ANALISIS KEAMANAN WEB DOMPET DHUAFA RIAU DENGAN MENGGUNAKAN PENETRATION TEST

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

DANY TRIA PUTRA RAMADHAN
12050316085

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2025

LEMBAR PERSETUJUAN

ANALISIS KEAMANAN WEB DOMPET DHUAFA RIAU DENGAN MENGGUNAKAN PENETRATION TEST

TUGAS AKHIR

Oleh:

DANY TRIA PUTRA RAMADHAN
12050316085

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 29 Desember 2025

Pembimbing I	Pembimbing II
Mona Fronita, M.Kom.	**Arif Marsal, Lc., MA.**
NIP. 198403032023212027	**NIP. 197608282009011011**

Ketua Program Studi

Angraini, S.Kom., M.Eng., Ph.D.
NIP. 198408212009012008

LEMBAR PENGESAHAN

ANALISIS KEAMANAN WEB DOMPET DHUAFA RIAU DENGAN MENGGUNAKAN PENETRATION TEST

TUGAS AKHIR

Oleh:

DANY TRIA PUTRA RAMADHAN
12050316085

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 9 Desember 2025

Pekanbaru, 9 Desember 2025
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Yuslenita Muda, S.Si., M.Sc.	**Angraini, S.Kom., M.Eng., Ph.D.**
NIP. 197701032007102001	**NIP. 198408212009012008**

DEWAN PENGUJI:

Ketua : **Eki Saputra, S.Kom., M.Kom.**

Sekretaris 1 : **Mona Fronita, M.Kom.**

Sekretaris 2 : **Arif Marsal, Lc., MA.**

Anggota 1 : **Angraini, S.Kom., M.Eng., Ph.D.**

Anggota 2 : **Zarnelly, S.Kom., M.Sc.**

Lampiran Surat :
Nomor : Nomor 25/2021
Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini:

Nama : Dany Tria Putra Ramadhan
NIM : 12050316085
Tempat/Tgl. Lahir : Tembilahan / 07 Desember 2001
Fakultas/Pascasarjana : Sains dan Teknologi
Prodi : Sistem Informasi

Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:
ANALISIS KEAMANAN WEB DEMPET DHUAFA RIAU DENGAN MENGGUNAKAN METODE PENETRATION TEST

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan ~~Disertasi/Thesis~~/Skripsi/~~Karya Ilmiah lainnya~~* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu ~~Disertasi/Thesis~~/Skripsi/~~Karya Ilmiah lainnya~~* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan ~~Disertasi/Thesis~~/Skripsi/(~~Karya Ilmiah lainnya~~)* saya tersebut, maka saya besedia menerima sanksi sesua peraturan perundang-undangan.

Demikianlah Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 15 JANUARY 2026
Yang membuat pernyataan

METERAI TEMPEL
10000
04311ANX242711A89

Dany Tria Putra Ramadhan
NIM : 12050316085

** pilih salah satu sesuai jenis karya tulis*

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan fakultas universitas. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 29 Desember 2025

Yang membuat pernyataan,

DANY TRIA PUTRA RAMADHAN

NIM. 12050316085

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur kehadirat Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas rahmat dan karunia-Nya yang telah diberikan tanpa ada kekurangan sedikitpun. Shalawat beserta salam tidak lupa kita ucapkan kepada Nabi junjungan kita yakni Nabi Muhammad *Salallahu Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu mendapat syafa'at di dunia maupun di akhirat nanti. *Aamiin Ya Rabbal 'Alaamiin*.

Persembahan kecil saya untuk kedua orang tua, ayah dan ibu. Ketika dunia menutup pintunya pada saya, mereka berdua membuka lengannya untuk saya. Ketika orang-orang menutup telinga mereka untuk saya, mereka berdua membuka hati untuk saya. Ketika saya kehilangan kepercayaan diri saya sendiri, mereka berdua merangkul dan memperbaiki semuanya. Tidak ada hentinya memberikan, doa, cinta, dorongan, semangat dan kasih sayang serta pengorbanan yang tak tergantikan oleh apapun dan siapapun. Saya ingin melakukan yang terbaik untuk setiap kepercayaan yang diberikan. Saya akan tumbuh menjadi yang terbaik yang saya bisa. Pencapaian ini adalah persembahan istimewa saya untuk ayah dan ibu. Teruntuk ayah semoga nikmat sehatmu selalu terjaga. Teruntuk ibu untuk semua doa, cinta, dan pengorbananmu, semoga Allah karuniakan surga terbaik untukmu.

Saya ucapkan terima kasih kepada Dosen Pembimbing, Penguji, dan Ketua Sidang Tugas Akhir yang telah memberikan bimbingan, masukan, dan arahan kepada saya dengan baik. Walaupun saya memiliki kekurangan dan keterbatasan. Dosen tetap memberikan pelajaran berupa pengalaman berharga yang belum pernah saya rasakan sebelumnya. Saya juga mengucapkan terima kasih kepada sahabat yang telah memberikan dukungan, semangat, dan juga pelajaran berharga dalam hidup saya selama ini. Kepada seluruh teman yang sudah membantu dalam menyelesaikan Tugas Akhir. Saya mendoakan yang terbaik untuk kesuksesan semua pihak yang sudah membantu.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, bersyukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini. Shalawat serta salam kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer di Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Pada penulisan Tugas Akhir ini, terdapat beberapa pihak yang sudah berkontribusi dan mendukung peneliti baik berupa materi, moril, dan motivasi. Peneliti ingin mengucapkan banyak terima kasih kepada:

1. Ibu Prof. Dr. Hj. Leny Nofianti, MS., SE., AK, CA sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Ibu Dr. Yuslenita Muda, S.Si., M.Sc sebagai Dekan Fakultas Sains dan Teknologi Univeritas Negeri Sultan Syarif Kasim Riau.
3. Ibu Angraini, S.Kom., M.Eng., Ph.D sebagai Ketua Program Studi Sis- tem Informasi sekaligus Dosen Penguji I yang telah meluangkan waktu dan memberikan arahan, saran, serta kritik dalam penyelesaian Tugas Akhir ini.
4. Bapak Anofrizen, S.Kom., M.Kom sebagai Penasihat Akademik yang telah meluangkan waktu dan memberi arahan kepada peneliti untuk dapat menyelesaikan Tugas Akhir dengan baik.
5. Ibu Mona Fronita, M.Kom sebagai Dosen Pembimbing 1 Tugas Akhir ini yang membimbing, dan memberikan motivasi, saran, dan nasihat kepada peneliti.
6. Bapak Arif Marsal, Lc., MA sebagai Dosen Pembimbing 2 Tugas Akhir ini yang membimbing, dan memberikan motivasi, saran, dan nasihat kepada peneliti.
7. Ibu Zarnelly, S.Kom., M.Sc sebagai Dosen Penguji II yang sudah meluangkan waktu, memberikan arahan, dan kritik dalam penyelesaian Tugas Akhir ini.
8. Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah banyak memberikan ilmunya kepada peneliti.
9. Terkhusus kepada ayah dan ibu tercinta atas segala doa dan dukungannya sehingga peneliti bisa bertahan pada masa studi dan menyelesaikan Pendidikan Strata 1 (S1).
10. Seluruh keluarga dan saudara, terima kasih atas doa dan dukungannya.

11. Diri sendiri yang mampu menguatkan dan meyakinkan tanpa jeda bahwa semuannya akan selesai pada waktunya.
12. Rekan peneliti yaitu Habib Indra Pratama yang menjadi titik awal terjadinya penelitian ini.
13. Rekan peneliti yang selalu mengingatkan dan sama-sama berjuang dalam masa perkuliahan.

Pengerjaan laporan ini terdapat banyak kesalahan dan kekurangan. Oleh karena itu, kritik dan saran dari pembaca yang membangun sangat diharapkan untuk kesempurnaan Laporan Tugas Akhir ini. Untuk itu, dapat menghubungi peneliti melalui *email* di 12050316085@students.uin-suska.ac.id. Semoga Laporan Tugas Akhir ini dapat memberikan sesuatu yang bermanfaat bagi siapa saja yang membacanya.

Pekanbaru, 29 Desember 2025

Penulis,

DANY TRIA PUTRA RAMADHAN

NIM. 12050316085

ANALISIS KEAMANAN WEB DOMPET DHUAFA RIAU DENGAN MENGGUNAKAN PENETRATION TEST

DANY TRIA PUTRA RAMADHAN
NIM: 12050316085

Tanggal Sidang: 9 Desember 2025
Periode Wisuda:

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

Perkembangan teknologi informasi pada era industri 4.0 mendorong meningkatnya penggunaan aplikasi berbasis web, namun juga diiringi oleh pertumbuhan serangan siber yang semakin kompleks. Kondisi ini menuntut setiap organisasi, termasuk Dompet Dhuafa Riau, untuk memastikan keamanan sistem informasi yang digunakan dalam pengelolaan dan penyaluran dana sosial. Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan, mengevaluasi tingkat keamanan, serta memberikan rekomendasi perbaikan pada situs web riau.dompetdhuafa.org melalui metode *penetration testing*. Pengujian dilakukan menggunakan tiga perangkat utama, yaitu *Zenmap*, *Sudomy*, dan *OWASP ZAP*. Hasil penelitian menunjukkan bahwa pada lapisan jaringan masih terdapat layanan yang berjalan tanpa enkripsi, seperti HTTP dan POP3, yang meningkatkan risiko penyadapan dan serangan *man-in-the-middle*. *Sudomy* mengungkapkan permukaan serangan yang luas melalui banyaknya parameter, URL, dan direktori internal yang dapat diakses publik. Sementara itu, *OWASP ZAP* menemukan sejumlah kelemahan pada lapisan aplikasi, termasuk ketiadaan token CSRF, absennya header keamanan utama, potensi XSS, *mixed content*, serta konfigurasi keamanan yang belum optimal. Secara keseluruhan, tingkat keamanan sistem berada pada kategori menengah–tinggi. Penelitian ini merekomendasikan penerapan enkripsi secara menyeluruh, hardening konfigurasi server, validasi dan sanitasi input, pembatasan akses direktori, serta penerapan header keamanan standar. Implementasi langkah-langkah tersebut diharapkan mampu meningkatkan ketahanan web Dompet Dhuafa Riau terhadap ancaman siber dan mendukung keberlangsungan layanan secara aman.

Kata Kunci: Aplikasi Web, Dompet Dhuafa Riau, Keamanan, Pengujian Penetrasi, Serangan Siber

SECURITY ANALYSIS OF DOMPET DHUAFA RIAU WEBSITE USING PENETRATION TESTING

DANY TRIA PUTRA RAMADHAN
NIM: 12050316085

Date of Final Exam: December 09rd 2025
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

The rapid development of information technology in the era of Industry 4.0 has driven the increasing use of web-based applications, accompanied by the growth of more complex cyberattacks. This condition requires every organization, including Dompet Dhuafa Riau, to ensure the security of information systems used in managing and distributing social funds. This study aims to identify potential vulnerabilities, evaluate the security level, and provide improvement recommendations for the website riau.dompetdhuafa.org through penetration testing. The testing was conducted using three main tools: Zenmap, Sudomy, and OWASP ZAP. The results revealed that at the network layer, several services still operate without encryption, such as HTTP and POP3, which increase the risk of eavesdropping and man-in-the-middle attacks. Sudomy exposed a wide attack surface through numerous parameters, URLs, and internal directories accessible to the public. Meanwhile, OWASP ZAP discovered several application-layer weaknesses, including the absence of CSRF tokens, missing security headers, potential XSS vulnerabilities, mixed content, and suboptimal security configurations. Overall, the system's security level is categorized as medium–high. The study recommends implementing comprehensive encryption, server configuration hardening, input validation and sanitization, directory access restrictions, and the adoption of standard security headers. These measures are expected to strengthen the resilience of Dompet Dhuafa Riau's website against cyber threats and support the secure continuity of its services.

