BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada penelitian sebelumnya yang sudah banyak dilakukan sebelumnya menunjukan bahwa melakukan serangan terhadapat *website* sangat dibutuhkan agar dapat mengetahui kelemahan ataupun celah suatu *website*, yang dimana dapat berguna untuk antisipasi kedepannya terhadap serangan yang sama.

Penelitian sebelumnya yang dilakukan oleh Yosua Ade Pohan, Yuhandri Yunus dan Sumijan pada tahun 2021 dalam sebuah jurnal yang berjudul Meningkatkan Keamanan *Webserver* Aplikasi Pelaporan Pajak Daerah Menggunakan Metode *Penetration Testing Execution Standard*. Dalam penelitian ini metode yang digunakan metode *penetration testing execution standard* untuk menganalisa sistem keamanan, hasil dari pengujian menggunakan *software* nikto, acunetix, burpsuite dan *Open Web Application Security Project* terdapat tujuh jenis kerentanan dua diantarannya adalah: *CSRF Attack, X-Frame Header Options is Missing*. Level kerentanan aplikasi atau *website* pada kategori medium[6].

Penelitian selanjutnya berjudul Analisis *Security Assessment* Menggunakan Metode *Penetration Testing* Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara, yang dilakukan oleh Bita Parga Zen, Rudy A.G Gultom dan Agus H.S Reksoprodjo, pada tahun 2020. Penelitian ini bertujuan untuk meningkatkan keamanan sistem komputer dari pencurian data ilegal dengan pelanggaran keamanan pada jaringan komputer, dalam pengujian peningkatan keamanan sistem pertahanan *firewall*. *Router* dan *server*. Pada tahapan *security assessment* menggunakan tahapan *vulnerability* standar OWASP dan CVSS. Hasil dari penelitian ini teredapat beberapa celah yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab[7].

Pada penelitian lain yang berjudul Analisis Perbandingan Metode *Website Security* PTES, ISSAF dan OWASP Di Dinas Komunikasi dan Informasi Kota Bandung. Yang dilakukan oleh Tio Revolino Syarif dan Didit Andri Jatmiko. Pada

tahun 2019 dalam penelitian kali ini akan membandingkan *framework* PTES, ISSAF dan OWASP. Hasil pengujian pada *framework* PTES mendapat sko resiko untuk *website* diskominfo saat ini yaitu 6, dikarenakan ada kelemahan pada kontrol keamanan yang dapat menimbulkan kerugian finansial yang terbatas. Pada hasil pengujian *framework* ISSAF adanya beberapa kerentanan diantaranya *Application Error Message, Error Message On Page, Vulnerable Javascript Library (CWE-16).* Yang terakhir hasil dari pengujian *framework* OWASP yang diketahui *website* diskominfo bandung memiliki risk ratting medium. Dengan kesimpulan bahwa *website* diskominfo bandung dapat menggunakan *framework* yang cocok yaitu PTES dan OWSP yang dapat dimengerti oleh user awam ataupun user berpengalaman[8].

Penelitian selanjutnya dari Albestty Islayati Rafeli, Henki Bayu Seta, dan I Wayan Widi. Yang berjudul Pengujian Celah Keamanan Menggunakan Metode OWASP *Web Security Testing Guide* (WSTG) Pada *Website* XYZ pada tahun 2022. Penelitian ini melakukan tujuh teknik pengujian *Information gathering, Business Logic Testing dan Client Side Testing, Configuration and Deployment Management Testing, Identity Management Testing, Input Validation Testing, Client Side Testing* dan *Testing For Error Handling.* Dalam melakukan pengujian ditemukan delapan *vulnerability* dengan kategori medium pada *website* XYZ[9].

Penelitian selanjutnya yang berjudul Analisis Keamanan *Website E-Learning* SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. Pada tahun 2020 oleh Setyo Utoro, Bayu Andi Nugroho, dkk. Dalam penelitian ini menggunakan metode PTES yang dimana terdapat tujuh tahapan ialah *preengagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post exploitation, dan reporting*. Dalam melakukan pengujian menggunakan tools diantaranya OWASPZAP, Wireshark, NMAP, Whois, dengan hasil pengujian ditemukannya celah keamanan pada *Web Server Transmits Cleartext Credentials, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)*[10].

