BAB II
TINJAUAN PUSTAKA

A. PENELITIAN TERDAHULU

Peneltian terdahulu dari (Ashar, 2022) yang berjudul Analisis Keamanan *Open Website* Menggunakan Metode OWASP dan ISSAF. Diskominfo Kerinci merupakan sebuah instansi yang bertanggung jawab atas pengelolaan media informasi di lingkup Pemerintahan Kabupaten Kerinci. Keberadaan website sebagai media informasi menjadi kebutuhan yang sangat penting untuk menyampaikan informasi kepada masyarakat. Website yang dikelola ini bersifat publik (*open website*) sehingga prinsip keamanan informasi harus diterapkan agar tidak mendapat serangan *cyber*. Penelitian ini melakukan analisis keamanan pada open website milik Diskominfo Kerinci dengan menggunakan dua metode yaitu metode *Open Web Application Security Project* (OWASP) dan metode *Information Systems Security Assessment Framework* (ISSAF). Penelitian terkait penggunaan metode OWASP dan ISSAF dalam pengujian keamanan sistem telah banyak dilakukan, beberapa pengujian menyebutkan bahwa metode ini sangat berpengaruh terhadap langkah dan hasil dari pengujian keamanan system. Hasil analisis keamanan dari dua metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada website.

Peneltian terdahulu dari (Mu'min et al., 2022) yang berjudul Analisis Keamanan Sistem Informasi Akademik Menggunakan *Open Web Application Security Project Framework*. Keamanan sistem informasi merupakan salah satu hal penting dalam perkembangan teknologi untuk melindungi data atau informasi yang komprehensif dan terstruktur. Sistem Informasi Akademik (SIA) memiliki layanan untuk menerima permintaan berupa halaman website protokol HTTP atau HTTPS dari klien yang disebut browser. Penyusup dapat meretas website tanpa sepengetahuan pemilik. Penelitian ini dilakukan untuk menemukan kerentanan SIA STIKES Guna Bangsa Yogyakarta. *Framework* yang digunakan adalah *Open Web*

Application Security Project (OWASP) yang biaa digunakan untuk mengevaluasi sistem atau aplikasi. *Tools* yang digunakan adalah *WhoIs, SSL Scan*, *Nmap,* dan *OWASP Zap*. Hasil yang didapatkan yaitu menemukan 12 kerentanan dengan empat kerentanan pada level medium yakni *Absence of Anti-CSRF Tokens*, *Cross-Domain Misconfiguration*, *Missing Anti-clickjacking Header*, dan *Vulnerable JS Library*, enam pada *level low* yakni *Cookie Without Secure Flag, Cookie without SameSite Attribute*, *Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*, Timestamp Disclosure – Unix, dan X-Content-Type-Options Header Missing, dan dua pada *level informational* yakni *Content-Type Header Missing* dan *Information Disclosure - Suspicious Comments.*

Peneltian terdahulu dari (Edy Listartha et al., 2022) yang berjudul Analisis Kerentanan Website Sma Negeri 2 Amlapura Menggunakan Metode Owasp (Open Web Application Security Project). Sekolah memiliki websiste sebagai media yang menampilkan informasi sekolah, dan media interaksi. Terjadinya transisi komunikasi secara tradisional ke dalam lingkup aplikasi berbasis website bisa saja dimanfaatkan oleh beberapa pelaku kejahatan dunia maya dengan tujuan mencuri informasi rahasia siswa-siswi dengan tujuan tertentu, maka mendeteksi kerentanan keamanan website adalah hal yang sangat penting untuk mengetahui tingkat resiko dengan menggunakan metode *Open Web Application Security Project* (OWASP) Risk Rating untuk mendeteksi kerentanan keamanan pada aplikasi berbasis website. Penelitian ini menghasilkan 2 faktor untuk memperkirakan *Likelihood* dan *Impact*, dari masing-masing faktor terdapat 3 resiko yang ditemukan yaitu *risk severity High, risk severity Medium* dan *risk severity Low*. Hasil penilaian resiko ini dapat membantu para pengelola dan pengembang sistem untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut.

