BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian ini berdasarkan pada penelitian sebelumnya oleh Setyo Utoro, Bayu Andi Nugroho, Meinawati, dan Septian Rheno Widianto pada tahun 2020 dengan judul Analisis Keamanan *Website E-Learning* SMKN 1 Cibatu Menggunakan Metode *Penetration Testing Execution Standard*. Analisis ini dapat mengetahui beberapa celah keamanan yang ada di *website E-Learning* SMKN 1 Cibatu diantaranya berupa *Web Server Transmits Cleartext Credential*, *Cross-Site Scripting* (XSS), dan *Cross-Site Request Forgery* (CSRF). Hasil penelitian analisis dengan menggunakan *tool Open Web Aplication Security Project* (OWASP) ditemukan beberapa kerentanan salah satunya *Clickjacking* dimana kerentanan tersebut memudahkan penyerang untuk menipu *user* agar menghapus akunnya dengan cara mengklik tombol yang sudah dimanipulasi oleh penyerang[4].

Penelitian terdahulu yang berjudul "ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA)". Berdasarkan penelitian yang dilakukan oleh Dewi Aryanti, Nurholis, dan Joy Nashar Utamajaya pada tahun 2021. Penelitian ini bertujuan untuk mendeteksi kerentanan keamanan pada aplikasi berbasis *website* Dinas Tenaga Kerja. Penelitian ini dilakukan dengan menggunakan metode *Open Web Application Security Project* (OWASP). Penelitian ini berhasil menemukan 7 risiko dengan 3 risiko memiliki *risk severity high*, 2 risiko memiliki *risk severity medium*, 2 risiko memiliki *risk severity low*[5]. Ringkasan penelitian ini dapat dilihat pada Tabel 2.1.

Selanjutnya penelitian terdahulu yang berjudul "ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4". Berdasarkan penelitian yang dilakukan oleh Moh Yunus pada tahun

2019. Penelitian ini bertujuan untuk menganalisa keamanan aplikasi berbasis web dengan framework *Open Web Application Security Project* (OWASP) versi 4 dengan menggunakan beberapa *tools security project* untuk mengetahui keamanan suatu aplikasi, sehingga dapat dijadikan sebagai standar penilaian keamanan untuk aplikasi berbasis web. Penelitian ini dilakukan dengan menggunakan metode *Open Web Application Security Project* (OWASP) Versi 4 yang dites pada sebuah aplikasi web dengan alamat "www.xyz.com". Berdasarkan hasil penelitian ini kerentanan pada *website* "www.xyz.com" dapat ditemukan kerentanan dari beberapa tahapan kategori seperti pada tahap *Authentication Testing Authorization*, *Session Management Testing*, *Input Validation Testing*, dan *Error Handling*[6]. Ringkasan penelitian ini dapat dilihat pada Tabel 2.1.

Selanjutnya penelitian terdahulu yang berjudul "ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT". Berdasarkan penelitian yang dilakukan oleh Imam Riadi, Anton Yudhana, dan Yunanri.W pada tahun 2019. Penelitian ini bertujuan untuk mengidentifikasi celah keamanan pada *website open journal system* (OJS). Penelitian ini menggunakan metode *vulnerability assessment* yang meliputi 4 proses yaitu *Footprinting* atau *Information Gathering*, *Scanning Vulnerability*, *Result Analysis*, dan *Countermeasure*. Dari 4 tahap pengujian menggunakan metode *vulnerability assessment* didapati pada tahap *Scanning Vulnerability*, tingkat kerentanan yang diperoleh dari *tool Open Web Application Security Project (OWASP)* yaitu kerentanan *high* 70, kerentanan *medium* 1929 dan 4050 kerentanan *low*. Total celah atau *vulnerability* yang ditemukan berjumlah 6049[7]. Ringkasan penelitian ini dapat dilihat pada Tabel 2.1

Selanjutnya penelitian terdahulu yang berjudul "ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10". Berdasarkan penelitian yang dilakukan oleh Yudiana, Anggi Elanda, dan Robby Lintang Buana pada tahun 2021. Penelitian ini bertujuan untuk mengetahui tingkat kerentanan pada sistem informasi *e-office* agar terhindar dari pihak yang tidak bertanggung jawab.

Penelitian ini menggunakan metode *Open Web Application Security Project* (OWASP) *TOP* 10 yang dikeluarkan oleh owasp.org. Penelitian ini berhasil menunjukkan 10 kerentanan yang sering terjadi terhadap sistem informasi berbasis *website* sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak pengembang sistem informasi *e-office* STMIK ROSMA[8]. Ringkasan penelitian ini dapat dilihat pada Tabel 2.1.

