Abstrak

Cross Site Scripting (XSS) menjadi salah satu isu keamanan aplikasi *web* yang sedang berkembang. User memasukan script tertentu pada aplikasi *web* dan akan tereksekusi pada saat user lain sebagai korban mengaksesnya melalui *web* browsernya. Informasi sensitif pada browser tersebut dapat terkirim kepada user lain yang tidak bertanggung jawab. Kerentanan aplikasi *web* terhadap celah ini mampu membuat resiko seperti pencurian account user. Hal ini cukup berbahaya karena privasi seseorang dapat terganggu.

Pencegahan dapat dilakukan dengan mengawasi variabel input serta output data pada aplikasi *web*. Tugas akhir ini memberikan salah satu solusi berupa modul aplikasi *web* PHP pencegah XSS dengan nama xrex. Xrex diimplementasikan dalam bentuk class PHP. Pendeteksian XSS dibantu *rules* dalam bentuk *regex* yang dibuat berdasar XSS *cheat sheet* [12]. Hasil analisis XSS *cheat sheet* membentuk 17 *regex* sebagai *rules*. Selanjutnya modul ini diuji dengan mengintegrasikannya pada aplikasi *web* dengan memberikan input berupa string serangan XSS serta string lain yang dianggap normal. Sebagai hasilnya dapat dilihat tidak adanya *false* negatif yang muncul, namun terdapat 7 *false* positif dikarenakan xrex belum mampu mengawasi *hyperlink* serta *image* yang mengacu pada host lain.

Kata kunci: Keamanan Aplikasi *Web*, XSS, Cross Site Scripting, PHP, *Regex*