p-ISSN: 2301-6949
e-ISSN : 2715-5064

Analisis Kerentanan Keamanan Web Menggunakan Metode OWASP Dan PTES di Web Pemerintahan Desa XYZ

Rifki Muhammad Fauzi*), Rudi Hermawan, Dewanto Rosian Adhy, Siti Maesaroh
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Mayasari Bakti, Tasikmalaya
[1,2,3,4]Jln. Tamansari, Kota Tasikmalaya, 46191, Indonesia
email: [1]rifkimochfauzi@gmail.com*, rudihermawan567@gmail.com, Dewanto72@gmail.com, sitimaesaroh40@gmail.com

Abstract *−− Attacks on web applications can result in many losses, such as theft of sensitive data and damage to an organization's reputation. Moreover, web-based applications are applications that are often used in agencies today. One of them is the XYZ village web application, namely https://XYZ.g-desa.id/, with various important data in it such as resident identity data including NIK, full name and resident address, which can result in identity theft and fraud., spam phishing and many other crimes. The XYZ Village website has a track record of downing the web 4 times and destroying the appearance of the website 1 time which is a concern for the XYZ village government. The XYZ village website also does not yet have priority repairs or maintenance by the XYZ village government because it does not yet have repair reporting and there is no reporting on how much crisis of security gaps on the web. Because it is necessary to test web security gaps to provide reporting on how safe the website is, the method used to test security gaps is to use an integrated approach with two methods, namely OWASP (Open Web Application Security Project) and PTES (Penentraion Testing Excution Standard). The results of testing using the OWASP and PTES methods are expected to provide reporting of vulnerabilities and provide recommendations for improvements so that there is increased security on the XYZ website*

Abstrak *−* Serangan terhadap aplikasi web dapat mengakibatkan banyak kerugiaan, seperti pencurian data sensitive dan merusak reputasi sebuah organisasi. Terlebih aplikasi berbasis web merupakan aplikasi yang sering banyak digunakan di instansi saat ini. Salah satu nya pada aplikasi web desa XYZ yaitu https://XYZ.g-desa.id/, Dengan beragam data penting di dalam nya seperti data identitas warga mencakup NIK, nama lengkap dan alamat penduduk, yang mana bisa mengakibatkan pencurian identitas, penipuan, spam phising dan masih banyak kejahatan lain nya. Web Desa XYZ mempunyai track record down web sebanyak 4 kali dan perusakan tampilan web sebanyak 1 kali yang menjadi kehawatiran bagi pemerintahan desa XYZ, web desa XYZ juga belum mempunyai prioritas perbaikan atau maintenance oleh Pemerintah desa XYZ karena belum mempunyai reporting perbaikan dan tidak adanya pelaporan seberapa krisis celah keamanan pada web tersebut. Oleh karena nya diperlukan pengujian celah keamanan web untuk memberikan reporting seberapa aman web tersebut, metode yang dipakai untuk melakukan pengujian celah keamanan adalah menggunakan pendekatan yang terintegrasi dengan dua metode yaitu OWASP (Open Web Aplication Scurity Project) dan PTES (Penentraion Testing Excution Standart). Hasil dari pengujian Menggunakan metode OWASP dan PTES ini nantinya diharapkan memberikan reporting celah Kerentanan dan memberikan rekomendasi perbaikan sehingga ada peningkatan keamanan pada web XYZ.

Kata kunci: Kerentanan Keamanan Web, OWASP (Open Web Aplication Scurity Project), OWASP TOP 10, PTES (Penentraion Testing Excution Standart)

*) **penulis korespondensi**: **Rifki Muhammad Fauzi**
Email: rifkimochfauzi@gmail.com

I.PENDAHULUAN

Ancaman keamanan terhadap aplikasi web terus meningkat seiring dengan berkembangnya teknologi. Penyerang yang cerdik terus mencari celah dan kerentanan dalam aplikasi web untuk mencuri data, merusak reputasi perusahaan, atau mencari keuntungan finansial[1]. Badan Siber dan Sandi Negara (BSSN) yang bekerja sama dengan Indonesian Honeynet Project (IHP) mencatat terdapat 12.895.554 jumlah total serangan siber pada aplikasi berbasis web[1]. Hal ini menjadi ke- khawatiran bagi beberapa pihak. Terlebih, sekarang banyak aplikasi web yang mengelola data sensitive seperti informasi pelanggan, kartu kredit, data bisnis bahkan data-data pribadi seseorang. Tak hanya itu, setelah di kaji lebih dalam dan berdasarkan data BSSN serta artikel jurnal yang penulis baca, Jumlah SDM di Indonesia masih kurang dalam melakukan penetration, hal ini yang menjadi salah satu sebab banyak nya kerentanan keamanan yang ada di Indonesia[2].