Penelitian terdahulu yang berjudul "ANALISIS SECURITY ASSESSMENT MENGGUNAKAN METODE PENETRATION TESTING DALAM MENJAGA KAPABILITAS KEAMANAN TEKNOLOGI INFORMASI PERTAHANAN NEGARA". Berdasarkan penelitian yang dilakukan oleh Bita Parga Zen, Rudy A.G Gultom, dan Agus H.S Reksoprodjo pada tahun 2020. Penelitian ini bertujuan untuk memahami resiko keamanan sistem dari serangan siber. Penelitian ini dilakukan dengan menggunakan metode *Penetration Testing* untuk mengetahui kerentanan (*vulnerability*) yang ada pada *website* teknologi informasi Pertahanan Negara. Penelitian ini berhasil menemukan beberapa kerentanan dan serangan siber seperti *Bruite Force Password* [9]. Ringkasan penelitian ini dapat dilihat pada Tabel 2.1.

Tabel 2.1 Penelitian Terdahulu

No	Judul Penelitian	Nama Peneliti (Tahun)	Metode Penelitian	Hasil
1.	ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA)"	Dewi Aryanti, Nurholis, dan Joy Nashar Utamajaya (2021)	Open Web Application Security Project (OWASP)	7 resiko dengan 3 resiko mempunyai tingkat kerentanan tinggi, 2 resiko sedang, 2 resiko rendah

No	Judul Penelitian	Nama Peneliti (Tahun)	Metode Penelitian	Hasil
2.	ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4	Moh Yunus (2019)	Menggunakan metode *Open Web Application Security Project* (OWASP) Versi 4 yang dites pada sebuah aplikasi web dengan alamat "www.xyz.com"	Kerentanan pada *website* "www.xyz.com" dapat ditemukan kerentanan dari beberapa tahapan kategori seperti pada tahap *Authentication Testing Authorization, Session Management*
3.	ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT	Imam Riadi, Anton Yudhana, dan Yunanri.W (2019)	Menggunakan metode *vulnerability assessment* yang meliputi 4 proses yaitu *Footprinting atau Information Gathering, Scanning Vulnerability*, *Result Analysis*, dan *Countermeasure*.	Pada tahap *Scanning Vulnerability,* tingkat kerentanan yang diperoleh dari *tool Open Web Application Security Project* (OWASP) yaitu Alert *high* 70, alert *medium* 1929 dan 4050 kerentanan *low*.

No	Judul Penelitian	Nama Peneliti (Tahun)	Metode Penelitian	Hasil
4.	ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10	Yudiana, Anggi Elanda, dan Robby Lintang Buana (2021)	Menggunakan metode *Open Web Application Security Project* (OWASP) TOP 10 yang dikeluarkan oleh owasp.org.	Berhasil menunjukkan 10 kerentanan yang sering terjadi terhadap sistem informasi berbasis *website* sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak pengembang sistem informasi *e-office* STMIK ROSMA
5.	ANALISIS SECURITY ASSESSMENT MENGGUNAKAN METODE PENETRATION TESTING DALAM MENJAGA KAPABILITAS KEAMANAN TEKNOLOGI INFORMASI PERTAHANAN NEGARA	Bita Parga Zen, Rudy A.G Gultom, dan Agus H.S Reksoprodjo (2020)	Menggunakan metode Penetration Testing untuk mengetahui kerentanan (*vulnerability*) yang ada pada *website* teknologi informasi Pertahanan Negara.	Berhasil menemukan beberapa kerentanan dan serangan siber seperti *Bruite Force Password*

Pada penelitian terdahulu diatas peneliti mengambil 5 referensi yang diambil dari jurnal ilmiah dan tahun yang diambil masih bisa dimasukan kedalam penelitian ini. Dari kelima judul referensi yang diambil, judul tersebut sangat berkaitan dengan judul penelitian yang peneliti ambil. Namun yang membedakan dari penelitian yang peneliti ambil adalah pada *tools* yang digunakan dalam penelitiannya, untuk penelitian terdahulu *tools* yang digunakan masih menggunakan versi yang lama sedangkan *tools* yang digunakan peneliti untuk melakukan penelitian sudah menggunakan *tools* yang terbaru.

