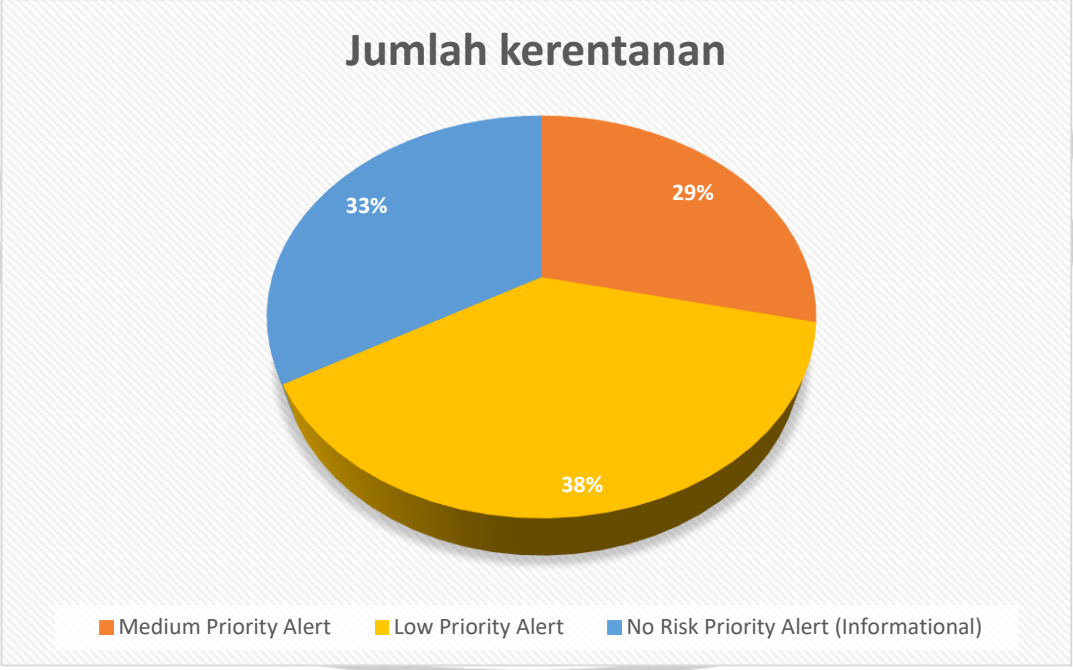
BAB IV

HASIL DAN PEMBAHASAN

4.1 Scanning

Scanning pada OWASP ZAP (Zed Attack Proxy) adalah proses pengujian keamanan website untuk mengidentifikasi kerentanan keamanan. Proses scanning ini dapat membantu mengidentifikasi masalah keamanan seperti SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan lainnya. Pada proses scanning OWASP ZAP selesai nantinya akan menyediakan laporan kerentanan keamanan pada website. Pada hasil scanning dapat dilihat pada **Gambar 4.1** terdapat hasil sebagai berikut Kerentanan Sedang sebanyak 6 kerentanan (29%), Kerentanan Rendah sebanyak 8 kerentanan (38%), dan Kerentanan Tidak Berdampak (Informatif) sebanyak 7 kerentanan (33%).

Gambar 4.1



Gambar 4.1 Presentase Jumlah Kerentanan

4.1.1 Kerentanan Sedang

Pada Kerentanan Sedang terdapat sebanyak 6 kerentanan dapat dilihat **Gambar 4.1.1** yang terdiri dari:

A.) Absence of Anti-CSRF Tokens

B.) Content Security Policy (CSP) Header Not Set (huruf atau angka)

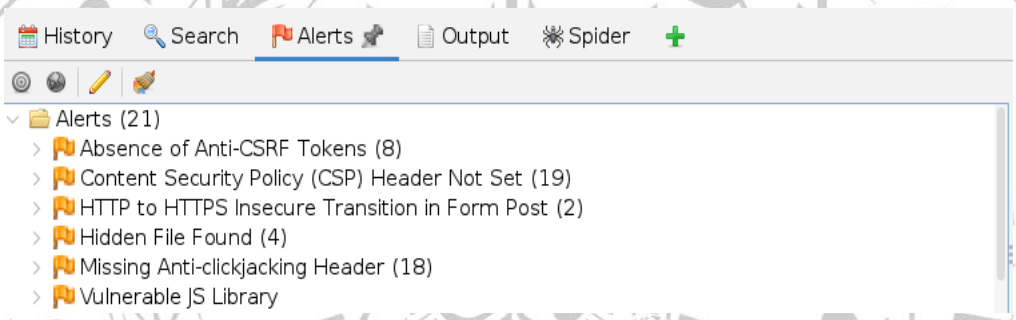
C.) HTTP to HTTPS insecure Transition in Form Post