Dalam pemahaman dan pengimplementasian metode penetration pun di Indonesia masih banyak yang belum mengenal metode penetration dan melakukan pengujian menggunakan satu metode penetration saja, yang mana pengujian dengan satu metode di rasa kurang efektive karena pengujian yang tidak general serta adanya keterbatasan cakupan (limited coverage). Hal ini dikarnakan Setiap metode penetrasi memiliki fokus dan keahlian tertentu, sehingga menggunakan satu metode saja tidak mampu mengidentifikasi seluruh rentang potensi kerentanannya yang mungkin ada dalam suatu sistem atau aplikasi, hal ini sangat perlu diteliti karena aplikasi web menjadi aplikasi yang sering banyak di gunakan oleh lembaga lembaga swasta dan lembaga lembaga pemerintah, banyak sekali kasus pembobolan situs web dan kebocoran data pada lembaga pemerintahan seperti adanya peretasan SQL injection, broken authentication dan juga web defacement[3][4] yang ditujukan untuk mempermalukan pemilik situs atau merusak reputasi lembaga, bahkan saat ini banyak di beberapa kasus instansi lain adanya pencurian data warga yang dipergunakan untuk memakai identitas dalam peminjaman uang dan pembobolan hak akses aplikasi yang menggunakan NIK dan identitas lain, seperti di lembaga pemerintahan desa XYZ.

Aplikasi web yang ada di Desa XYZ memiliki catatan downserver sebanyak 4 kali, yang menimbulkan kekhawatiran terkait kemungkinan adanya cracking atau peretasan. Selain itu, aplikasi ini pernah mengalami peretasan perubahan tampilan sebanyak 1 kali, yang menjadi sumber kekhawatiran bagi pemerintah Desa XYZ. Terlebih di dalam web XYZ

terdapat data yang termasuk data penting dan bersifat sensitif, seperti NIK, alamat, dan nama lengkap penduduk. Selain itu, dalam wawancara di temukan fakta bahwa aplikasi web ini belum pernah mengalami penetrasi sebelumnya, sehingga tidak ada analisis yang dilakukan terhadap kerentanan keamanannya. Pemerintah Desa XYZ juga belum melakukan pemeliharaan karena belum adanya prioritas perbaikan dan panduan perbaikan bagi aplikasi tersebut. Oleh karena itu, Melakukan pengujian penentrasi pada web Desa XYZ dianggap penting karena pemerintah Desa XYZ belum mendapatkan informasi yang memadai tentang sejauh mana ancaman terhadap aplikasi web Desa XYZ. Hal ini berguna Agar adanya evaluasi menyeluruh terhadap pengidentifikasian dan pelaporan untuk mengatasi potensi kerentanan sebelum merugikan pemerintah Desa XYZ lebih dalam lagi.

Berdasarkan hal itu dengan adanya permasalahaan yang kompleks pada web desa XYZ diperlukan suatu pengujian yang efektive dan terstuktur, Salah satu metodenya adalah menggunakan metode OWASP. OWASP berfokus pada keamanan aplikasi web yang sangat relevan dalam era digital saat ini, OWASP memiliki standar keretenan yang dinamakan OWASP Top 10. OWASAP Top 10 menyajikan risiko keamanan yang paling umum di dunia aplikasi web, OWASP juga mempunyai tools tersendiri yaitu adanya OWASP ZAP, namun Owasp zap dirasa kurang efektive dalam melakukan scanning yang general[1], langkah langkah pada owasp pun masih belum terstuktur, metode ini memerlukan metode lain untuk pengintegrasian yang mencakup seluruh parameter keamanan web. Dalam penelitian ini digunakan metode lainnya yaitu metode PTES yang memiliki panduan terstruktur untuk melakukan pengujian penetrasi, metode PTES membantu pengujian secara menyeluruh dan sistematis, mengusung pendekatan berlapis dengan fase seperti informasi, perencanaan, pengujian, dan pelaporan. Ini membantu mengidentifikasi dan menanggapi risiko keamanan secara lebih baik.[4]. Untuk meningkatkan keamanan aplikasi web secara teratur, salah satu solusinya adalah menggabungkan metode PTES (Penetration Testing Execution Standard) dan OWASP (Open Web Application Security Project), Dengan menggabungkan 2 metode ini diharapkan mampu memberikan hasil pengujian yang paling menyeluruh dan efektif. Penelitian ini nantinya menghasilkan reporting kerentanan yang ada pada web desa XYZ, memberikan rekomendasi solusi perbaikan terhadap celah keamanan web, serta menghasilkan seberapa efektivitas melakukan penetration dengan menggabungkan 2 metode penentrasi. Penelitian ini diharapkan mampu meningkatkan keamanan pada web desa XYZ

