Pengujian Kerentanan Celah Keamanan Website Menggunakan Threat Modelling Pada Website Prodi Teknologi Rekayasa Komputer Jaringan

Muhammad Aqsa[1], Anwar[2*], Muhammad Davi[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[1]aqsa_12@gmail.com
[2*]anwarsy@ pnl.ac.id (penulis korespondensi)
[3]muhammad.davi@pnl.ac.id

***Abstrak*— Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis secara mendalam celah keamanan yang ada pada website Program Studi Teknologi Rekayasa Komputer Jaringan (TRKJ) dan website siperi. Selain itu, penelitian ini juga berupaya untuk membandingkan munculnya celah keamanan antara website *HTTP* dengan *HTTPS*. Pengujian keamanan juga dilakukan pada *database server* yang digunakan pada kedua website tersebut dengan menggunakan pendekatan *Threat Modeling* yang komprehensif. Metode yang digunakan dalam penelitian ini meliputi pengumpulan data primer dan sekunder, serta analisis mendetail terhadap celah keamanan yang ditemukan. Teknik pengujian dilakukan dengan standarisasi menggunakan *OWASP (Open Web Application Security Project)* dan metode-metode *Threat Modelling* yang relevan. Dampak dan risiko dari celah keamanan yang ditemukan dinilai menggunakan *CVSS score (Common Vulnerability Scoring System)* untuk memberikan penilaian yang akurat terhadap kerentanan pada website tersebut. Hasil penelitian menunjukkan bahwa terdapat beberapa celah kebocoran informasi yang cukup signifikan pada website *HTTP* TRKJ yang memungkinkan eksploitasi oleh penyerang. Hal ini berpotensi merugikan pengelola website serta pengguna yang berinteraksi dengan website tersebut. Di sisi lain, pengamanan database server pada kedua website ini sangat baik, dengan website *HTTP* TRKJ yang bahkan lebih menyembunyikan detail informasi mengenai jenis dan versi layanan yang digunakan. Hasil penelitian ini diharapkan dapat memberikan rekomendasi yang kuat untuk memperkuat integritas, kerahasiaan, dan ketersediaan informasi di website TRKJ, sehingga dapat meningkatkan tingkat keamanan secara keseluruhan.**
Kata kunci — keamanan website, *Threat Modeling, OWASP, Database, Cybersecurity*

Abstract*— This research aims to identify and analyze in depth the security vulnerabilities present on the website of the Computer Network Engineering Technology Study Program (TRKJ) and the Siperi website. Additionally, this study seeks to compare the occurrence of security vulnerabilities between HTTP and HTTPS websites. Security testing is also conducted on the database servers used by both websites using a comprehensive Threat Modeling approach. The methods used in this research include the collection of primary and secondary data, as well as detailed analysis of the security vulnerabilities found. Testing techniques are standardized using OWASP (Open Web Application Security Project) and relevant Threat Modelling methods. The impact and risks of the discovered security vulnerabilities are assessed using the CVSS score (Common Vulnerability Scoring System) to provide an accurate evaluation of the website's vulnerabilities. The results of the study indicate that there are several significant information leakage vulnerabilities on the HTTP TRKJ website that can potentially be exploited by attackers. This poses a risk to both the website administrators and the users interacting with the website. On the other hand, the database server security of both websites is very good, with the HTTP TRKJ website even better concealing details about the types and versions of services used. The findings of this study are expected to provide strong recommendations to enhance the integrity, confidentiality, and availability of information on the TRKJ website, thereby improving overall security levels.
Keywords — website security, threat modeling, OWASP, Database, cybersecurity

I. Pendahuluan

Penggunaan teknologi informasi dan website di Program Studi Teknologi Rekayasa Komputer dan Jaringan telah menjadi bagian penting dari proses pendidikan dan interaksi mahasiswa. Namun, dengan perkembangan teknologi juga muncul ancaman keamanan siber yang kompleks. Oleh karena itu, penting untuk menguji kerentanan keamanan pada website program studi guna menjaga integritas, kerahasiaan, dan ketersediaan informasi.

Penelitian ini dilakukan untuk mengidentifikasi potensi kerentanan yang bisa dieksploitasi oleh pihak tidak bertanggung jawab. Pengujian dilakukan dengan menggunakan metode threat modelling, yang memberikan pendekatan sistematis untuk mengidentifikasi ancaman, kerentanan, serta dampaknya terhadap keamanan website.

Tujuan dari penelitian ini adalah untuk memperoleh pemahaman yang lebih baik mengenai potensi ancaman serta memberikan solusi yang tepat untuk meningkatkan keamanan website. Keberhasilan implementasi solusi ini akan mendukung integritas, keamanan informasi, dan reputasi program studi, serta memastikan pengalaman pengguna yang aman dan nyaman.

A. SQL (Structured Query Language) database

SQL (Structured Query Language) adalah bahasa yang dirancang khusus untuk mengelola basis data relasional. Melalui query SQL, pengguna dapat melakukan berbagai

operasi pada data, seperti menambah, menghapus, atau mencari informasi, terutama dalam konteks manajemen pesanan pembelian (PO). SQL memungkinkan departemen pembelian membangun database yang berisi detail pesanan, jumlah, dan supplier, sehingga karyawan dapat memantau status dan menganalisis tren pembelian secara efektif [11].

B. MySQL

MySQL adalah sistem manajemen basis data relasional (RDBMS) yang terkenal karena kecepatan, kemudahan penggunaan, dan kepopulerannya, terutama dalam pengembangan aplikasi web dinamis. MySQL berintegrasi dengan PHP dan menggunakan bahasa query SQL, sehingga memudahkan pengembang dalam menangani data yang kompleks. Keandalan, fleksibilitas, dan kemampuannya menangani berbagai jenis data menjadikan MySQL pilihan utama bagi proyek yang memerlukan basis data yang responsif dan mudah dikelola [7].

C. Website

Website adalah kumpulan halaman web yang saling terkait dan dapat diakses melalui internet, terdiri dari berbagai jenis data digital seperti teks, gambar, animasi, suara, dan video. Halaman web dibangun menggunakan HTML dan ditampilkan oleh browser untuk menyajikan informasi dalam format yang mudah dipahami pengguna. Website menyediakan pengalaman yang interaktif dan dinamis, memungkinkan berbagi informasi dan hiburan dalam berbagai format visual dan multimedia [12].

D. Web server

Web server adalah perangkat lunak yang menerima permintaan (request) dari web browser dalam bentuk HTTP dan mengirimkan halaman web atau data yang diminta oleh client. Fungsi utama web server adalah menjadi perantara antara client dan server, memastikan transfer data dalam bentuk HTML atau dokumen lain. Selain itu, web server berperan dalam mengelola akses data dan menerapkan metode keamanan, menjadikannya komponen penting dalam pengembangan aplikasi web yang efisien [1].