D.) Hidden File Found

E.) Missing Anti-clickjacking Header

F.) Vulnerable JS Library

Gambar 4.1.1



Gambar 4.1.1 Kerentanan Sedang

Pada Kerentanan Sedang dapat dilihat pada **Gambar 4.1.1** dimana terdapat 6 kerentanan, kerentanan tersebut dapat mempengaruhi kinerja website apabila tidak segera ditangani salah satunya seperti kerentanan Absence of Anti-CSRF Tokens yang dimana kerentanan tersebut membuat penyerang memaksa pengguna untuk melakukan tindakan tidak dikehendaki tanpa sepengetahuan mereka. Jika sebuah website tidak menerapkan Anti-CSRF Tokens website maka akan mendapat serangan berupa penyerang membuat situs palsu dan menyisipkan kode berbahaya pada situs yang sah untuk memaksa pengguna untuk secara tidak sadar melakukan tindakan yang diinginkan oleh penyerang.

4.1.2 Kerentanan Rendah

Pada Kerentanan Rendah terdapat sebanyak 8 kerentanan dapat dilihat **Gambar 4.1.2** yang terdiri dari:

A.) Big Redirect Detected (Potential Sensitive Information Leak)

B.) Cookie No HttpOnly Flag

C.) Cookie Without Secure Flag

D.) Cross-Domain JavaScript Source File Inclusion

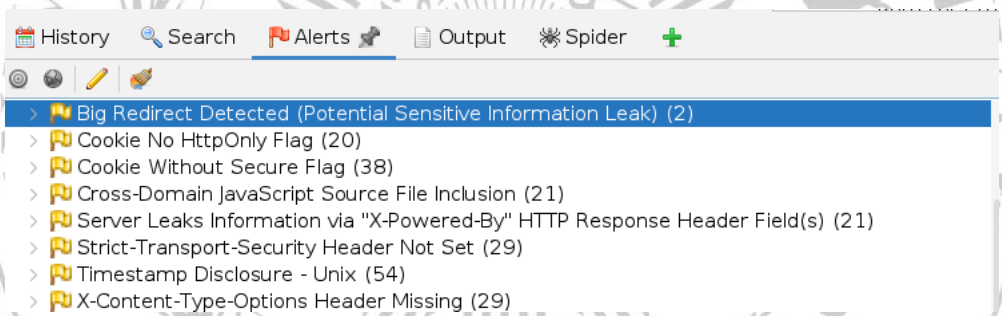
E.) Server Leaks Information Via “X-Powered-By” HTTP Response Header Field

F.) Strict-Transport-Security Header Not Set

G.) Timestamp Disclosure - Unix

H.) X-Content-Type-Options Header Missing

Gambar 4.1.2



Gambar 4.1.2 Kerentanan Rendah

Pada Kerentanan Rendah dapat dilihat pada **Gambar 4.1.2** dimana terdapat 8 kerentanan, Kerentanan Rendah dapat memberikan serangan yang berbahaya bagi website apabila secara terus-menerus tidak ditangani salah satunya kerentanan Big Redirect Detected (Potential Sensitive Information Leak) yang dimana kerentanan tersebut mengindikasikan adanya potensi kebocoran informasi sensitif yang terkait dengan pengalihan atau redirect. Apabila kerentanan Big Redirect Detected (Potential Sensitive Information Leak) tidak segera ditangani dapat menyebabkan kebocoran informasi yang sangat penting pada website.

4.1.3 Kerentanan Tidak Berdampak (Informatif)

Pada Kerentanan Tidak Berdampak terdapat sebanyak 7 kerentanan dapat dilihat **Gambar 4.1.3** yang terdiri dari:

A.) Authentication Request Identified

B.) Information Disclosure – Suspicious Comments

C.) Modern Web Application

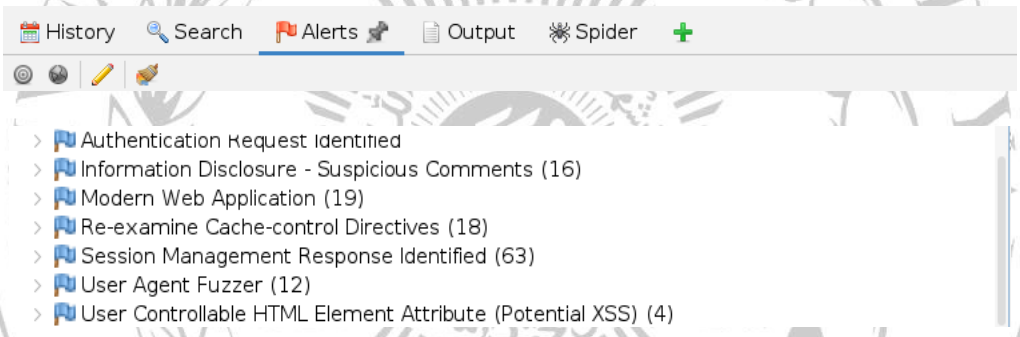
D.) Re-Example Cache-Control Directives

E.) Session Management Response Identified

F.) User Agent Fuzzer

G.) User Controllable HTML Element Attribute (Potential XSS)