Keywords: *Dompet Dhuafa Riau, Cyber Attacks, Penetration Testing, Web Application Security*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

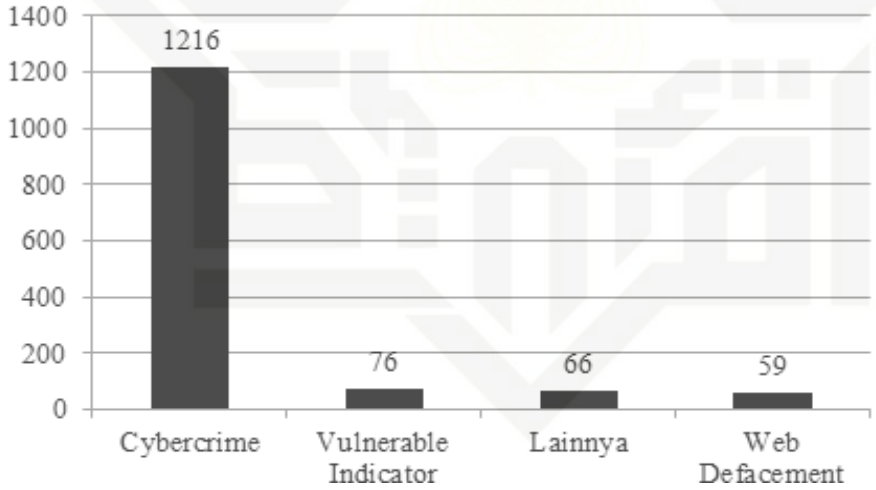
DAFTAR SINGKATAN

CSP	:	*Content Security Policy*
DAST	:	*Dynamic Application Security Testing*
Id-SIRTII/CC	:	*Indonesia Security Incident Respons Team On Internet*
	:	*Infrastructure/Coordination Center*
LAZ	:	Lembaga Amil Zakat
MASTG	:	*Mobile Application Security Testing Guide*
MOBSF	:	*Mobile Security Framework*
OWASP ZAP	:	*Open Web Application Security Project Zed Attack Proxy*
XSS	:	*Cross Site Scripting*
XXE	:	*XML External Entities*

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada era industri 4.0 sudah menjadi sebuah revolusi besar bagi perkembangan kehidupan manusia, yang dapat mempengaruhi dalam berbagai aspek dari ekonomi, pendidikan, sosial, serta kehidupan pribadi. Segala kemudahan yang di peroleh dari teknologi informasi tidak menutup kemungkinan memiliki dampak buruk bagi kehidupan, banyak orang yang memanfaatkan hal tersebut sebagai tindak kejahatan untuk mendapatkan kesenangan pribadi, beragam cara yang dilakukan para pelaku kejahatan yaitu dengan memanfaatkan keamanan dari jaringan komputer, keamanan menjadi aspek terpenting dalam suatu sistem agar tidak rentan terhadap *Cyber Attack*. Berdasarkan Id-SIRTII/CC (*Indonesia Security Incident Respons Team On Internet Infrastructure/Coordination Center*) pada Gambar 1.1 menunjukkan aduan siber yang diterima Tim Pusat Kontak Siber BSSN dengan kategori tertinggi selama tahun 2023.



Gambar 1.1. Kategori Tertinggi Aduan Siber 2023

Cybercrime menjadi jenis kriminalitas yang sangat merugikan perekonomian dengan perkiraan kerugian sebesar $575 miliar setiap tahunnya di seluruh dunia, Oleh karena itu meningkatnya *Cybercrime* diimbangi juga dengan lonjakan investasi baru-baru ini dalam teknologi baru untuk keamanan komputer di seluruh dunia dengan Istilah ”Keamanan *Cyber*” yang mengacu pada pendekatan dan prosedur untuk menjaga informasi digital (Perwej, Abbas, Dixit, Akhtar, dan Jaiswal, 2021).

Keamanan *Cyber* mengacu pada teknologi, teknik, dan prosedur yang digunakan untuk mencegah komputer, program, jaringan, dan data diretas, dirusak, atau diakses tanpa izin. Spesialis keamanan siber dan forensik semakin banyak menangani berbagai ancaman siber hampir secara real-time. Kemampuan untuk mendeteksi, menganalisis, dan mempertahankan diri dari ancaman-ancaman tersebut dalam kondisi hampir *real-time* tidak mungkin terjadi tanpa penggunaan intelijen ancaman, data besar, dan teknik pembelajaran mesin. Keamanan *Cyber* adalah praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan berbahaya. Ini juga dikenal sebagai keamanan teknologi informasi atau keamanan informasi elektronik (Perwej dkk., 2021).

Pengujian sistem keamanan aplikasi berbasis *website* adalah hal yang penting di era perkembangan aplikasi berbasis web yang melaju dengan pesat. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbagai teknik ancaman. Tingginya serangan keamanan yang dilakukan oleh seorang attacker sering menargetkan website yang bersifat publik, seperti sebuah website yang besifat sosial kemasyarakatan dibidang amal zakat. Oleh karena itu organisasi perlu melakukan asesmen pada aplikasi berbasis *website* agar organisasi mampu mendeteksi kerentanan dan memahami resiko yang dihadapi (Editya dan Mulyati, 2018).

Salah satu *website* lembaga amal yang bergerak dalam bidang sosial dan kemanusiaan di Provinsi Riau, Indonesia. yaitu Dompet Dhuafa Riau menggunakan Wordpress sebagai platform manajemen kontennya, hal ini menjadi krusial dikarenakan Dompet Dhuafa Riau itu sendiri menjadi pihak yang menyalurkan dana dari donatur kepada pihak yang membutuhkan menjadi rawan terhadap serangan siber dikarenakan Wordpress memiliki 92% kerentanan yang ditemukan di situs web yang didukung WordPress disebabkan oleh plugin pihak ketiga dan kesalahan pemrograman (Gupta, 2023).

Pada tahun 2020, Terdapat 582 kelemahan keamanan ditemukan di *core WordPress* dan tema serta plugin pihak ketiga ditemukan dengan melakukan identifikasi menggunakan penetration testing. Cross-site scripting vulnerabilities adalah yang paling umum, mencakup lebih dari 36,2% dari seluruh kerentanan baru yang ditemukan. 9,1% kerentanan disebabkan oleh SQL Injection, dan 6,5% disebabkan oleh *Cross-Site Request Forgery* (Gupta, 2023).

Terdapat metode efektif yang dikenal sebagai uji penetrasi yang bertujuan mengidentifikasi kerentanan dan kelemahan dalam sistem keamanan suatu situs web. Uji penetrasi (*penetrate'on testing*), juga dikenal sebagai uji penetrasi etis atau uji penetrasi keamanan, adalah proses evaluasi keamanan yang dilakukan secara sis-

tematis untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem komputer, jaringan, atau aplikasi (Alfaren dkk., 2022). Tujuan utama dari uji penetrasi adalah untuk mengetahui sejauh mana suatu sistem dapat bertahan dari serangan yang dilakukan oleh penyerang yang berpotensi memiliki niat jahat. Proses uji penetrasi melibatkan serangkaian langkah, mulai dari perencanaan, pengumpulan informasi, analisis kerentanan, eksploitasi, hingga pelaporan hasil.

Salah satu alat penetration testing yang dapat digunakan adalah OWASP ZAP, yang terfokus pada keamanan aplikasi web. OWASP ZAP, singkatan dari *Open Web Application Security Project Zed Attack Proxy*, adalah alat uji penetrasi yang sangat populer dan sering digunakan dalam pengujian keamanan aplikasi web. Alat ini bersifat *open-source*, yang berarti dapat diakses dan dimodifikasi oleh siapa saja sesuai kebutuhan (Hasibuan, Handoko, dkk., 2023). ZAP merupakan aplikasi untuk menemukan kerentanan dalam suatu aplikasi web dengan cara menyediakan scanner otomatis. Kelebihan dari ZAP ini di antaranya bersifat mudah diinstal, *community based*, *open source*, *intercepting proxy*, *traditional* & *ajax spider*, *active scanner*, *growing add ons*, *forced browsing*, *fuzzer*, *dynamic*, *smart card support*, *SSL cerificates*, *integrared*, dan *web socket support* (Rizkillah dan Astutik, 2023)

Penelitian ini diharapkan dapat memberikan peringatan dini bagi organisasi Dompet Dhuafa Riau dalam meningkatkan keamanan situs web mereka. Selain itu, penelitian ini juga akan berkontribusi pada pemahaman lebih lanjut tentang pentingnya metode uji penetrasi dalam menghadapi ancaman keamanan *cyber* saat ini. Melalui pemahaman yang lebih baik tentang ancaman keamanan *cyber* dan upaya perlindungan yang sesuai, Organisasi seperti Dompet Dhuafa Riau dapat melakukan kegiatan mereka dengan lebih aman. Demikian, penelitian ini memiliki dampak yang signifikan dalam menghadapi tantangan keamanan informasi yang terus berkembang di era digital ini.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penelitian ini adalah bagaimana tingkat keamanan *website* Dompet Dhuafa Riau dalam menghadapi ancaman *cyber* saat ini serta apa saja potensi ancaman keamanan yang mungkin dihadapi oleh *website* Dompet Dhuafa Riau.

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang perlu diperhatikan, di antaranya:

1. Pengujian penetration test hanya menggunakan *tools OWASP ZAP*, *Sudomy*, *Whois*, dan *Zenmap*.
2. Penelitian ini hanya untuk menganalisis kerentanan pada *website* Dompet

Dhuafa Riau.

3. Penelitian akan membatasi diri pada penggunaan metode uji penetrasi sebagai alat utama untuk mengidentifikasi kerentanan keamanan. Metode ini akan digunakan untuk mensimulasikan serangan yang mungkin dilakukan oleh penyerang asing, tanpa melibatkan serangan yang sebenarnya.

1.4 Tujuan

Tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengidentifikasi potensi kerentanan dan celah keamanan dalam situs web Dompet Dhuafa Riau.
2. Melakukan uji penetrasi untuk mengevaluasi tingkat keamanan saat ini.
3. Menyajikan rekomendasi perbaikan yang untuk meningkatkan keamanan web berdasarkan hasil OWASP ZAP.

1.5 Manfaat

Manfaat tugas akhir ini adalah:

1. Memberikan informasi mengenai keamanan *website*:
   Penelitian ini akan membantu Dompet Dhuafa Riau untuk melihat keamanan website mereka dengan mengidentifikasi kerentanan dan celah keamanan yang mungkin ada. Ini akan mengurangi risiko serangan *cyber*, pencurian data, dan potensi kerusakan yang dapat merugikan organisasi.
2. Kontribusi pada penelitian keamanan *cyber*:
   Penelitian ini juga dapat berkontribusi pada pemahaman lebih lanjut tentang keamanan *cyber* dalam konteks bisnis. Hasil penelitian ini dapat digunakan sebagai referensi oleh peneliti dan profesional keamanan *cyber* lainnya.

1.6 Sistematika Penulisan

Sistematika penulisan terbagi dalam empat bab, meliputi pendahuluan, landasan teori, metode penelitian, hasil dan pembahasan, dan penutup. Berikut penjelasan singkat ke empat bab tersebut:

BAB 1. PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB 2. LANDASAN TEORI

Pada bab ini menjelaskan teori-teori terkait landasan pelaksanaan penelitian, meliputi teori *website*, penetration testing dengan menggunakan *tools OWASP ZAP*, dan penelitian terdahulu yang relevan untuk mendukung penelitian ini.

BAB 3. METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara metodis proses penelitian, mencakup penjelasan-penjelasan tentang pendekatan penelitian, prosedur penelitian, keabsahan data, tempat dan waktu penelitian, narasumber, teknis analisis data penelitian, alat analisis data penelitian serta instrument penelitian. Tujuannya secara tidak langsung memberikan gambaran tentang ruang lingkup dan batasan penelitian kepada para pembaca.

BAB 4. ANALISA DAN HASIL

Pada bab ini menjelaskan mengenai data yang diperoleh dari proses pengujian keamanan website. Bab ini memuat uraian hasil pemindaian port layanan, hasil enumerasi struktur website, serta temuan kerentanan pada website. Dan juga bab ini menyajikan analisis tingkat risiko berdasarkan *OWASP Risk Rating Methodology* dan CVSS v3.1. Pembahasan dilakukan secara terstruktur dengan menginterpretasikan setiap temuan serta menghubungkannya dengan standar keamanan web, sehingga memberikan gambaran komprehensif mengenai kondisi keamanan *website* Dompet Dhuafa Riau.

BAB 5. PENUTUP

Bab ini berisi kesimpulan dari keseluruhan penelitian yang telah dilaksanakan, yang merangkum tingkat keamanan website berdasarkan hasil pengu- jian dan analisis. Selain itu, bab ini menyajikan rekomendasi perbaikan untuk meningkatkan keamanan sistem pada sisi jaringan maupun aplikasi, serta usulan langkah pengembangan bagi penelitian selanjutnya. Bab ini juga memuat keterbatasan penelitian untuk memberikan gambaran mengenai ruang lingkup dan kendala yang ditemui selama proses penelitian berlangsung.