Penelitian selanjutnya berjudul Analisis Metode Web *Security* PTES *(Penetration Testing Execution Standart)* Pada Aplikasi *E-Learning* Universitas Negeri Padang. Oleh Fadilla Yulia Fauzan dan Syukhri pada tahun 2021. Tujuan dari penelitian ini menguji keamanan e-learning universitas negeri padang menggunakan metode PTES, pengujian dilakukan menggunakan tools Zenmap yang terdapat celah enam port terbuka, Acunetix terdapat lima kerentanan teratas tiga diantaranya *Cross-site Request Forgery, Weak Password, TLS 1.0 Enable* dan SQLMap dengan teknik SQL *Injection* tidak berhasil dilakukan karena website e-learning universitas negeri padang sudah menggunakan keamanan SSL/HTTPS. Dengan kesimpulan pada tahap scanning terdapat 96 celah kerentanan dan pada tahap exploitasi dinyatakan gagal[11].

Tabel 2. 1 Menunjukkan penelitian terkait metode PTES

Penelitian	Metode	Hasil
Yosua Ade Pohan, Yuhandri Yunus dan Sumijan. Yang berjudul Meningkatkan Keamanan *Webserver* Aplikasi Pelaporan Pajak Daerah Menggunakan Metode *Penetration Testing Execution Standard*.	*Penetration Testing Execution Standard* (PTES)	Hasil dari pengujian menggunakan *software* nikto, acunetix, burpsuite dan *Open Web Application Security Project* terdapat tujuh jenis kerentanan dua diantarannya adalah: *CSRF Attack, X-Frame Header Options is Missing.* Level kerentanan aplikasi atau *website* pada kategori medium
Bita Parga Zen, Rudy A.G Gultom dan Agus H.S Reksoprodjo. Berjudul Analisis *Security Assessment* Menggunakan Metode *Penetration Testing* Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara	*Penetration Testing*	Hasil dari penelitian ini teredapat beberapa celah yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab

Tio Revolino Syarif dan Didit Andri Jatmiko. Analisis Perbandingan Metode *Website Security* PTES, ISSAF dan OWASP Di Dinas Komunikasi dan Informasi Kota Bandung	Penetration Testing Execution Standard (PTES)	Hasil pengujian *framework* ISSAF adanya beberapa kerentanan diantaranya *Application Error Message, Error Message On Page, Vulnerable Javascript Library (CWE-16)*. Yang terakhir hasil dari pengujian *framework* OWASP yang diketahui *website* diskominfo bandung memiliki risk ratting medium
Albestty Islayati Rafeli, Henki Bayu Seta, dan I Wayan Widi. Pengujian Celah Keamanan Menggunakan Metode PTES dan *Web Security Testing Guide* (WSTG) Pada *Website* XYZ.	PTES dan *Web Security Testing Guide* (WSTG)	Dalam melakukan pengujian ditemukan delapan *vulnerability* dengan kategori medium pada *website* XYZ
Setyo Utoro, Bayu Andi Nugroho, dkk. Analisis Keamanan *Website E-Learning* SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard.	Penetration Testing Execution Standard.	Dalam melakukan pengujian menggunakan tools diantaranya OWASPZAP, Wireshark, NMAP, Whois, dengan hasil pengujian ditemukannya celah keamanan pada *Web Server Transmits Cleartext Credentials, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)*
Fadilla Yulia Fauzan dan Syukhri. Analisis Metode Web *Security* PTES *(Penetration Testing Execution Standart)* Pada Aplikasi *E-Learning* Universitas Negeri Padang.	Metode Web *Security* PTES *(Penetration Testing Execution Standart)*	Dengan kesimpulan pada tahap scanning terdapat 96 celah kerentanan dan pada tahap exploitasi dinyatakan gagal

2.2 Dasar Teori

2.2.1 Analisis

Analisa merupakan suatu cara membagi suatu objek menjadi bagian-bagian, yaitu membebaskan, menguraikan, menguraikan suatu yang terkait pada, cocok dengan sifat komponen analisa dipecah menjadi analisa bagian, analisa fungsional, analisa proses. Salah satu cara analisa yang dijadikan acuan periset ialah“Domain data suatu permasalahan wajib dimengerti serta proses analisa wajib bergerak dari data dasar ke detail implementasi[12].

