Sistem Fuzzer Menggunakan *Static Code Analysis* Untuk Serangan XSS

Adzkar Fauzie Rahman[1], Vera Suryani[2], Aulia Arif Wardana[2]

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]adzkarfauzie@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstract

XSS *(Cross Site Scripting)* is one of the security holes in website applications that can result in fatal errors such as data leaks and account takeovers. Website applications that are currently developing have been developed with various frameworks and various libraries. There are many types of frameworks and libraries that exist, there is no method that can analyze website applications that have XSS security holes without having to follow the frameworks and libraries used by website applications. The static code analysis method is used to find the location of security holes in website applications. After finding the location of the possible XSS vulnerability, a *fuzzing attack simulation* is carried out according to the payload of the analyzed XSS vulnerability.

Keywords: ***XSS, payload, static code analysis, fuzzing attack simulation, website aplication***