BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi aplikasi berbasi web begitu pesat di era industri 4.0 saat ini, sehingga pengujian sistem keamanan aplikasi berbasis web menjadi sangat penting. Begitu banyak situs web yang dibangun belum memperhatikan apakah web tersebut sudah aman dari berbagai macam gangguan atau belum, baik web milik perorangan maupun suatu organisasi, oleh karena itu gangguan sering terjadi dan merugikan individu atau organisasi. Contoh dari gangguan paling umum adalah *malicious codes, viruses, worms dan trojans, malware, malicious insiders, stolen devices, phishing, social engineering* dan serangan berbasis web (Bendovschi, 2015). *Malicious codes* atau dikenal dengan *malware* merupakan jenis serangan yang cukup sering ditemukan menyerang situs web.

Di Indonesia, ada contoh kasus *hacking cybercrime* dan contoh penanganan kasus perusakan oleh pemerintah. Berdasarkan Kompas.com bahwa pada akhir bulan Mei 2021 situs milik BPJS yaitu bpjs-kesehatan.go.id diduga diretas dengan terjadinya kebocoran data milik 279 juta penduduk Indonesia dijual diforum *online* bernama Raid Forum. Data tersebut dijual dengan harga 0,15 Bitcoin (sekitar Rp. 84,4 juta, kurs 20 Mei 2021) tersebut berisi NIK, nomor ponsel, *e-mail*, alamat, hingga gaji. Menurut pendalaman yang dilakukan oleh Kementrian Komunikasi dan Informatika (Kemenkominfo) bahwa sampel data tersebut diduga kuat identik dengan data milik BPJS Kesehatan (Kompas.com, 2021).

Berdasarkan permasalahan tersebut, untuk melindungi situs web dari serangan, disarankan agar pemilik web baik itu perorangan maupun organisasi melakukan *selftest* untuk mengetahui tingkat kerentanan terhadap situs web tersebut. S*elftest* dapat membuat pemilik *website* mengetahui kerentanan dari sistem yang ada untuk kemudian dipahami. Metode *selftest* yang bisa dilakukan salah satunya yaitu *penetration test* (Dirgahayu et al., 2015).

Berdasarkan CNNIndonesia.com pada 2019 pengamat Keamanan Siber Kun Arief mengatakan 98% situs Kementerian atau Lembaga (K/L) dan Badan Usaha Milik Negara (BUMN) rentan untuk diretas (CNNIndonesia.com, 2019). Pada perekrutannya, BUMN melakukan seleksi bersama melalui *website* https://rekrutmenbersama.fhcibumn.id/. Informasi/data peserta menjadi sangat penting melihat dari contoh kasus *hacking cybercrime* yang terjadi terhadap *website* bpjs-kesehatan.go.id sehingga perlunya melakukan *vulnerability assesment* untuk mengetahui tingkat kerentanan pada web tersebut. Aparatur Sipil Negara (ASN) adalah profesi bagi pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi pemerintah. https://kolabjar-asnpintar.lan.go.id/ merupakan *website* pelatihan untuk ASN. Perlindungan informasi/data pada web tersebut sama pentingnya dengan web rekrutmen BUMN, namun terdapat perbedaan dalam pembuatan kedua web. Pada web rekrutmen BUMN dibuat menggunakan *framework codeigniter* sedangkan untuk web pelatihan ASN menggunakan *laravel.*

Penelitian terkait oleh Ghozali pada tahun 2019 mendeteksi kerentanan keamanan aplikasi berbasis *website* terhadap *website* PT. Gitsolution dengan

metode *Open Web Application Security Project* (OWASP) *Risk Rating* ditargetkan terhadap 2 aplikasi berbasis *website* yang memiliki karakter berbeda sebagai sampelnya, yaitu *framework codeigniter* dan *PHP Native.* Penelitian ini dilakukan mekanisme metode asesmen risiko pada sistem informasi harga komoditas yang dimana sistem tersebut merupakan informasi harga pokok untuk kehidupan sehari-hari yang dikelola oleh salah satu instansi pemerintah indonesia. Hasil akhir dari resiko keseluruhan menunjukan tingkat keparahan keamanan serupa, sehingga tidak ada jaminan menghindari kerentanan keamanan dengan menggunakan *framework codeigniter* atau *PHP Native* (Ghozali et al., 2019).

Penelitian Purba yang berjudul *Analisis Keamanan Website Prodi Sistem Informasi Uinsu Menggunakan Metode Application Scanning,* menguji sebuah website prodi Sistem Informasi UINSU yang menggunakan framework Laravel dengan salah satu aplikasi pengujian menggunakan OWASP ZAP. Pengujian dilakukan agar dapat meningkatkan keamanan *website* Prodi SI UINSU guna melindungi pengolahan data dan informasi yang ada baik berupa agenda, opini mahasiswa serta *profile* prodi. Kelamahan terdapat pada data dan fitur yang belum *updat* serta *backline* yang kurang baik. Hasil yang didapatkan yaitu tidak terdapatnya token CSRF yang seharusnya digunakan pada setiap *form* yang ada pada sebuah web serta keamanan lebih untuk cookies website (Purba et al., 2022).

Penelitian yang berjudul *Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner* yang dilakukan oleh Zirwan pada 2020 bertujuan untuk mengetahui tingkat keamanan web resmi versi ke 3 Institut Teknologi Padang (ITP). Alasan versi ke 3 diluncurkan ialah untuk menutupi celah

keamanan yang terjadi pada versi 2 dimana pada versi ini masih menggunakan teknologi *scripting* yang rentan menjadi target *attacker*. Hasil penelitian menunjukkan bahwa pengujian terhadap *website* Institut Teknologi Padang menggunakan *Acunetix* mendapatkan *threat* level 3 yaitu terdapat level ancaman tinggi dan dilakukan penanganan terhadap ancaman yang didapatkan dan dilakukan pengujian kembali sehingga level ancaman menjadi turun menjadi *threat* level 1 (Zirwan, 2022).