Penelitia terdahulu dari (Riandhanu, 2022) yang berjudul Analisis Metode *Open Web Application Security Project* (OWASP) Menggunakan *Penetration Testing* pada Keamanan Website Absensi. Penggunaan teknologi dalam berbagai bidang meningkatkan mobilitas, salah satunya dengan pembuatan website untuk berbagi dan mengelola informasi. Keamanan sistem informasi yang tidak baik dapat mengganggu infrastruktur suatu organisasi atau perusahaan. Masalah kerentanan atau gangguan keamanan sistem banyak terjadi di internet. Masalah tersebut dapat berjenis serangan *Malware*, Eksploitasi dan Injeksi *database*. Masalah tersebut dapat diminimalisir dengan menerapkan pengamanan web dari gangguan atau serangan hacker dengan cara *penetration testing* (Pentest) yaitu pengujian yang dilakukan terhadap web secara legal dengan aktifitas menyerupai *hacker*. Untuk mendeteksi keamanan web dibutuhkan sebuah analisis terhadap kerentanan sebuah web yang sesuai dengan standarisasi kemanan *Open Web Application Security Project* (OWASP) dengan menggunakan *tools security*. Analisis kerentanan aplikasi berbasis web dengan metode OWASP dengan menggunakan *tools security* mampu mengetahui tingkat keamanan suatu aplikasi, berdasarkan hasil pengujian yang telah dilakukan dimana hasil dari penelitian memberikan beberapa saran atau rekomendasi tentang kerentanan situs web, yang dapat digunakan oleh tim developer situs web untuk meningkatkan keamanan situs web tersebut.

Peneltian terdahulu dari (Kuncoro et al., 2021) yang berjudul Analisis Metode *Open Web Application Security Project* (OWASP) pada Pengujian Keamanan Website: *Literature Review*. Keamanan sistem komputer semakin diperlukan dengan meningkatnya pengguna koneksi Internet. Dalam hal ini dapat memicu terjadinya tindak kejahatan pada sistem komputer. Diperlukan pengujian keamanan sistem untuk menemukan celah keamanan dalam mengantisipasi terjadinya tindak kejahatan pada sistem komputer. Makalah ini mengkaji literatur terkait dengan pengujian keamanan sistem komputer menggunakan metode *Open*

Web Application Security Project (OWASP). Metode *Scoping Review* digunakan dalam seleksi literatur dalam makalah ini, kemudian literatur dipetakan dalam beberapa elemen dan didapatkan 6 literatur yang sesuai. Tujuan dari makalah ini adalah menganalisis penggunaan *framework* OWASP dalam pengujian keamanan sistem komputer. Secara keseluruhan dalam implementasi *framework* telah memberikan hasil yang maksimal dalam pengujian keamanan sistem untuk menemukan celah keamanan, namun beberapa faktor perlu dipertimbangkan dalam proses pengujian keamanan sistem agar hasil pengujian lebih maksimal.

Peneltian terdahulu dari (Ghozali et al., 2019) yang berjudul Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (*Open Web Application Security Project*) untuk Penilaian Risk Rating. Mendeteksi kerentanan keamanan aplikasi berbasis website adalah hal yang penting, dan dapat memperkirakan risiko yang ada terhadap keberlangsungan suatu bisnis. Terjadinya transisi bisnis tradisional ke dalam lingkup aplikasi berbasis website dimanfaatkan oleh beberapa pelaku kejahatan dunia maya dengan tujuan mencuri informasi rahasia pengguna demi keuntungan pribadi. Pada Penelitian ini dilakukan mekanisme metode asesmen risiko pada sistem informasi harga komoditas utama yang dibangun oleh PT. Gitsolution. Dimana sistem tersebut merupakan informasi harga pokok untuk kehidupan sehari-hari yang dikelola oleh salah satu instansi pemerintah yang ada di Indonesia. Untuk mengetahui tingkat risiko pada sistem informasi harga komoditas utama menggunakan metode *Open Web Application Security Project* (OWASP) Risk Rating untuk mendeteksi kerentanan keamanan pada aplikasi berbasis website. Penelitian ini menghasilkan 2 faktor untuk memperkirakan *Likelihood* dan *Impact*, dari masing- masing faktor terdapat 3 risiko yang ditemukan yaitu *risk severity High, risk severity Medium dan risk severity Low*. Hasil penilaian risiko ini dapat membantu para pengelola dan pengembang sistem untuk menyadari risiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi risiko tersebut.