2.2 Landasan Teori

2.2.1 *Penetration Testing Execution Standard* (PTES)

Penetration Testing Execution Standar ialah satu aktivitas di mana seorang coba mensimulasikan gempuran yang dapat dilaksanakan pada jaringan perusahaan atau organisasi tertentu untuk mendapati kekurangan yang ada dengan mempraktekan gempuran lewat sela keamanan atau kerentanan dan lakukan analisis keamanan mekanisme. Praktik gempuran yang sudah dilakukan dibikin serupa dengan kasus yang sudah dilakukan dengan seorang *black hat*. Maksudnya untuk tentukan dan ketahui tipe gempuran yang hendak dilaksanakan pada sistem dan karena yang dapat muncul karena kekurangan atau kerentanan dalam mekanisme. Saat lakukan *penetration testing*, diperlukan analisis secara intens untuk tiap kerentanan yang disebabkan oleh kekurangan sistem. Nanti sesudah dilaksanakan analisis keseluruhannya sampai usai, akan diabadikan dan dikasih ke admin situs yang berkaitan dan jalan keluar dan imbas yang bisa disebabkan dari sela keamanan yang ada. Dalam PTES ada banyak tingkatan yang dipakai seperti *Pre-engagement Interaction* yang di mana pada tahapan ini dilaksanakan proses penyiapan seperti mempersiapkan alat dan bahan dan teknik yang dipakai saat lakukan *pentest*. Tingkatan seterusnya yakni *Intelegence Gathering* yang di mana pada tingkatan ini dilaksanakan proses penelusuran info yang diperlukan seperti domain web, ip *address*, dns, dan domain info.

Tingkatan setelah itu *Threat Modelling* yang di mana pada tahapan ini dilaksanakan proses untuk mengenali ancaman dan resiko pada website. Tingkatan setelah itu adalah *Vulnerabillity Analysis* yang di mana pada tahapan ini dilaksanakan proses untuk menganalisa kerentanan yang ada pada website. Tingkatan setelah itu *Exploitation* yang di mana akan dilaksanakan percobaan *penetration testing* berdasar informasi yang sudah didapat pada tingkatan sebelumnya. Tingkatan seterusnya yakni *Post Exploitation* yang di mana akan dilaksanakan untuk masuk ke mekanisme

jaringan sasaran dan lakukan analisis infrastruktur yang ada. Tingkatan seterusnya yakni *Reporting* yang di mana akan dilaksanakan laporan (*report*) hasil analisis dan *penetration testing* yang sudah dilaksanakan awalnya, disamping itu pada tahapan *reporting* dibuatkan *report* mengenai referensi dan penuntasannya[10].

2.2.2 Keamanan Informasi

Keamanan info menurut G. J. Simons, mendeskripsikan "bagaimana usaha agar bisa menahan penipuan (cheating) atau dapat mengetahui ada penipuan pada sistem yang berbasiskan info, di mana infonya sendiri tidak mempunyai makna fisik ".Keamanan sistem info sebuah sistem yang perlu jadi perhatian karena memiliki sifat untuk umum dan global yang pada intinya tidak aman[11]. Keamanan info dipakai membuat perlindungan sebuah sistem baik komputer atau non komputer, sarana, data, dan info dari penyimpangan beberapa pihak yang tidak berwenang. Keamanan mekanisme ialah satu mekanisme yang ditujukan untuk amankan computer dari sebuah masalah dan semua ancaman yang membahayakan keamanannya yang meliputi keamanan data pemakai[12].

2.2.3 Sistem Informasi

Sistem Info menurut Fridayanthie dan Charter, mengartikan "sistem info ialah aktivitas dari proses yang di organisasikan yang dipakai untuk menyiapkan info ambil keputusan dan pengaturan pada suatu organisasi"[13]. Sistem Info sebagai beberapa kumpulan orang yang bekerja bersama untuk capai arah tertentu. Dalam kerangka lain sistem info dapat memberikan dukungan dalam sebuah ambil keputusan. Sistem info dapat disimpulkan satu kombinasi yang teratur perseorangan, piranti keras, perangkat lunak, jaringan computer dan komunikasi data dan pangkalan data dalam kumpulkan, menebarkan, dan mengubah info pada suatu wujud organisasi[14]. Sistem info ialah sebuah elemen yang sama-sama terkait dengan kumpulkan, merekayasa, simpan dan menebarkan info dan memberi saran untuk penuhi arah[15].

2.2.4 *Website*

Web atau *website* adalah himpunan halaman situs yang sama-sama tersambung dan file-filenya sama-sama berkaitan satu dengan lain. *Website* terbagi

dalam *page*, dan kelompok halaman yang dimaksud *homepage*. *Homepage* ada pada posisi paling atas, dengan halaman-halaman berkaitan yang ada di bawahnya. Umumnya tiap halaman di bawah *homepage* dimaksud *child page*, yang berisi *hyperlink* ke halaman lain dalam web[16].