BAB 2
LANDASAN TEORI

2.1 *Website*

Website merupakan kumpulan komponen yang terdiri dari teks, gambar, dan suara animasi, *website* menjadi media informasi yang menarik dan sangat dim- inati untuk dipergunakan sebagai media mengembangkan informasi. Teknologi *website* mengolah data menjadi sebuah informasi dengan cara mengidentifikasi, mengumpulkan, mengelola dan menyediakan untuk bisa diakses secara bersama-sama (Widagdo, Haviluddin, Setyadi, Taruk, dan Pakpahan, 2018).

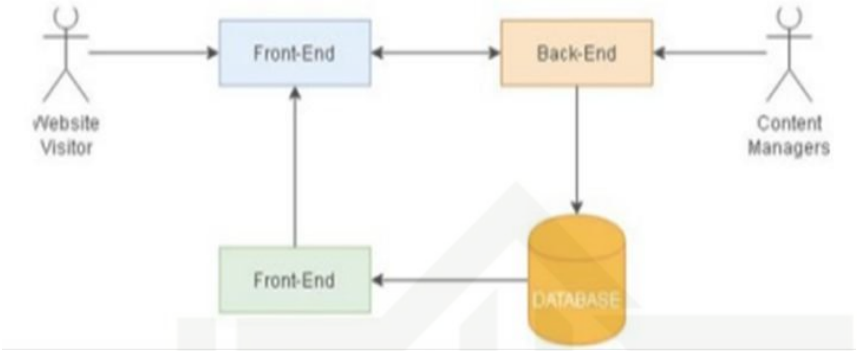
Terdapat dua konsep utama yang menjelaskan tentang situs web. Pertama, situs web merupakan kumpulan halaman yang memuat informasi dalam berbagai format seperti teks, gambar, animasi, dan suara. Halaman tersebut dapat memiliki sifat statis atau dinamis, dan terhubung membentuk sebuah struktur yang saling terkait dalam jaringan situs (Sharif, 2022). Kedua, aplikasi berbasis web merupakan jenis aplikasi yang dapat diakses melalui peramban web tanpa perlu proses instalasi, bergantung pada internet, dan tidak terikat pada sistem operasi. Fleksibilitasnya memungkinkan pengguna untuk mengakses dan memanfaatkan fungsinya secara daring (Wibowo, Nishom, dan Abidin, 2024).

Situs web sebagai kumpulan halaman dengan berbagai jenis informasi dapat memiliki karakteristik yang bervariasi dari statis hingga dinamis, serta terhubung membentuk struktur yang mengarah pada jaringan situs secara keseluruhan. Di sisi lain, aplikasi berbasis web tidak memerlukan instalasi dan dapat diakses melalui peramban web, memanfaatkan internet, dan tidak bergantung pada sistem operasi tertentu, memungkinkan pengguna untuk mengakses dan menggunakan layanannya secara *online* (Williams, 2020). Dua konsep ini memberikan gambaran tentang struktur dan fungsionalitas situs web serta aplikasi web berbasis browser dalam menyajikan informasi dan layanan secara daring kepada pengguna.

2.2 *Content Management System* (CMS)

Content Management System (CMS) adalah sistem yang digunakan untuk mengelola konten situs web. CMS adalah aplikasi komputer yang memungkin- kan penerbitan, pengeditan, modifikasi, dan pengorganisasian, penghapusan, dan pemeliharaan konten dari antarmuka pusat. CMS menyediakan prosedur untuk mengelola alur kerja dalam lingkungan kolaboratif. Biasanya, CMS terdiri dari dua elemen: Aplikasi Manajemen Konten (CMA) dan Aplikasi Pengiriman Konten (CDA). Di CMA, pengelola konten dapat mengelola pembuatan, modifikasi, dan

penghapusan konten dari situs web. Dalam CDA, situs web diperbarui untuk digunakan, dan elemen CDA mematuhi informasi untuk memperbarui situs web (Halim, Hebrard, Hartono, Halim, dan Russel, 2020).



Gambar 2.1. Cara Kerja Web CMS

Berdasarkan Gambar 2.1 dapat diketahui bahwasannya CMS dapat membuat, mengatur, mengedit, dan mempublikasikan konten ke website hanya dengan satu aplikasi yang diperlukan. Kegiatan CMS adalah pembuatan, penyimpanan, pengambilan, deskripsi, dan publikasi atau menampilkan berbagai jenis konten. Ada berbagai macam contoh CMS salah satunya adalah *WordPress*. *WordPress* merupakan contoh CMS berbasis web, pembuatannya memakai bahasa pemrograman PHP serta database nya menggunakan Mysql (Rahmah, Derta, Musril, dan Okra, 2022).

2.3 *Wordpress*

WordPress pada Gambar 2.2 adalah aplikasi web sumber terbuka berba- sis PHP dan SQL yang dibuat pada tahun 2003. Awalnya, ini dibuat sebagai sis- tem *blogging* tetapi dengan popularitas dan kemudahan penggunaannya itu dikembangkan lebih lanjut sebagai CMS situs web. *WordPress* bebas digunakan dan dimodifikasi untuk siapa saja tanpa biaya lisensi (FIRST, 2019).

Gambar 2.2. Logo *Wordpress*

Pembuat *WordPress* menggunakan teknologi terbaru untuk memastikan pengembangan sistem menyediakan fitur-fitur modern dan bekerja dengan lancar di setiap platform. Pengembang adalah memperbarui *plugin* secara berkala yang dapat dengan mudah ditambahkan ke situs dan memperluas penggunaannya. Juga, *Wordpress* memberikan fleksibilitas dalam memodifikasi kode dan menyesuaikannya. Sekali pengguna mengunduh paket instalasi, semua fitur dapat ditemukan di dalamnya dan ada diinstal secara manual (FIRST, 2019).

Baik itu pemula, pengembang menengah, atau pengguna yang lebih berpengalaman, *Wordpress* efektif untuk semua tingkat desainer dan pengembang. Pengguna menemukan banyak fitur berguna mengenai manajemen konten situs web. Pengelolaan konten efektif memantau lalu lintas sehingga menghasilkan analisis situs web yang lebih baik (Bhandari, 2020).

Berdasarkan statistik [isitwp] 60,4 persen pengembang menggunakan perangkat lunak *Wordpress* untuk membuat halaman website. Namun disayangkan dengan semakin tingginya pemanfaatan *website* semakin banyak pula serangan-serangan yang dilakukan oleh pihak yang tidak bertanggung jawab untuk men- curi informasi maupun untuk merusak integeritas suatu organisasi (Azis dan Yazid, 2021).

Pada tahun 2021 terdapat celah keamanan pada platform *website Wordpress* yakni CVE-2021-29447. Celah keamanan ini berupa kelemahan pada *Wordpress* versi 5.6 hingga 5.7 yang menggunakan PHP versi 8, dengan melakukan serangan XML *External Entity* (XXE). Menurut *National Vulnerability Database* di Amerika, kerentanan pada CVE ini berada pada nilai 6,5 yang berarti level kerentanannya adalah medium, namun menurut perusahaan Github kerentanan pada CVE-2021-29447 berada pada tingkat high dengan nilai 7,1. Hal ini menunjukkan bahwa kerentanan pada CVE ini masuk ke dalam kategori berbahaya dan sangat direkomendasikan untuk segera dilakukan perbaikan (Azis dan Yazid, 2021).

2.4 *Penetration Testing*

Penetration testing adalah upaya yang dilakukan secara sah untuk mengeksploitasi sistem komputer dengan tujuan membuat sistem tersebut menjadi aman (Hidayatulloh dan Saptadiaji, 2021). *Penetration testing* yang dilakukan dengan baik dapat menghasilkan rekomendasi untuk mengatasi dan memperbaiki masalah yang ditemukan selama pengujian.

Penetration testing adalah serangkaian proses yang melibatkan prosedur dan teknik untuk mengevaluasi keamanan sistem komputer atau jaringan dengan melakukan simulasi penyerangan (Ashari, Affandi, Putra, dan Nur, 2023). Tujuan

utamanya adalah untuk mengidentifikasi potensi kerentanan dalam sistem sehingga celah-celah keamanan tersebut dapat ditemukan dan kemudian ditutup atau diperbaiki. *Penetration testing* dilakukan sebagai langkah preventif untuk mengatasi risiko peretasan pada suatu sistem (Wibowo dkk., 2024).

2.5 OWASP

Open Web Application Security Project (OWASP) adalah sebuah *framework* yang bersifat *open source* dengan fokus utama pada perbaikan keamanan perangkat lunak aplikasi (Idris, Syarif, dan Winarno, 2022). OWASP merupakan sebuah organisasi yang didedikasikan untuk menemukan dan mengatasi kerentanan keamanan dalam aplikasi web. Berdasarkan standar yang dikeluarkan oleh OWASP, ada sebelas langkah yang dapat dilakukan untuk menilai dan menguji keamanan pada sebuah *website*, termasuk *Information Gathering*, *Configuration Management*, *Secure Transmission*, *Authentication*, *Session Management*, *Authorization*, *Cryptography*, *Data Validation*, *Denial of Service*, dan *Error Handling*. Langkah-langkah ini membantu dalam mengidentifikasi dan mengatasi celah keamanan yang mungkin ada dalam aplikasi web sehingga dapat meningkatkan tingkat keamanan secara keseluruhan (Guntoro, Costaner, dan Musfawati, 2020).

Menurut (Mulyanto, Haryanti, dan Jumirah, 2021), *Open Web Applica- tion Security Project* (OWASP) adalah sebuah organisasi internasional nirlaba yang didirikan oleh *Open Web Application Security Project* (OWASP) Foundation pada tanggal 21 April 2004 di Amerika Serikat. Fokus utama dari OWASP adalah meningkatkan keamanan perangkat lunak dan berkomitmen untuk membantu organisasi dalam pengembangan, perolehan, operasi, dan pemeliharaan aplikasi yang dapat dipercaya, dengan tujuan memastikan keamanan dalam pembuatan dan pengembangan aplikasi. Misi OWASP adalah melindungi perangkat lunak sehingga individu dan organisasi dapat membuat keputusan yang tepat terkait dengan risiko keamanan.

2.6 OWASP ZAP

OWASP ZAP adalah alat berbasis Java yang hadir dengan antarmuka grafis intuitif, memungkinkan penguji keamanan aplikasi web untuk melakukan *fuzzing*, *scripting*, *spidering*, dan *proxy* untuk menyerang aplikasi web (Williams, 2020). OWASP ZAP dapat memeriksa kelemahan yang dapat menjadi target serangan dari *hacker* supaya dapat merusak fungsi dari *website*, kemudian dengan *Com- mon Vulnerability Scoring System* hal ini dapat di gunakan agar mengetahui tingkatan kerentanan berupa nilai yang menggambarkan tingkatan kerentanan *low*, *medium*, *high*, *critical* supaya dapat membantu suatu organisasi untuk memberi nilai

kerentanan pada website dan tindakan apa yang harus di ambil selanjutnya (Reza, 2022).

OWASP ZAP dapat digunakan sebagai aplikasi mandiri atau sebagai proses daemon. *OWASP ZAP* (*Zed Attack Proxy)* digunakan secara luas dalam pengujian penetrasi untuk menemukan kerentanan atau celah keamanan dalam aplikasi *web-site*, dan menyediakan fitur pemindaian otomatis yang berguna dalam proses ini (Guntoro dkk., 2020). OWASP ZAP adalah perangkat sumber terbuka, yang berarti bahwa siapa pun dapat mengakses, menggunakan, dan berkontribusi pada pengembangan alat ini. Hal ini menjadikannya salah satu alat yang sangat berharga dalam mengidentifikasi dan mengatasi kerentanan keamanan pada aplikasi web (Editya dan Mulyati, 2018).