Gambar 4.1.3



Gambar 4.1.3 Kerentanan Tidak Berdampak (Informatif)

Pada Kerentanan Tidak Berdampak (Informatif) dapat dilihat pada **Gambar 4.1.3** dimana terdapat 7 kerentanan, meskipun kerentanan tidak berdampak hanya sebagai kerentanan informatif tetapi kerentanan-kerentanan tersebut perlu adanya tindakan pencegahan seperti salah satunya kerentanan Authentication Request Identified, kerentanan tersebut mengidentifikasi terhadap pemintaan otentikasi terkait dengan proses login atau otentikasi pengguna. Apabila tidak ada tindakan terhadap kerentanan ini maka nantinya kerentanan tersebut menjadi kerentanan rendah yang berdampak.

4.2 OWASP Risk Rating

OWASP Risk Rating adalah sebuah metode pemeringkatan resiko kerentanan pada website yang memprioritaskan upaya dalam mengatasi keamanan berdasarkan potensi dampak dan eksploitasinya. OWASP Risk Rating dihitung dengan mempertimbangkan dua faktor utama yaitu Kemungkinan Eksploitasi (Likelihood Factors) dan Dampak Resiko (Impact Factor). Pada penelitian ini terdapat 3 kategori OWASP Risk Rating berdasarkan pengelompokan kerentanan dari Kerentanan Sedang dapat dilihat pada **Tabel 4.2.1**, Kerentanan Rendah dapat dilihat pada **Tabel 4.2.2**, dan Kerentanan Tidak Berdampak (Informatif) dapat dilihat pada **Tabel 4.2.3**.

4.2.1 Kerentanan Sedang

Pada saat proses scanning telah dilakukan mendapatkan kerentanan-kerentanan Sedang yang ada pada Website SIMPKN Informatika yang dimana kerentanan tersebut dianalisa dan dikelompokkan berdasarkan OWASP Risk Rating yang terdiri dari 2 pengelompokan yaitu Likelihood Factors (Kemungkinan Eksploitasi) dan Impact Factors (Dampak Resiko) dapat dilihat pada **Tabel 4.2.1** terdapat penilaian Kerentanan Sedang yang didapat setelah proses pengelompokan. Perhitungan Likelihood Factors (Kemungkinan Eksploitasi) dapat dihitung berdasarkan rumus berikut:

$$\textbf{Likelihood Factors} = \frac{\textbf{Threat Agent Factors + Vulnerabillity Factors}}{\textbf{8}} \quad \textbf{(4.1)}$$

Yang dimana Likelihood Factors mendapatkan hasil 4.375 dapat dilihat pada **Tabel 4.2.1**, Setelah melakukan perhitungan Likelihood Factors terdapat perhitungan Impact Factors (Dampak Resiko) dapat dihitung berdasarkan rumus berikut:

$$\textbf{Impact Factor} = \frac{\textbf{Technical Impact Factors + Business Impact Factors}}{\textbf{8}} \quad \textbf{(4.2)}$$

Setelah melakukan perhitungan Impact Factors mendapatkan hasil 3.125 dapat dilihat pada **Tabel 4.2.1** dari kedua hasil tersebut dapat dianalisa bahwa Kerentanan Sedang pada Website SIMPKN Informatika termasuk kedalam kategori MODERATE. Untuk hasil perhitungan OWASP Risk Rating didapat hasil kategori kerentanan masuk kedalam kerentanan MODERATE yang dimana pada **Tabel 4.2.1** aspek Kerentanan Sedang terdapat pada Threat Agent Factors, Vulnerability Factors, Technical Impact Factors, dan Bussines Impact Factors. Yang dimana aspek-aspek tersebut dapat mempengaruhi penilaian pada kinerja Website SIMPKN Informatika.

