BAB 2

TINJAUAN PUSTAKA

Pada bab ini menjelaskan penelitian sebelumnya yang terkait dengan penelitian selanjutnya dan juga teori dasar yang digunakan sebagai pendukung penelitian.

2.1 Penelitian Terkait

Adapun penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada skripsi ini yaitu:

Table 2 . 1 Penelitian Terkait

Penelitian 1	
Penulis dan Tahun	(Sanjaya *et al.,* 2020)
Judul	Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration Testing* Menggunakan Framework ISSAF
Metode	*Information System Security Assessment Framework* (ISSAF)
Hasil	Pada penelitian ini menggunakan *Framework* ISSAF, didapatkan hasil bahwa terdapat celah keamanan yang berbahaya seperti *SQL Injection* dan XSS pada *website X Institute*. Celah lainnya adalah *port* TCP terbuka sehingga ada resiko serangan dari pihak luar, serta bug pada sistem yang bisa dijadikan celah keamanan.
Peneilitian 2	
Penulis dan Tahun	(Hidayat *et al.,* 2018)
Judul	Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Gratis Terhadap Serangan *Packet Sniffing*
Metode	*Information System Security Assessment Framework* (ISSAF)
Hasil	Pada penelitian ini dengan menggunakan metode ISSAF dengan target yang diuji adalah wifi di Universitas Siliwangi diperoleh hasil bahwa Universitas Siliwangi secara keseluruhan memiliki jaringan wifi dan keamanan sistem pengguna komputer yang sangat rentan dengan tingkat kerawanan yang tinggi, kesadaran pengguna komputer terhadap keamanan sistem masih rendah, dan gratis. Pengguna wifi tidak memahami banyaknya serangan hacker pada jaringan yang lemah.
Penelitian 3	
Penulis dan Tahun	(Wardhana & Seta, 2021)
Judul	Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada *Website* Universitas XYZ
Metode	*Information System Security Assessment Framework* (ISSAF)

Hasil	Hasil dari penelitian ini adalah *website* pada Universitas XYZ tidak aman dari serangan seperti *Brute-force Attack, Cross-Site Request Forgery (CSRF) Attack, Session Hijacking melalui Cookie*, maupun *IDOR (Insecure Direct Object Reference).*
Penelitian 4	
Penulis dan Tahun	(Hermanto & Haeruddin, 2022)
Judul	Peningkatan Sistem Keamanan *Website* Menggunakan Metode OWASP
Metode	*Open Web Application Security Project* (OWASP)
Hasil	Hasil dari penelitian ini adalah *website* UIB memiliki tingkat resiko yang rendah, namun tetap harus melakukan perbaikan terhadap ancaman yang muncul untuk mencegah serangan yang lebih merugikan *website*.
Penelitian 5	
Penulis dan Tahun	(Hendita *et al.*, 2022)
Judul	Implementasi Owasp *Zap* Untuk Pengujian Keamanan Sistem Informasi Akademik
Metode	*Open Web Application Security Project* (OWASP)
Hasil	Penelitian ini menemukan bahwa *website* Sistem Informasi Akademik Universitas Pancasila memiliki 19 kerentanan setelah dilakukan penetration test. Kualitas *website* berada pada level sedang, sehingga perlu perbaikan lebih lanjut oleh pengembang sistem.
Penelitian 6	
Penulis dan Tahun	(Ghozali et al., 2018)
Judul	Mendeteksi Kerentanan Keamanan Aplikasi *Website* Menggunakan Metode OWASP *(Open Web Application Security Project)* untuk Penilaian *Risk Rating*
Metode	*Open Web Application Security Project* (OWASP)
Hasil	Hasil dari penelitian ini Terdapat 7 risiko dengan 3 risiko memiliki *risk severity high*, 2 risiko memiliki *risk severity medium*, 2 risiko memiliki *risk severity low* pada domain http://202.91.11.42/CI dan Terdapat 8 risiko dengan 3 risiko memiliki *risk severity high*, 2 risiko memiliki *risk severity medium,* 3 risiko memiliki *risk severity low* pada domain http://202.91.11.42/ .
Penelitian 7	
Penulis dan Tahun	(Hidayatulloh & Saptadiaji, 2021)
Judul	Penetration Testing pada *Website* Universitas ARS Menggunakan *Open Web Application Security Project* (OWASP)
Metode	*Open Web Application Security Project* (OWASP)
Hasil	Hasil penelitian menunjukkan bahwa keamanan *website* Universitas ARS sudah baik karena aspek keamanan informasi CIA TRIAD (confidentiality, integrity, availability) terpenuhi. Namun, terdapat kekurangan pada aspek keamanan integration karena Header X-Frame-Options tidak diatur pada kelima subdomain, yang

	dapat menyebabkan informasi menjadi rentan saat dimuat di *website* lain.