Peneltian terdahulu dari (Hidayatulloh & Saptadiaji, 2021) yang berjudul *Penetration Testing* pada Website Universitas ARS Menggunakan *Open Web Application Security Project* (OWASP). Abstrak – Universitas ARS adalah perguruan tinggi yang memanfaatkan website dalam melakukan kegiatan perkuliahannya. Seluruh informasi yang berkaitan dengan perkuliahan dimuat di website Universitas ARS. Banyak resiko yang akan terjadi apabila web server yang digunakan oleh website Universitas ARS tidak memiliki keamanan yang baik, banyak ancaman dari pihak yang tidak bertanggung jawab memanfaatkan celah keamanan untuk merugikan Universitas ARS. Tujuan penelitian ini adalah melakukan identifikasi kerentanan yang terdapat dalam website Universitas ARS dan melakukan pengujian serta analisis untuk mengetahui kondisi kerentanan website Universitas ARS menggunakan *Open Web Application Security Project* (OWASP). Metode penelitian yang digunakan sebagai parameter keamanan website adalah OWASP Top-10 2017. Jumlah subdomain yang diuji adalah 5 subdomain yang teridentifikasi dengan melakukan scanning menggunakan *tool The Harvester*. Hasil dari penelitian ini adalah ditemukannya kerentanan website Universitas ARS yang berhasil dipindai adalah 13 kerentanan. Dari 13 kerentanan tersebut ada 1 kerentanan yang berada pada tingkat ancaman yang sedang dan 12 berada pada tingkat ancaman yang rendah. Berdasarkan seluruh pengujian kerentanan yang dilakukan dapat disimpulkan bahwa website Universitas ARS memiliki keamanan yang sangat baik, memenuhi ketiga aspek keamanan informasi, memiliki web server dan software sistem informasi akademik yang aman.

Peneltian terdahulu dari (Rafeli et al., 2022) yang berjudul Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ. XYZ sebagai website research tentunya memiliki banyak data sensitif seperti data pribadi pengguna baik researcher ataupun responden dan data hasil *research.* Data ini rentan akan kebocoran data ataupun dicuri dan dilakukan penyalahgunaan dengan orang yang tidak bertanggung jawab sehingga merugikan banyak orang. *Penetration Testing*

merupakan cara untuk menggambarkan metode yang digunakan oleh orang tidak bertanggung jawab untuk dapat mengakses data secara ilegal kedalam sistem. WSTG merupakan singkatan dari *Web Security Testing Guide*, yaitu sebuah panduan project pengujian keamanan *Cyber* terutama dibidang pengembang aplikasi web dan keamanan professional. Pada penelitian ini dilakukan tujuh teknik yaitu *Information gathering, Configuration and Deployment Management Testing, Identity Management Testing, Input Validation Testing, Testing For Error Handling, Business Logic Testing dan Client Side Testing*. Pada penelitian ini ditemukan delapan *vulnerability* dengan kategori medium pada website XYZ.

B. LANDASAN TEORI

1. Analisis

Analisis adalah kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu. (Septiani et al., 2020)

2. Sistem Informasi Akademik

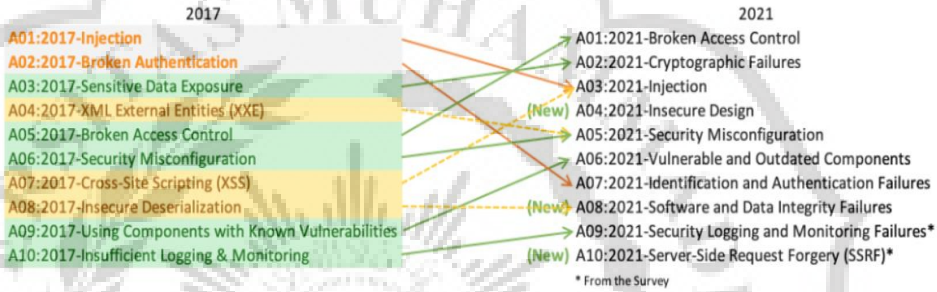
Sistem Informasi Akademik merupakan sebuah sistem yang dibangun dengan tujuan untuk mengelola data-data akademik dan segala kegiatan administrasi perkuliahan mahasiswa sehingga dapat memberikan kemudahan bagi pengguna dalam kegiatan administrasi akademik kampus secara online. Sistem Informasi Akademik merupakan salah satu dari berbagai sistem yang ada di Lingkungan Kampus. (Irawan, 2018)