Tabel 4.2.1 OWASP Risk Rating Kerentanan Sedang

Likelihood factors	
Threat Agent Factors	
Skills required	Some technical skills [3]
Motive	Possible reward [4]
Opportunity	Special access or resources required [4]
Population Size	Intranet Users [4]
Vulnerability Factors	
Easy of Discovery	Difficult [3]
Ease of Exploit	Easy [5]
Awareness	Hidden [4]
Intrusion Detection	Logged without review [8]
Likelihood score:	**4.375**

Impact factors		
Technical Impact Factors		
3	Loss of confidentiality	Extensive non-sensitive data disclosed [6]
4	Loss of Integrity	Minimal seriously corrupt data [3]
4	Loss of Availability	Minimal secondary services interrupted [1]
4	Loss of Accountability	Attack fully traceable to individual [1]
Business Impact Factors		
3	Financial damage	Damage costs less than to fix the issue [1]
5	Reputation damage	Loss of major accounts [4]
4	Non-Compliance	Minor violation [2]
8	Privacy violation	Thousands of people [7]
	Impact score:	**3.125**

Overall Risk Severity :	MODERATE

	Impact		
Likelihood	Low	->Moderate<-	High
Low	Note	Low	Moderate
->Moderate<-	Low	->Moderate<-	High
High	Moderate	High	Critical

Dapat dilihat pada **Tabel 4.2.1** bahwa Likelihood Factors mendapatkan hasil yang ada pada nilai Kerentanan Sedang salah satunya Threat Agent Factors pada bagian Motive yang dimana memiliki pengertian bahwa penyerangan masuk kedalam kategori pencarian kerentanan oleh penyerang untuk mendapatkan imbalan, aspek tersebut masuk kedalam Kerentanan Sedang. Pada Impact Factors dapat dilihat pada **Tabel 4.2.1** bahwa salah satu aspek penilaian Bussines Impact Factors pada bagian Privacy Violation masuk kedalam kategori Kerentanan Sedang yang dimana kerentanan pada website dapat menyebabkan dampak pada ribuan orang.

4.2.2 Kerentanan Rendah

Setelah melakukan analisa kerentanan pada OWASP ZAP (Zed Attack Proxy) mendapatkan kerentanan-kerentanan Rendah yang ada pada Website SIMPKN Informatika yang dimana kerentanan tersebut dianalisa dan dikelompokkan berdasarkan OWASP Risk Rating yang terdiri dari 2 pengelompokan yaitu Likelihood Factors (Kemungkinan Eksploitasi) dan Impact Factors (Dampak Resiko) dapat dilihat pada **Tabel 4.2.2**, Untuk perhitungan Likelihood Factors (Kemungkinan Eksploitasi) dapat melihat rumus **4.1** yang dimana Likelihood Factors mendapatkan hasil 2.875 dapat dilihat pada **Tabel 4.2.2**. Setelah melakukan perhitungan Likelihood Factors terdapat perhitungan Impact Factors (Dampak Resiko) dapat dihitung berdasarkan rumus **4.2** perhitungan Impact Factors mendapatkan hasil 3 dapat dilihat pada **Tabel 4.2.2** dari kedua hasil tersebut dapat dianalisa bahwa Kerentanan Rendah pada Website SIMPKN Informatika termasuk kedalam kategori LOW.

Untuk hasil perhitungan OWASP Risk Rating didapat hasil kategori kerentanan masuk kedalam kerentanan LOW yang dimana pada **Tabel 4.2.2** aspek Kerentanan Rendah terdapat pada Threat Agent Factors, Vulnerability Factors, Technical Impact Factors, dan Bussines Impact Factors. Yang dimana aspek-aspek tersebut dapat mempengaruhi penilaian pada kinerja Website SIMPKN Informatika.

Tabel 4.2.2 OWASP Risk Rating Kerentanan Rendah

Likelihood factors	
Threat Agent Factors	
Skills required	No technical skills [1]
Motive	Low or no reward [1]
Opportunity	Full access or expensive resources required [0]
Population Size	System Administrators [2]
Vulnerability Factors	
Easy of Discovery	Easy [7]
Ease of Exploit	Easy [5]
Awareness	Hidden [4]
Intrusion Detection	Logged and reviewed [3]
Likelihood score:	**2.875**

Impact factors		
Technical Impact Factors		
1	Loss of confidentiality	Minimal non-sensitive data disclosed [2]
1	Loss of Integrity	Minimal slightly corrupt data [1]
0	Loss of Availability	Minimal secondary services interrupted [1]
2	Loss of Accountability	Attack fully traceable to individual [1]
Business Impact Factors		
7	Financial damage	Minor effect on annual profit [3]
5	Reputation damage	Loss of major accounts [4]
4	Non-Compliance	Clear violation [5]
3	Privacy violation	Thousands of people [7]
Impact score:		**3**

Overall Risk Severity :	Low

Likelihood	**Impact** Low	**->Moderate<-**	High
->Low<-	Note	**->Low<-**	Moderate
Moderate	Low	Moderate	High
High	Moderate	High	Critical

Dapat dilihat pada **Tabel 4.2.2** bahwa Likelihood Factors mendapatkan hasil yang ada pada nilai Kerentanan Rendah salah satunya Vulnerability Factors pada

bagian Awareness yang dimana memiliki pengertian bahwa analisa kerentanan pada Threat Agent pada Kerentanan Rendah berpotensi dalam penyerangan website yang didapat pada analisa **Tabel 4.2.2** yang masuk kedalam kategori kerentanan tersembunyi dari Threat Agent. Pada Impact Factors dapat dilihat pada **Tabel 4.2.2** pada nilai Kerentanan Rendah salah satunya Technical Impact Factors pada bagian Loss Of integrity aspek tersebut memiliki pengertian kerusakan data apabila terjadi penyerangan pada Kerentanan Rendah masuk kedalam kerusakan data yang minimal, aspek tersebut masuk kedalam Kerentanan Rendah karena data masih bisa digunakan tanpa ada kerusakan.