Web merupakan satu kelompok halaman *website* dan dokumen yang menebar ke sejumlah komputer server yang berada di penjuru dunia dan tekoneksi lewat jaringan internet. Web ialah sebuah bagian yang terbagi dalam tulisan, gambar, suara, dan animasi hingga jadi media info yang menarik dikunjungi oleh orang lain. Web atau disingkat situs, bisa didefinisikan satu kelompok halaman *website* yang terdiri di atas beberapa situs yang berisi info berbentuk data digital, audio, dan animasi yang lain yang disajikan lewat jaringan internet[17].

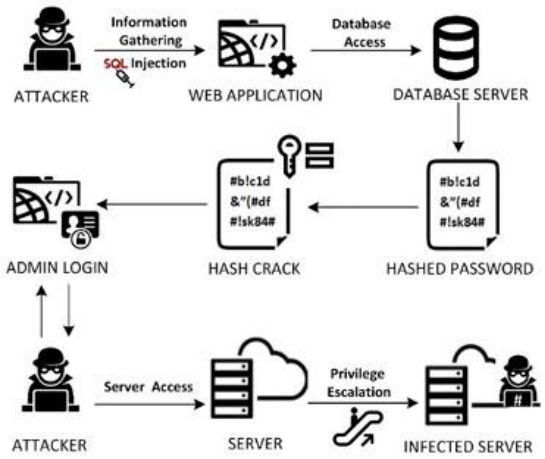
2.2.5 *Open Web Application Security Project* (OWASP)

Menurut website resminya *Open Web Application Security Project* (OWASP), mendeskripsikan "komunitas terbuka yang diperuntukkan untuk memungkinkannya organisasi meningkatkan, beli, dan memelihara program yang bisa dipercayai ".Untuk pedoman pengetesan *Open Web Application Security Project* (OWASP) versi terkini memakai versi 4.0. Di tahun 2004 persisnya di bulan Desember pedoman pengetesan *Open Web Application Security Project* (OWASP) di terbitkan, dengan versi pertama kalinya yakni versi 1.0. Versi 2.0 pedoman pengetesan *Open Web Application Security Project* (OWASP) di-launching persisnya di tanggal 25 Desember 2006. Pedoman pengetesan *Open Web Application Security Project* (OWASP) versi 3.0 di*launching* dengan selang waktu dua tahun persisnya di tanggal 15 September 2008. Seterusnya di tahun 2014 pedoman pengetesan *Open Web Application Security Project* (OWASP) kembali melaunching versi 4.0. Komunitas *Open Web Application Security Project* (OWASP) untuk pertamanya kali mengeluarkan 10 daftar resiko keamanan program web yang paling rawan di tahun 2003.

Daftar 10 resiko keamanan itu diberi nama *Open Web Application Security Project* (OWASP) TOP 10. Komunitas *Open Web Application Security Project* (OWASP) melaunching *Open Web Application Security Project* (OWASP) *TOP* 10 - 2004 untuk keduanya di tahun 2004. Dengan seiringnya perubahan tehnologi dan bertambahnya kejahatan siber, Komunitas OWASP melaunching kembali *Open Web Application Security Project* (OWASP) TOP 10 di tahun 2007, 2010, 2013, 2017 dan yang paling akhir di tahun 2021. *Open Web Application Security Project* (OWASP)

TOP 10 selainnya berisi daftar risiko keamanan program web yang paling riskan, *Open Web Application Security Project* (OWASP) TOP 10 berisi mengenai keterangan sekitar daftar risiko, langkah mencegah sela keamanan, dan contoh skenario dari serangan[18].

2.2.6 SQL *Injection*



Gambar 2.1 Skema SQL *Injection*[19]

SQL *Injection* sebagai salah satunya teknik *hacking* yang dipakai untuk masuk atau menyelusup di dalam sistem *database* web, yang bertujuan untuk mengetahui isi database dan beberapa informasi yang ada di *website* itu. Teknik itu bisa dilakukan karena ada sintaks program yang kurang kuat dan tidak ada proteksi keamanan sistem web dari pengurus web atau *administrator*. SQL *Injection* ialah sebuah teknik hacking yang memerlukan port 80 dan selalu dilakukan *hacker* pada server. Sintaks SQL bisa dilakukan injeksi pada perintah SQL sebagai input lewat halaman *website*[19].

2.2.7 *Kali Linux*

Kali linux adalah sebuah sistem operasi berbasis linux dengan memiliki berbagai tools untuk melakukan penetration, hacking, dan juga forensic. Kali linux dirilis pada tanggal 13 Maret 2013 yang dulunya sempat bernama BackTrack linux. Sistem operasi tersebut dapat didownload secara gratis di website resmi pada url (‘https://www.kali.org/get-kali/’). Banyak software open source yang diberikan oleh pihak developer kali linux seperti Maltego, Nmap yang digunakan untuk information gathering, dan SQL Map yang digunakan untuk web application analysis [20].