Berdasarkan dari hasil penelitian terkait yang dilakukan pengujian dengan metode Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) diperoleh bahwa, kerentanan pada sistem informasi *website* atau aplikasi masih memiliki sistem keamanan yang lemah. Penelitian terkait penggunaan metode ISSAF dan OWASP telah dilakukan dalam pengujian keamanan sistem.

Pada penelitian selanjutnya, akan dilakukan penetrasi testing dengan menggunakan metode penelitian yaitu metode OWASP *Top* 10 2017. Analisis keamanan dengan menggunakan metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada *website*.

2.2 Kajian Teori

2.2.1 Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang menggunakan protokol komunikasi sebagai media komunikasi untuk saling bertukar data, informasi, program aplikasi dan perangkat keras seperti printer, scanner, harddisk ataupun CD-*Drive* untuk saling berkomunikasi secara elekronik (Saputri, 2016). Potensi jaringan komputer antara lain:

1. Integrasi dan penggunaan peralatan yang beragam.
2. Komunikasi jaringan komputer memungkinkan komunikasi antar pengguna komputer.
3. Perlindungan data dan informasi menggunakan jaringan komputer untuk mendistribusikan proses dan aplikasi, mengurangi kemungkinan bottleneck atau tumpukan pekerjaan.
4. Jaringan komputer yang teratur mampu mengalirkan data dari komputer klien ke server dengan cepat untuk integrasi.

Berdasarkan letak geografis, Jaringan komputer terbagi menjadi tiga jenis:

1. *Local Area Network* (LAN)
2. *Metropolitan Area Network* (MAN)
3. *Wide Area Network* (WAN)

2.2.2 Keamanan Jaringan komputer

Keamanan jaringan adalah komputer yang terhubung ke internet, memiliki ancaman keamanan yang lebih besar daripada komputer yang tidak terhubung ke internet. dengan pengendalian yang hati-hati maka resiko ancaman keamanan jaringan dapat dikurangi, namun pada dasarnya keamanan jaringan bertentangan dengan akses jaringan, dimana jika akses jaringan semakin mudah diakses, maka akses keamanan jaringan semakin rentan terhadap ancaman *kejahatan Cyber Security,* begitu pula sebaliknya (Kholiq & Khoirunnisa, 2019).

2.2.3 *Website*

Menurut (Rumaf *et al*., 2022) *Website* adalah sebuah alamat (URL) yang berfungsi sebagai tempat menyimpan data dan informasi berdasarkan topik tertentu. Website dapat dikategorikan menjadi dua jenis, yaitu:

1. Web Statis

   Web yang berisi atau menampilkan informasi yang sifatnya statis (tetap).

2. Web dinamis

   Web yang menampilkan informasi dan juga dapat berinteraksi dengan user yang bersifat dinamis.

2.2.4 *Web Server*

*Web serve*r adalah perangkat lunak yang berfungsi sebagai penerima permintaan *(request)* berupa halaman *website* melalui HTTP atau HTTPs dari *client (browser)* dan pengembalian *(respons)* berupa halaman web yang biasanya berupa HTML. Web server juga memiliki fungsi tidak hanya mengolah data tetapi juga mengirimkan data berupa file, foto dan video berdasarkan permintaan dari client. Server web juga dapat dijalankan secara online (Fachri *et al.,* 2021).

2.2.5 *Mail Server*

Mail server adalah aplikasi untuk mengelola pengiriman pesan melalui *email*. *Server* ini menerima pesan dari *email client* yang digunakan oleh pengguna atau dari server email lainnya. Sebagai pusat kendali sistem email, mail server terdiri dari area penyimpanan, konfigurasi *user*, daftar *user,* dan modul komunikasi (Sumarto & Yuliani, 2017).

2.2.6 *SquirrelMail*

SquirrelMail adalah paket webmail standar yang ditulis dalam PHP4. Dalam pemrograman PHP-nya, Squ*irrelMail* mendukung protokol POP, IMAP, dan SMTP. Instalasi dan konfigurasi S*quirrelMa*il cukup sederhana. Tidak seperti aplikasi lainnya, *SquirrelMai*l interaktif dan dapat dikonfigurasi sesuai keinginan pengguna (Basorudin, 2018).