2.2.2 Website

Website atau situs *website* adalah sebagai kumpulan halaman yang digunakan untuk menampilkan informasi gambar bergerak atau diam, teks, suara, animasi, dan gabungan dari semuanya, baik yang bersifat statis ataupun dinamis yang saling terkait yang masing-masing dihubungkan dengan jaringan-jaringan halaman[13]. *Hyperlink* merupakan hubungan anatar satu halaman *website* dengan halaman *website* lainnya. Sedangakan teks yang dijadikan media penghubung disebut *hypertext*[2].

2.2.3 Kali Linux

Kali linux merupakan sebuah ditribusi linux berbasis debian yang ditunjukan untuk pengujian penetrasi dan keamanan tingkat lanjut. Kali linux juga memiliki banyak tools yang ditujukan untuk berbagai tugas tentang keamanan informasi. Kali linux dikenal sebagai backtrack linux karena terdapat penggabungan antar tiga distro linux[12].

2.2.4 Serangan jaringan

Serangan terhadap jaringan terbagi dua yaitu serangan fisik dan serangan logic. Serangan fisik yaitu serangan yang terjadi pada serangan hardware-nya dimana menyebabkan kerusakan atau gangguan pada kabel, harddisk dan konsleting. Serangan logic yaitu serangan yang terjadi pada perangkat lunak jaringannya. Jenis serangan ini paling rawan terjadi[14].

1. Google *Dork*

   Dork atau *dork query*, adalah *string* pencarian yang menggunakan operator penelusuran lanjutan untuk menemukan informasi yang tidak tersedia pada sebuah situs *website*. Google dorking dapat menyediakan informasi yang sulit ditemukan melalui pencarian sederhana[15].

2. *Cross Site Scripting* (XSS)

   Cross Site Scripting (XSS) merupakan salah satu kejahatan terhadapat keamanan aplikasi melalui masukan pada peramban. Penyerangan dilakukan dengan cara mengelabui target dan mengarahkannya untuk masuk menuju halaman tertentu yang sudah disediakan dan diberikan code tertentu oleh penyerang[16].

2.2.5 Laravel

Laravel adalah salah satu *framework website open source* yang digunakan untuk membangun aplikasi web dengan menggunakan bahasa pemrograman PHP. Laravel dirilis pada tahun 2011 oleh Taylor Otwell dan sejak saat itu telah menjadi salah satu *framework website* PHP yang paling populer.

Laravel menggunakan pola arsitektur *Model-View-Controller* (MVC) dan menyediakan banyak fitur bawaan seperti sistem autentikasi, sistem routing, migrasi *database*, dan banyak lagi. Selain itu, Laravel juga memiliki sistem templating yang sangat kuat, yang memungkinkan para pengembang web untuk membuat tampilan *website* yang dinamis dan menarik.

Laravel sangat populer di kalangan pengembang *website* karena mudah dipelajari, memiliki dokumentasi yang sangat baik, dan tersedia banyak paket pihak ketiga yang dapat mempercepat proses pengembangan. Laravel juga sangat fleksibel dan dapat diadaptasi untuk berbagai jenis proyek *website*, mulai dari proyek kecil hingga proyek yang sangat kompleks[5].

2.2.6 Framework Codeigniter

Merupakan aplikasi sumber terbuka yang berupa kerangka kerja PHP dengan model MVC (Model, View, Controller) untuk membangun situs web dinamis dengan menggunakan PHP. *Framework codeigniter* adalah sebuah framework PHP yang dapat membantu mempercepat developer dalam pengembangan aplikasi web berbasis PHP[17].

2.2.7 Status Code

Status code adalah informasi yang dikirimkan oleh server *website* ke browser atau klien ketika browser atau klien melakukan permintaan terhadap suatu sumber daya di *website*. Status code ini memberikan informasi tentang apakah permintaan tersebut berhasil dilakukan atau tidak, dan memberikan detail tentang apa yang terjadi jika terdapat masalah. Berikut adalah beberapa status code umum dalam *networking*:

1. 1xx *(Informational)*: Status code ini memberikan informasi bahwa permintaan diterima dan sedang diproses. Contohnya adalah 100 *Continue*, yang memberitahu bahwa server menerima permintaan dan klien seharusnya melanjutkan mengirimkan permintaannya.
2. 2xx *(Successful)*: Status code ini memberikan informasi bahwa permintaan telah berhasil dilakukan. Contohnya adalah 200 OK, yang memberitahu bahwa permintaan berhasil dilakukan dan server mengirimkan sumber daya yang diminta.
3. 3xx *(Redirection)*: Status code ini memberikan informasi bahwa permintaan memerlukan aksi tambahan untuk menyelesaikan permintaan. Contohnya adalah 301 *Moved Permanently*, yang memberitahu bahwa sumber daya yang diminta sudah dipindahkan ke URL baru.
4. 4xx *(Client Error)*: Status code ini memberikan informasi bahwa permintaan yang dikirimkan oleh klien tidak dapat diproses oleh server. Contohnya adalah 404 *Not Found*, yang memberitahu bahwa sumber daya yang diminta tidak ditemukan di server.