II.PENELITIAN YANG TERKAIT

Penelitian yang terkait sebelumnya dengan penelitian ini adalah Penelitian sebelumnya pada keamanan web secara luas hanya berfokus pada identifikasi dan mitigasi celah keamanan di OWASP Top 10, seperti Broken Authentication, Sensitive Data Exposure, dan Security Misconfiguration. Dan hanya berfokus pada kerentanan tertentu dalam exsploitasinya[5] dalam beberapa penelitian sebelumnya juga ditemukan sedikit yang menggabungkan pendekatan dengan menganalisis terhadap penggabungan dua metode penentration dan terhadap celah keamanan lain yang mungkin terjadi, seperti Clickjacking dan lain sebagai nya. Penelitian ini memperluas lingkup penelitian sebelumnya dengan mengintegrasikan metodologi OWASP Top 10 dengan pendekatan yang lebih holistic dengan menggabungkan dua metode penentration, yang memungkinkan identifikasi dan evaluasi lebih komprehensif terhadap kerentanan keamanan web, termasuk yang mungkin terabaikan menguraikan ulasan penelitan yang pernah dilakukan sebelumnya oleh peneliti lain yg relevan dengan penelitian yang dilakukan. Pada bagian ini dimasukan juga perbedaan penelitian yang dilakukan sebelumnya oleh penelitian sebelumnya dengan penelitian yang dilakukan oleh penulis sehingga dapat diketahui perbedaaan penelitian yang dilakukan.

III. METODE PENELITIAN

A. *Metode pengumpulan Data*

Dalam Penelitian ini penulis mengadopsi pendekatan penelitian kualitatif sebagai metodologi inti dalam menganalisis kerentanan keamanan web pemerintahan Desa XYZ. Metode penelitian kualitatif dipilih karena memberikan keleluasaan dalam menggali pemahaman mendalam tentang kompleksitas keamanan aplikasi web.

Langkah pertama dalam melakukan penelitian ini adalah melakukan pengumpulan data sebagai berikut :

1. wawancara

Pada tahap ini peneliti melakukan wawancara pada pengelola situs web atau staff pengelola yaitu bapak dede Mulyadi di desa XYZ kecamatan Pagerageung dengan dilakukan secara langsung. Sehingga menghasilkan beberapa Informasi terkait web Desa XYZ yang dilampirkan di Halaman lampiran

2. Observasi

Pada tahap ini dilakukan Observasi langsung terhadap situs web memberikan pandangan mengenai keberlanjutan dan kerentanan yang mungkin terlihat dalam penggunaan sehari-hari. Yang akan memperkaya pemahaman peneliti terhadap aspek yang mungkin menjadi kerentanan keamanan web yang akan di teliti

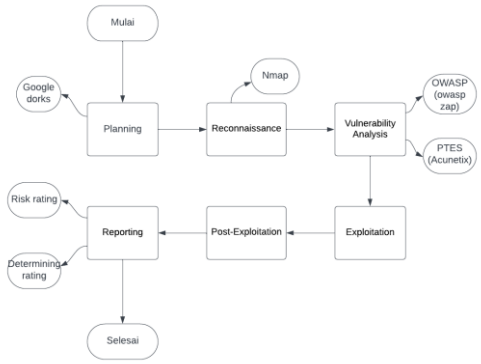
3. Studi Literature

Pada tahap ini penulis melakukan Studi literatur yang melibatkan analisis mendalam terhadap kerangka kerja keamanan web, praktik, dan temuan riset sebelumnya yang terkait dengan metode OWASP dan PTES. Informasi dari literatur ini mendukung konseptualisasi dan perbandingan hasil penelitian dengan konteks keamanan web yang lebih luas

B. Metode Pengujian dan Analisis

Tabel Pengujian dan analisis dalam penelitian ini mengunakan penggabungan dua metode OWASP dan PTES sebagai pedoman pengujian kerentanan keamanan.

Berikut adalah tahapan pengujian untuk menganalisis kerentanan web menggunakan metode OWASP dan PTES pada web Desa XYZ.



