

We plan to research and present information regarding the background, logistics, dangers, and impact of cross site scripting (XSS) and SQL injection vulnerabilities associated with websites and web-based applications. As part of the presentation we plan to show how these code injection and local or remote execution exploits can be used to gain unauthorized access to a web resource, divulge information stored within databases, hijack website sessions, and even self-propagate to other websites and end-users. The goal of the presentation is to educate future web developers of the importance of protecting against these types of attacks and offering suggestions for doing so.

Cross site scripting (XSS) attacks can occur on websites which allow users to enter data that is displayed back to them or other users. Exploit code is submitted through a form or other submission mechanism and the code, which is legitimately returned by the web server, is executed locally on their machine and usually results in some private data regarding use of the site, such as cookie variables, to be stored or transmitted to a third party. In most cases, this occurs without any indication to the end-user. It has been estimated that last year, nearly 80% of all web-related documented security vulnerabilities were related to a cross site scripting exploit. SQL injection or insertion attacks occur when a malicious user of a web resource submits data which is processed as part of a database query. The submission extends the query to return and display, delete, or alter information other than that intended by the application. This allows the malicious user to not only modify or remove, but also access confidential or restricted information, often resulting in monetary loss or identity theft of legitimate users of the website or application. SQL injection attacks have also been responsible for countless interruptions of service on governmental and corporate websites.