5. 5xx *(Server Error)*: Status code ini memberikan informasi bahwa server mengalami kesalahan saat memproses permintaan. Contohnya adalah 500 Internal *Server Error*, yang memberitahu bahwa terdapat masalah internal pada server saat memproses permintaan.

2.2.8 Burpsuite

Burp Suite merupakan aplikasi testing celah keamanan yang dikembangkan oleh Portswigger. Burp Suite sering digunakan oleh auditor keamanan, peneliti, dan penguji untuk analisis dari sistem yang berbeda. Fungsionalitas inti Burp adalah untuk mencegat dan menampilkan HTTP request secara terstruktur. BurpSuite merupakan aplikasi open source[18].

2.2.9 NMAP

Nmap *(Network Mapper)* merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Nmap dirancang untuk memeriksa jaringan besar secara cepat, Nmap dapat bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan[19].

2.2.10 WPScan

WPScan adalah salah satu tool open source yang digunakan untuk melakukan pemindaian keamanan pada WordPress. WPScan dapat digunakan untuk mengidentifikasi kerentanan pada instalasi WordPress dan plugin yang digunakan, mencari celah keamanan yang dapat dimanfaatkan oleh penyerang, serta memindai password yang lemah atau mudah ditebak.

WPScan dapat melakukan pemindaian secara otomatis atau manual pada situs web WordPress. Selain itu, WPScan juga dapat melakukan brute force password, mencari plugin yang rentan, mencari tema yang rentan, dan melakukan pemindaian terhadap username dan email pengguna. WPScan juga menyediakan fitur untuk melakukan pencarian secara spesifik pada basis data WPVulnDB yang berisi informasi tentang kerentanan keamanan pada WordPress.

WPScan juga dapat digunakan dengan command line interface (CLI) dan dapat diintegrasikan dengan tool keamanan lainnya seperti Nmap, Metasploit, dan lain-lain. WPScan dapat membantu para pengembang dan administrator WordPress untuk menemukan dan memperbaiki kerentanan pada situs web mereka, sehingga meningkatkan keamanan situs web dan melindungi pengguna dari serangan oleh penyerang yang tidak bertanggung jawab.

2.2.11 Wappalyzer

Wappalyzer adalah sebuah *extension* atau *add-on browser* yang digunakan untuk menganalisis teknologi yang digunakan pada suatu situs web. Wappalyzer memungkinkan pengguna untuk mengetahui teknologi apa yang digunakan pada suatu situs web, seperti bahasa pemrograman, framework, server web, CMS, dan lain-lain. Wappalyzer dapat digunakan pada berbagai browser seperti Chrome, Firefox, Opera, dan Edge. Setelah diinstal pada browser.

Wappalyzer akan menampilkan ikon pada browser yang dapat di klik untuk mengungkap teknologi yang digunakan pada suatu situs web. Informasi teknologi yang ditampilkan dapat meliputi bahasa pemrograman, server web, CMS, framework, analitik web, dan lain-lain. Selain itu, Wappalyzer juga memiliki fitur untuk memindai situs web secara otomatis dan menampilkan teknologi yang digunakan. Pengguna juga dapat mengintegrasikan Wappalyzer dengan tool security lainnya seperti Burp Suite, Metasploit, dan lain-lain.

Wappalyzer dapat membantu pengembang web, administrator jaringan, dan peneliti keamanan untuk mengidentifikasi teknologi yang digunakan pada situs web. Informasi ini dapat membantu pengguna untuk menilai keamanan suatu situs web dan mengidentifikasi kerentanan yang mungkin ada pada teknologi yang digunakan. Selain itu, Wappalyzer juga dapat membantu pengguna untuk memilih teknologi yang tepat untuk situs web yang mereka kembangkan atau kelola[18].