Gambar 2.3. Logo *Software OWASP ZAP*

Adapun ancaman yang dapat diidentifikasi oleh OWASP ZAP yang tertera pada Gambar 2.3 sebagai berikut:

1. *Cloud Metadata Potentially Exposed*
   Kerentanan Serangan *Metadata Cloud* berupaya menyalahgunakan server NGINX yang tidak dikonfigurasi dengan benar untuk mengakses metadata instans yang dikelola oleh penyedia layanan *cloud* seperti AWS, GCP, dan Azure. Semua provider ini menyediakan metadata melalui alamat IP internal yang tidak dapat dirutekan ini dapat diekspos oleh server NGINX yang tidak dikonfigurasi dengan benar dan diakses dengan menggunakan alamat IP ini di bidang *header host* (Sugara dan Sriyasa, 2024).
2. *PII Disclosure*
   PII disclosure merujuk pada pengungkapan *Personally Identifiable Information* (Informasi Identitas Pribadi). PII adalah setiap data yang dapat digunakan untuk mengidentifikasi seseorang secara spesifik. *PII disclosure* terjadi ketika informasi-informasi tersebut diungkapkan, baik secara sengaja maupun tidak sengaja, kepada pihak yang tidak berwenang atau publik umum (Goyat dkk., 2020).

3. *Absence of Anti-CSRF Tokens*

   Serangan berbasis *Absence Of Anti-CSRF Tokens* yang terdeteksi melalui aplikasi OWASP-ZAP. Serangan *Cross Site Request Forgery* (CSRF) dapat terjadi disebabkan karena tidak adanya mekanisme perlindungan terhadap token keamanan (*request token*) pada sebuah *website*, sehingga penyerang dapat mengirim suatu request (sumbit suatu form) secara illegal. Serangan CSRF dapat sukses dilakukan dengan memaksa pengguna untuk melakukan permintaan mengubah data seperti profil pribadi, alamat *email*, dan bahkan yang lebih berbahaya adalah melakukan transfer dana (Hasibuan dkk., 2023).

4. *Content Security Policy* (CSP) *Header Not Set*

   Content Security Policy (CSP) adalah lapisan keamanan tambahan yang membantu mendeteksi dan memitigasi jenis serangan tertentu, termasuk *Cross Site Scripting* (XSS) dan serangan injeksi data. Serangan-serangan ini digunakan untuk segala hal mulai dari pencurian data hingga perusakan situs atau distribusi *malware*. CSP menyediakan serangkaian header HTTP standar yang memungkinkan pemilik situs web mendeklarasikan sumber konten yang disetujui dan boleh dimuat oleh *browser* di halaman tersebut - tipe yang tercakup adalah JavaScript, CSS, bingkai HTML, font, gambar, dan objek yang dapat disematkan seperti applet Java, ActiveX, file audio dan video (Sugara dan Sriyasa, 2024).

5. *Missing Anti-clickjacking Header*

   Missing anti clickjacking header adalah sebuah keretanan yang mengakibatkan *website* dapat terserang serangan *clickjacking*. Serangan ini bertujuan untuk mengelabui user agar mengklik sesuatu yang sebenarnya tidak diinginkan oleh *user*. Bahayanya, identitas pribadi seperti *email* dan *password* bisa dicuri melalui teknik penyerangan ini. Untuk menghindari hal tersebut diperlukan HTTP header tambahan yaitu *X-Frame-Option*, *X Frame Option* berfungsi untuk menjaga keamanan dari serangan sejenis *Clickjacking* yaitu dengan mengnonaktifkan *iframe* atau *object* didalam *website* (Hasibuan dkk., 2023).

6. *Cookie No HttpOnly Flag*

   Keretanan dari *Cookie No HttpOnly Flag* dapat menyebabkan terjadinya serangan *Cross Site Scripting* (XSS), kebocoran dari *Cookie* juga dapat menyebabkan penyerang dengan mudah mengakses *Cookie* dan menggunakan ini sebagai media mencari tahu atau mengambil informasi sensitif yang terkandung dalam *Cookie* (Hasibuan dkk., 2023).

7. *Cookie Without Secure Flag*

   Cookie Without Secure Flag mengacu pada penggunaan cookie HTTP tanpa mengaktifkan *flag* "*Secure*". Ini adalah masalah keamanan web yang dapat membuat *cookie* rentan terhadap intersepsi oleh pihak yang tidak berwenang. Penggunaan *cookie* tanpa *flag secure* memungkinkan penyerang untuk mencuri informasi otentikasi pengguna, yang dapat digunakan un- tuk mengambil alih sesi pengguna atau melakukan serangan impersonasi (Squarcina, Tempesta, Veronese, Calzavara, dan Maffei, 2020).

8. *Cokkie Without SameSite Attribute*

   Cookie adalah mekanisme penyimpanan data kecil yang digunakan oleh situs web untuk menyimpan informasi di browser pengguna. Atribut *SameSite* adalah fitur keamanan yang diperkenalkan untuk mengontrol bagaimana *cookies* dikirim dalam permintaan lintas situs (*cross-site requests*). *Cookies* tanpa atribut SameSite dapat menyebabkan risiko keamanan, terma- suk serangan *Cross-Site Request Forgery* (CSRF). Atribut *SameSite* memberikan lapisan perlindungan tambahan dengan membatasi bagaimana *cookies* dikirim dalam konteks lintas situs (Bashir, Arshad, Kirda, Robertson, dan Wilson, 2019).

9. *Cross-Domain Javascript Source File Inclusion*

   Cross-Domain JavaScript Source File Inclusion mengacu pada praktik memuat file JavaScript dari domain yang berbeda dengan domain asal halaman web. Ini adalah teknik umum dalam pengembangan web modern, tetapi juga membuka vektor serangan potensial jika tidak diimplementasikan dengan benar (Darwis, Musdar, dkk., 2022).

10. *Server Leaks Information via "X-Powered-By" HTTP Response Header Filed(s)*

    Server web/aplikasi sedang bocor informasi melalui satu atau lebih headerrespon HTTP "*X-Powered-By*". Akses terhadap informasi semacam itu dapat memudahkan penyerang mengidentifikasi kerangka kerja/komponen lain yang dibutuhkan oleh aplikasi web dan kerentanannya terhadap komponen-komponen tersebut (Rizkillah dan Astutik, 2023).

11. *Strict-Transport-Security Header Not Set*

    Strict Transport Security (HSTS) adalah mekanisme keamanan web yang dirancang untuk melindungi situs web dan pengguna dari serangan *downgrade protocol* dan *cookie hijacking*. Ketika *website* belum mengaktifkan *Strict-Transport-Security Header* sebagai mekanisme keamanan server *website*, untuk mendorong browser menggunakan koneksi HTTPS yang aman. Ko-

munikasi antara pengguna dan *website* terdapat celah yang dimanfaatkan penyerang untuk penyadapan. Celah pada *website* ini berpotensi terkena serangan *Man-in-the-Middle* (Darmawan, Naibaho, dan De Kweldju, 2024).

12. *Timestamp Disclosure – Unix*

    Timestamp Disclosure – Unix merupakan kerentanan yang disebabkan oleh tampilnya informasi *timestamp unix* pada *browser*. Kerentanan ini dapat dimanfaatkan oleh penyerang sebagai sarana pengumpulan informasi untuk melakukan serangan. Verifikasi dilakukan dengan cara memeriksa *timestamp* yang tampil mengandung informasi penting atau tidak secara man- ual. Masalah kerentanan ini bisa diabaikan jika *timestamp* yang ditampilkan tidak kritis, jika tidak *code program* pada sistem harus dimodifikasi untuk tidak mengungkapkan informasi *timestamp* (Hasibuan dkk., 2023).

13. *X-Content-Type-Options Header Missing*

    Header Anti-MIME-Sniffing X-Content-Type-Options tidak disetel ke '*nosniff* '. Ini memungkinkan versi *Internet Explorer* dan *Chrome* yang lebih lama untuk melakukan *sniffing MIME* pada badan respons, yang berpotensi menyebabkan badan respons ditafsirkan dan ditampilkan sebagai tipe konten selain tipe konten yang dideklarasikan. *Firefox* versi saat ini (awal 2014) dan lawas akan menggunakan tipe konten yang dideklarasikan (jika ada yang disetel), daripada melakukan *sniffing MIME* (Purba, Amandha, Purnama, dan Ikhwan, 2022).

14. *Charset Mismatch*

    Pemeriksaan ini mengidentifikasi respons yang mana Header Jenis Konten HTTP mendeklarasikan sebuah karakter himpunan yang berbeda dari himpunan karakter yang ditentukan oleh isi HTML atau XML. Jika ada ketidakcocokan set karakter antara header HTTP dan konten, Ketidakcocokan pengkodean karakter dapat menyebabkan masalah keamanan serius, termasuk potensi untuk serangan injeksi dan *bypass* mekanisme sanitasi input (Ashari dkk., 2023).

15. *Information Disclosure – Suspicious Comments*

    Halaman ini berisi satu atau beberapa komentar yang dapat mengungkapkan informasi sensitif kepada penyerang. Kerentanan ini memungkinkan penyerang untuk melihat informasi yang seharusnya tidak dapat diakses atau data yang bukan milik mereka. Ada banyak cara untuk menemukan celah ini. Dan ada juga banyak jenis data yang dapat diekspos secara illegal (Ashari dkk., 2023).

16. *Modern Web Application*

    Modern Web Application menunjukkan bahwa aplikasi web target memiliki karakteristik tertentu yang umumnya terkait dengan praktik pengembangan web kontemporer.

17. *Re-examine Cache-control Directives*

    Dalam konteks arahan periksa ulang *cache-control*, disarankan untuk menetapkan *header HTTP cache-control* sebagai '*no-cache*, *no-store*, *must-revalidate*' untuk konten yang memerlukan keamanan yang lebih tinggi. Bila aset perlu di-*cache*, sebaiknya pertimbangkan untuk menggunakan arahan '*public*, *max-age*, *immutable*'. Konfigurasi *cache-control* ini secara kolektif memainkan peran penting dalam memperkuat perlindungan konten sensitif dan meningkatkan posisi keamanan secara keseluruhan (Fernandez, Hureau, Duda, dan Korczynski, 2024).

18. *Session Management Response Identified*

    Session Management Response Identified mengacu pada temuan keamanan yang menunjukkan masalah atau kelemahan dalam manajemen sesi pada sebuah aplikasi web. Bagaimana aplikasi web menangani sesi pengguna, seperti pembuatan, pemeliharaan, dan penghancuran sesi. Kesalahan dalam manajemen sesi dapat menyebabkan serangan serius, seperti *session hijacking*, *session fixation*, atau *cross-site request forgery* (CSRF).

19. *User Controllable HTML Element Attribute* (*Potential XSS*)

    User Controllable HTML Element Attribute (*Potential XSS*) adalah jenis kerentanan yang terjadi ketika pengguna dapat mengontrol atau memasukkan nilai ke dalam atribut elemen HTML, yang kemudian diproses oleh aplikasi tanpa validasi atau sanitasi yang memadai. Ini dapat membuka jalan bagi serangan *Cross-Site Scripting* (XSS), di mana penyerang dapat menyisipkan kode berbahaya yang dieksekusi di browser korban. Serangan ini dapat digunakan untuk mencuri data sensitif, seperti *cookie* pengguna, melakukan serangan *phishing*, atau mengendalikan sesi pengguna (Sharif, 2022).

2.7 *Sudomy*

Sudomy adalah alat bantu untuk enumerasi subdomain yang membantu mengumpulkan subdomain dan menganalisis domain melalui proses rekognisi otomatis. Selain itu, alat ini dapat digunakan untuk kegiatan OSINT (*Open-Source Intelligence*) (Ramadhan, Aresta, dan Hariyadi, 2020).

Sudomy merupakan tools yang digunakan untuk pencacahan subdomain dan

menganalisis domain dengan melakukan pengintaian secara otomatis, pencacahan ini menggunakan dua metode yaitu pasif dan aktif. Metode pasif yaitu memanfaatkan pihak ketiga, seperti menggunakan web API, sedangkan metode aktif yaitu menggunakan aplikasi yang sudah terinstall (Reza, 2022).

Pengembangan aplikasi *Information Gathering* mengikuti kaidah ISSAF dengan menerapkan dua teknik, yaitu *passive* dan *active*. Teknik *passive* memperoleh informasi melalui berbagai cara dengan memanfaatkan sumber daya pihak ketiga seperti Web API, pustaka Information Gathering, atau OSINT Source dengan proses scraping (Hariyadi dan Fazlurrahman, 2019). Sementara itu, teknik *active* menggunakan aplikasi terinstal dengan fitur serupa, melibatkan fungsi *Information Gathering* melalui *brute force, wordlists*, atau metode baru lainnya.

