

ABSTRAK

Perkembangan internet mengubah dampak bagi kehidupan masyarakat segala sesuatu informasi cepat terselesaikan. Dampak adanya perkembangan internet berdampak pula pada perkembangan dunia penyerangan/ *hecker* pada sistem informasi/ *website* yang merupakan hasil dari perkembangan internet, terdapat banyak *website* menjadi korban penyerangan oleh *hecker*/peretas. Oleh karena itu soal keamanan informasi menjadi topik dalam dunia teknologi informasi. Terkait celah keamanan pada aplikasi *web*, biasanya celah tersebut muncul karena adanya *bug* atau kesalahan pemrograman yang lupa untuk diatasi oleh pemrogram. Misalkan lupa untuk melakukan *filter* suatu masukan, sehingga jika memasukkan karakter-karakter berbahaya seperti tanda petik(') akan mengakibatkan kesalahan dan munculnya sebuah *error* pada halaman *web* dan biasanya, hal tersebut dimanfaatkan oleh hecker untuk mencoba mendapatkan informasi dari *error* tadi. Oleh karena itu dilakukan pendeteksian dan pengamanan serangan *web*, pada penelitian ini akan dibangun sistem untuk mendeteksi serangan-serangan terhadap *web* serangan-serangan tersebut adalah *Cross-Site Scripting (XSS)*, *SQL Injection* dan *Remote File Inclusion (RFI)*. Metode pendeteksian terhadap serangan tersebut menggunakan *Web Application Firewall* dan *Modsecurity*. Walaupun nilai dari sebuah keamanan tidak ada yang mutlak, harapannya dengan sistem yang akan dibangun nantinya dapat mengurangi peluang seorang hecker untuk dapat meretas aplikasi *website*.

Kata Kunci : *hecker*, *-Site Scripting (XSS)*, *SQL Injection* dan *Remote File Inclusion (RFI)*, *Web Application Firewall* dan *Modsecurity*

ABSTRACT

The development of the internet change the impact for people's lives everything information quickly. The impact of development the internet impact among the rise of the assault / hecker on information systems / website that is the result of development, There are many website victims assault by hecker. Hence information about security be the subject of information technology in the world Related gap security on the application, website usually the slit arose because there is a bug or programming errors who forgot to overcome by programmer. An example forget to do a, filter input so if include character dangerous As a stringed () will result in a mistake and the emergence of an error on page and usually, website this used by heaker to try to get information from the error by heaker to try to get information from the error above. Hence done detection and security attack, website to research will be built System to detect attack against attack was website *Cross-Site Scripting (XSS)*, *SQL Injection* and *Remote File Inclusion (RFI)* The detection of the attack using a web application firewall and modsecurity. Although the value of a security nobody absolute, the expectation with the system to be built later can reduce the chances of a heaker to be able to compromise the application website.

Key word : *hecker, -Site Scripting (XSS), SQL Injection and Remote File Inclusion (RFI), Web Application Firewall dan Modsecurity*