SQL Secure

Wednesday, May 17, 2023 5:49 PM

SQL is seldom a non-frequented application in major businesses; therefore, it's security should be postured as an utmost priority as the copious amounts of data that is utilized within said application should be protected. However, SQL injection is a tactic utilized by adversaries to completely vulnerate data within organizations.

More specifically, when defining a URL routing, there needs to be a keen attention to detail as databases often are targeted by bad-actors with malicious scripts, otherwise known as SQL injection. Any kind of REST-type web services operation can be often troubling to protect as they are the ideal target for SQL injection.

In the industry today, multiple major corporations suffer private data loss, interference, and extortion. Therefore, even though this kind of threat has existed for quite some time, there is significant effort within the cyber security community to ensure this threat is mitigated if not expunged. Consequentially, there are ongoing efforts and developments in new defense tactics and methodologies regarding heightened cyber-hygiene.

Some solutions involve large companies investing into their R&D teams, while others involve the consult of Cybersecurity professionals who run their own practice. Nowadays these options are not mutually exclusive, as they are joining to become omnipresent in the CySec industry. Conjoined forces however are still not enough to ensure heightened security as SQL Injections remain in the top 3 most popular attacks and of course this is quite concerning. Thus, my interest and subsequent decision to create a preliminary SQL injection scanner.