Dengan menyaring situs pihak ketiga yang digunakan, proses enumerasi DNS dapat dilakukan secara efektif dan efisien. Hal ini memungkinkan penghasilan hasil yang lebih banyak dengan waktu yang lebih singkat. Sebagai contoh, *Sudomy* tidak mengandalkan sumber daya mesin pencari seperti Google, Baidu, Ask, Yahoo, dan Bing karena hasilnya cenderung kurang maksimal dan terdapat faktor lain seperti terhambat oleh captcha (Ramadhan dkk., 2020).

2.8 *Whois*

Whois adalah protokol kueri yang digunakan untuk mengakses basis data registrasi yang menyimpan informasi terkait nama domain, alamat IP, dan *Autonomous System Number* (ASN). Informasi yang diperoleh mencakup data *registrant*, *registrar*, *nameserver*, hingga tanggal pendaftaran domain. Dalam praktiknya, Whois banyak dimanfaatkan pada tahap information gathering untuk mengidentifikasi profil awal target sebelum dilakukan pemindaian lebih lanjut. Namun, penelitian terbaru menunjukkan bahwa data *Whois* sering kali tidak konsisten, terutama jika dibandingkan dengan protokol modern seperti RDAP, sehingga perlu kehati-hatian dalam penggunaannya (Fernandez dkk., 2024).

2.9 *Zenmap*

Zenmap adalah antarmuka grafis dari *Network Mapper* (Nmap), memudahkan visualisasi hasil pemindaian jaringan dengan menghadirkan fungsionalitas seperti penyimpanan profil, perbandingan hasil scan, dan peta topologi jaringan. *Tools* ini memungkinkan administrator jaringan dan keamanan professional untuk melakukan po*rt scanning*, *host discovery*, *service detection*, dan *vulnerability assessment* melalui antarmuka visual yang intuitif. *Zenmap* dilengkapi dengan fitur *Network Topology* yang dapat menampilkan struktur jaringan dalam bentuk grafis, memudahkan analisis hubungan antar host dan identifikasi potensi celah keamanan

dalam infrastruktur jaringan (Chhillar dan Shrivastava, 2021).

2.10 Keamanan *Website*

Keamanan suatu *website* adalah prioritas utama bagi pengelola dan pengguna situs. Seringkali, pengguna hanya mempertimbangkan desain tampilan dan konten untuk menarik pengunjung, tanpa memperhatikan aspek keamanan. Namun, mengabaikan keamanan *website* dapat berdampak serius pada pengguna sendiri, karena data penting dalam *website* dapat diretas atau tampilan *website* dapat dimodifikasi oleh pihak yang tidak berwenang. Keamanan *website* yang baik adalah melindungi komputer, aplikasi, dan jaringannya untuk menjaga keamanan informasi yang terdapat di dalamnya. Dengan demikian, penting untuk memahami bahwa keamanan bukan hanya tanggung jawab pengelola, tetapi juga setiap pengguna yang berinteraksi dengan *website* tersebut (Mulyanto dkk., 2021).

Menurut (Editya dan Mulyati, 2018), keamanan adalah salah satu aspek utama dalam konteks sistem jaringan internet. Pada dasarnya, internet dibangun melalui jaringan komputer yang saling terhubung. Dalam hal ini, jumlah pengguna yang terhubung dalam suatu jaringan memiliki dampak signifikan terhadap keamanan data dan informasi yang dikirim dan diterima. Keamanan informasi menjadi krusial karena dapat rentan terhadap berbagai serangan dan potensi penyalahgunaan data. Oleh karena itu, menjaga keamanan dalam lingkungan internet menjadi suatu keharusan yang tidak bisa diabaikan yang dijelaskan pada Tabel 2.1.

2.11 *Tools* Yang Digunakan

Berikut adalah beberapa keunggulan *tools* yang dimiliki antara OWASP ZAP, dan *Sudomy*:

Tabel 2.1. *Tools* Penguji Keamanan *Website*

No	Tools	Fungsi	Keunggulan
1.	OWASP ZAP	1. Pemindaian Keamanan Aplikasi Web. 2. Manajemen Sesi Pengguna. 3. Pemantauan Lalu Lintas HTTP. 4. Pemecah Sandi Otomatis.	1. Mendukung uji penetrasi aplikasi web dengan berbagai fitur. 2. Memiliki *Graphical User Interface* (GUI) yang ramah pengguna. 3. Dapat diintegrasikan dengan alat lain dan otomatis. 4. Terus diperbarui oleh komunitas OWASP.

Tabel 2.1. *Tools Penguji Keamanan* Website

No	*Tools*	Fungsi	Keunggulan
2.	*Sudomy*	1. Pemindaian Subdomain. 2. Pemetaan Infrastruktur. 3. Analisis Pasif Subdomain.	1. Pemindaian Cepat dan Efisien. 2. Dukungan untuk Pemindaian Subdomain pasif. 3. Integrasi dengan beberapa Sumber Data.
3.	*Zenmap*	1. Pemindaian Port dan Layanan. 2. Deteksi Sistem Operasi Target. 3. Analisa Keamanan Berbasis Jaringan. 4. Analisa Keamanan Berbasis Jaringan	1. Antarmuka grafis dari *Nmap* yang memudahkan penggunaan. 2. Menyediakan visualisasi hasil pemindaian jaringan 3. Mendukung berbagai profil pemindaian dari sederhan hingga lanjutan. 4. Banyak digunakan dalam administrasi dan uji penetrasi.

2.12 Analisis dan Penilaian Risiko Keamanan

2.12.1 *OWASP Risk Rating Methodology*

Analisis dan penilaian risiko keamanan adalah proses sistematis untuk mengidentifikasi, mengukur, dan menprioritaskan risiko yang mengancam aset informasi. Tujuan utamanya adalah menentukan tingkat ancaman terhadap kerahasiaan, integritas, dan ketersediaan serta menyediakan dasar prioritas untuk tindakan mitigasi dan pengendalian.

Metode penilaian risiko yang digunakan pada penelitian ini mengacu pada *OWASP Risk Rating Methodology* (untuk konteks aplikasi web) yang dipadukan dengan metrik kuantitatif dari CVSS v3.1 untuk memperkuat objektivitas penilaian (Williams, 2020).

Dalam praktiknya, penilaian risiko dirancang sebagai kombinasi antara penilaian kualitatif (OWASP) dan penilaian kuantitatif (CVSS/score). Langkah umum yang dilakukan meliputi:

1. Identifikasi risiko
2. Penilaian kemungkinan (*likelihood*)
3. Penilaian dampak (*impact*)
4. Penghitungan skor akhir

5. Klasifikasi tingkat risiko
6. Rekomendasi mitigasi

Metode ini sejalan dengan panduan manajemen risiko yang dikeluarkan lembaga standar seperti NIST, yang menekankan pentingnya pengukuran *likelihood* dan *impact* dalam proses risiko (Br Ginting dan Simanjorang, 2024).

1. Penilaian Kemungkinan (*Likelihood*)

   Likelihood menilai seberapa besar kemungkinan kerentanan dapat dieksploitasi dan setiap sub-faktor diberi nilai 0–10 berdasarkan tingkat kemudahan atau kesulitannya, kemudian dirata-rata untuk mendapatkan skor *likelihood* (Williams, 2020). Menurut OWASP, *likelihood* dihitung dari beberapa sub-faktor seperti Tabel 2.2:

Tabel 2.2. Sub-faktor Penilaian *Likelihood*

Sub-faktor	Deskripsi
Ease of discovery	Seberapa mudah kerentanan ditemukan.
Ease of exploit	Seberapa mudah kerentanan dieksploitasi.
Awareness	Apakah exploit/CVE sudah publik dan diketahui luas.
Intrusion detection	Aktivitas eksploitasi terdeteksi oleh sistem.

2. Penilaian Dampak (*Impact*)

   Impact mengukur konsekuensi apabila kerentanan dieksploitasi. Dampak dinilai terhadap tiga aspek teknis utama: *Confidentiality*, *Integrity*, dan *Availability*. Masing-masing aspek diberi nilai 0–10 dan hasil akhirnya dihitung sebagai rata-rata ketiga nilai tersebut pada Tabel 2.3. Penggunaan metrik CIA konsisten dengan skema dasar CVSS v3.1 (FIRST, 2019).

Tabel 2.3. Aspek Penilaian Dampak (*Impact*)

Aspek	Penjelasan
Confidentiality	Dampak terhadap kerahasiaan data apabila bocor.
Integrity	Dampak terhadap keaslian atau modifikasi data.
Availability	Dampak terhadap ketersediaan sistem

3. Penghitungan Skor Akhir (*Final Risk Score*)

   Skor akhir (*final score*) dihitung menggunakan rumus sederhana pada 2.1:

$$Risk\ Score = \frac{Likelihood \times Impact}{2}$$

4. Klasifikasi Tingkat Risiko

   Hasil skor ini kemudian diklasifikasikan ke dalam tingkat risiko berikut pada Tabel 2.4:

Tabel 2.4. Klasifikasi Tingkat Risiko

Rentang Nilai	Kategori Risiko
0.0 – 3.9	*Low*
4.0 – 6.9	*Medium*
7.0 – 8.9	*High*
9.0	*Critical*

   Untuk meningkatkan validitas, hasil skor akhir juga dibandingkan dengan nilai *CVSS Base Score* apabila kerentanan tersebut memiliki CVE (*Common Vulnerabilities and Exposures*) (Williams, 2020).

5. Klasifikasi dan Prioritas Risiko

   Setelah skor akhir diperoleh, setiap temuan risiko diklasifikasikan dan diprioritaskan untuk perbaikan. Urutan prioritas umumnya dimulai dari *critical*, kemudian *high, medium*, dan terakhir *low*.

2.12.2 CVSS v3.1 (*Common Vulnerability Scoring System*)

CVSS versi 3.1 adalah sistem standar global yang digunakan untuk memberikan skor kuantitatif terhadap tingkat keparahan kerentanan keamanan perangkat lunak. CVSS dikembangkan oleh *Forum of Incident Response and Security Teams* (FIRST) dan digunakan secara luas dalam pelaporan keamanan, termasuk oleh NVD (*National Vulnerability Database*).

1. Komponen Utama CVSS v3.1

   (a) *Base Metric*

   Menilai karakteristik kerentanan yang tidak berubah di seluruh lingkungan, meliputi:

   i. *Attack Vector* (AV): seberapa jauh penyerang dapat melakukan eksploitasi.
   ii. *Attack Complexity* (AC): tingkat kesulitan serangan.
   iii. *Privileges Required* (PR): hak akses yang dibutuhkan.
   iv. *User Interaction* (UI): apakah serangan memerlukan interaksi pengguna.
   v. *Impact Metrics* (C,I,A): dampak pada *confidentiality*, *intergrity*, *availability*.

(b) *Temporal metrics*

Mengukur aspek yang berubah seiring waktu (misalnya ketersediaan *exploit* atau *patch*).

(c) *Enviromental Metrics*

Menyesuaikan nilai berdasarkan konteks organisasi, sepertu kepentingan asset yang terdampak.

2. Skala Penilaian CVSS v3.1

Skor CVSS v3.1 seperti pada Tabel 2.5 menggambarkan tingkat keparahan kerentanan secara kuantitatif, dengan rentang nilai antara 0,0 hingga 10,0. Semakin tinggi skor yang diperoleh, semakin besar pula risiko dan dampak yang ditimbulkan oleh kerentanan tersebut (FIRST, 2019).

Tabel 2.5. Skala Penilaian CVSS v3.1

Nilai CVSS	Kategori Risiko	Keterangan Umum
0.0	*None*	Tidak ada risiko atau kerentanan tidak berpengaruh terhadap keamanan.
0.1 – 3.9	*Low*	Risiko rendah; dampak kecil dan sulit dieksploitasi.
4.0 – 6.9	*Medium*	Risiko sedang; dapat dieksploitasi dengan kondisi tertentu.
7.0 – 8.9	*High*	Risiko tinggi; mudah dieksploitasi dan dapat menyebabkan gangguan signifikan.
9.0 – 10.0	*Critical*	Risiko sangat tinggi; kerentanan dapat dieksploitasi dengan mudah dan menimbulkan dampak besar.

2.12.3 Penelitian Terdahulu

Peneliti dalam studi ini menyuguhkan beberapa penelitian sebelumnya sebagai acuan analisis dan untuk memperkaya kajian literatur.