E. Keamanan Jaringan dan Protokol

Keamanan jaringan sangat penting, terutama saat jaringan lokal terhubung ke internet. Organisasi harus memprioritaskan perlindungan dari ancaman siber seperti serangan DDoS, hacker, virus, dan trojan. Berbagai teknik seperti phishing dan eksploitasi celah keamanan sering digunakan oleh penyerang. Untuk melindungi sistem, organisasi perlu menggunakan firewall, antivirus, dan sistem deteksi ancaman [4].

F. Hypertext Transfer Protocol (HTTP)

HTTP adalah protokol pada lapisan aplikasi yang digunakan untuk mengakses dokumen hypertext yang membentuk World Wide Web. Meski HTTP/1.1 lebih efisien daripada HTTP/1.0, keduanya tidak menyediakan keamanan, sehingga rentan terhadap penyadapan dan perubahan data yang dikirim tanpa terdeteksi [4].

G. Linux sebagai Sistem Operasi

Linux, berbasis kernel Unix, adalah sistem operasi yang fleksibel dan murah, populer di kalangan profesional keamanan. Kali Linux, salah satu distribusi khusus, dirancang untuk pengujian penetrasi dan audit keamanan, menjadikannya alat yang kuat untuk mendeteksi kerentanan [9].

H. Threat Modeling

Threat Modelling adalah pendekatan keamanan untuk mengidentifikasi bagian sistem yang rentan terhadap serangan. Dengan metode ini, risiko dapat dievaluasi dan mitigasi dilakukan secara proaktif, meningkatkan keamanan sistem secara keseluruhan [3].

I. Penetration Testing (PTES)

Penetration testing mensimulasikan serangan untuk menemukan kelemahan jaringan. Jenis serangan yang umum mencakup SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF). Masing-masing serangan ini memanfaatkan kelemahan validasi input, memungkinkan penyerang mendapatkan akses tidak sah, mencuri data, atau menyebarkan malware [8].

J. Port Scanning Nmap

Port scanning menggunakan Nmap membantu mengidentifikasi port aktif pada server, yang bisa digunakan penyerang untuk merencanakan serangan lebih lanjut. Teknik ini juga bermanfaat bagi administrator untuk menilai keamanan server dan firewall [2].

K. Open Web Application Security Project (OWASP)

OWASP adalah organisasi non-profit yang didirikan untuk meningkatkan keamanan perangkat lunak, membantu organisasi mengembangkan aplikasi yang lebih aman [4].

L. Acunetix

Acunetix adalah perangkat lunak yang mendeteksi dan mengatasi kerentanan web seperti SQL Injection dan XSS. Program ini terintegrasi dengan pengembangan perangkat lunak, memberikan laporan lengkap tentang keamanan aplikasi web [6].

M. Common Vulnerability Scoring System (CVSS)

CVSS adalah metodologi penilaian kerentanan untuk memberikan skor yang objektif dan standar terhadap kerentanan yang ditemukan. Sistem ini membantu organisasi dalam memprioritaskan perbaikan berdasarkan tingkat ancaman yang dinilai [6].

II. Metodologi Penelitian

A. Data dan Pengumpulan Data

Dalam penelitian ini, data yang digunakan adalah data primer, yang diperoleh melalui pengukuran langsung oleh peneliti. Fokus utama dari pengumpulan data primer ini adalah untuk mendapatkan informasi terkait kerentanan celah keamanan pada website program studi TRKJ. Proses pengumpulan data dilakukan melalui serangkaian uji coba yang dirancang untuk mengevaluasi keamanan website program studi yang telah dipilih sebagai objek penelitian. Dengan melakukan pengujian ini, peneliti dapat mengidentifikasi potensi celah keamanan dan mengumpulkan informasi yang diperlukan untuk analisis lebih lanjut.

Pengumpulan data primer melibatkan berbagai langkah yang sistematis dalam pengujian keamanan pada website program studi TRKJ. Proses ini termasuk dalam identifikasi potensi kerentanan dan analisis risiko yang dapat muncul dari celah keamanan yang ditemukan. Setiap hasil dari pengujian akan didokumentasikan dengan detail untuk memberikan gambaran yang mendalam tentang kondisi keamanan website yang sedang dievaluasi. Dokumentasi yang lengkap dan terperinci ini bertujuan untuk menyajikan pemahaman yang jelas mengenai status keamanan dari website yang diuji dan untuk membantu dalam merumuskan rekomendasi perbaikan yang tepat.

B. Rancangan Sistem (Software/Hardware)

Dalam pengujian keamanan website Prodi Teknologi Rekayasa Komputer Jaringan (TRKJ), kami menggunakan Threat Modelling sebagai landasan utama. Tahapan pengujian dimulai dengan fase perencanaan, di mana tujuan dan lingkup pengujian ditetapkan dengan memilih metode dan teknik yang sesuai. Kami mengumpulkan informasi tentang sistem dan basis data untuk mendukung analisis risiko oleh karena itu berikut pengujian yang akan dilakukan di dalam penelitian ini dapat dilihat pada Gambar 1.

Gambar 1 Rancangan Sistem

Identifikasi ancaman dilakukan dengan menggabungkan analisis statis dan dinamis, Pengujian keamanan fokus pada mekanisme autentikasi dan otorisasi untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses informasi sensitif. Skenario pengujian yang dikembangkan berdasarkan analisis risiko mencakup simulasi serangan seperti SQL injection dan mencari file konfigurasi, yang merupakan bagian penting dari proses pengujian. Langkah-langkah pengujian meliputi identifikasi celah keamanan, verifikasi autentikasi dan otorisasi, serta melibatkan logging dan monitoring untuk mendeteksi aktivitas yang mencurigakan.

Selain itu, proses pencarian celah juga melibatkan penggunaan alat seperti Nmap untuk melakukan port scanning dan mengidentifikasi port yang aktif serta potensi kerentanannya. Nmap dapat membantu dalam menemukan port terbuka yang bisa menjadi titik masuk bagi penyerang. Proses lain yang penting adalah pencarian direktori tersembunyi (hidden directory), yang dilakukan untuk menemukan folder atau file yang mungkin tidak terlihat pada permukaan tetapi dapat berisi informasi sensitif atau celah keamanan. Hasil dari semua pengujian ini didokumentasikan dalam laporan akhir, yang mencakup temuan ancaman, tingkat keparahan, dan rekomendasi untuk perbaikan. Laporan ini menjadi panduan dalam menerapkan perbaikan dan memperkuat keamanan. Pengujian celah keamanan basis data harus dilakukan secara berkala untuk menjaga keamanan sistem dan mengurangi risiko yang mungkin merugikan Prodi TRKJ.