Gambar.1 Alur Penelitian

1.Perencanaan (Planning)

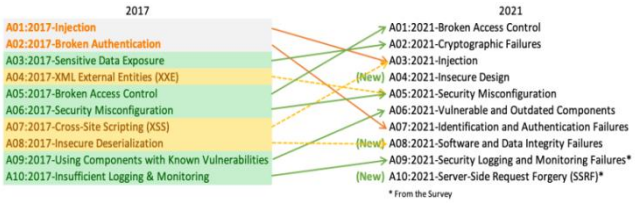
Tahapan pertama adalah tahapan perencanan dimana berguna untuk mengidentifikasi dan menganalisis tentang web yang akan di uji Dengan tools yang akan dipakai penulis yaitu menggunakan Google Dorks. dalam tahap planning penulis juga melakukan perizinan penentrasian web secara resmi yang ditulis dalam surat perijinan dan persetujuan dari pemilik ataupun pemelihara web.

2.Pemahaman Aplikasi/Sistem (Reconnaissance)

Tahapan ini dilakukan untuk melakukan pengumpulan informasi target secara relevan mencangkup Alamat IP, Sub Domain, atau rangkaian jaringan melalui tools yang akan dipakai penulis yaitu Nmap dan pengumpulan data atau informasi melalui tahap wawancara maupun observasi .

3.Analisis Kerentanan (Vulnerability Analysis)

Selanjutnya pada tahap ketiga di lakukan pemindaian web guna mencari kerentanan yang ada. Tahapan ini juga sering di sebut tahapan Vulnerability Scanning. Penulis menggunakan tools OWASP ZAP dan Acunetix, serta melakukan Threat Modeling yang mengacu pada OWASP Top 10 sebagai panduan vulnerability yang sering terjadi[6], OWASP TOP 10 tersebut adalah sebagai berikut :



Gambar.2 Owasp Top 10

4.Eksploitasi (Exploitation)

Pada tahapan ini dilakukan pengesploitasi kerentanan yang ditemukan pada tahap scanning, guna melihat seberapa jauh resiko yang di dapat serta memvalidasi kerentanan yang terpindai. Tahapan ini menggunakan aplikasi tools bruipsuite dan beberapa tools lainnya sesuai dengan temuan yang ada pada tahap Scanning

5.Pemeliharaan Akses (Post-Exploitation)

Proses ini memastikan bahwa akses tetap terjaga serta menerapkan backdoor sesuai dengan seberapa parah resiko yang ditemukan pada tahap exploitation juga dilakukan penilaian menggunakan CVSS.

6.Pembuatan reporting dan penilaian akhir resiko kerentanan web

Pada tahapan ini dilakukan penilaian resiko menggunakan Risk Rating Methodology dan Determining Severity of the Risk, Pada tahapan ini, estimasi kemungkinan dan dampak digabungkan untuk menghasilkan perhitungan tingkat keparahan risiko secara menyeluruh. Proses ini melibatkan penentuan apakah kemungkinannya rendah, sedang, atau tinggi, dan metode serupa diterapkan untuk menilai dampaknya dilakukan dari Skala dari 0 hingga 9 dan dibagi menjadi tiga segmen yaitu :

Tingkat Kemungkinan dan Dampak	
0 hingga <3	RENDAH
3 hingga <6	SEDANG
6 sampai 9	TINGGI

Gambar 3. Tingkat Kemungkinan Dan Dampak

Dalam penilaian kerentanan aplikasi web desa XYZ dilakukan menggunakan Metode Risk Rating methodologi dengan dibagi menjadi dua fokus yaitu skala Faktor ancaman kerentanan secara keseluruhan dan skala faktor Teknik serta bisnis secara keseluruhan, faktor tersebut diambil berdasarkan standar dari Open Web Aplication Scurity Project[7]. Selanjutnya dilakukan penilaian menggunakan Determining Serverity of the risk dimana sebagai penilaian tingkat keparahan dari setiap resiko yang mencangkup exsploitabilitas, Dampak dan jangkauan.