Penelitian yang dilakukan oleh Ghozali, dkk (2019), penelitian ini fokus pada penerapan metode asesmen risiko dalam konteks sistem informasi harga komoditas utama yang dikembangkan oleh PT. Gitsolution. Sistem ini memiliki peran penting dalam menyediakan informasi harga pokok yang berpengaruh pada kehidupan sehari-hari, dan digunakan oleh salah satu instansi pemerintah di Indonesia. Untuk mengukur tingkat risiko dalam sistem informasi harga komodi- tas utama ini, penelitian ini menerapkan Metode *Open Web Application Security Project* (OWASP) *Risk Rating* untuk mengidentifikasi potensi kerentanan keamanan pada aplikasi berbasis website. Hasil penelitian menghasilkan dua faktor pent- ing, yaitu Likelihood (Kemungkinan) dan Impact (Dampak), yang digunakan untuk mengevaluasi risiko. Dari kombinasi kedua faktor ini, ditemukan tiga tingkat re-

siko, yaitu *risk severity high*, *risk severity medium*, dan *risk severity low*. Temuan hasil penilaian risiko ini memberikan wawasan yang berharga bagi para pengelola dan pengembang sistem, memungkinkan mereka untuk menyadari risiko potensial yang mungkin timbul, serta memungkinkan pengambilan tindakan proaktif untuk mencegah dan mengatasi risiko tersebut.

Penelitian yang dilakukan oleh Wicaksono, dkk (2020), tentang Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing dan DAST. Penelitian ini bertujuan untuk mengidentifikasi celah keamanan pada situs web menggunakan Metode *Penetration Test dan Dynamic Application Security Testing* (DAST). Celah keamanan yang diuji khususnya melibatkan *Broken Access Control*, *Cross Site Scripting* (XSS), dan *SQL Injection*. Setelah identifikasi celah keamanan, upaya perbaikan dilakukan pada situs web. Hasil pengujian menunjukkan bahwa celah keamanan *Broken Access Control* dapat dicegah dengan membuat kode (id) yang sulit ditebak. Untuk mencegah XSS, langkah-langkah dilakukan dengan mengkonversi data ke entitas karakter saat pengguna memasukkan sintaks JavaScript. Selain itu, untuk mencegah *SQL Injection*, disarankan untuk menggunakan fungsi "*escape ()*" saat melakukan pencarian pada basis data.

Penelitian yang dilakukan oleh Rosaliah, dkk (2021), pengujian celah keamanan *website* SIM menggunakan Metode OWASP TOP 10, yang mencakup tes terhadap sepuluh kerentanan keamanan umum, seperti *Injection* (SQLMap), *Broken Authentication* (Hydra), S*ensitive Data Exposure* (Dirb), *Broken Access Control* (Burp Suite), *XML External Entities - Burp Suite* (XXE), *Security Misconfiguration*, (*SSLScan dan Heartbleed Bug*),(*Cross Site Scripting - manual* dan *Burp Suite*), *Insecure Deserialization* (*Burp Suite*), penggunaan komponen dengan kerentanan yang diketahui (*Metasploit Framework*), dan ketidakcukupan *logging* dan monitoring (*Metasploit Framework*). Temuan utama meliputi celah keamanan *Broken Authentication*, *Sensitive Data Exposure*, dan *Security Misconfiguration*, dengan tambahan temuan *clickjacking* yang tidak termasuk dalam TOP 10 OWASP.

Penelitian yang dilakukan oleh Fachri, dkk (2021), tentang Analisis Keamanan Webserver Menggunakan *Penetration Test*. Pengujian penetrasi ini dilakukan pada web server yang merupakan Sistem Informasi Akademik pada perguruan tinggi. Metode yang digunakan dalam penelitian ini mencakup *information gathering, vullnerability assessmant, gaining acces, maintaining acces, clearing track.* Hasil penelitian menampilkan bahwa terdapat empat kelemahan pada web server yaitu *level high*, empat kelemahan *level medium*, dan dua kerentanan dengan *level low*. Ditemukannya beberapa port yang masih terbuka dalam web server yang menyebabkan peretas dengan mudah masuk kedalam sistem untuk mengekploitasi

informasi yang terdapat dalam Sistem Informasi Akademik. Hasil ujicoba simulasi serangan terhadap sistem berhasil masuk dengan mendapatkan *username* dan *password*.

Penelitian yang dilakukan oleh Erbeliza (2023), tujuan penelitian ini ialah untuk menganalisis dan mengidentifikasi kerentanan atau celah keamanan yang dapat merugikan penyedia dan pengguna aplikasi *mobile commerce Jakmall* berbasis Android dengan *Mobile Security Framework* (MOBSF) dan *OWASP Mobile Application Security Testing Guide* (MASTG). Penelitian ini dilaksanakan dengan 5 (lima) tahapan yaitu *Preparation* (persiapan), *Intelligence Gathering* (pengumpulan data), *Mapping the Application* (memetakan kerentanan), *Exploitation* (eksploitasi), dan *Reporting* (laporan). Hasil penelitian mendapatkan bahwa aplikasi *mobile commerce Jakmall* memiliki isu celah keamanan dalam cakupan *Data Storage* pada parameter (MSTG-STORAGE-5) dan dalam cakupan *Authentication Architectures* pada parameter (MSTG-AUTH-5 dan MSTG-AUTH-6) seperti pada Tabel 2.6.

Tabel 2.6. Perbandingan Penelitian Terdahulu

Peneliti	Hasil Penelitian	Komentar
Bahrun Ghozali, Kusrini Kusrini, Sudarmawan Sudarmawan(2019)	Hasil penelitian mengidentifikasi tingkat risiko berdasarkan faktor *Likelihood* dan *Impact*, menghasilkan tiga tingkat risiko: *high*, *medium*, dan *low*. Temuan ini memberikan wawasan berharga untuk pengelola dan pengembang sistem, memungkinkan pengambilan tindakan proaktif untuk mencegah dan mengatasi risiko keamanan. Penelitian ini berkontribusi pada pengelolaan risiko keamanan sistem informasi krusial di tingkat pemerintahan.	Dari penelitian tersebut, peneliti hanya menggunakan satu metode yaitu OWASP ZAP, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.
Bagus Wicaksono, Rr. Yuliana Rachmawati Kusumaningsih, Catur Iswahyudi(2020)	Pada pengujian celah keamanan dengan metode DAST pada *website* bagusw.win, termasuk *Cross-Site scripting*, *Broken Access Control*, dan *SQL Injection*, berhasil teridentifikasi. Evaluasi hasil pengu- jian menunjukkan bahwa website tersebut rentan terhadap serangan XSS, di mana input-an skrip dapat dieksekusi.	Dalam penelitian tersebut mengungkapkan bahwasannya *SQL Injection* termasuk kedalam kelemahan *website* yang di analisis, na- mun pada hasilnya tidak da- pat ditemukan kerentanan dari *database* yang di identifikasi.

Tabel 2.6. Perbandingan Penelitian Terdahulu

Peneliti	Hasil Penelitian	Komentar
	Selain itu, celah keamanan dalam *Bro- ken Access Control* juga terungkap, memungkinkan penyerang dengan mudah menebak *ID user* lain. Terakhir, pengujian *SQL Injection* menghasilkan *error* pada query database, yang dapat diatasi dengan menambahkan metode "escape ()" pada query tersebut. Evaluasi ini membuka peluang untuk memperbaiki celah keamanan melalui langkah yang telah diidentifikasi, seperti mengubah input sebelum diakses ke database dan memperkuat kontrol akses.	
Fahmi Fachri, Abdul Fadlil, Imam Riadi(2021)	Tentang keamanan web server melalui *penetration test* menemukan empat kelemahan tingkat tinggi, empat tingkat menengah, dan dua tingkat rendah pada Sistem Informasi Akademik perguruan tinggi. Temuan mencakup keberadaan port terbuka yang memudahkan peretas untuk masuk dan mengeksploitasi informasi. Uji coba simulasi serangan berhasil mendapatkan username dan password, menyoroti kerentanan signifikan dalam keamanan web server.	Temuan ini memberikan dasar untuk perbaikan dan penguatan keamanan sistem. Dari penelitian tersebut,peneliti hanya menggunakan satu metode yaitu *SQL Lite*, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.
Yum Thurfah Afifa Rosaliah, Jayanta Jayanta, Bayu Hananto (2021)	Penelitian ini menemukan beberapa celah keamanan signifikan, termasuk masalah pada *Broken Authentication*, *Sensitive Data Exposure*, dan *Security Misconfiguration*, mengindikasikan ketidakamanan dalam otentikasi, perlindungan data sensitif, dan konfigurasi keamanan. Selain itu, temuan tambahan melibatkan celah keamanan *Clickjacking*, menunjukkan adanya kerentanan tambahan yang perlu diperhatikan dan diatasi.	Dari penelitian tersebut, penelitihanya menggunakan satu metode yaitu OWASP ZAP, tanpa melakukan perbandingan dengan metode penetration testing yang lainnya, sehingga dampak yang lain tidak maksimal

Tabel 2.6. Perbandingan Penelitian Terdahulu

Peneliti	Hasil Penelitian	Komentar
Shaqila Erbeliza (2023)	Hasil penelitian ini menggunakan *Mo- bile Security Framework* (MOBSF) dan *OWASP Mobile Application Security Testing Guide* (MASTG) untuk menganal-isis keamanan aplikasi *mobile commerce Jakmall* berbasis Android. Hasilnya me-nunjukkan adanya celah keamanan pada bagian *Data Storage* (MSTGSTORAGE-5) dan *Authentication Architectures* (MSTG-AUTH-5 dan MSTG-AUTH-6). Temuan ini memberikan wawasan pent-ing untuk perbaikan keamanan aplikasi Jakmall.	Dari penelitian tersebut, peneliti hanya menggu-nakan satu metode yaitu OWASP ZAP dan MASTG, tanpa melakukan per-bandingan dengan metode penetration testingyang lain-nya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.

BAB 3
METODOLOGI PENELITIAN

3.1 Alur Penelitian

Penelitian ini terdiri dari lima tahapan untuk menganalisis kerentanan keamanan pada situs web Dompet Dhuafa Riau. Tahapan tersebut meliputi, perencanaan analisis *website*, metode pengumpulan data, pengujian kerentanan web, metode analisis dan penilaian risiko dan, hasil serta rekomendasi perbaikan. Alur penelitian ini ditampilkan pada Gambar 3.1.

Gambar 3.1. Alur Penelitian

3.2 Perencanaan Analisis *Website*

Penelitian ini melakukan *penetration testing* terkontrol terhadap domain riau.dompetdhuafa.org: (1) memuat mengenai ruang lingkup dan batasan pengujian; (2) *reconnaissance* menggunakan *Whois* untuk verifikasi metadata domain serta *Sudomy* untuk enumerasi subdomain; (3) *discovery* layanan menggunakan *Zenmap*/*Nmap* untuk memetakan port dan versi layanan secara non-intrusif; (4) pemindaian kerentanan aplikasi menggunakan *OWASP ZAP* dengan penyimpanan report dan PoC non-destruktif; (5) konsolidasi hasil dan rekomendasi perbaikan, verifikasi silang, klasifikasi temuan berdasarkan OWASP Top 10, dan penentuan level risiko.

3.3 Metode Pengumpulan Data

Untuk melakukan penelitian ini penulis menggunakan 2 metode untuk mengumpulkan data yaitu, sebagai berikut:

3.3.1 Observasi

Dalam penelitian ini, Metode pengumpulan data dilakukan dengan teknik observasi menggunakan beberapa *tools* untuk memperoleh informasi dasar tentang target. Observasi ini meliputi penggunaan *Whois* untuk mengetahui detail domain, serta *Sudomy* untuk enumerasi subdomain. Hasil observasi kemudian menjadi dasar untuk tahap scanning dan analisis kerentanan menggunakan *Zenmap*/*Nmap* dan *OWASP ZAP*.

3.3.2 Studi Literatur

Studi literatur digunakan sebagai penyusun kerangka teori penelitian dan perbandingan hasil penelitian sebelumnya. Adapun studi literatur yang dilakukan pada penelitian ini bersumber dari beberapa referensi antara lain jurnal, *proceeding*, buku, tugas akhir, dan media digital seperti internet maupun *website*.