C. Metode Penelitian

Pada penelitian ini akan menggunakan beberapa metode untuk melakukan penyusunan skripsi ini, yaitu

1) Monitoring celah keamanan: Menganalisa berbagai jenis kerentanan yang terdapat pada website dengan cara melakukan pemindaian konfigurasi untuk mengidentifikasi kesalahan konfigurasi pada sistem operasi dan perangkat lunak, kemudian mengklasifikasikan kerentanan berdasarkan tingkat keparahannya. Tingkat keparahan kerentanan ditentukan berdasarkan dampak yang dapat ditimbulkan oleh kerentanan tersebut.
2) Pengujian: Setelah melakukan analisa dari studi literatur, langkah selanjutnya adalah melakukan pengujian terhadap database dan website informasi yang bertujuan untuk memastikan bahwa setiap komponen sistem beroperasi sesuai standar kualitas yang telah ditentukan. sehingga dapat menghindari serangan-serangan seperti XSS, pencurian data dan SQL injection yang dapat mengambil data atau melihat data tanpa seijin dari pihak penyedia.

D. Teknik Pengujian

Teknik pengujian yang dapat digunakan untuk pengujian kerentanan celah keamanan basis data terhadap website Prodi TRKJ adalah Threat Modeling. Threat Modelling yaitu suatu pendekatan pengujian perangkat lunak yang dilakukan dengan memodelkan potensi ancaman terhadap keamanan suatu sistem tanpa harus mengetahui detail implementasi internalnya.

Threat modeling memungkinkan pengidentifikasian celah keamanan dengan mengidentifikasi potensi ancaman, mengevaluasi dampak potensial, dan merumuskan langkah-langkah mitigasi untuk mengatasi risiko keamanan. Dengan memodelkan ancaman yang mungkin muncul terhadap sistem, Threat modeling memberikan gambaran mengenai kerentanan keamanan yang dapat terjadi.

Salah satu langkah dalam Threat modeling adalah menilai tingkat kerugian yang mungkin dihadapi. Teknik ini menggunakan kategori ancaman yang lebih umum dan berfokus pada tingkat risiko dengan membagi ancaman menjadi beberapa elemen yang berbeda. Setiap elemen

memiliki bobot yang berbeda dalam penilaian risiko, Elemen-elemen ini meliputi:

- Melakukan pencarian informasi kerentanan yang terdapat pada website menggunakan nmap dan dirsearch, setelah itu melakukan penelitian menggunakan CVSS.
- Menilai seberapa mudah ancaman tersebut dapat dieksploitasi oleh penyerang. Ini termasuk analisis terhadap tingkat kesulitan untuk memanfaatkan kerentanan, pengujian dilakukan dengan menggunakan tools acunetix
- Melakukan analisis berdasarkan acunetix terkait informasi yang sensitif menggunakan perangkat lunak *burp suite*
- Melakukan pengujian keamanan *database* menggunakan sqlmap

Teknik ini mencakup langkah-langkah seperti identifikasi aset penting, pemetaan aliran data, analisis risiko, dan pengembangan rencana mitigasi. Alat-alat seperti Nmap, sqlmap, Burp Suite, Nikto, dan Acunetix tetap dapat digunakan dalam pengujian keamanan untuk mengidentifikasi dan mengatasi potensi kerentanan.

Dalam pengujian keamanan website Prodi TRKJ, pemilihan tools yang tepat harus disesuaikan dengan kebutuhan dan tujuan pengujian. Kombinasi tools, seperti Nmap dan Nikto untuk scanning awal, dengan Burp Suite untuk eksploitasi dan pengujian input/output, dapat meningkatkan efektivitas pengujian keamanan secara menyeluruh.

Melalui pengujian keamanan yang rutin menggunakan Threat modeling, pemilik website Prodi TRKJ dapat memastikan perlindungan data penting dan menjaga integritas sistem mereka dari potensi serangan. Dengan demikian, keberlanjutan keamanan website Prodi TRKJ dapat diperkuat melalui pendekatan yang holistik dan proaktif terhadap identifikasi dan mitigasi risiko keamanan.

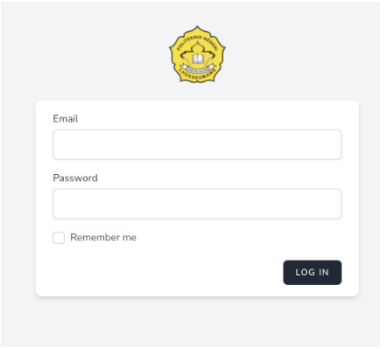
III. Hasil dan Pembahasan

Pada penelitian kali ini dilakukan pengujian terhadap website Prodi TRKJ sebagai website HTTP dan website siperi sebagai website HTTPS. untuk tampilan halaman landing page website TRKJ tersebut dapat dilihat pada Gambar 2. Dan untuk halaman tampilan Website siperi dapat Dilihat pada Gambar 3 tampilan website siperi.

website program studi TRKJ menjadi sarana utama dalam menyajikan informasi, pembelajaran, dan interaksi antara civitas akademik. website ini juga menampilkan profil dosen yang berpengalaman dan berkualifikasi tinggi, serta fasilitas laboratorium dan sumber daya pembelajaran yang mendukung proses belajar mengajar.

Pada Website SIPERI (Sistem Informasi Pendidikan dan Riset) merupakan platform digital yang dirancang untuk mendukung seluruh aspek kegiatan akademik dan penelitian di lingkungan kampus.

Gambar 2 Halaman website Prodi TRKJ



Gambar 3 Halaman website siperi

Pada website Prodi Teknologi Rekayasa Komputer Jaringan dilakukan pengujian menggunakan beberapa tools yang sudah banyak dan familiar dan tersebar di internet salah satu nya itu nmap yang digunakan untuk mencari segala sesuatu bentuk informasi yang terdapat pada website TRKJ. hasil informasi tersebut dirangkum sesuai dengan kebutuhan untuk analisis threat modelling. dapat dilihat pada tabel 1 hasil scanning menggunakan Nmap untuk website HTTP dan untuk informasi website HTTPS dapat dilihat pada tabel 2 hasil scanning menggunakan Nmap untuk website HTTPS

Tabel I
Hasil *scanning* menggunakan Nmap untuk website HTTP

No	Website Prodi Teknologi Rekayasa Komputer Jaringan
1	website prodi Teknologi Rekayasa Komputer Jaringan menggunakan jenis OS linux redhat enterprise dan menjalankan Apache sebagai web server
2	Protokol komunikasi menggunakan TLS (Transport Layer Security)
3	jumlah layanan dengan status "filtered" adalah 12
4	Database server yang digunakan adalah MySQL

