

## ABSTRACT

Calvin / 54150305 / 2019 / Application of SQL (Structured Query Language) Injection Security Systems to URLs (Uniform Resource Locator) Websites Using BASE64 Cryptography / Advisor: Joko Susilo, S.Kom., M.M., M.Kom.



The website is a tool used to disseminate information through the internet, both in the form of text, images, sounds, and videos. On the internet, almost all information that is shared is privacy and important, and dangerous if it is obtained by an unauthorized party. All information shared is linked through a URL, so the URL is often used as a medium for committing crimes. Various ways can be done to commit the crime. One of them is using the SQL Injection method. And one way to prevent SQL Injection is to use BASE64 cryptography.

This study examines the security of a website developed by most of the developers who still do not pay attention to the security system. The purpose of this study is to warn and inform readers to protect the database from threatening attacks.

This study uses qualitative methods with observation as the main data collection method followed by in-depth interviews with programmer from best agency to support research. The analysis uses decomposition, testing, and direct verification with the programmer.

The results of the study show that there are many ways to secure a website / database. Because in the case, there are many ways to secure it, but it is not realized / known for its use.

This research shows that SQL Injection attacks can cause confidential data to leak through unexpected loopholes. So that special handling is needed so that attacks from SQL Injection can be handled and do not cause harm done by irresponsible people.

**Keywords:** Security, SQL Injection, Cryptography, URL, BASE64