3.4 Pengujian Kerentanan Web

3.4.1 *Port & Service Scanning*

Fungsi pengujian *port* dan *service scanning* menggunakan *Zenmap* adalah untuk memetakan host dalam jaringan, mendeteksi port yang terbuka beserta layanan dan versinya, sehingga memudahkan identifikasi potensi kerentanan serta membantu administrator maupun peneliti keamanan dalam menganalisis dan memperkuat sistem.

3.4.2 *Vulnerability Testing*

Pengujian kerentanan dilakukan menggunakan aplikasi *OWASP ZAP*, di mana proses pengujian mencakup penentuan URL situs web sebagai target utama. *OWASP ZAP* kemudian melakukan pemindaian otomatis untuk menjelajahi dan mengidentifikasikan potensi kerentanan *website* yang menjadi target.

3.5 Metode Analisis dan Penilaian Risiko Keamanan

Setelah proses pemindaian dan pengujian kerentanan dilakukan menggunakan *Zenmap*, *Sudomy*, dan *OWASP ZAP*, langkah berikutnya adalah menganalisis tingkat risiko dari setiap temuan. Penilaian risiko pada penelitian ini mengacu pada *OWASP Risk Rating Methodology* yang dikombinasikan dengan pedoman *Common Vulnerability Scoring System* (CVSS v3.1). Setiap temuan dikelompokkan berdasarkan kategori OWASP Top 10:2021 untuk menentukan tingkat keparahan dan prioritas mitigasi.

Penilaian risiko dilakukan dengan menghitung nilai *Likelihood* (kemungkinan eksploitasi) dan *Impact* (dampak terhadap sistem). Nilai akhir ditentukan menggunakan persamaan 3.1 dan untuk hasil skor akan dikategorikan berdasarkan tingkat risiko *OWASP* seperti yang dapat dilihat pada Tabel 3.1. Proses ini menghasilkan klasifikasi risiko yang digunakan pada tahap selanjutnya untuk menyusun rekomendasi perbaikan sistem keamanan web.

$$RiskScore = \frac{Likelihood \times Impact}{2}$$

Tabel 3.1. Klasifikasi Tingkat Risiko

Rentang Nilai	Kategori Risiko
0.0 – 3.9	Rendah
4.0 – 6.9	Sedang
7.0 – 10.0	Tinggi

3.6 Hasil dan Rekomedasi Perbaikan

Berdasarkan hasil pengujian yang dilakukan terhadap situs riau.dompetdhuafa.org menggunakan tiga alat utama, yaitu *Zenmap*, *Sudomy*, dan *OWASP ZAP*, diperoleh temuan bahwa sistem masih memiliki sejumlah kerentanan yang tergolong dalam klasifikasi *OWASP Top* 10:2021. Temuan tersebut mengindikasikan adanya kelemahan pada aspek konfigurasi keamanan, enkripsi data, serta penggunaan komponen perangkat lunak yang rentan.

Secara keseluruhan, tingkat risiko yang teridentifikasi berada pada kategori rendah hingga tinggi, dengan risiko tertinggi disebabkan oleh penggunaan layanan tidak terenkripsi dan komponen yang sudah tidak diperbarui. Oleh karena itu, rekomendasi perbaikan difokuskan pada penerapan pembaruan sistem dan patch keamanan secara berkala, penggunaan protokol aman (HTTPS/TLS versi terbaru), penerapan *security headers* untuk mencegah serangan berbasis web, serta pembatasan akses terhadap port dan layanan yang tidak diperlukan. Dengan implementasi langkah-langkah mitigasi tersebut, diharapkan tingkat keamanan situs dapat meningkat dan potensi eksploitasi terhadap sistem dapat diminimalkan secara signifikan.

BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian keamanan yang dilakukan terhadap *website* riau.dompetdhuafa.org dengan memanfaatkan tiga perangkat utama *Zenmap*, *Sudomy*, dan OWASP ZAP maka dapat disimpulkan sebagai berikut:

1. Identifikasi Potensi Kerentanan dan Celah Keamanan
   Penelitian ini berhasil mengidentifikasi berbagai potensi kerentanan dan celah keamanan pada sisi jaringan dan aplikasi web. Pada lapisan jaringan, ditemukan layanan yang masih berjalan tanpa enkripsi, sedangkan pada lapisan aplikasi ditemukan kelemahan konfigurasi keamanan, eksposur endpoint dan parameter publik, serta tidak diterapkannya beberapa mekanisme proteksi standar. Temuan ini menunjukkan bahwa sistem masih memiliki permukaan serangan yang cukup luas.
2. Evaluasi Tingkat Keamanan Melalui Uji Penetrasi
   Hasil uji penetrasi menunjukkan bahwa tingkat keamanan *website* berada pada kategori menengah hingga tinggi. Meskipun layanan HTTPS dan IMAPS telah diterapkan, konfigurasi TLS belum sepenuhnya mengikuti standar keamanan terbaru. Selain itu, hasil pemindaian *Sudomy* dan *OWASP ZAP* menunjukkan adanya kelemahan seperti absennya anti-CSRF token, *header* keamanan (*CSP*, *HSTS*, *X-Content-Type-Options*, dan *X-Frame-Options*), serta penggunaan *mixed content*, yang berpotensi dimanfaatkan untuk serangan seperti *man-in-the-middle*, *injection*, *clickjacking*, *Cross-Site Scripting* (XSS), dan kebocoran informasi teknis.
3. Rekomendasi Perbaikan Keamanan Web
   Berdasarkan hasil pengujian menggunakan OWASP ZAP dan *tools* pendukung lainnya, penelitian ini menghasilkan rekomendasi perbaikan berupa penerapan enkripsi secara konsisten, penguatan konfigurasi TLS, *hardening server* dan aplikasi, validasi dan sanitasi data masukan, pembatasan akses terhadap direktori dan endpoint internal, serta penerapan *header* keamanan standar. Selain itu, disarankan pula pelaksanaan pemantauan, patching, dan evaluasi keamanan secara berkala guna meningkatkan ketahanan sistem terhadap ancaman keamanan siber secara berkelanjutan.

5.2 Saran

Berikut beberapa saran yang dapat diterapkan untuk meningkatkan keamanan sistem *website* Dompet Dhuafa Riau berdasarkan hasil uji keamanan:

1. Pembaruan Komponen dan *Library*

   Pengelola sistem disarankan untuk melakukan pembaruan rutin terhadap *library* dan *framework* yang digunakan agar terhindar dari eksploitasi terhadap komponen yang sudah diketahui memiliki celah keamanan (*vulnerable components*).

2. Penerapan *Security Header* dan CSP

   Implementasikan *security header* seperti *Content-Security-Policy*, *Strict-Transport-Security*, *X-Frame-Options*, dan *X-Content-Type-Options* untuk mencegah serangan berbasis browser seperti *XSS*, *Clickjacking*, dan *MIME sniffing*.

3. Penguatan Konfigurasi Server

   Nonaktifkan port atau layanan yang tidak esensial, gunakan enkripsi TLS/SSL, serta pastikan semua layanan yang berjalan dilengkapi autentikasi yang kuat sesuai dengan pedoman NIST SP 800-53 Rev.5.

4. Pemantauan dan Pengujian Berkala

   Lakukan pemindaian keamanan secara periodik menggunakan OWASP ZAP dan *Nmap*, serta terapkan sistem pemantauan *log* dan audit untuk mendeteksi aktivitas mencurigakan secara dini.

Dengan penerapan langkah-langkah tersebut, tingkat keamanan situs Dompet Dhuafa Riau diharapkan meningkat secara signifikan serta mampu menjaga kerahasiaan, integritas, dan ketersediaan data secara berkelanjutan.

DAFTAR PUSTAKA

Alfaren, G., dkk. (2022). Analisis serangan penetration testing: Sebuah review sistematik. *JIIFKOM (Jurnal Ilmiah Informatika dan Komputer)*, *1*(2), 21–26.

Ashari, I., Affandi, M., Putra, H. T., dan Nur, M. T. (2023). Security audit for vulnerability detection and mitigation of upt integrated laboratory (ilab) it-era website based on owasp zed attack proxy (zap). *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, *7*(1), 24–34.

Azis, R., dan Yazid, S. (2021). Pengujian kerentanan website wordpress dengan menggunakan penetration testing untuk menghasilkan website yang aman. *Jurnal Restikom: Riset Teknik Informatika Dan Komputer*, *3*(3), 93–105.

Bashir, M. A., Arshad, S., Kirda, E., Robertson, W., dan Wilson, C. (2019). A longitudinal analysis of the ads. txt standard. Dalam *Proceedings of the internet measurement conference* (hal. 294–307).

Bhandari, M. (2020). Comparison of wordpress, joomla and drupal.

Br Ginting, E. R., dan Simanjorang, M. M. (2024). Pengaruh kepercayaan diri (self confidence) terhadap hasil belajar matematika siswa.

Chhillar, K., dan Shrivastava, S. (2021). Vulnerability scanning and management of university computer network. Dalam *2021 10th international conference on internet of everything, microwave engineering, communication and networks (iemecon)* (hal. 01–06).

Darmawan, C., Naibaho, J. P. P., dan De Kweldju, A. (2024). Penerapan metode vulnerability assessment untuk identifikasi keamanan website berdasarkan owasp id tahun 2021. *Edumatic: Jurnal Pendidikan Informatika*, *8*(1), 272–281.

Darwis, E., Musdar, I. A., dkk. (2022). Analisis kerentanan website renovac- tion menggunakan rangkaian security tools project berdasarkan framework owasp. *KHARISMA Tech*, *17*(1), 1–15.

Editya, G. H., dan Mulyati, S. (2018). Aplikasi mobile one time password menggunakan algoritma md5 dan sha1 untuk meningkatkan keamanan website. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *1*(2), 618–623.

Fernandez, S., Hureau, O., Duda, A., dan Korczynski, M. (2024). Whois right? an analysis of whois and rdap consistency. Dalam *International conference on passive and active network measurement* (hal. 206–231).

FIRST, E. (2019). *Common vulnerability scoring system version 3.1: Specification document*. FIRST.

Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M. K., Thomas, R., . . . Kim, T.-H. (2020). Blockchain-based data storage with privacy and authentication in internet of things. *IEEE Internet of Things Journal*, *9*(16), 14203–14215.

Guntoro, G., Costaner, L., dan Musfawati, M. (2020). Analisis keamanan web server open journal system (ojs) menggunakan metode issaf dan owasp (studi kasus ojs universitas lancang kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45–55.

Gupta, D. (2023). A critical review of wordpress security scanning tools and the development of a next-generation solution.

Halim, E., Hebrard, M., Hartono, H., Halim, K. O., dan Russel, W. (2020). Exploration wordpress as e-commerce rad-cms for smes in indonesia. Dalam *2020 international conference on information management and technology (icimtech)* (hal. 818–823).

Hariyadi, D., dan Fazlurrahman, F. (2019). Membangun telegrambot untuk crawling malware osint menggunakan raspberry pi. *Indonesian Journal of Business Intelligence (IJUBI)*, *2*(1), 18–24.

Hasibuan, A. F., Handoko, D., dkk. (2023). Analisis keretanan website dengan aplikasi owasp zap. *Jurnal Ilmu Komputer dan Sistem Informasi*, *2*(2), 141–154.

Hidayatulloh, S., dan Saptadiaji, D. (2021). Penetration testing pada website universitas ars menggunakan open web application security project (owasp). *Jurnal Algoritma*, *18*(1), 77–86.

Idris, M., Syarif, I., dan Winarno, I. (2022). Web application security education platform based on owasp api security project. *EMITTER international journal of engineering technology*, 246–261.

Mulyanto, Y., Haryanti, E., dan Jumirah, J. (2021). Analisis keamanan website sman 1 sumbawa menggunakan metode vulnerability asesement: Analisis keamanan website sman 1 sumbawa menggunakan metode vulnerability asesement. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *3*(3), 394–400.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., dan Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669–710.

Purba, P. M., Amandha, A. C., Purnama, R. H., dan Ikhwan, A. (2022). Anal- isis keamanan website prodi sistem informasi uinsu menggunakan metode application scanning. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(4), 325–329.

Rahmah, Z., Derta, S., Musril, H. A., dan Okra, R. (2022). Perancangan website

eduji menggunakan cms wordpress. *Intellect: Indonesian Journal of Learning and Technological Innovation, 1*(2), 205–218.

Ramadhan, R. A., Aresta, R. M., dan Hariyadi, D. (2020). Sudomy: information gathering tools for subdomain enumeration and analysis. Dalam *Iop conference series: Materials science and engineering* (Vol. 771, hal. 012019).