Laravel dan *CodeIgniter* keduanya merupakan *framework* PHP yang populer digunakan untuk mengembangkan web (Laaziri et al., 2019). Kerentanan dapat menimbulkan risiko keamanan yang signifikan pada aplikasi web yang dibangun menggunakan *laravel* dan *codeigniter* jika tidak segera ditangani. Beberapa kerentanan umum terhadap kedua *framework* tersebut yang sering ditemukan pada penelitian-penelitian sebelumnya meliputi: *SQL Injection*, *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF) dan lain sebagainya.

Penelitian ini dilakukan tidak terlepas dari hasil studi penelitian sebelumnya yang telah dilakukan sebagai bahan pembanding dan kajian. Penelitian ini secara garis besar persamaannya mengacu pada penelitian yang dilakukan oleh Ghozali, yaitu menggunakan metode OWASP untuk pengujian keamanan pada *framework CodeIgniter*, serta pada penelitian Purba yang melakukan pengujian pada *website* dengan *framework Laravel*. Berdasarkan dua penelitian tersebut pada penelitian ini akan melakukan pengujian pada web rekrutmen BUMN yang menggunakan *framework codeigniter* dan web pelatihan ASN yang menggunakan *framework laravel* dengan aplikasi OWASP ZAP dan *Acunetix* dengan tujuan untuk

membandingkan hasil dari kedua *framework* dan kedua aplikasi yang berbeda dengan parameter perbandingan keamanan menggunakan OWASP Top 10 sebagai indikator hasil pengujian.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana mengidentifikasi kerentanan sistem pada *website* rekrutmen BUMN dan pelatihan ASN yang menggunakan *framework laravel* dan *codeigniter*?
2. Bagaimana hasil pengujian dan analisis kerentanan *website* yang menggunakan *framework laravel* dan *codeigniter* menggunakan *Acunetix dan Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP)?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini, yaitu:

1. Penelitian yang dilakukan terbatas hanya pengujian keamanan situs web yang menggunakan *framework laravel* dan *codeigniter.*
2. Menerapkan pengujian dengan *Acunetix* dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP) dengan target situs yang menggunakan *framework laravel* dan *codeigniter.*

3. Menerapkan pengujian dengan *Acunetix* dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP) untuk identifikasi pengujian kerentanan situs web.
4. Seluruh identifikasi pengujian kerentanan pada situs web menggunakan aplikasi dan dijalankan secara otomatis.
5. Perbandingan kerentanan berdasarkan OWASP Top 10 untuk kedua *framework* dan berdasarkan dua alat pengujian.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Melakukan identifikasi kerentanan sistem pada *website* yang menggunakan *framework laravel* dan *codeigniter.*
2. Mengetahui hasil pengujian dan analisis pengujian keamanan web menggunakan *Acunetix* dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP).

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebaga berikut:

1. Mengetahui *framework* yang lebih baik dengan pengujian menggunakan *Acunetix* dan OWASP ZAP.
2. Mengetahui alat pengujian yang lebih baik dalam pengujian terhadap web.

3. Mengetahui kerentanan yang terdapat pada *website* yang menggunakan *framework Laravel* dan *CodeIgniter*.
4. Mendapatkan informasi perihal *pentration tes*t terhadap *website* yang menggunakan *framework Laravel* dan *CodeIgniter*.

1.6 Metodologi Penelitian

Metode yang digunakan dalam penelitian ini akan dilakukan dengan tahap-tahap sebagai berikut:

a. Studi Literatur

Tahap ini bertujuan untuk menjelaskan kajian pustaka dari teori-teori penunjang yang mendukung konstruksi penelitian. Kegiatan ini dilakukan dengan membaca buku, jurnal, artikel laporan penelitian, dan situs-situs di internet yang berkaitan dengan masalah pada penelitian ini.

b. Identifikasi Bahan Uji

Melakukan identifikasi bahan uji seperti *hardware* dan *software* yang digunakan, spesifikasi web dengan *framework Laravel*, dan spesifikasi web dengan *framework CodeIgniter*.

c. Implementasi dan Pengujian

Mengimplementasikan pengujian terhadap situs web yang akan di uji dengan *penetration test* berdasarkan aplikasi *Acunetix* dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP), kemudian membandingkan keamanan dan kerentanan terhadap kedua aplikasi tersebut dengan setiap tahapan yang ada pada aplikasi tesebut sebagai parameter perbandingannya.

d. Penarikan Kesimpulan

Hasil penelitian kemudian dilakukan penarikan kesimpulan berdasarkan kerentanan kedua *framework* tersebut sehingga didapatkan hasil akhir yang menunjukkan lebih rentan *framework Laravel* atau *CodeIgnitor*.

1.7 Sistematika Penulisan

Sistematika dalam penyusunan laporan ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini dijelaskan mengenai latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini akan menjelaskan penelitian terkait, teori-teori yang digunakan dalam melakukan uji coba, penulisan, serta perangkat yang dibangun sebagai dasar penulisan skripsi.

BAB III METODOLOGI PENELITIAN

Bab ini dijelaskan tentang uraian langkah-langkah atau metode yang digunakan selama penelitian, identifikasi kebutuhan penelitian, serta cara implementasi dan pengujian.

BAB IV HASIL DAN PEMBAHASAN

Menjelaskan analisa hasil dari uji coba yang dilakukan untuk mendapatkan nilai perbandingan dari penelitian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan dan saran guna memperbaiki kekurangan yang terdapat pada penelitian yang dilakukan.