Tabel II
Hasil scanning menggunakan Nmap untuk website HTTPS

No	Website SIPERI

1	website prodi Teknologi Rekayasa Komputer Jaringan menggunakan jenis OS Unix redhat enterprise dan menjalankan LiteSpeed sebagai web server
2	TLS untuk koneksi HTTPS pada port 443.
3	jumlah layanan dengan status "filtered" adalah 16
4	Database server yang digunakan adalah MySQL 5.5.5 10.11.8 MariaDB cll lve

A. Pengujian dan analisis dalam sub direktori website

Pada pengujian merupakan salah satu kategori yang berfokus kesalahan konfigurasi. Dari hasil pengujian, terdapat beberapa endpoint yang bisa menunjukkan adanya informasi yang sensitif yang dapat menyebabkan dampak kerugian yang signifikan bagi user dan juga pengelola website.

jumlah dari berbagai status HTTP yang ditemukan dapat dilihat pada tabel 3 status response code. dan untuk HTTPS dapat dilihat pada tabel 4 HTTPS status response code.

Tabel III
HTTP status response code

no	kode	Respon	jumlah
1	200	OK	6
2	302	Found	1
3	403	Forbidden	19
4	404	Not Found	3

Tabel IV
HTTPS status response code

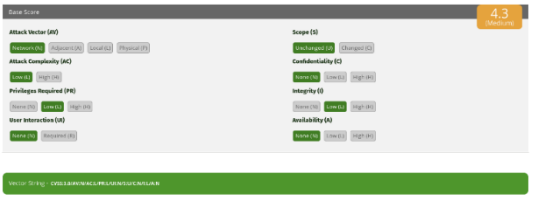
no	kode	Respon	jumlah
1	200	OK	4
2	302	Found	1
3	403	Forbidden	16
4	404	Not Found	66

Berdasarkan hasil pengujian pencarian informasi yang sensitif mencari direktori menetapkan nilai cvss score untuk website HTTP TRKJ dapat dilihat pada gambar 4.4 penilaian cvss TRKJ dan untuk Penilaian website siperi dapat dilihat pada gambar 4.5 penilaian score siperi.

Pada website HTTP TRKJ terdapat nilai akhir dari penilaian menggunakan cvss calculator adalah 5.3. Dapat dilihat pada gambar 4 penilaian cvss TRKJ. nilai awal dari dampak adalah 1.4 dan nilai jenis eksploitasinya adalah 3.9 kemudian dijumlah sehingga menjadi nilai Base 5.3.

Sedangkan pada website HTTPS SIperi nilai mendapatkan nilai dari 4.3 menggunakan perhitungan dari CVSS kalkulator nilai awal dari perhitungan tersebut adalah 1.4 nilai jenis eksploitasinya adalah 2.8 kemudian dijumlah sehingga menjadi nilai Base 4.3 dapat dilihat pada gambar 5 penilaian CVSS Siperi.

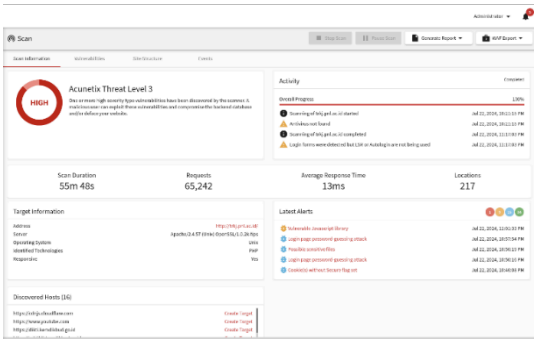
Gambar 4 Penilaian CVSS TRKJ



Gambar 5 Penilaian CVSS SIPERI.

B. Pengujian dan analisis menggunakan tools menggunakan Acunetix

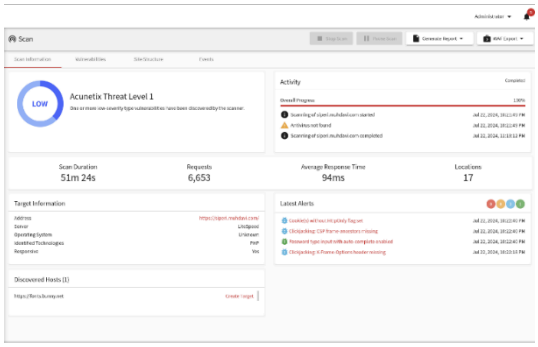
Pengujian menggunakan tools menggunakan Acunetix untuk mengetahui celah atau kerentanan serta membandingkan tingkat kerentanan yang terdapat pada website HTTP Trkj dan website HTTPS siperi, dapat dilihat pada gambar 6 acunetix HTTP dan gambar 7 acunetix HTTPS.



Gambar 4.6 Acunetix HTTP

Pada website HTTP TRKJ dilakukan pengujian menggunakan acunetix, total dari proses pengujian tersebut terjadi selama 55 menit, jumlah request ada sebanyak 65,242 request dan jumlah rata rata respon time dari acunetix kepada website HTTP TRKJ adalah 13 ms dan pada website TRKJ jumlah sub lokasinya berjumlah 217 direktori dan total kemungkinan adanya indikasi celah keamanan pada website TRKJ dari low hingga critical adalah berjumlah 59

kerentanan, yang berhasil ditemukan pada website HTTP TRKJ menggunakan tools Acunetix.



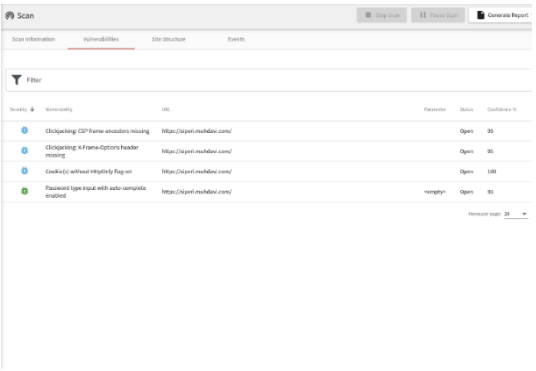
Gambar 4.7 Acunetix HTTPS

Pada website HTTPS siperi dilakukan juga pengujian menggunakan acunetix, dari hasil pengujian yang dilakukan selama total 51 menit, jumlah request yang diperlihatkan oleh acunetix adalah 6,653 request dan rata rata dan jumlah rata rata respon time dari acunetix kepada website HTTPS siperi adalah 94 ms dan jumlah sub lokasinya itu sebanyak 17 direktori, dan total adanya kemungkinan atau indikasi celah ditemukannya kerentanan pada website HTTPS siperi hanya terdapat jenis dengan tingkat kategori low dengan total 4 kerentanan yang terdapat pada website siperi dengan pengujian menggunakan tools Acunetix.

