Assignment 1 Ajitava Das

The OWASP Top 10 is a widely recognized list of the most critical web application security risks. These vulnerabilities can allow attackers to gain unauthorized access to sensitive data, take control of systems, and disrupt operations.

Here is a brief overview of the 10 OWASP vulnerabilities:

1. Broken Access Control: This vulnerability occurs when an attacker is able to access resources that they are not authorized to access. This can be done by exploiting weaknesses in authentication and authorization mechanisms, or by manipulating input validation.
2. Cryptographic Failures: This vulnerability occurs when cryptographic algorithms are not implemented correctly, or when weak cryptographic keys are used. This can allow attackers to decrypt sensitive data, forge digital signatures, or impersonate other users.
3. Injection: This vulnerability occurs when an attacker is able to inject malicious code into a web application, such as a SQL query or a command line command. This can allow the attacker to execute arbitrary commands on the server, or to access sensitive data.
4. Insecure Design: This vulnerability occurs when a web application is designed in a way that makes it insecure. This can include things like storing sensitive data in plain text, using insecure communication protocols, or not properly validating user input.
5. Security Misconfiguration: This vulnerability occurs when a web application is not configured securely. This can include things like running unnecessary services, using default passwords, or not keeping software up to date.
6. Vulnerable and Outdated Components: This vulnerability occurs when a web application uses components that have known vulnerabilities. This can include things like third-party libraries, plugins, and frameworks.
7. Identification and Authentication Failures: This vulnerability occurs when a web application's authentication mechanisms are weak or insecure. This can allow attackers to brute-force passwords, hijack sessions, or impersonate other users.
8. Software and Data Integrity Failures: This vulnerability occurs when a web application's software or data is not properly protected. This can allow attackers to modify or tamper with data, or to execute arbitrary code.
9. Security Logging and Monitoring Failures: This vulnerability occurs when a web application does not adequately log and monitor security events. This can make it difficult to detect and respond to attacks.
10. Server-Side Request Forgery (SSRF): This vulnerability occurs when an attacker is able to trick a web application into making unauthorized requests to other servers. This can allow the attacker to access sensitive data on those servers, or to execute arbitrary commands.