2.2.12 Dirbuster

Dirb merupakan alat pemindai konten web. Dirb akan mencari objek web yang ada dan tersembunyi dengan meluncurkan serangan bruteforce berbasis wordlists terhadap server web dan menganalisis responsnya[20].

2.2.13 *Penetration testing execution standard* (PTES)

Penetration Testing Execution Standard (PTES) ialah satu diantara *framework penetration testing* yang dibangun pada tahun 2010, dengan memberikan contoh yang terstruktur dan mendetail yang mampu memberikan acuan bagi penggunanya dalam melakukan pengujian yang berkualitas[21]. *Penetraion testing* adalah sebuah cara untuk melakukan evaluasi keamanan pada sistem komputer atau jaringan. Evaluasi dilakukan dengan melakukan metode simulasi penyerangan[10]. PTES memiliki tujuh tahapan utama yaitu:

1. *Pre-engagement Interactions*

   Tahap pertama PTES melibatkan berbagai persiapan sebelum melakukan pengujian penetrasi. Langkah ini termasuk pengumpulan informasi tentang sistem target, seperti infrastruktur jaringan dan aplikasi yang digunakan. Selain itu, PTES juga melibatkan interaksi dengan klien untuk memastikan bahwa semua aspek pengujian penetrasi sudah dipahami.
2. *Intelligence Gathering*

   Tahap kedua PTES melibatkan pengumpulan informasi tambahan tentang sistem target, seperti alamat IP dan konfigurasi jaringan. Langkah ini melibatkan penggunaan berbagai teknik pengumpulan informasi, seperti pencarian publik, pemindaian *por*t, dan pengumpulan informasi dari situs *website*.
3. *Threat Modeling*

   Tahap ketiga PTES melibatkan penilaian risiko dan ancaman terhadap sistem target. Langkah ini melibatkan pengembangan profil penyerang dan mengidentifikasi titik lemah potensial dalam sistem.

4. *Vulnerability Analysis*

   Pada tahap ini, peneliti melakukan analisis kerentanan dengan memanfaatkan hasil dari tahap *intelligence gathering* dan threat modeling untuk menentukan kerentanan yang ada pada target.

5. *Exploitation*

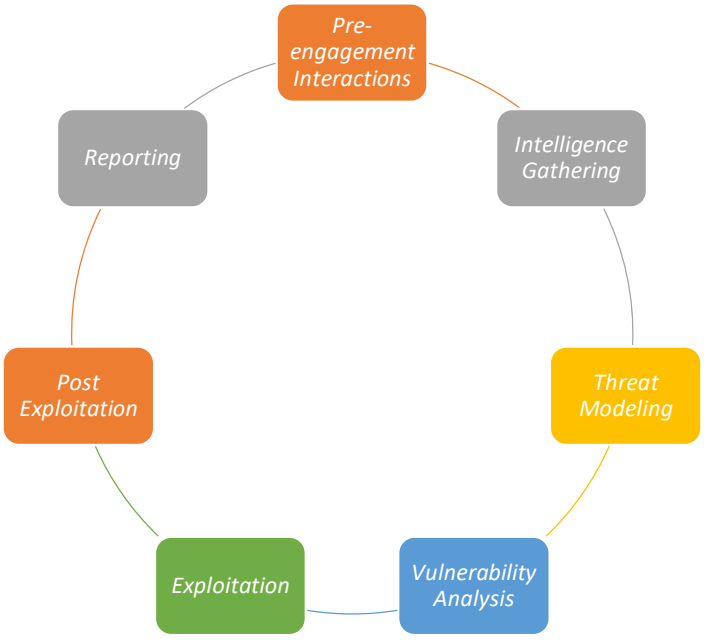
   Tahap ini melibatkan pemanfaatan kerentanan yang ditemukan pada target untuk mendapatkan akses dan memanipulasi sistem atau aplikasi.

6. *Post Exploitation*

   Tahap ini melibatkan pemanfaatan akses yang diperoleh dari tahap exploitation untuk mendapatkan informasi atau data yang diinginkan.

7. *Reporting*

   Pada tahap ini, peneliti melakukan penyusunan laporan hasil pengujian, termasuk kerentanan yang ditemukan, metodologi yang digunakan, serta rekomendasi untuk memperbaiki kerentanan yang ada[13].



Gambar 2. 1 Tahapan Penetration Testing Execution Standard (PTES)[11].