C. Pengujian dan analisis konfigurasi manajemen keamanan

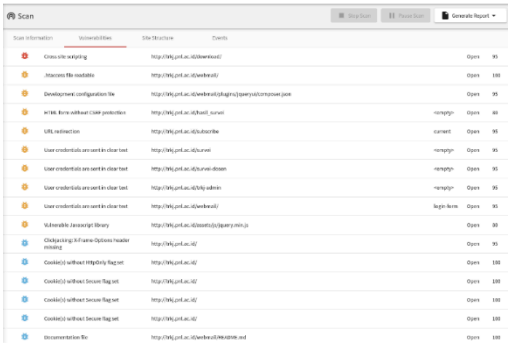
Pengujian dilakukan menggunakan tools acunetix bertujuan untuk mencari kesalahan konfigurasi bagian keamanan akses read pada sebuah website berdasarkan standar owasp dengan kode A05:2021-Security Misconfiguration. Manajemen Konfigurasi yang aman berfokus pada memastikan bahwa aplikasi web dan server dikonfigurasikan dengan benar untuk meminimalkan risiko keamanan. Ini berarti semua pengaturan dan konfigurasi pada aplikasi dan server harus dilakukan dengan tepat untuk mencegah celah keamanan yang dapat dimanfaatkan oleh penyerang.

Pada website HTTPS siperi tidak ditemukan atau tidak terdapat celah keamanan yang mengungkapkan informasi yang sensitif yang dapat merugikan baik kepada pihak pengguna maupun dapat dilihat pada gambar 8 hasil pengujian siperi.



Gambar 4.8 Hasil pengujian SIPERI

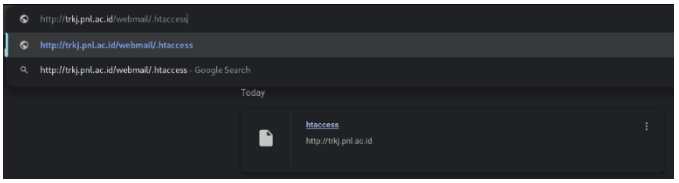
Pada website HTTP TRKJ menggunakan acunetix menghasilkan beberapa informasi yang sensitif dan mungkin menimbulkan dampak kerugian yang dapat menyebabkan terjadinya serangan pada website TRKJ dan juga mungkin saja dapat menimbulkan kerugian pada sisi pengguna dapat dilihat pada gambar 9 hasil pengujian TRKJ.



Gambar 4.9 Hasil pengujian TRKJ

Konfigurasi PHP ini mengatur berbagai pengaturan terkait PHP, seperti ukuran maksimum file yang diunggah dan pengelolaan sesi. Pengaturan ini ditujukan untuk PHP versi 5; jika server menggunakan PHP 7 atau lebih baru, modul harus diperbarui.

file tersebut juga dapat diakses dan diunduh dengan menggunakan web browser dengan cara menyematkan url dapat dilihat pada gambar 10 download file .htaccess TRKJ



Gambar 10 Download file .htaccess TRKJ

D. Pengamanan untuk owasp dengan kode A05:2021

Mengamankan situs web dari hasil temuan di atas melibatkan beberapa langkah untuk menangani masalah konfigurasi keamanan dan melindungi informasi sensitif. Berikut adalah langkah-langkah untuk mengatasi dan memperbaiki masalah yang ditemukan pada website TRKJ

berdasarkan standar OWASP dan hasil pengujian yang disebutkan:

1) Mengamankan File *.htaccess:* yang dapat diakses publik mengungkapkan konfigurasi server yang sensitif. Untuk mengatasi masalah ini dengan cara membatasi Akses ke File *.htaccess* memastikan file *.htaccess* tidak dapat diakses oleh publik. Dengan cara menambahkan aturan pada file *.htaccess* atau di konfigurasi *server web* untuk mencegah akses ke file *.htaccess* dan file konfigurasi lainnya.
2) Memperbarui Konfigurasi pada file PHP: konfigurasi PHP diperbarui untuk versi PHP terbaru yang digunakan oleh server. Disesuaikan dengan pengaturan seperti upload_max_filesize, post_max_size, dan session.cookie_secure sesuai kebutuhan keamanan yang diperlukan pada server.
3) Implementasi Header Keamanan dengan cara menggunakan header HTTP keamanan untuk melindungi situs dari serangan umum. menambahkan header keamanan seperti Content-Security-Policy, X-Content-Type-Options, dan Strict-Transport-Security yang bertujuan untuk meningkatkan keamanan website.

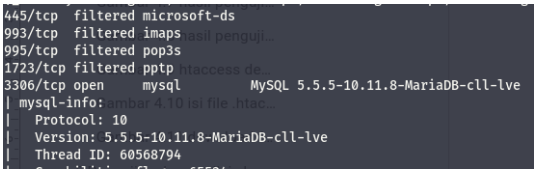
E. Pengujian dan analisis keamanan database

Percobaan menemukan celah keamanan pada database bertujuan agar celah tersebut tidak dimanfaatkan oleh orang yang tidak berwenang sehingga celah tersebut tidak dapat digunakan atau dapat dimanfaatkan oleh penyerang untuk melakukan serangan.

Pada website TRKJ ditemukan atau diketahui bahwa website TKJ menggunakan tipe atau jenis database server nya itu mysql namun untuk versi yang digunakan tidak dapat diketahui, hal tersebut disebabkan disembunyikan oleh pihak pengelola yang dapat dipastikan untuk perlindungan terhadap databasenya sangat bagus dan terjaga untuk hasil scanning nmap dapat dilihat pada gambar 11 database TRKJ.

Gambar 11 Database TRKJ

Hal yang berbeda terjadi pada scanning nmap pada website HTTPS Siperi, pada website siperi ditemukan database apa yang digunakan serta versi berapa yang digunakan dapat dilihat pada gambar 12 database Siperi. Database server yang digunakan pada website HTTPS siperi adalah MySQL 5.5.5 10.11.8 MariaDB cll lve.



Gambar 12 Database siperi

Dari hasil informasi diatas dapat diketahui bahwa kedua jenis website tersebut menggunakan jenis database server mysql tetapi hanya website siperi saja yang diketahui menggunakan versi berapa sedangkan pada website TRKJ untuk versinya tidak dapat dilihat atau diamankan oleh pengelola keamanan untuk menyembunyikan versi berapa yang digunakan.