2.2.7 POP3

Post Office Protocol (POP3) adalah protokol untuk mengambil email dari server. SMTP, di sisi lain, digunakan untuk mengirim email dari komputer pengirim ke server (Sumarto & Yuliani, 2017).

2.2.8 IMAP

IMAP *(Internet Message Access Protocol)* dan POP *(Post Office Protocol)* adalah protokol email. Keduanya memungkinkan pengguna untuk mengakses email melalui *software* email *client* seperti *Microsoft Outlook* dan *Mozilla Thunderbird* (Basorudin, 2018).

2.2.9 SMTP

SMTP *(Simple Mail Transfer Protocol)* adalah protokol yang umum digunakan untuk pengiriman email di internet. Protokol ini digunakan untuk mengirim data dari komputer pengirim ke server email penerima. SMTP dirancang karena sistem email membutuhkan server email yang menyimpan sementara pesan hingga diambil oleh penerima yang sah (Sumarto & Yuliani, 2017).

2.2.10 DNS

DNS *(Domain Name System)* adalah sistem yang menyimpan informasi tentang nama *host* dan domain dalam basis data terdistribusi di jaringan komputer, termasuk Internet. DNS memberikan alamat IP untuk setiap nama host dan mencatat server transmisi surat *(mail exchange server)* yang terkait (Sumarto & Yuliani, 2017).

2.2.11 IP *Address*

Menurut (Mulyana, 2013) IP *Address* adalah alamat yang diberikan pada

jaringan komputer dan peralatan jaringan yang menggunakan protokol TCP/IP. *Transmission Control Protocol/Internet Protocol* (TCP/IP) adalah sekelompok protokol yang berfungsi untuk mengatur komunikasi data komputer di internet. Setiap komputer yang terhubung ke internet memiliki alamat IP dan setiap IP yang dimiliki oleh komputer/server/perangkat jaringan lain yang terhubung ke internet tidak boleh sama. Alamat IP versi 4 (IPv4) adalah serangkaian angka biner 32-bit yang digunakan untuk mengidentifikasi perangkat jaringan. Alamat IP adalah angka 32-bit yang dipisahkan oleh titik untuk setiap 8 bit. Dalam penggunaannya, alamat IP ditulis dalam empat angka desimal yang masing-masing angka dipisahkan oleh titik. Contoh alamat IP dapat dilihat pada tabel di bawah ini:

Table 2 . 2 Bilangan biner dan desimal

BILANGAN BINER	BILANGAN DESIMAL
11000000.10101000.00000000.00000001	192.168.0.1
11000000.10101000.00000001.01100101	192.168.1.101
11000000.10101000.00000001.01100110	192.168.1.102
11000000.10101000.00000001.01100111	192.168.1.103

Alamat IP adalah identitas jaringan *(network ID)* dan identitas komputer atau perangkat lain *(host ID)* yang terhubung ke jaringan komputer. Alamat IP digunakan untuk mengirim dan menerima paket data dari perangkat lain yang terhubung ke jaringan komputer.

2.2.12 *Virtualbox*

VirtualBox adalah perangkat lunak virtualisasi yang memungkinkan eksekusi sistem operasi tambahan di dalam sistem operasi utama. Misalnya, jika Anda memiliki *Windows* di komputer Anda, Anda dapat menjalankan sistem operasi lain di dalam *Windows* tersebut (Farida, 2019).

2.2.13 *Linux*

Linux adalah sistem operasi *open-source* berbasis GNU/Linux dengan berbagai varian seperti *Archlinux, Debian, Open Suse, Redhat, Slackware,* dll. Namun, dengan banyaknya varian, beberapa pengguna mungkin merasa aplikasi yang disediakan kurang sesuai dengan kebutuhan mereka. Hal ini menyebabkan banyak pengguna melakukan remastering, yaitu proses membuat sistem operasi baru

dengan mengurangi atau menambah fitur-fitur dari distro GNU/Linux yang sudah ada. Beberapa distro GNU/Linux hasil remaster dikhususkan untuk kebutuhan tertentu, seperti Kali Linux yang ditujukan untuk penetration testing (Edy Budi Harjono, 2016).

2.2.14 *Acunetix*

Acunetix adalah perangkat lunak *scanner* aplikasi web yang dapat mengidentifikasi kelemahan pada *website*. Kelebihannya adalah memberikan solusi untuk kelemahan yang ditemukan dan melacak setiap kerentanan. *Acunetix* juga menyediakan fungsi tambahan untuk pengujian lanjutan pada *website* yang diuji (Zirwan, 2022).

