOPIC – WEAK AUTHENTICATION

WEAK AUTHENTICATION

The authentication mechanisms are weak because they fail to adequately protect against brute-force attacks. Logic flaws or poor coding in the implementation allow the authentication mechanisms to be bypassed entiauthentication".rely by an attacker. This is sometimes called "broken

Difference between authentication and authorization

- Authentication is the process of verifying that a user is who they claim to be.
- Authorization involves verifying whether a user is allowed to do something.

How do authentication vulnerabilities arise?

Most vulnerabilities in authentication mechanisms occur in one of two ways:

- The authentication mechanisms are weak because they fail to adequately protect against brute-force attacks.

- Logic flaws or poor coding in the implementation allow the authentication mechanisms to be bypassed entirely by an attacker. This is sometimes called "broken authentication".

What is the impact of vulnerable authentication?

The impact of authentication vulnerabilities can be severe. If an attacker bypasses authentication or brute-forces their way into another user's account, they have access to all the data and functionality that the compromised account has. If they are able to compromise a high-privileged account, such as a system administrator, they could take full control over the entire application and potentially gain access to internal infrastructure.

Remediation

- **Implement secure authentication protocols**: Replace HTTP basic or digest authentication with more secure authentication methods such as HTTPS or Transport Layer Security (TLS). These protocols encrypt the communication between the client and the server, ensuring that the credentials cannot be easily intercepted.

- **Enforce strong password policies**: Implement password policies that require users to create strong passwords with a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, enforce regular password changes to minimize the risk of compromised credentials.

Remediation

- **Implement multi-factor authentication (MFA)**: Implement MFA to add an extra layer of security. This can include methods such as SMS verification codes, biometric authentication, or hardware tokens. MFA makes it significantly more difficult for an attacker to gain unauthorized access even if they have obtained the user's credentials.

- **Regularly update and patch systems**: Keep all software and systems up to date with the latest security patches. Vulnerabilities in authentication methods can be patched by software vendors, so it is crucial to regularly update and patch systems to protect against known vulnerabilities.

THANK YOU