Untuk pengujian kerentanan *sql* pada kedua *website* tersebut menggunakan teknik serangan *sql injection* dan menggunakan *tools sqlmap* untuk mencoba melakukan memasukan *query sql* untuk mendapatkan informasi yang sensitif pada website TRKJ dan juga website Siperi. Untuk perintah tools *sqlmap* dan parameter yang digunakan dapat dilihat pada gambar 13 *sqlmap* parameter.

(a)

(b)

Gambar 13 Sqlmap parameter

Pada gambar 13 pengujian sqlmap terdapat beberapa parameter yang bertujuan untuk menemukan potensi ada atau tidaknya celah kerentanan tersebut. Parameter "-u" dimaksudkan adalah url dari target yang akan dilakukan injections menggunakan sqlmap pada penggunjian *website* siperi kali ini diinputkan url *https://siperi.muhdavi.com/penjadwalan/index* sedangkan perintah parameter "-u" pada sqlmap untuk website TRKJ adalah *http://trkj.pnl.ac.id/download?page=1*.

Pada pengujian kali ini, beberapa parameter penting digunakan untuk mengatur berbagai aspek dari proses pengujian keamanan. Parameter *--level=5* mengatur tingkat agresivitas pengujian. Dengan nilai 5, pengujian dilakukan dengan tingkat agresivitas yang tinggi, berarti teknik yang diterapkan akan lebih mendalam dan menyeluruh. Parameter ini menentukan bahwa pengujian kali ini tidak hanya mencari celah secara dasar, tetapi juga menggunakan metode yang lebih intensif.

Selanjutnya, *parameter --risk=3* mengatur tingkat risiko yang dapat diterima selama pengujian. Nilai 3 menunjukkan tingkat risiko yang moderat, berarti pengujian akan mempertimbangkan beberapa risiko yang lebih tinggi namun tetap berada dalam batas yang dianggap dapat diterima. Parameter ini memastikan bahwa risiko yang dihadapi tidak terlalu ekstrim namun cukup untuk mengidentifikasi potensi masalah yang signifikan.

Pada parameter *--dbms=mysql* digunakan untuk menentukan jenis database yang akan diuji. Dalam hal ini, parameter ini menunjukkan bahwa database yang diuji adalah MySQL. Ini membantu alat pengujian menyesuaikan teknik dan metode yang digunakan berdasarkan jenis sistem database yang ada.

Untuk Parameter *--tamper=space2comment ,random case* menentukan teknik tamper yang digunakan selama pengujian. Teknik tamper ini bertujuan untuk mengubah data input sehingga dapat melewati mekanisme perlindungan terhadap *SQL injection.* Dalam pengujian ini, teknik tamper yang diterapkan meliputi penggantian spasi dengan komentar dan penggunaan kasus acak, untuk mengatasi perlindungan yang mungkin ada.

Selain itu, *parameter --random-agent* menginstruksikan alat untuk menggunakan *User-Agen*t acak saat melakukan permintaan HTTP. Hal ini penting untuk membantu menghindari deteksi oleh *firewall* atau sistem anti-intrusi yang mungkin memantau pola permintaan.

Terakhir, parameter --batch mengatur alat untuk menjalankan pengujian dalam mode batch. Dalam mode ini, pengujian dilakukan secara otomatis tanpa memerlukan interaksi pengguna, memungkinkan proses yang lebih efisien dan minim gangguan.

Hal ini dapat disebabkan oleh adanya filter sanitasi input pada konfigurasi database server yang digunakan ataupun ada kemungkinan parameter yang dipilih dalam percobaan ini tidak memungkinkan SQL injection. Dikarenakan tidak adanya kerentanan yang terdapat pada database server mysql dapat dinyatakan dari segi konfigurasi keamanan database server yang digunakan sangat baik dan juga sangat menjaga integritas data pengguna.

F. Analisa perbandingan keamanan website TRKJ dan SIPERI

Pada analisis ini, peneliti mencoba membandingkan dua buah situs web, yaitu https://siperi.muhdavi.com dan http://trkj.pnl.ac.id, berdasarkan standar keamanan *OWASP Top 1*0. *Standar OWASP Top 10* mencakup sepuluh kategori utama kerentanan yang sering ditemukan dalam aplikasi web dan merupakan panduan penting dalam mengidentifikasi dan menangani masalah keamanan. Analisis ini mencakup pemeriksaan mendalam dari berbagai aspek keamanan, termasuk injeksi, autentikasi yang rusak, paparan data sensitif, dan lainnya. Perbandingan ini bertujuan untuk memberikan gambaran menyeluruh tentang sejauh mana masing-masing situs web mematuhi standar keamanan yang direkomendasikan dan mengidentifikasi area yang membutuhkan perbaikan lebih lanjut dapat dilihat pada tabel 5 perbandingan *http* dan *https*.

TabelV
hasil scanning menggunakan Nmap untuk website TRKJ dan SIPERI

No	Kategori Standar OWASP	Siperi	TRKJ
1	*A1: Injection*	Tidak	Tidak
2	*A2: Broken Authentication*	Tidak	Tidak
3	*A3: Sensitive Data Exposure*	Tidak	Ya (Sensitive files accessible, credentials sent in clear text)
4	*A4: XML External Entities (XXE)*	Tidak	Tidak
5	*A5: Broken Access Control*	Tidak	Tidak
6	*A6: Security Misconfiguration*	Tidak	Ya (Development configuration file, .htaccess readable)
7	*A7: Cross-Site Scripting (XSS)*	Tidak	Ya
8	*A8: Insecure Deserialization*	Tidak	Tidak
9	*A9: Using Components with Known Vulnerabilities*	Tidak	Ya (Vulnerable JavaScript library)
10	*A10: Insufficient Logging & Monitoring*	Tidak	Tidak
11	*A11: Cross-Site Request Forgery (CSRF)*	Tidak	Ya (HTML form without CSRF protection)
12	*A12: Clickjacking*	Ya (CSP frame-ancestors missing, X-Frame-Options header missing)	Ya (X-Frame-Options header missing)
13	*A13: Unsecure Cookie Configuration*	Ya (Cookies without HttpOnly flag)	Ya (Cookies without HttpOnly and Secure flag)

14	*A14: Password Management*	Ya (Password type input with auto-complete enabled)	Ya (Password type input with auto-complete enabled)
15	*A15: Denial of Service (DoS)*	Ya (Slow HTTP DoS)	Tidak
16	*A16: Unencrypted Connection*	Tidak	Ya (Unencrypted connection)
17	*A17: Sensitive Information Disclosure*	Tidak	Ya (Email addresses found)
18	*A18: Insecure Configuration Management*	Tidak	Ya (Possible sensitive files accessible)
19	*A19: Insufficient Subresource Integrity*	Tidak	Ya (Subresource Integrity not implemented)

Pada website siperi ditemukan beberapa kelemahan yang tidak terlalu banyak dibandingkan website TRKJ hal ini dapat dilihat pada tabel tabel 4.3 hasil scanning menggunakan Nmap untuk website HTTP. berikut penjelasan hasil temuan dari pengujian website siperi :

1) A12: *Clickjacking*

Situs ini memiliki kerentanan Clickjacking karena tidak adanya *header CSP frame-ancestors* dan *X-Frame-Options*. Hal ini memungkinkan situs lain menampilkan konten dari https://siperi.muhdavi.com dalam *iframe*, yang dapat menipu pengguna melakukan tindakan tanpa sepengetahuan mereka. Tindakan yang direkomendasikan adalah menambahkan *header X-Frame-Options* dengan nilai *DENY* atau *SAMEORIGIN*, dan mengimplementasikan *Content Security Policy (CSP)* yang ketat.