2.2.15 *Common Vulnerability Scoring System* (CVSS)

CVSS adalah kerangka terbuka untuk mengkomunikasikan karakteristik dan dampak kerentanan aplikasi. Terdiri dari tiga kelompok pengukuran yaitu *Base, Temporal, dan Environmental*. *Base* menggambarkan kualitas intrinsik kerentanan, Temporal mencerminkan perubahan karakteristik kerentanan seiring waktu, dan *Environmental* mencerminkan karakteristik kerentanan yang unik untuk lingkungan pengguna. Berikut adalah tabel dari peringkat kerentanan *score* (Walkowski *et al*., 2021).

Table 2 . 3 Skor kerentanan CVSS

No	*CVSS Score*	*Criticality*
1	0,0	*None*
2	0,1 – 3,9	*Low*
3	4,0 – 6,9	*Medium*
4	7,0 – 8,9	*High*
5	9,0 – 10,0	*Critical*

2.2.16 *Common Weakness Enumeration* (CWE)

CWE adalah proyek komunitas yang berisi katalog kelemahan dan kerentanan perangkat lunak. Tujuannya adalah memahami kelemahan perangkat lunak dan menciptakan alat otomatis untuk mengidentifikasi, memperbaiki, dan mencegah kerentanan. Proyek ini disponsori oleh Mitre (Wu *et al.*, 2016).

2.2.17 *Common Vulnerability and Exposures* (CVE)

CVE adalah kamus publik yang berisi identitas kerentanan keamanan informasi. Ini memfasilitasi berbagi data di database tentang keamanan informasi di jaringan yang berbeda dan menyediakan dasar untuk mengevaluasi alat keamanan organisasi. Identitas CVE memungkinkan penanganan yang lebih cepat dan mudah jika laporan alat evaluasi keamanan dilengkapi dengan identitas tersebut (Walkowski et al., 2021).

2.2.18 *Penetration Testing*

Penetrasi testing adalah kegiatan dimana seseorang mencoba mensimulasikan serangan yang dapat dilakukan terhadap jaringan organisasi/perusahaan tertentu untuk menemukan kelemahan pada sistem jaringan tersebut (Darmayuda, 2021).

Menurut (Johnson, 2020) Pengujian penetrasi adalah pengujian keamanan yang meniru serangan dunia nyata untuk mengidentifikasi metode menghindari fitur keamanan pada aplikasi, sistem, atau jaringan. Ini melibatkan serangan nyata pada sistem dan data yang menggunakan alat dan teknik yang umum digunakan oleh penyerang. Uji penetrasi mencari kombinasi kerentanan pada satu atau lebih sistem untuk mendapatkan lebih banyak akses daripada yang bisa didapat melalui satu kerentanan saja.

Pengujian penetrasi adalah pengujian keamanan yang meniru serangan penyerang untuk mengidentifikasi metode menghindari fitur keamanan pada aplikasi, sistem, atau jaringan. Uji penetrasi mencari kombinasi kerentanan pada satu atau lebih sistem untuk mendapatkan lebih banyak akses daripada yang bisa dicapai melalui satu kerentanan saja. Hal ini membantu menentukan:

1. Toleransi sistem terhadap pola serangan dunia nyata.
2. Tingkat kecanggihan yang dibutuhkan penyerang untuk berhasil mengkompromikan sistem.
3. Tindakan pencegahan tambahan yang dapat mengurangi ancaman terhadap sistem.

Kemampuan pembela untuk mendeteksi serangan dan merespons dengan tepat.

2.2.19 *Open Web Application Security Project* (OWASP)

Open Web Application Security Project (OWASP) adalah framework open-source yang fokus pada perbaikan keamanan perangkat lunak aplikasi. OWASP berperan dalam menemukan celah keamanan pada aplikasi *website*. Berdasarkan standar yang dikeluarkan oleh OWASP, terdapat sebelas langkah untuk menilai dan menguji keamanan *website*, yaitu*: Cryptography, Data Validation, Configuration Management, Authentication, Authorization, Secure Transmission, Information Gathering, Error Handling* dan *Denial of Service* (Guntoro *et al.,* 2020).

