**SAD ASSIGNMENT-2**

**What is Burp Suite and what are its features?**

Burp Suite is a popular security tool used for web application security testing. It provides features such as a proxy for intercepting and analyzing HTTP/S traffic, a scanner for automated vulnerability detection, and various tools for manualtesting, including intruders and repeaters. It is widely used to identify issues such as SQL injection, cross-site scripting (XSS), and session management flaws. Its ability to integrate automated and manual testing makes it a favorite among security professionals.

**What is SQL Injection?**

SQL Injection is a type of attack where malicious SQL statements are injected into a web application's input fields. It exploits vulnerabilities in the application's database interaction, allowing attackers to retrieve, modify, or delete sensitive information. SQL injection can lead to unauthorized access, data breaches, and other serious security issues. It is one of the most common web application vulnerabilities and can be prevented through input validation and using parameterized queries.

**Explain Cross-Site Scripting in brief.**

Cross-Site Scripting (XSS) is a web security vulnerability where attackers inject malicious scripts into trusted websites. These scripts run in the browser of other users, allowing the attacker to steal session cookies, login credentials, or other sensitive information. XSS attacks typically occur when a web application does not properly sanitize user input, allowing untrusted data to be included in the webpage without validation or escaping.

**How can we prevent Cross-Site Scripting attacks?**

Preventing Cross-Site Scripting (XSS) attacks involves validating and sanitizing user input, escaping untrusted data, and using security frameworks that automatically encode output. Content Security Policy (CSP) can also be implemented to limit what scripts can run on a page. Developers should ensure that user-supplied data is never rendered directly without proper validation, and web applications should be regularly tested for XSS vulnerabilities.

**What is Session management in web applications?**

Session management refers to the techniques used by web applications to maintain a user's state as they interact with the application. This is critical for ensuring that each user’s data and experience are kept separate. A session is typically established when a user logs in and is maintained through the use of session IDs. These IDs are stored in cookies or URL parameters. Effective session management is essential for protecting user information and preventing attacks such as session hijacking.

**What is Advanced Encryption Standard(AES)?**

The Advanced Encryption Standard (AES)is a symmetric encryption algorithm widely used to protect sensitive data. It was established by the U.S. National Institute of Standards and Technology (NIST) in 2001 and has become the global standard for encryption. AES operates on fixed block sizes (128 bits) and supports key sizes of 128, 192, and 256 bits. It provides high levels of security and is used in various applications, from securing online communications to encrypting data at rest.