2) A13: *Unsecure Cookie Configuration*

Beberapa cookie tidak memiliki atribut *HttpOnly*, yang membuatnya rentan terhadap pencurian melalui skrip sisi klien. Tindakan yang direkomendasikan adalah memastikan semua *cookie* memiliki atribut *HttpOnly* dan *Secure*, sehingga hanya dapat diakses oleh server.

3) A14: *Password Management*

Input kata sandi memiliki atribut *auto-complete* yang diaktifkan. Ini meningkatkan risiko pencurian kata sandi jika perangkat pengguna jatuh ke tangan yang salah. Tindakan yang direkomendasikan adalah menonaktifkan *auto-complete* untuk input tipe kata sandi dengan menambahkan atribut a*utocomplete="off"*.

4) A15: Denial of Service (DoS)

Kerentanan ini menunjukkan kemungkinan serangan *Slow HTTP DoS*, yang dapat membuat server menjadi tidak responsif dengan menguras sumber daya. Tindakan yang direkomendasikan adalah mengimplementasikan batas waktu koneksi *HTTP*, penggunaan *firewall*, dan pemantauan trafik untuk mendeteksi dan mencegah serangan semacam ini.

Secara keseluruhan, https://siperi.muhdavi.com memiliki beberapa kelemahan yang dapat dieksploitasi, namun jumlahnya lebih sedikit dibandingkan dengan situs lainnya.

Website http://trkj.pnl.ac.id menunjukkan lebih banyak celah keamanan dibandingkan dengan https://siperi.muhdavi.com tabel 4.3 hasil scanning menggunakan Nmap untuk website HTTP. Salah satu masalah utama adalah penggunaan pustaka JavaScript yang rentan dan beberapa file konfigurasi yang dapat diakses publik seperti .htaccess dan composer.json. Hal ini memberikan penyerang informasi yang cukup untuk melakukan serangan yang lebih terarah. Selain itu, terdapat beberapa formulir HTML yang tidak memiliki perlindungan *CSRF*, memungkinkan serangan melalui pengiriman permintaan palsu atas nama pengguna yang sah. Pengiriman kredensial pengguna dalam teks biasa tanpa enkripsi (HTTP) sangat berisiko karena data dapat disadap selama transmisi. Juga, terdapat banyak file dokumentasi dan file sensitif lainnya yang dapat diakses publik, yang seharusnya dibatasi aksesnya. Berikut beberapa kelemahan lainnya dan penjelasan yang ditemukan pada website TRKJ :

1) *A2: Broken Authentication*

Kredensial pengguna dikirim dalam teks biasa tanpa enkripsi. Ini adalah masalah serius karena data dapat disadap selama transmisi. Tindakan yang direkomendasikan adalah menggunakan HTTPS untuk semua transmisi data dan mengimplementasikan enkripsi untuk kredensial pengguna.

2) *A3: Sensitive Data Exposure*

Beberapa file sensitif seperti *.htaccess, php.ini,* dan konfigurasi pengembangan dapat diakses publik. Ini memberikan informasi penting yang dapat dimanfaatkan oleh penyerang. Tindakan yang direkomendasikan adalah membatasi akses ke file-file ini atau menghapusnya dari direktori yang dapat diakses publik.

3) *A6: Security Misconfiguration*

Situs ini memiliki banyak file konfigurasi pengembangan yang dapat diakses publik. Hal ini menunjukkan bahwa server tidak dikonfigurasi dengan baik untuk keamanan. Tindakan yang direkomendasikan adalah memperketat izin file dan memastikan hanya pengguna yang sah yang dapat mengakses file konfigurasi.

4) *A7: Cross-Site Scripting (XSS)*

XSS memungkinkan penyerang menyuntikkan skrip berbahaya ke dalam halaman web. Tindakan yang direkomendasikan adalah melakukan validasi dan penyaringan input pengguna, serta menggunakan mekanisme escaping yang tepat untuk menghindari injeksi skrip.

5) *A9: Using Components with Known Vulnerabilities*

Situs ini menggunakan pustaka JavaScript yang rentan terhadap serangan. Tindakan yang direkomendasikan adalah memperbarui pustaka ke versi terbaru yang aman.

6) *A11: Cross-Site Request Forgery (CSRF)*

Beberapa formulir HTML tidak memiliki perlindungan *CSRF*. Ini memungkinkan penyerang mengirim permintaan palsu atas nama pengguna yang sah. Tindakan yang

direkomendasikan adalah mengimplementasikan token *CSRF* di setiap formulir.

7) A12: *Clickjacking*

Seperti situs sebelumnya, situs ini juga rentan terhadap *Clickjacking* karena tidak adanya header *X-Frame-Options*. Tindakan yang direkomendasikan adalah menambahkan header *X-Frame-Options* dengan nilai *DENY* atau *SAMEORIGIN*.

8) A13: Unsecure Cookie Configuration

Cookie tidak memiliki atribut *HttpOnly* dan *Secure*. Tindakan yang direkomendasikan adalah menetapkan atribut *HttpOnly* dan *Secure* pada semua *cookie* untuk melindungi data sensitif.

9) *A16: Unencrypted Connection*

Koneksi tidak dienkripsi, sehingga data dapat disadap selama transmisi. Tindakan yang direkomendasikan adalah menggunakan HTTPS untuk semua transmisi data.

10) *A17: Sensitive Information Disclosure*

Banyak alamat email ditemukan di berbagai halaman situs. Ini meningkatkan risiko serangan spam atau phishing. Tindakan yang direkomendasikan adalah mengaburkan alamat email atau menggunakan mekanisme perlindungan email.

11) *A18: Insecure Configuration Management*

Beberapa file sensitif seperti web.config dan .user.ini dapat diakses publik. Tindakan yang direkomendasikan adalah membatasi akses atau menghapus file sensitif dari direktori yang dapat diakses publik.