Dalam penilaian skala keseluruhan menggunakan Risk Rating methodologi diambil dari rumus sebagai berikut :

-Nama kerentanan =(f1+f2+f3+dst)/jumlah faktor = nilai kerseluruhan terhadap kerentanan 1/ (K1)
-Kemungkinan Nilai Keseluruhan = (K1 +k2+…)/ jumlah factor
-Skala Nilai faktor keseluruhan terhadap web = Kemungkinan Nilai Keseluruhan

Sedangkan penilaian skala keseluruhan menggunakan Determining Serverity of the risk adalah sebagai berikut :
Penilaian ini menggunkan sekala 1-3 dengan keterangan sebagai berikut

Tabel 1. Skala Skor Penilaian Instrumen

Skor	Skala
Rendah	1
Sedang	2
Tinggi	3

- Total Skor = Skor Eksploitabilitas + Skor Dampak + Skor Jangkauan

- contoh perhitungan untuk penilaian kerentanan:
- Kerentanan: (nama kerentanan)
- Eksploitabilitas: Tinggi (3)
- Dampak: Tinggi (3)
- Jangkauan: Sedang (2)
- Total Skor = 3 (Eksploitabilitas) + 3 (Dampak) + 2 (Jangkauan) = 8

Untuk rentang total skor adalah sebagai berikut

Tabel 2 Skala Skor Penilaian

Skala	Keterangan
3-5	Rendah
6-7	Sedang
8-9	Tinggi

.

IV.HASIL DAN PEMBAHASAN

Pembahasan Berdasarkan hasil pemindaian menggunakan OWASP ZAP dan Acunetix, ditemukan berbagai kerentanan spesifik dengan tingkat kerentanan yang berbeda. OWASP ZAP memiliki kerentanan yang lebih beragam dengan 2 tingkat kerentanan tinggi, 8 tingkat kerentanan sedang, dan 4 tingkat kerentanan rendah. Sementara itu, Acunetix menemukan 1 tingkat kerentanan sedang dan 3 tingkat kerentanan rendah. Perbandingan antara kedua hasil pemindaian tersebut menunjukkan perbedaan dalam fokus deteksi kerentanan antara OWASP ZAP dan Acunetix. Hasil kerentana tersebut berupa :

Kerentanam hasil Owasp zap

Tabel 3 Hasil Analisis Kerentanan Yang Terpindai OWASPZAP

Nama kerentanan	Tingkat Keterangan
Generic Padding Oracle	*High*
Sql Injection	*High*
Absence of Anti-CSRF Tokens	*Medium*
CSP : Wildcard Directive	*Medium*
CSP : script-src unsafe-inline	*Medium*
CSP : style-src unsafe-inline	*Medium*
Conten Security Policy (CSP) Header	*Medium*
Cross-Domain Misconfiguration	*Medium*
Hidden File Found	*Medium*
Missing Anti Clickjacking Header	*Medium*
vulnerable JS Library	*Medium*
Cookie no httpOnly flag	*Low*
Cross-Domain JavaScript Source file	*Low*
Server leaks information viaa x-power by http response	*Low*

Kerentanan hasil Acunetix

Tabel 4 Hasil Analisis Kerentanan Yang Terpindai Acunetix

Nama kerentanan	Tingkat Keterangan
HTML Form without CSRF protection (8)	*Medium*
clikjacking xframe options header missing(1)	*Low*
cookie without httponly flagset (1)	*Low*
uploaded files are not safely checked (1)	*Low*

Dari dua tabel di atas, terlihat bahwa OWASP ZAP menemukan kerentanan dalam berbagai aspek keamanan seperti *CSRF*, *CSP*, dan kebocoran informasi server, sementara Acunetix lebih fokus pada beberapa kerentanan spesifik seperti *CSRF*, *Clickjacking*, dan pengaturan cookie.

Selain hasil kerentanan web yang terpindai menggunakan OWAP ZAP dan Acunetix penulis juga melakukan validasi mendalam melakukan Attacking untuk mengvalidasi kerentanan serta memberikan rekomendasi sebagai berikut :

Tabel 5 Hasil Validasi Dan Solusi Perbaikan

Nama kerentanan	Solusi
Generic Padding Oracle	Implementasikan metode enkripsi yang lebih kuat dan pastikan untuk menghindari padding oracle attack.
Sql Injection	Gunakan prepared statements atau parameterized queries untuk mencegah serangan SQL injection.
Absence of Anti-CSRF Tokens	Sertakan token anti-CSRF pada setiap formulir yang memerlukan aksi pengguna untuk mencegah serangan CSRF.
CSP : Wildcard Directive	Hindari penggunaan direktif wildcard dalam kebijakan Konten Security Policy (CSP) dan tetapkan sumber daya yang diizinkan secara spesifik.
CSP : script-src unsafe-inline	Hapus direktif unsafe-inline dari kebijakan CSP dan atur kebijakan dengan hati-hati untuk memperbolehkan skrip hanya dari sumber yang dapat dipercaya.
CSP : style-src unsafe-inline	Hapus direktif unsafe-inline dari kebijakan CSP dan atur kebijakan dengan hati-hati untuk