2.2.20 OWASP *ZAP*

Zed Attack Proxy (*ZAP*) adalah aplikasi *scanner* kerentanan yang dikembangkan oleh organisasi OWASP. *Tools* ini merupakan proyek yang sangat aktif dan terus dikembangkan secara *open-source*, memungkinkan siapa saja untuk berkontribusi. *Zap* adalah tools server proxy ini digunakan untuk memanipulasi lalu lintas yang lewat, termasuk lalu lintas dengan protokol HTTPS. Selain itu, tools ini juga dapat beroperasi dalam mode daemon yang dikendalikan melalui REST API. *ZAP* telah menjadi bagian dari Radar *Teknologi ThoughtWorks* dan berasal dari cabang Paros, sebuah *proxy* pentesting lainnya. Meskipun terdapat sebagian besar peningkatan dan pengembangan baru, sekitar 20% kode sumber *ZAP* masih berasal dari Paros (Hendita et al., 2022).

2.2.21 OWASP *TOP* 10

OWASP *Top* 10 adalah daftar 10 celah keamanan teratas yang dirilis oleh komunitas OWASP, yang berpotensi mengancam keamanan sebuah *website*. Daftar ini terus berkembang mengikuti perkembangan teknologi *website*. Pertama kali dirilis pada tahun 2003, OWASP *Top* 10 telah mengalami pembaruan minor pada tahun 2004, 2007, 2010, dan 2017. Tujuan dari OWASP *Top* 10 adalah untuk meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi risiko celah keamanan yang sering dihadapi dalam banyak kasus. Dalam versi terbaru, OWASP *Top* 10 2017 menyajikan beberapa perubahan dalam struktur pengujian keamanan yang disarankan. (Dharmawan et al., 2022). Berikut adalah beberapa saran pengujian yang disajikan bisa dilihat pada gambar 2.1:

Gambar 2 . 1 OWASP *Top* 10 2017

Sumber : https://owasp.org/www-project-top-ten/2017/Top_10

1. *Injection:*

   Melakukan pengujian terhadap celah keamanan seperti SQL *Injection, NoSQL Injection,* OS *Injection, dan* LDAP *Injection* yang terjadi saat data yang tidak diverifikasi dikirim ke intepreter sebagai perintah atau *query.*

2. *Broken Authentication:*

   Melakukan pengujian terhadap fungsi otentikasi dan manajemen sesi yang sering kali tidak diimplementasikan dengan benar, memungkinkan penyerang untuk mengeksploitasi *password*, kunci, atau token sesi untuk masuk ke sistem dengan identitas pengguna yang ada.

3. *Sensitive Data Exposure:*

   Melakukan pengujian terhadap perlindungan data sensitif pengguna seperti data keuangan, kesehatan, dan identitas pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

4. *XML External Entities:*

   Melakukan pengujian terhadap *website* yang masih menggunakan XML untuk menangani dokumen, karena dapat memungkinkan penyerang mendapatkan

informasi tentang *server website*, file internal, mengeksekusi perintah pada server, atau menyebabkan serangan *denial of service.*

5. *Broken Access Control:*

   Melakukan pengujian terhadap pengaturan akses yang tidak tepat, yang memungkinkan penyerang untuk mengubah hak akses mereka dan mengakses informasi sensitif atau melakukan tindakan yang seharusnya tidak diizinkan.

6. *Security Misconfiguration:*

   Melakukan pengujian terhadap kesalahan dalam konfigurasi sistem seperti pesan *error* yang terlihat, pengaturan HTTP *header* yang tidak terenkripsi, atau pengaturan default yang tidak aman.

7. *Cross-Site Scripting (XSS):*

   Melakukan pengujian terhadap celah keamanan yang memungkinkan penyerang untuk menyisipkan *skrip JavaScript* dalam input pengguna, yang dapat menyebabkan *deface* pada *website* atau mengarahkan pengguna ke *website* berbahaya.

8. *Insecure Deserialization:*

   Melakukan pengujian terhadap celah keamanan yang terjadi ketika aplikasi membaca string tanpa melakukan filter, yang dapat mengakibatkan eksekusi perintah yang tidak diinginkan dan serangan *privilege escalation atau injection.*

9. *Using Components with Known Vulnerabilities:*

   Melakukan pengujian terhadap penggunaan komponen dalam aplikasi (seperti framework*, library,* dan modul) yang diketahui memiliki celah keamanan, karena penyerang dapat mengeksploitasi celah tersebut untuk menyerang sistem.

10. *Insufficient Logging and Monitoring:*

    Melakukan pengujian terhadap sistem *logging* dan *monitoring* yang tidak memadai, yang dapat menyebabkan kesulitan dalam menganalisis serangan yang terjadi pada aplikasi.