OWASP #3 – Injection

Gavin Lillard (IST-103)

Applications are subject to injection attacks when it is not correctly created to handle unexpected commands and/or queries. This means that any application that accepts user input may encounter injections. These injections affect protocols that handle databases and servers, like SQL or LDAP. SQL attacks are the most common amongst injection attacks since it deals with a very common language for database management (ImmuniWeb, 2021). The main goal of an injection attack is to access user data, much like what happened in the Heartland Breach in 2008. Many customers were exposed to the compromising of their personal and payment details dealt by the hand of SQL injection attacks.

Sadly, injection attacks have a very low skill ceiling. It does not require any coding experience at all. In most cases, just by playing around with an URL syntax you can stumble upon an injection weakness. There is also an abundance of online tutorials and automated tools for SQL injecting. Luckily, in correspondence to such a low skill ceiling there are very simple solutions to prevent these injections. OWASP (2023) has recommended that injection flaws be deterred with thorough manual source code review and automated testing of “all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs”. Basically, checking all web-application resources to ensure security. Also using both SAST and DAST tools. These steps would ensure that your application can test and secure your database and its handling of data queries, strong APIs, prior controls that protect against disclosure of sensitive data and exploitation of special characters inside syntax. Overall, diligence is the biggest key to fighting against injections.

Works Cited

Anon, Anon. “Injection Practical Overview | OWASP Top 10 | Exploits and Solutions.” *Immuniweb.com*, 2021, www.immuniweb.com/blog/OWASP-injection.html. Accessed 22 Apr. 2025.