	memperbolehkan gaya hanya dari sumber yang dapat dipercaya.
Content Security Policy (CSP) Header	Terapkan kebijakan CSP yang ketat untuk memblokir pelaksanaan skrip yang tidak diinginkan atau berbahaya.
Cross-Domain Misconfiguration	Konfigurasikan header CORS (Cross-Origin Resource Sharing) dengan benar untuk membatasi akses lintas domain hanya pada sumber yang dipercaya.
Hidden File Found	Periksa dan hapus atau amankan file tersembunyi yang tidak perlu dari akses publik.
Missing Anti Clickjacking Header	Tambahkan header X-Frame-Options pada respons HTTP dengan nilai "DENY" atau "SAMEORIGIN" untuk mencegah serangan Clickjacking.
Vulnerable JS Library	Perbarui pustaka JavaScript yang rentan ke versi yang lebih baru yang telah diperbaiki atau lebih aman.
HTML Form without CSRF protection (8)	Sertakan token anti-CSRF pada setiap formulir HTML untuk mencegah serangan CSRF.
Cookie no httpOnly flag	Atur cookie dengan flag HttpOnly untuk mencegah akses melalui skrip JavaScript.
Cross-Domain JavaScript Source file	Lindungi sumber JavaScript lintas domain dengan mengonfigurasi header CORS dan izinkan hanya sumber yang dipercaya.
Server leaks information via X-Powered-By	Matikan informasi server pada header HTTP X-Powered-By untuk mengurangi informasi yang dapat dimanfaatkan oleh penyerang.
Clickjacking X-Frame Options header missing	Tambahkan header X-Frame-Options pada respons HTTP dengan nilai "DENY" atau "SAMEORIGIN" untuk mencegah Clickjacking.
Cookie without httponly flagset	Atur cookie dengan flag HttpOnly untuk mencegah akses melalui skrip JavaScript.
Uploaded files are not safely checked	Periksa dan validasi setiap file yang diunggah untuk memastikan keamanan sebelum memproses atau menyimpannya.

Setelah itu dilakukan penilaian menggunakan Risk Rating Methodologi dan Determining Serverity of the risk dengan hasil sebagai berikut :

Tabel 6 Hasil Penilaian Menggunakan Risk Rating Methodologi

Nama Kerentanan	Risk rating Methodologi		
	Faktor Ancaman dan kerentanan	Dampak Teknis	Dampak Bisnis
Generic Padding Oracle	7,3	7,2	2,2
Sql Injection	8,1	8	2,7
Absence of Anti-CSRF Tokens	6,2	5	3,2
CSP : Wildcard Directive	5,3	5	3,5
CSP : script-src unsafe-inline	7,1	6,2	3,7
CSP : style-src unsafe-inline	6,2	5,2	3,5
Conten Security Policy (CSP) Header	5,0	5	2,7
Cross-Domain Misconfiguration	6,1	5,5	3
Hidden File Found	4,6	4,5	2,2
Missing Anti Clickjacking Header	5,3	4,7	2,5
vulnerable JS Library	8,1	7,5	4
Cookie no httpOnly flag	5,1	4,7	2,5
Cross-Domain JavaScript Source file	7,0	6,5	4
Server leaks information viaa x-power by http response	4,3	3,7	1,2
HTML Form without CSRF protection	6,2	5,5	3,5
clikjacking xframe options header missing(	5,3	4,7	2,5
cookie without httponly flagset	5,1	4,7	2,5
uploaded files are not safely checked	4,6	4,2	2,2

Risk rating Methodologi :

1. faktor ancaman dan factor kerentanan

- Kemungkinan nilai keseluruhan = 7,3 + 8,1 + 6,2 + 5,3 + 7,1+ 6,2 + 5,0 + 6,1 + 4,6 +5,3 +8,1+5,1+7,0 +4,3 +6,2+5,3+5,1+4,6 / 18
- Nilai faktor ancaman dan factor kerentanan pada web Keseluruhan = **5,9 (Medium)**

2.Dampak Teknis

- Kemungkinan nilai keseluruhan = 7,2 +8+5+5+6,2+5,2+5+5,5+4,5+4,7+7,5 +4,7+6,5+3,7+5,5+4,7+4,7+4,2/ 18
- Nilai faktor ancaman dan factor kerentanan pada web Keseluruhan = **5,4 (Medium)**

3.Dampak Bisnis

- Kemungkinan nilai keseluruhan = 2,2+2,7 +3,2+3,5+3,7+3,5+2,7+3+2,2+2,5+4+2,5+4+1,2+3,5+2,5+2, 5+2,5 / 18
- Nilai faktor ancaman dan factor kerentanan pada web Keseluruhan = **2,8 (Low)**