4.2.3 Kerentanan Tidak Berdampak (Informatif)

Setelah melakukan analisa kerentanan pada OWASP ZAP (Zed Attack Proxy) mendapatkan kerentanan-kerentanan Tidak Berdampak (Informatif) yang ada pada Website SIMPKN Informatika yang dimana kerentanan tersebut dianalisa dan dikelompokkan berdasarkan OWASP Risk Rating yang terdiri dari 2 pengelompokan yaitu Likelihood Factors (Kemungkinan Eksploitasi) dan Impact Factors (Dampak Resiko) dapat dilihat pada **Tabel 4.2.3**, Untuk perhitungan Likelihood Factors (Kemungkinan Eksploitasi) dapat melihat rumus **4.1** yang dimana Likelihood Factors mendapatkan hasil 0.875 dapat dilihat pada **Tabel 4.2.3.** Setelah melakukan perhitungan Likelihood Factors terdapat perhitungan Impact Factors (Dampak Resiko) dapat dihitung berdasarkan rumus **4.2** perhitungan Impact Factors mendapatkan hasil 1.125 dapat dilihat pada **Tabel 4.2.3** dari kedua hasil tersebut dapat dianalisa bahwa Kerentanan Tidak Berdampak (Informatif) pada Website SIMPKN Informatika termasuk kedalam kategori NOTE.

Untuk hasil perhitungan OWASP Risk Rating didapat hasil kategori kerentanan masuk kedalam kerentanan Tidak Berdampak (Informatif) yang dimana pada **Tabel 4.2.3** aspek Kerentanan Tidak Berdampak (Informatif) terdapat pada Threat Agent Factors, Vulnerability Factors, Technical Impact Factors, dan Bussines Impact Factors. Yang dimana aspek-aspek tersebut sebagai informasi bahwa terdapat kerentanan-kerentanan Tidak Berdampak (Informatif) apabila tidak diperbaiki maka kedepannya kerentanan tersebut berdampak pada kinerja Website SIMPKN Informatika.

Tabel 4.2.3 OWASP Risk Rating Kerentanan Tidak Berdampak (Informatif)

Likelihood factors	
Threat Agent Factors	
Skills required	No technical skills [1]
Motive	Low or no reward [1]
Opportunity	Full access or expensive resources required [0]
Population Size	System Administrators [2]
Vulnerability Factors	
Easy of Discovery	Practically impossible [1]
Ease of Exploit	Theoretical [1]
Awareness	Not Applicable [0]
Intrusion Detection	Active detection in application [1]
Likelihood score:	**0.875**

Impact factors		
	Technical Impact Factors	
1	Loss of confidentiality	Not Applicable [0]
1	Loss of Integrity	Not Applicable [0]
0	Loss of Availability	Not Applicable [0]
2	Loss of Accountability	Not Applicable [0]
	Business Impact Factors	
1	Financial damage	Damage costs less than to fix the issue [1]
1	Reputation damage	Minimal damage [1]
0	Non-Compliance	Not Applicable [0]
1	Privacy violation	Thousands of people [7]
	Impact score:	**1.125**

Overall Risk Severity :	Note

	Impact		
Likelihood	**->Low<-**	Moderate	High
->Low<-	**->Note<-**	Low	Moderate
Moderate	Low	Moderate	High
High	Moderate	High	Critical

Dapat dilihat pada **Tabel 4.2.3** bahwa Likelihood Factors mendapatkan hasil yang ada pada nilai Kerentanan Tidak Berdampak (Informatif) salah satunya Vulnerability Factors pada bagian Motive masuk kedalam kerentanan yang tidak mendapatkan hadiah dikarenakan kerentanan tersebut sulit dilakukan penyerangan apabila tidak memiliki keterampilan penetrasi keamanan. Pada Impact Factors dapat dilihat pada **Tabel 4.2.3** pada nilai kerentanan Tidak Berdampak (Informatif) salah satunya Bussiness Impact Factors pada bagian Reputation Damage pada saat terjadi penyerangan masuk kedalam kerusakan minimal dikarenakan membutuhkan pencarian kerentanan yang lebih berdampak dari Kerentanan Tidak Berdampak (Informatif).

