« Collaborative Discussion 1: UML flowchart

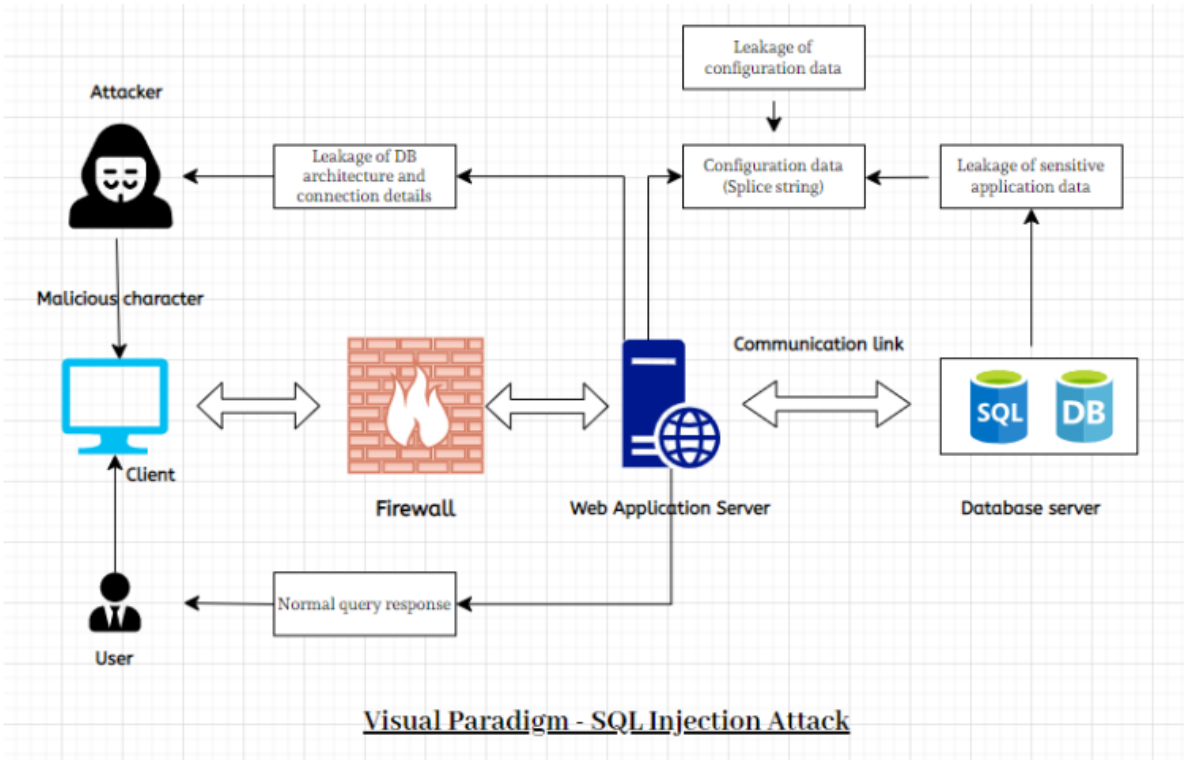
Gokul Kurunthasalam

Initial Post

A SQL injection attack involves inserting, or "injecting," a SQL query through the client's input data into the programme. A successful SQL injection attack can read sensitive data from the database, change database data (Insert/Update/Delete), perform database administration tasks (like shutting down the DBMS), recover the content of a specific file on the DBMS file system, and in some cases, send commands to the operating system.

Attackers can become administrators of the database server, spoof identities, alter already-existing data, cause repudiation problems like canceling transactions or changing balances, allow full disclosure of all data on the system, destroy data or otherwise make it unavailable, and cause repudiation issues.

In the SQL injection diagram that comes next, I explain what you can do to stop an attack that uses the OWASP technique. Websites with poor security pose possible security vulnerabilities that attackers could exploit. There are ten vulnerabilities in the website, according to the Open Web Application Security Project's (OWASP) Top 10 vulnerabilities of 2017. Since developers of websites often don't care about security, there is a good chance that attackers will use these holes to destroy, steal, or delete databases on the website. There are several malicious assaults on web applications, one of which is SQLinjection. (Riadi, Imam, Rusydi Umar, and Wasito Sukarno, 2018)



All web applications are vulnerable to attack, with SQL Injection being the most commonly used method. An attacker exploits the SQL Injection security flaw by typing text into a web application's SQL command. Attackers employ SQL operations like update, insert, select, where, and delete to modify and run shoddy SQL code in web applications. (Bach-Nutman, 2020).

References:

Bach-Nutman, Matthew. "Understanding the top 10 owasp vulnerabilities." *arXiv preprint arXiv:2012.09960* (2020).

Riadi, Imam, Rusydi Umar, and Wasito Sukarno. "Vulnerability of injection attacks against the application security of framework based bebsites open web access security project (OWASP)." *J. Inform* 12, no. 2 (2018): 53-57.

A SQL Injection Detection Method based on Adaptive Deep Forest - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Schematic-diagram-of-SQL-injection-attack_fig1_336205720 [accessed 12 Dec, 2022]