Determining Serverity of the risk:

Tabel 7 Hasil Penilaian Menggunakan Determining Serverity of the risk

Nama Kerentanan	Determining Serverity of the risk		
	Eksploitabilitas	Dampak	Jangkauan
Generic Padding Oracle	Sedang (2)	Tinggi (3)	Rendah (1)
Sql Injection	Tinggi (3)	Tinggi (3)	Sedang (2)
Absence of Anti-CSRF Tokens	Rendah (1)	Rendah (1)	Rendah (1)
CSP : Wildcard Directive	Sedang (2)	Sedang (2)	Rendah (1)
CSP : script-src unsafe-inline	Sedang (2)	Sedang (2)	Rendah (1)
CSP : style-src unsafe-inline	Sedang (2)	Sedang (2)	Rendah (1)
Conten Security Policy (CSP) Header	Sedang (2)	Sedang (2)	Rendah (1)
Cross-Domain Misconfiguration	Sedang (2)	Sedang (1)	Rendah (1)
Hidden File Found	Sedang (2)	Sedang (1)	Rendah (1)
Missing Anti Clickjacking Header	Rendah (1)	Rendah (1)	Rendah (1)
vulnerable JS Library	Sedang (2)	Tinggi (3)	Rendah (1)
Cookie no httpOnly flag	Sedang (2)	Sedang (1)	Rendah (1)
Cross-Domain JavaScript Source file	Sedang (2)	Sedang (1)	Rendah (1)
Server leaks information viaa x-power by http response	Rendah (1)	Rendah (1)	Rendah (1)
HTML Form without CSRF protection	Sedang (2)	Sedang (1)	Rendah (1)
clikjacking xframe options header missing(	Rendah (1)	Rendah (1)	Rendah (1)
cookie without httponly flagset	Sedang (2)	Sedang (1)	Rendah (1)
uploaded files are not safely checked	Rendah (1)	Rendah (1)	Rendah (1)

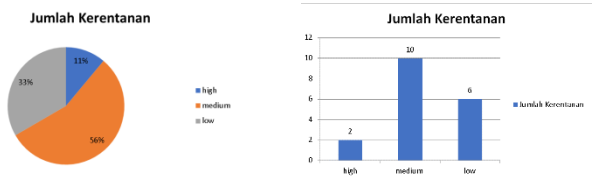
Hasil dari prioritas perbaikan berdasarkan rumus adalah sebagai berikut :

Tabel 8 Hasil prioritas perbaikan

Nama kerentanan	Tingkat Keterangan
Generic Padding Oracle	6
Sql Injection	8
Absence of Anti-CSRF Tokens	3
CSP : Wildcard Directive	5
CSP : script-src unsafe-inline	5
CSP : style-src unsafe-inline	5
Conten Security Policy (CSP) Header	5
Cross-Domain Misconfiguration	4
Hidden File Found	4
Missing Anti Clickjacking Header	3
vulnerable JS Library	6
Cookie no httpOnly flag	4
Cross-Domain JavaScript Source file	4
Server leaks information viaa x-power by http response	3
HTML Form without CSRF protection	4
clikjacking xframe options header missing(	3
cookie without httponly flagset	4
uploaded files are not safely checked	3

Tabel Determining Serverity of the risk diatas berfungsi sebagai penetapkan prioritas untuk melakukan perbaikan pada kerentanan yang ditemukan, dengan kerentanan yang memiliki total skor tertinggi dapat menjadi prioritas utama untuk perbaikan nya dalam artian prioritas perbaikan pertama ada pada kerentanan *Sql Injection*.

Hasil Keseluruhan kerentanan yang ada pada web desa XYZ adalah :



Gambar 4. Hasil Keseluruhan kerentanan yang ada pada web desa XYZ

V.KESIMPULAN

Berdasarkan penelitian ditemukan bahwa sebagian besar kerentanan berada dalam kategori sedang hingga rendah, dengan beberapa kerentanan yang masuk dalam kategori tinggi. Faktor ancaman dan kerentanan keseluruhan memiliki nilai sebesar 5,9, yang mengindikasikan kategori sedang. Hal ini menunjukkan bahwa web memiliki tingkat kerentanan yang signifikan, meskipun sebagian besar kerentanan masuk dalam kategori sedang hingga rendah, Dalam hal dampak teknis terhadap kerentanan pada web desa XYZ juga, dinilai ada pada skor 5,4, yang termasuk dalam kategori medium. Sementara itu, dampak bisnis terhadap kerentanan web memiliki nilai sebesar 2,8, yang masuk dalam kategori rendah. Hal ini menunjukkan bahwa meskipun terdapat kerentanan teknis, dampak bisnisnya cenderung rendah.