3. Website

Website adalah kumpulan dari beberapa halaman web dimana informasi dalam bentuk teks, gambar, suara, dan lain-lain dipersentasikan dalam bentuk hypertext dan dapat diakses oleh perangkat lunak yang disebut dengan browser. Informasi pada sebuah website pada umumnya di tulis dalam format HTML. Informasi lainya disajikan dalam bentuk grafis (dalam format GIF,JPG,PNG,dll), suara (dalam format AU,WAV,dll), dan objek multimedia lainya (seperti MIDI,ShockwaveQuicktime Movie,3D World,dll). (Hartono, 2012)

4. OWASP (*Open Web Application Security Project*)

Open Web Application Security Project (OWASP) merupakan organisasi nonprofit berfokus pada peningkatan keamanan perangkat lunak. OWASP menjadi framework yang digunakan oleh pengembang dan ahli teknologi untuk mengamankan website. OWASP memberikan platform bagi pengembang untuk meningkatkan keamanan sistem melalui proyek yang open-source bersama dengan tools dari OWASP sebagai pendukung dalam pengujian sistem.(Kuncoro et al., 2021)



Gambar 1. Perbandingan OWASP Top 10 tahun 2017 dan OWASP Top tahun 2021(OWASP, 2021)

a. A01:2021-Broken Access Control

A01:2021-Kontrol Akses Rusak naik dari posisi kelima; 94% aplikasi diuji untuk beberapa bentuk kontrol akses yang rusak. 34 *Common Weakness Enumerations* (CWE) yang dipetakan ke Kontrol Akses Rusak memiliki lebih banyak kemunculan dalam aplikasi daripada kategori lainnya.

b. A02:2021-Cyptographic Failures

A02:2021-Kegagalan Kriptografi bergeser satu posisi ke posisi #2, yang sebelumnya dikenal sebagai Paparan Data Sensitif, yang merupakan gejala umum daripada akar penyebabnya. Fokus baru di sini adalah pada kegagalan yang terkait dengan kriptografi yang sering kali menyebabkan paparan data sensitif atau kompromi sistem.

c. A03:2021-Injection

A03:2021-Injeksi turun ke posisi ketiga. 94% aplikasi diuji untuk beberapa bentuk injeksi, dan 33 CWE yang dipetakan ke dalam kategori ini memiliki kemunculan terbanyak kedua dalam aplikasi. Cross-site Scripting sekarang menjadi bagian dari kategori ini dalam edisi ini.

d. A04:2021-Insecure Design

A04:2021-Desain Tidak Aman adalah kategori baru untuk tahun 2021, dengan fokus pada risiko yang terkait dengan kelemahan desain. Jika kita benar-benar ingin "bergerak ke kiri" sebagai sebuah industri, maka diperlukan lebih banyak penggunaan pemodelan ancaman, pola dan prinsip desain yang aman, serta arsitektur referensi.

e. A05:2021-Security Misconfiguration

A05:2021-Kesalahan Konfigurasi Keamanan naik dari peringkat #6 pada edisi sebelumnya; 90% aplikasi diuji untuk beberapa bentuk kesalahan konfigurasi. Dengan semakin banyaknya pergeseran ke perangkat lunak yang sangat mudah dikonfigurasi, tidak mengherankan jika kategori ini naik peringkat. Kategori sebelumnya untuk Entitas Eksternal XML (XXE) sekarang menjadi bagian dari kategori ini.

f. A06:2021-Vulnerable and Outdated Components

A06:2021-Komponen yang Rentan dan Usang sebelumnya berjudul Menggunakan Komponen dengan Kerentanan yang Diketahui dan menempati urutan #2 dalam survei komunitas Top 10, tetapi juga memiliki data yang cukup untuk masuk dalam Top 10 melalui analisis data. Kategori ini naik dari peringkat #9 pada tahun 2017 dan merupakan masalah yang diketahui dan kami kesulitan untuk menguji dan menilai risikonya. Ini adalah satu-satunya kategori yang tidak memiliki Kerentanan dan Eksposur Umum (CVE) yang dipetakan ke CWE yang disertakan, sehingga

eksploitasi default dan bobot dampak 5.0 diperhitungkan ke dalam skor mereka.