4.3 Mitigation

Dalam mitigasi terdapat pengklasifikasian kerentanan berdasarkan dampak kerentanan website yang dibagi menjadi 3 tabel. Kerentanan Sedang dapat dilihat pada **Tabel 4.3.1**, Kerentanan Rendah dapat dilihat pada **Tabel 4.3.2**, dan Kerentanan Tidak Berdampak (Informatif) dapat dilihat pada **Tabel 4.3.3.** Pengklasifikasian mitigasi memudahkan dalam memberikan rekomendasi pencegahan dalam kerentanan website yang nantinya dapat memperbaiki dan meningkatkan keamanan Website SIMPKN Informatika.

4.3.1 Kerentanan Sedang

Tabel 4.3.1 Mitigation Kerentanan Sedang

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
1.	Absence of Anti-CSRF Tokens	1.) Memberikan input token anti-CSRF (Cross-Site Request Forgery) pada setiap formulir website dan permintaan yang dapat mengubah status server. Token harus unik untuk setiap sesi pengguna dan dihasilkan secara acak oleh server. 2.) Memberikan token yang berbeda untuk setiap tindakan atau operasi yang memerlukan perlindungan CSRF (Cross-Site Request Forgery), seperti mengubah kata sandi atau menghapus data. 3.) Mempertimbangkan untuk membatasi penggunaan metode HTTP tertentu pada operasi yang dapat menyebabkan perubahan status server seperti menggunakan metode POST

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		daripada GET untuk formulir yang mengubah data,
2.	Content Security Policy (CSP) Header Not Set	1.) Memastikan setiap halaman websitemenyertakan Header Content Security Policy (CSP) .Perbarui kebijakan keamanan konten secara berkala seiring berkembangnya website dan kebutuhan keamanan. 2.) Mempebaiki dan menyesuaikan kebijakan jika terjadi masalah dengan konten atau fungsi yang diinginkan. 3.) Selalu memantau laporan kebijakan dan perbaiki pelanggaran yang terdeteksi.
3.	HTTP to HTTPS insecure Transition in Form Post	1.) Memastikan seluruh website diakses melalui HTTPS, tidak hanya halaman formulir. Setel server website mengarahkan semua permintaan HTTP ke HTTPS. 2.) Memastikan semua tautan dan sumber daya pada website, termasuk skrip dan

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		gambar, diakses melalui HTTPS. 3.) Menghindari penggunaan sumber daya yang diambil dari situs HTTP jiks website diakses melalui HTTPS.
4.	Hidden File Found	1.) Memastikan bahwa file yang tidak perlu atau sensitif memiliki batas akses yang tepat. 2.) Menkripsi file yang mengandung informasi sensitif untuk melindungi data bahkan jika file tersebut diakses secara tidak sah. 3.) Memastikan semua perangkat lunak server, termasuk sistem operasi dan aplikasi, selalu diperbarui dengan pembaruan keamanan terbaru.
5.	Missing Anti-clickjacking Header	1.) Menggunakan Content Security Policy (CSP) untuk memberikan kontrol lebih terhadap konten yang dimuat dan ditampilkan pada website.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		2.) Mengaktifkan HTTP Strict Transport Security (HSTS) untuk memaksa pengguna untuk menggunakan koneksi aman (HTTPS) dan mencegah menjadi HTTP. Dapat mempengaruhi efektivitas pengaturan anti-clickjacking. 3.) Menerapkan sistem pemantauan untuk mendeteksi aktivitas yang mencurigakan atau upaya clickjacking.
6.	Vulnerable JS Library	1.) Memperbarui JS Library secara berkala mengikuti perilisan resmi dari pengembang. 2.) Menerapkan kebijakan keamanan konten (CSP) unruk membatasi sumber dan jenis skrip yang dapat dimuat pada halaman anda. 3.) Pengimplementasian Subresource Integrity (SRI) untuk memastikan bahwa file skrip yang dimuat dari server

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		eksternal tidak mengalami perubahan tidak sah.