12) *A19: Insufficient Subresource Integrity*

Tidak ada integritas subresource yang diterapkan untuk memverifikasi keaslian sumber daya yang diunduh. Tindakan yang direkomendasikan adalah mengimplementasikan *Subresource Integrity (SRI)* untuk semua sumber daya eksternal.

13) *A20: Insufficient Content Security Policy (CSP)*

Situs ini tidak memiliki kebijakan keamanan konten yang diterapkan. Tindakan yang direkomendasikan adalah mengimplementasikan C*ontent Security Policy (CSP)* yang ketat untuk mencegah serangan *XSS* dan injeksi konten.

Secara umum, kedua situs memiliki kelemahan yang signifikan dalam hal keamanan. Namun, http://trkj.pnl.ac.id menunjukkan lebih banyak kelemahan dibandingkan dengan https://siperi.muhdavi.com. Masalah seperti pengiriman kredensial dalam teks biasa dan penggunaan pustaka yang rentan tidak ditemukan di https://siperi.muhdavi.com, yang menandakan bahwa situs ini sedikit lebih aman. Meski demikian, kedua situs memerlukan perbaikan segera dalam beberapa area untuk meningkatkan tingkat keamanan mereka secara keseluruhan.

Kedua situs memerlukan perhatian serius untuk mengatasi celah keamanan yang ditemukan. Situs https://siperi.muhdavi.com perlu fokus pada penanganan *serangan Slow HTTP DoS*, *Clickjacking*, dan pengaturan atribut *cookie*. Sementara itu, http://trkj.pnl.ac.id memerlukan perbaikan lebih luas yang mencakup pengamanan file konfigurasi, implementasi *CSRF*, dan pengamanan transmisi data. Implementasi kebijakan keamanan konten *(CSP)* dan penggunaan koneksi terenkripsi (HTTPS) sangat direkomendasikan untuk kedua situs guna mencegah serangan yang lebih canggih di masa mendatang.

IV. Kesimpulan

Penelitian ini melakukan perbandingan celah keamanan yang terdapat pada website Program Studi Teknologi Rekayasa Komputer Jaringan (TRKJ) dengan protokol HTTP dan website SIPERI dengan protokol HTTPS dengan menggunakan metode threat modelling dan standarisasi dari owasp. Pada website HTTP terdapat 13 jumlah kerentanan yang ditemukan dan pada website HTTPS sejumlah 4 kerentanan yang berhasil ditemukan.

Hasil analisis menunjukkan bahwa adanya kerentanan celah dari terbukanya akses informasi berdasarkan hasil pengujian dari sub direktori yang mungkin saja dari informasi tersebut dapat dieksploitasi oleh penyerang untuk mengakses data sensitif atau mengganggu fungsi normal dari website.

Pada website HTTPS dengan alamat https://siperi.muhdavi.com/ terdapat lebih sedikit celah keamanan atau kerentanan yang ditemukan berdasarkan pengujian menggunakan tools acunetix. Sedangkan pada website HTTP dengan alamat http://trkj.pnl.ac.id/ terdapat beberapa muncul celah keamanan informasi yang dapat digunakan untuk melakukan serangan kepada website atau mengacaukan sistem yang dapat mengakibatkan kerugian .

Walaupun terdapat kerentanan ataupun celah pada website HTTP dari segi keamanan serta kerahasian konfigurasi untuk database server lebih terjaga kerahasiaannya dibandingkan website HTTPS, ini dapat dilihat dari versi database disembunyikan oleh website TRKJ namun tidak dilakukan pada website siperi.

Referensi

[1] Dwiyanto, S., Rachmat, E., Sari, A. P., & Gustiawan, O. (2020). Implementasi Virtualisasi Server Berbasis Docker Container. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 165–175. https://doi.org/10.30656/prosisko.v7i2.2520

[2] Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://doi.org/10.30656/prosisko.v7i2.2522

[3] Faridi, M. K. (2021). *Pemodelan Ancaman pada Sistem E-Health Menggunakan Metode OWASP dan Metode DREAD*. https://dspace.uii.ac.id/ bitstream/handle/ 123456789/33162/17917115 Muhammad Khairul Faridi.pdf?sequence=1& isAllowed=y

[4] Hasibuan, A. F., & Handoko, D. (2023). Analisis Kerentanan Website Dengan Aplikasi Owasp Zap. *Jurnal Ilmu Komputer Dan Sistem Informasi*, *2*(2), 257–270. https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51

[5] Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

[6] Irfan Murti Raazi, Ima Dwitawati, & Putri Nabila. (2023). Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh. JINTECH: Journal Of Information Technology, 4(1), 1–15. https://doi.org/10.22373/jintech.v4i1.2409

[7] Kadarsih, K., & Andrianto, S. (2022). Membangun Website SMA PGRI Gunung Raya Ranau Menggunakan PHP dan MYSQL. *JTIM: Jurnal Teknik Informatika Mahakarya*, *03*(2), 37–44.

[8] Kholiq, A., & Khoirunnisa, D. (2019). Analisis Keamanan Wireless Local Area Network (WLAN) dengan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus: PT. Win Prima Logistik). *Jurnal Ilmiah Fakultas Teknik LIMITS*, *1*(1), 46–55. https://teknik.usni.ac.id/jurnal/ABDUL KHOLIQ.pdf

[9] Muhammad Anis Al Hilmi, Fauziah Herdiyanti, Renol Burjulius, & Sonty Lena. (2022). Pengujian Keamanan Sistem Operasi Linux Studi Kasus : Celah Keamanan FTP pada Metasploitable2. *IKRA-ITH Informatika : Jurnal Komputer Dan Informatika*, *8*(1), 110–115. https://doi.org/10.37817/ikraith-informatika.

[10] Mutedi, A., & Tjahjono, B. (2022). Systematic Literature Review: Preventing SQL Injection Attacks Using Tools OWASP CSR Web Application Firewall. *Maret*, *7*(1), 151–156. http://openjournal.unpam.ac.id/index.php/informatika

[11] Setiyadi, D. (2019). Structured Query Language (SQL) untuk Purchase Order (PO) menggunakan SQL Server. *Bina Insani ICT Journal*, *6*(1), 75–88.

[12] Susilawati, T., Yuliansyah, F., Romzi, M., & Aryani, R. (2020). Membangun Website Toko Online Pempek Nthree Menggunakan Php Dan Mysql. *Jurnal Teknik Informatika Mahakarya (JTIM)*, *3*(1), 35–44.

[13] Prayama, D., Yuhefizar, & Amelia Yolanda. (2021). Protokol HTTPS, Apakah Benar-benar Aman? Journal of Applied Computer Science and Technology, 2(1), 7–11. https://doi.org/10.52158/jacost.v2i1.118