g. A07:2021-Identification and Authentication Failures

A07:2021-Kegagalan Identifikasi dan Otentikasi sebelumnya adalah Otentikasi Rusak dan turun dari posisi kedua, dan sekarang mencakup CWE yang lebih terkait dengan kegagalan identifikasi. Kategori ini masih menjadi bagian integral dari 10 Besar, tetapi peningkatan ketersediaan kerangka kerja standar tampaknya membantu.

h. A08:2021-Software and Data Integrity Failures

A08:2021-Kegagalan Integritas Perangkat Lunak dan Data adalah kategori baru untuk tahun 2021, yang berfokus pada pembuatan asumsi terkait pembaruan perangkat lunak, data penting, dan jalur pipa CI/CD tanpa memverifikasi integritas. Salah satu dampak dengan bobot tertinggi dari data Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) yang dipetakan ke dalam 10 CWE dalam kategori ini. Insecure Deserialization dari tahun 2017 sekarang menjadi bagian dari kategori yang lebih besar ini.

i. A09:2021-Seciruty Logging and Monitoring Faiures

A09:2021-Kegagalan Pencatatan dan Pemantauan Keamanan sebelumnya adalah Pencatatan & Pemantauan yang Tidak Memadai dan ditambahkan dari survei industri (#3), naik dari sebelumnya #10. Kategori ini diperluas untuk mencakup lebih banyak jenis kegagalan, sulit untuk diuji, dan tidak terwakili dengan baik dalam data CVE/CVSS. Namun, kegagalan dalam kategori ini dapat secara langsung berdampak pada visibilitas, peringatan insiden, dan forensik.

j. A10:2021-Server-Side Request Forgery (SSRF)

A10:2021-Pemalsuan Permintaan Sisi Server ditambahkan dari survei komunitas Top 10 (#1). Data menunjukkan tingkat kejadian yang relatif rendah dengan cakupan pengujian di atas rata-rata, serta peringkat di atas rata-rata untuk potensi Eksploitasi dan Dampak. Kategori ini mewakili skenario di mana anggota komunitas keamanan memberi tahu kami bahwa ini penting, meskipun tidak diilustrasikan dalam data saat ini.

5. Penetration Testing

Penetration Testing merupakan pengujian dengan cara menyimulasikan serangan terhadap suatu sistem. Serangan tersebut dilakukan untuk memeriksa apakah adanya kerentanan yang dapat dieksploitasi. Pengujian ini juga dapat melibatkan analisis sistem 11 tertentu untuk memeriksa potensi kerentanan terhadap upaya peretasan yang mungkin terjadi.(Irawan, 2022)

Dalam Penetration Testing, terdapat tiga metode yang dapat dilakukan, antara lain sebagai berikut:

a. *Black Box Testing*:

Pada *Black-Box Testing*, penguji sebagai pihak eksternal dan tidak memiliki pengetahuan apa pun tentang sistem yang akan diuji. Penguji tidak diberikan diagram arsitektur atau *source code* apa pun terkait sistem. Metode ini menentukan kerentanan dalam sistem yang dapat dieksploitasi dari luar jaringan. Pengetahuan terbatas yang diberikan kepada penguji penetrasi membuat metode ini menjadi yang tercepat untuk dilakukan.

b. Gray-Box Testing

Tingkatan selanjutnya dari *Black-Box Testing* adalah *Gray-Box Testing*. Penguji pada metode ini, memiliki tingkatan akses dan pengetahuan pengguna, serta berpotensi memiliki hak istimewa yang lebih tinggi pada sistem (administrator). Dengan adanya akun internal ini, memungkinkan pengujian keamanan di dalam ruang

lingkup sistem. Tujuan *Gray-Box Testing* adalah untuk memberikan penilaian keamanan jaringan yang lebih terfokus dan efisien daripada penilaian pada *Black-Box Testing*.

c. *White Box Testing*

Tidak seperti metode *Black-Box* dan *Gray-Box Testing*, penguji penetrasi pada *White-Box Testing* diberikan akses penuh ke *source code*, dokumentasi arsitektur, dan sebagainya. Tantangan utama pada metode ini adalah menyaring banyaknya data yang tersedia untuk mengidentifikasikan titik kelemahan potensial. Penguji penetrasi *White-Box* dapat melakukan analisis kode statis, analisis *source code (code review)*, *debugger*, dan *Tools* lainnya. Hal ini menjadikan *White-Box Testing* sebagai metode yang paling memakan waktu