4.3.2 Kerentanan Rendah

Tabel 4.3.2 Mitigation Kerentanan Rendah

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
1.	Big Redirect Detected (Potential Sensitive Information Leak)	1.) Memastikan tidak ada informasi seperti sensitive token akses, kata sandi, atau data pengguna lainnya yang disertakan dalam URL yang digunakan untuk pengalihan. 2.) Memastikan untuk memvalidasi dan membersihkan input pengguna sebelum menggunakannnya dalam pembuatan URL atau pengalihan lainnya. 3.) Memeriksa konfigurasi Web Server untuk memastikan bahwa tidak ada pengaturan yang memungkinkan pengalihan yang tidak aman.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
2.	Cookie No HttpOnly Flag	1.) Memastikan semua Cookie yang digunakan dalam website diatur menggunakan pengaturan HttpOnly. 2.) Memeriksa konfigurasi server apakah mendukung pengaturan HttpOnly untuk cookie. 3.) Penggunaan CSP (Content Security Policy) dapat membantu membatasi sumber daya yang dapat dimuat oleh halaman website, termasuk cookie.
3,	Cookie Without Secure Flag	1.) Memastikan semua cookie yang digunakan dalam website diatur dengan pengaturan Secure Flag. Memastikan bahwa cookie hanya ditransmisikan melalui koneksi yang aman (HTTPS). 2.) Mengimplementasikan HTTPS di website untuk mengamankan seluruh komunikasi antara server dan browser pengguna.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		3.) Memantau Log website untuk mendeteksi aktivitas yang mencurigakan atau terkait dengan cookie. Hal ini dapat membantu dalam mengidentifikasi jika cookie tanpa pengaturan Secure Flag disalahgunakan oleh penyerang.
4.	Cross-Domain JavaScript Source File Inclusion	1.) Melakukan validasi input pengguna secara menyeluruh. Hindari menerima atau mengeksekusi input pengguna tanpa validasi. Selalu membersihkan dan memvalidasi semua input, termasuk yang berasal dari URL, formulir, atau parameter permintaan. 2.) Memastikan untuk menghindari pengeksekusian pada Javascript. Menggunakan metode penghapusan kode atau pembersihan yang tepat untuk memastikan data input tidak dieksekusi sebagai kode JavaScript.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		3.) Memastikan menerapkan Same- Origin Policy yang membatasi akses JavaScript hanya ke sumber yang berasal dari domain yang sama.
5.	Server Leaks Information Via "X-Powered-By" HTTP Response Header Field	1.) Mengkonfigurasi server web untuk menghilangkan header "X-Powered-By" dari respons HTTP. Dapat dilakukan pada pengaturan server seperti Apache atau Nginx. 2.) Memeriksa konfigurasi server web anda dan pastikan tidak ada pengaturan secara eksplisit mengirimkan "X-Powered-By" ke klien. 3.) Menggunakan Firewall atau WAF (Web Application Firewall) untuk memfilter dan menghapus header "X-Powered-By" dari respons HTTP sebelum mencapai klien. Firewall atau WAF (Web Application Firewall) dapat menjadi lapisan pertahanan tambahan yang

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		efektif melindungi informasi sensitif server.
6.	Strict-Transport-Security Header Not Set	1.) Memastikan untuk mengatur header Strict-Transport-Security di server website. Header ini memberi tahu browser untuk selalu mengakses situs web melalui HTTPS dan untuk mengabaikan setiap upaya klien mengakses situs melalui HTTP. 2.) Menetapkan waktu maksimum (max-age) yang sesuai untuk Strict-Transport-Security header. Berguna untuk menentukan berapa lama browser akan mengingat kebijakan HTTPS untuk situs website. 3.) Memastikan konfigurasi server website mendukung pengaturan Strict-Transport-Security header. Beberapa contoh server seperti Apache, Nginx, dan IIS menyediakan opsi untuk mengkonfigurasi header ini secara langsung.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		Pastikan mengatifkannya dan mengatur nilai yang sesuai.
7.	Timestamp Disclosure - Unix	1.) Memastikan pesan error yang dihasilkan sistem Unix tidak mengandung informasi timestamp yang sensitif. Seperti informasi terkait waktu pembuatan atau modifikasi file dalam pesan error yang ditampilkan oleh pengguna. 2.) Memastikan konfigurasi server website terutama server website seperti Apache, Nginx, atau server FTP dan pastikan bahwa pengaturan yang berkaitan dengan informasi timestamp telah dikonfigurasi. 3.) Memastikan semua aplikasi yang berjalan disistem Unix diperbarui ke versi terbaru. Pembaruan keamanan untuk memperbaiki kerentanan yang dapat dimanfaatkan oleh penyerang.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
8.	X-Content-Type-Options Header Missing	1.) Memastikan untuk mengatur header X-Content-Type-Options dalam konfigurasi sever website atur nilainya menjadi “nosniff” untuk mencegah browser melakukan MIME sniffing. 2.) Memperbarui konfigurasi server website untuk mendukung penambahan header X-Content-Type-Options. Untuk server Apache, dapat menggunakan modul mod_headers sedangkan untuk server Nginx dapat menggunakan direktif add_header untuk tujuan yang sama. 3.) Melakukan pengecekan berkala untuk memeriksa apakah header X-Content-Type-Options telah ditetapkan dengan benar di semua respon HTTP.

