ABSTRAK

Layanan internet memudahkan bagi pengguna dapat berbagi layanan bersama dan saling bertemu melalui aplikasi web yang sudah ada pada saat ini. Semua informasi dengan mudah didapatkan dari aplikasi web yang ada. Namun dengan adanya teknologi informasi saat ini aplikasi web dijadikan sebagai incaran *hacker*. Ada banyak ancaman yang sering menyerang pada aplikasi web salah satunya ialah *SQL Injection, Cross-Site Scripting* dll. *SQL injection* adalah sebuah aksi hacking yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah *SQL* yang ada di memori aplikasi *client*.

Keamanan pada aplikasi web kurang mendapatkan perhatian dari *developer* dan akibatnya banyak serangan terhadap web melalui internet, maka dari itu padaproyek akhir ini dibuat pengamanan khusus yakni *Web Application Firewall* dengan *tools shadow daemon*. *Web Application Firewall* (WAF) adalah suatu metode untuk pengamanan pada aplikasi web, yang bertujuan untuk mencegah adanya ancaman dari *attacker*. Sistem dibangun untuk mencegah *SQL injection, cross-site Scripting* dan *command injection* pada web server.

Banyak sekali yang melakukan serangan informasi seperti ancaman *SQL injection, cross-site scripting* dan *command injection*. Contohnya yaitu kasus website komisi pemilihan umum (KPU) diretas oleh hacker asal jogja pada tahun 2004, dengan menggunakan *SQL Injection* peretas berhasil mengubah tampilan website dengan informasi yang sangat nyeleneh. Maka dari itu dibutuhkan keamanan pada aplikasi *web application firewall* dengan *toolls shadow daemon*. Pada proyek akhir ini akan dibangun *prototype firewall* dengan *tools shadow daemon* berbasis ubuntu pada web server. Untuk mengamankan web server dari serangan pada *SQL Injections*, *Cross-Site Scripting*, dan *Command Injection.*

Kata Kunci: Waf, *Shadow Daemon, SQL Injection, Cross-Site Scripting, Command Injection.*