

ABSTRACT

The website security system becomes very important when the website has important data which is very risky if it is attacked or stolen by irresponsible parties, such as the website belonging to the Health BPJS (Social Security Administration Agency) which is strongly suspected by the Ministry of Communication and Information Technology (Kemenkominfo) the theft of Indonesian people's data and sold at a price of 0.15 bitcoin in a forum. Based on these problems, the purpose of this research is to test two frameworks that are often used in making websites, namely CodeIgnitor and Laravel using the Acunetix and OWASP ZAP testing tools. The results obtained in the testing process are that the CodeIgnitor framework using the BUMN recruitment website gets 2 alerts with Acunetix and 16 alerts with OWASP ZAP, while the Laravel framework using the Kolabjar website gets 12 alerts for Acunetix and 14 alerts for OWASP ZAP. The application of the OWASP Top 10 concluded that the CodeIgnitor framework is more at risk of being exposed to threats because there is a SQL Injection threat and enters the code indicator A03, whereas in Laravel there is indicator code A01 in both tools which are not found in CodeIgnitor.

Keywords: *Acunetix, CodeIgnitor, Laravel, OWASP ZAP, Security*

ABSTRAK

Sistem keamanan *website* menjadi sangat penting ketika *website* tersebut memiliki data penting yang sangat riskan jika terkena serangan maupun pencurian data dari pihak yang tidak bertanggung jawab, seperti *website* milik BPJS (Badan Penyelenggara Jaminan Sosial) Kesehatan yang diduga kuat oleh Kementerian Komunikasi dan Informatika (Kemenkominfo) terjadinya pencurian data masyarakat Indonesia dan dijual dengan harga 0,15 *bitcoin* di sebuah forum. Berdasarkan permasalahan tersebut, tujuan dari penelitian ini untuk menguji dua *framework* yang sering digunakan dalam pembuatan *website* yaitu *CodeIgnitor* dan *Laravel* dengan menggunakan alat pengujian *Acunetix* dan OWASP ZAP. Hasil yang didapatkan pada proses pengujian bahwa *framework CodeIgnitor* dengan menggunakan *website* rekrutmen BUMN mendapatkan 2 *alert* dengan *Acunetix* dan 16 *alert* dengan OWASP ZAP, sedangkan untuk *framework Laravel* dengan menggunakan *website* kolabjar mendapatkan 12 *alert* untuk *Acunetix* dan 14 *alert* untuk OWASP ZAP. Penerapan OWASP Top 10 didapatkan kesimpulan *framework CodeIgnitor* lebih riskan terkena ancaman karena terdapat ancaman *SQL Injection* dan masuk pada indikator kode A03, sedangkan pada *Laravel* terdapat kode indikator A01 pada kedua *tools* yang tidak terdapat pada *CodeIgnitor*.

Kata kunci: *Acunetix*, *CodeIgnitor*, Keamanan, *Laravel*, OWASP ZAP