4.3.3 Kerentanan Tidak Berdampak (Informatif)

Tabel 4.3.3 Mitigation Kerentanan Tidak Berdampak (Informatif)

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
1.	Authentication Request Identified	1.) Meningkatkan metode otentikasi yang ada pada website. Seperti autentikasi dua faktor (2FA) atau autentikasi multifactor (MFA). Menambah lapisan keamanan dan membuat website lebih sulit bagi penyerang untuk mengakses akun bahkan jika kata sandi diketahui. 2.) Memastikan untuk mendorong pengguna untuk menggunakan kata sandi yang kuat dan unik. Informasikan pada pengguna untuk secara teratur mengubah kata sandi secara teratur. 3.) Memonitor aktivitas pengguna untuk mendeteksi pola yang mencurigakan atau aktivitas yang tidak biasa. Memudahkan dalam mengidentifikasi upaya akses yang tidak sah.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
2.	Information Disclosure – Suspicious Comments	1.) Memastikan bahwa sistem website melakukan validasi input dengan ketat untuk mencegah penggunaan komentar yang mencurigakan atau berbahaya, seperti kode JavaScript yang tidak aman atau karakter khusus yang dapat dieksploitasi. 2.) Menggunakan enkripsi data untuk melindungi informasi sensitif, termasuk komentar pengguna. Dengan cara ini akan membuat membuat penyerang kesulitan untuk membaca tanpa kunci enkripsi yang benar. 3.) Melakukan reaksi cepat terhadap ancaman apabila terindikasi bahwa komentar mencurigakan telah menyebabkan kerentanan pada website.
3.	Modern Web Application	1.) Memastikan seluruh aplikasi website diakses melalui protocol HTTPS untuk menyandikan data yang

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		ditransmisikan antara pengguna dan server. 2.) Selalu melakukan validasi input pengguna secara ketat untuk mencegah serangan injeksi, seperti SQL Injection, XSS (Cross-Site Scripting), dan CSRF (Cross-Site-Request forgery). Gunakan teknik sanitasi dan escapement yang tepat untuk menghindari penyerangan website. 3.) Melakukan Logging dan pemantauan berguna untuk melacak aktivitas pengguna dan mendeteksi potensi insiden keamanan pada website.
4.	Re-Example Cache-Control Directives	1.) Memastikan untuk mengatur Cache-Control directives secara tepat untuk setiap simber daya website. Seperti tidak mengizinkan penyimpanan cache untuk data sensitif atau rahasia, dan pastikan cache direfresh secara teratur untuk

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		menghindari penyimpanan data yang kadaluwarsa. 2.) Melakukan pengujian menyeluruh pada penggunaan cache dalam website. Pastikan bahwa cache digunakan dengan aman. 3.) Memastikan perangkat lunak termasuk website server dan framework diperbarui dengan versi terbaru yang mengatasi kerentanan keamanan terkait dengan cache.
5.	Session Management Response Identified	1.) Memastikan bahwa data sensitif seperti informasi otentikasi atau token sesi tidak disertakan dalam respons yang dikirimkan kepada pengguna. 2.) Mempertimbangkan penggunaan token untuk menggantikan data sensitif dengan token yang tidak bermakna. Cara ini dapat membantu melindungi data sensitif bahkan jika respons disusupi.

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		3.) Menggunakan enkripsi untuk melindungi data sensitif jika terutama respons mengandung informasi yang perlu dilindungi. Pastikan bahwa protocol komunikasi anda menggunakan HTTPS.
6.	User Agent Fuzzer	1.) Memperkuat proses validasi input pada website. Gunakan pendekatan whitelist (Daftar Putih) untuk memastikan bahwa hanya karakter yang diperlukan dan aman diterima dari User Agent. Hindari menggunakan blacklist (Daftar Hitam) karena dapat memungkinkan karakter yang berbahaya melawati filter. 2.) Memastikan bahwa semua karakter khusus yang dimasukkan oleh User Agent atau dihindari dengan benar sebelum diproses oleh website. 3.) Memastikan bahwa semua perangkat lunak yang digunakan pada website, termasuk server website,

NO	KERENTANAN	REKOMENDASI PENCEGAHAN
		bahasa pemograman, dan library pihak ketiga. Selalu diperbarui dengan versi terbaru sehingga perbaikan keamanan dapat mencegah penyerangan website.
7.	User Controllable HTML Element Attribute (Potential XSS)	1.) Memastikan sebelum menampilkan nilai dari atribut element HTML yang dapat dikontrol oleh pengguna, pastikan untuk menghindari karakter khusu HTML dengan mengubahnya menjadi entitas HTML yang sesuai. 2.) Melakukan validsasi yang ketat terhadap nilai input yang diterima dari pengguna sebelum memasukkannya ke dalam atribut elemen HTML. 3.) Menggunakan Logging untuk memantau aktivitas pengguna pada website. Dengan memantau aktivitas tersebut, dapat dengan cepat mendeteksi dan menanggapi serangan yang berhasil.