Vansh Pahuja
D12A/50

Css lab

→ Aim: To simulate SQL injection attack and cross site scripting attack.

→ Theory:

1) SQL injection attack:

1) A SQL injection attack consists of insertion or injection of a SQL query via the input data from the client to the application.
2) A successful injection SQL exploit can read sensitive data from database, modify database data, recover the content of a given file present on the database and in some cases can issue commands to the O.S.
3) SQL injection attacks allow attackers to spoof identity, tamper with exsting data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable and become administrators of the database servers.
4) SQL injection is very common with PHP and Asp applications due to the prevalence of older interfaces.
5) Due to the nature of programmatic interfaces available, J2EE and Asp.NET applications are less likely to have easily exploited SQL injections.

B) Cross Site Scripting Attack (XSS):

1) According to OWASP, XSS and Cross site request forgery (CSRF) are most popular attack methods used by hackers.

2) Cross site scripting attack exploits user's trust in website XSS is one of the most dangerous vulnerabilities in web application.

3) XSS is used to get control of user's browsers in order to execute a malicious script within the trusted website and victim remains gullible of attackers malignent intentions.

4) As a result, embedded code is successfully executed, the attacker might then be able to access any sensitive browser information or cookies.

5) Reflected xss attack is a type of vulnerability that is exploited when the i/p provided by client is processed by server side script without properly sanitizing input.

6) When attacker injects his malicious script in search query, it is called reflected xss attack as script gets executed and affects the server response.

→ Conclusion:

Thus, I have successfully studied and simulated SQL injection and Cross site scripting attack.