Penelitian ini telah memberikan hasil yang signifikan terkait kondisi keamanan dan kerentanan web Desa XYZ. Melalui penggabungan dua metode penetrasi, yaitu metode OWASP dan metode PTES, penelitian berhasil menguji kerentanan keamanan web secara exploitasi dengan menemukan validasi 4 kerentanan dari hasil scaning. Temuan dari penelitian menunjukkan bahwa kedua metode tersebut secara efektif mampu berkaiatan satu sama lain, hasil akhir dari penelitian ini berupa reporting prioritas perbaikan dan solusi perbaikan sebagaimana telah dicantumkan dalam hasil di atas.

Sebagai saran untuk pengembangan selanjutnya, dapat dilakukan attacking lebih dalam terhadap kerentanan yang ada serta menambahkan atau menggabungkan metode penetration yang lain seperti ISSAF yang berfokus pada pengujian server[8]. Serta menambahkan pengujian dari tools lain sesuai dengan perkembangan teknologinya.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada Universitas Mayasari Bakti atas dukungan dan fasilitas yang diberikan selama proses penelitian ini. Tanpa bantuan mereka, penelitian ini tidak akan terwujud. Penulis juga ingin mengucapkan terima kasih kepada instansi pemerintahan Desa XYZ atas kesediaan mereka untuk menjadi tempat penelitian. Tanpa partisipasi dan kerjasama dari pihak desa, penelitian ini tidak akan dapat dilaksanakan dengan lancar.

DAFTAR PUSTAKA

[1] M. S. S. Wardaya, "PENETRATION TESTING TERHADAP WEBSITE ASOSIASI PEKERJA PROFESSIONAL INFORMASI SEKOLAH INDONESIA (APISI)," *J. Kaji. Pendidik. Ekon. dan Ilmu Ekon.*, vol. 2, no. 1, pp. 1–19, 2019, [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-84865607390&partnerID=tZOtx3y1%0Ahttp://books.google.com/books?hl=en&lr=&id=2LIMMD9FVXkC&oi=fnd&pg=PR5&dq=Principles+of+Digital+Image+Processing+fundamental+techniques&ots=HjrHeuS_

[2] Mabes TNI Angkatan Laut, "keamanan siber Indonesia berada di 3 posisi terbawah di antara negara G20," *Naval-CSIRT*, 2022. https://naval-csirt.tnial.mil.id/keamanan-siber-indonesia-peringkat-ke-3-terbawah-di-antara-negara-negara-g20/#:~:text=Berdasarkan Laporan National Cyber Security,terendah diantara seluruh negara G20.

[3] A. Bastian, H. Sujadi, and L. Abror, "Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan Sql Injection," *INFOTECH J.*, vol. 6, no. 2, pp. 65–70, 2020.

[4] D. N. Cunong, M. Saputra, and W. Puspitasari, "Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modan Dan Pelayanan Terpadu Satu Pintu Pemerintahan Xyzyz Menggunakan Standar Penetration Testing Executionstandard (Ptes)," *e-Proceeding Eng.*, vol. 7, no. 1, pp. 2090–2095, 2020.

[5] J. J. B. H. Yum Thurfah Afifa Rosaliah, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM," *Senamika*, vol. 2, no. September, pp. 752–761, 2021.

[6] Riyan Farismana and Dian Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 2, pp. 26–32, 2023, doi: 10.55606/jutiti.v3i2.2853.

[7] H. Setiawan, L. E. Erlangga, S. Siddiq, and Y. A. Gunawan, "Analisis Kerawanan Pada Aplikasi Website Menggunakan Standar OWASP Top 10 Untuk Penilaian Risk Rating," *Info Kripto*, vol. 17, no. 1, pp. 15–21, 2023, doi: 10.56706/ik.v17i1.64.

[8] T. Syarif Revolino and D. Jatmiko Andri, "Analisis Perbandingan Metode Web Security PTES, ISSAF dan OWASP di Dinas Komunikasi Dan Informasi Kota Bandung," *Elibrai.unikom*, p. 8, 2019, [Online]. Available: https://elibrary.unikom.ac.id/880/13/21.10112427_TIO REVOLINO SYARIF_JURNAL BAHASA INDONESIA.pdf