Reza, V. A. (2022). *Pemindai kerentanan terhadap website jago masak dengan metode pengujian penetrasi owasp zap* (Unpublished doctoral dissertation). UNIVERSITAS BINA DARMA.

Rizkillah, M., dan Astutik, F. (2023). Analisis kerentanan web server pada aplikasi elearning (studi kasus universitas muhammadiyah mataram). *Journal of Information Technology and System Integration, 1*(1), 1–7.

Sharif, M. H. U. (2022). Web attacks analysis and mitigation techniques. *International Journal of Engineering Research & Technology (IJERT)*, 10–12.

Squarcina, M., Tempesta, M., Veronese, L., Calzavara, S., dan Maffei, M. (2020). Can i take your subdomain? exploring related-domain attacks in the modern web. *arXiv preprint arXiv:2012.01946*.

Sugara, V. I., dan Sriyasa, I. W. (2024). Analisis keamanan web menggunakan open web application security web (owasp). *The Indonesian Journal of Computer Science*, *13*(2).

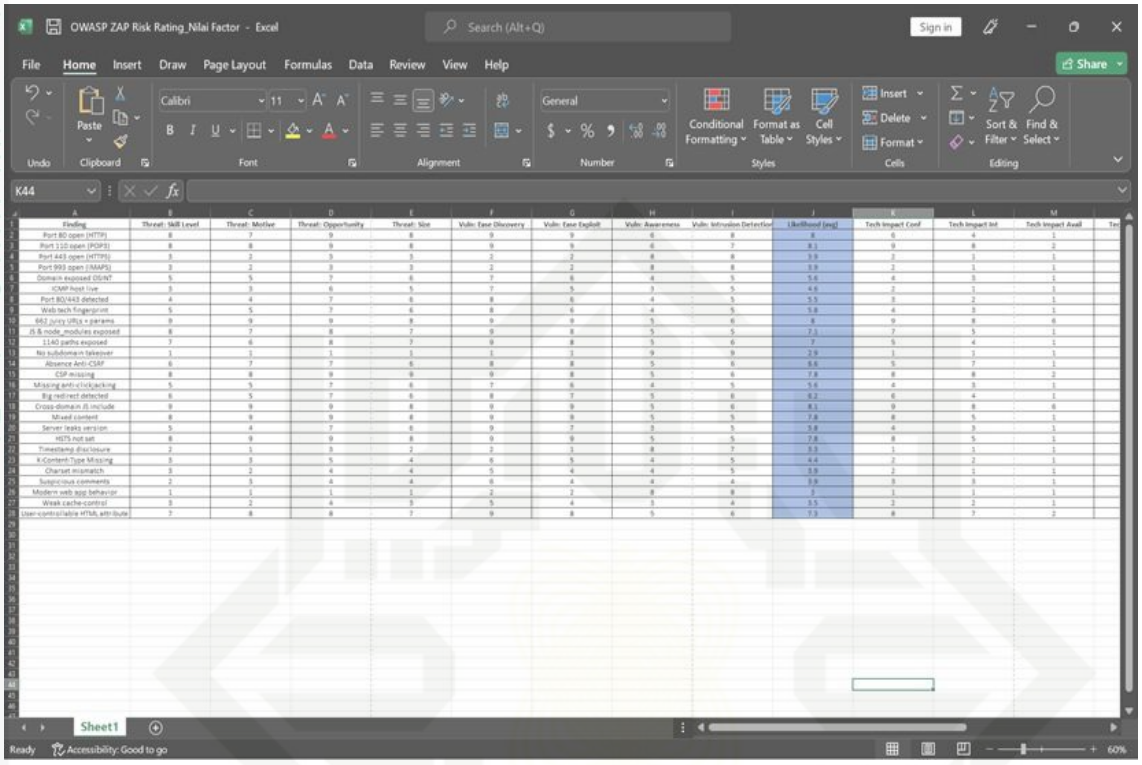
Wibowo, D. S., Nishom, M., dan Abidin, T. (2024). Pengumpulan informasi pada situs web dengan menyusun kerangka kerja keamanan siber nist. *Jurnal Informatika: Jurnal Pengembangan IT*, *9*(1), 1–6.

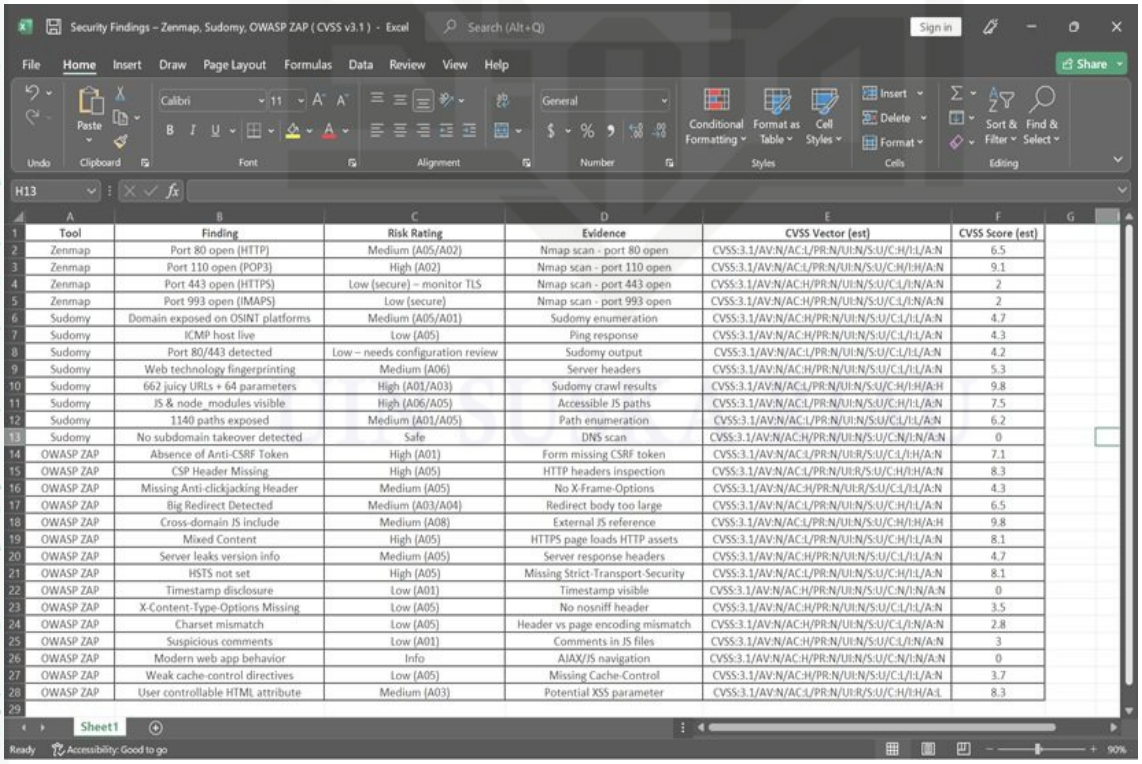
Widagdo, P. P., Haviluddin, H., Setyadi, H. J., Taruk, M., dan Pakpahan, H. S. (2018). Sistem informasi website fakultas ilmu komputer dan teknologi informasi universitas mulawarman. Dalam *Prosiding sakti (seminar ilmu komputer dan teknologi informasi)* (Vol. 3, hal. 5–9).

Williams, J. (2020). Owasp risk rating methodology. *OWASP. Available online: https://owasp. org/www-community/OWASP_Risk_ Rating_Methodology (accessed on 11 January 2021)*.

LAMPIRAN A

DATA PENILAIAN RISIKO





Tool	Finding	Risk Rating	Evidence	CVSS Vector (est)	CVSS Score (est)
Zenmap	Port 80 open (HTTP)	Medium (A05/A02)	Nmap scan - port 80 open	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N	6.5
Zenmap	Port 110 open (POP3)	High (A02)	Nmap scan - port 110 open	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	9.1
Zenmap	Port 443 open (HTTPS)	Low (secure) – monitor TLS	Nmap scan - port 443 open	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	2
Zenmap	Port 993 open (IMAPS)	Low (secure)	Nmap scan - port 993 open	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	2
Sudomy	Domain exposed on OSINT platforms	Medium (A05/A01)	Sudomy enumeration	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	4.7
Sudomy	ICMP host live	Low (A05)	Ping response	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	4.3
Sudomy	Port 80/443 detected	Low – needs configuration review	Sudomy output	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	4.2
Sudomy	Web technology fingerprinting	Medium (A06)	Server headers	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	5.3
Sudomy	662 juicy URLs + 64 parameters	High (A01/A03)	Sudomy crawl results	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Sudomy	JS & node_modules visible	High (A06/A05)	Accessible JS paths	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N	7.5
Sudomy	1140 paths exposed	Medium (A01/A05)	Path enumeration	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	6.2
Sudomy	No subdomain takeover detected	Safe	DNS scan	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N	0
OWASP ZAP	Absence of Anti-CSRF Token	High (A01)	Form missing CSRF token	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N	7.1
OWASP ZAP	CSP Header Missing	High (A05)	HTTP headers inspection	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N	8.3
OWASP ZAP	Missing Anti-clickjacking Header	Medium (A05)	No X-Frame-Options	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N	4.3
OWASP ZAP	Big Redirect Detected	Medium (A03/A04)	Redirect body too large	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N	6.5
OWASP ZAP	Cross-domain JS include	Medium (A08)	External JS reference	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
OWASP ZAP	Mixed Content	High (A05)	HTTPS page loads HTTP assets	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N	8.1
OWASP ZAP	Server leaks version info	Medium (A05)	Server response headers	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	4.7
OWASP ZAP	HSTS not set	High (A05)	Missing Strict-Transport-Security	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N	8.1
OWASP ZAP	Timestamp disclosure	Low (A01)	Timestamp visible	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N	0
OWASP ZAP	X-Content-Type-Options Missing	Low (A05)	No nosniff header	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	3.5
OWASP ZAP	Charset mismatch	Low (A05)	Header vs page encoding mismatch	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	2.8
OWASP ZAP	Suspicious comments	Low (A01)	Comments in JS files	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	3
OWASP ZAP	Modern web app behavior	Info	AJAX/JS navigation	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N	0
OWASP ZAP	Weak cache-control directives	Low (A05)	Missing Cache-Control	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	3.7
OWASP ZAP	User controllable HTML attribute	Medium (A03)	Potential XSS parameter	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L	8.3

DAFTAR RIWAYAT HIDUP

Dany Tria Putra Ramadhan lahir di Tembilahan pada tanggal 07 Desember 2001. Peneliti merupakan anak ketiga dari 3 bersaudara Bapak Sulaiman dan Ibu Rasyidah. Pada tahun 2006 peneliti memulai pendidikan di TK Cinta Bunda Tembilahan Kota. Kemudian peneliti meneruskan Sekolah Dasar Negeri di SDN 009 Tembilahan Kota pada tahun 2007 sam- pai tahun 2013. Setelah menyelesaikan pendidikan Sekolah Dasar, peneliti melanjutkan pendidikan di MTSN Indragiri Hilir pada tahun 2013 sampai tahun 2016. Kemudian peneliti melanjutkan pendidikan di SMK Negeri 1 Tembilahan pada tahun 2016 sampai tahun 2019 dan peneliti melanjutkan Strata Satu (S1) di Universitas Islam Negeri Sultan Syarif Kasim Riau pada Fakultas Sains dan Teknologi Jurusan Sistem Informasi tahun 2020 melalui jalur mandiri. Selama perkuliahan peneliti aktif dalam mengikuti kegiatan yang berada di dalam kampus maupun di luar kampus, Seperti mengikuti Kegiatan Kemah Bakti Mahasiswa pada tahun 2021 dan menjadi panitia Kemah Bakti Mahasiswa pada tahun 2022. Peneliti juga melaksanakan Kerja Praktek (KP) di Balai Pemasyarakatan Kelas II Pekanbaru. Kemudian pada tahun 2023 peneliti melaksanakan Kuliah Kerja Nyata (KKN) di Kelurahan Pekan Arba, Kecamatan Tembilahan, Kabupaten Indragiri Hilir, Provinsi Riau. Terkait dengan pertanyaan kepada peneliti tentang penelitian yang dikerjakan dapat menghubungi kontak melalui *email* 12050312714@students.uin-suska.ac.id untuk menjalin komunikasi yang lebih baik.