Jurnal Sistem Informasi dan Sains Teknologi
Vol.7 No.2, Agustus 2025
ISSN 2684-8260

ANALISA DAN PERBAIKAN KEAMANAN PADA WEBSITE SDN 9 BANTAN

Muhammad Zuhri Febriansyah[1], Agus Tedyyana[2]
Jurusan Teknik Informatika, Politeknik Negeri Bengkalis
Email: **muhammadzuhrifebriansyah@gmail.com[1], agustedyyana@polbeng.ac.id [2]**

ABSTRAK

Keamanan website saat ini menjadi salah satu fokus utama, karena website berisi informasi dan data yang sensitif dan berharga. Penelitian ini dilakukan agar dapat mengetahui tingkat keamanan website dan memberikan perbaikan pada celah-celah keamanan yang ditemukan pada website SDN 9 Bantan dengan menggunakan metode *Vulnerability Assesment* dan menggunakan *tools OWASP ZAP* dan *Mozilla Observatory*. Dari hasil pemindaian, ditemukan beberapa celah pada website SDN 9 Bantan seperti *Content Security Policy Header Not Set* yang memungkinkan serangan *XSS* bisa terjadi, ketiadaan *anti-clickjacking header* membuka celah *clickjacking*, tidak adanya *Content Security Policy* (CSP) meningkatkan risiko serangan XSS, redirection yang tidak aman dapat dimanfaatkan untuk phishing, tidak adanya *Strict Transport Security* (HSTS) membuat situs mudah terkena serangan *Man-in-the-Middle* (MitM), dan *tanpa X-Frame-Options* meningkatkan risiko serangan clickjacking.. Untuk mengatasi celah keamanan ini, dilakukan *Vulnerability Assessment* untuk menentukan tingkat risiko dari celah keamanan website SDN 9 Bantan yang berada pada tingkat *medium*. Setelah proses perbaikan beberapa celah keamanan berhasil dihilangkan pada *Mozilla Observatory*. Namun pada *Content Security Policy Header Not Set* masih terdeteksi pada *OWASP ZAP*

Kata Kunci *:* Analisa*, Website*, Perbaikan, Keamanan*, Vulnerability Assesment*

I. PENDAHULUAN

Keamanan website saat ini menjadi salah satu fokus utama, karena website berisi informasi dan data yang sensitif dan berharga bagi pemilik website. Jika website memiliki tingkat keamanan yang buruk, maka website akan menjadi sasaran empuk para peretas yang tidak bertanggung jawab dan informasi serta data yang ada di dalamnya dapat digunakan secara tidak semestinya. Saat ini banyak instansi pendidikan seperti universitas, maupun sekolah-sekolah, yang menjadi sasaran para peretas, seperti pernah terjadi peretasan pada Website SMAN 1 Kota Sukabumi yang dijadikan situs judi online yang seharusnya beris informasi terkait sekolah tersebut [1]. Sebelumnya juga terjadi peretasan pada Website Sekolah Vokasi Universitas Gadjah Mada (UGM) peretas meninggalkan pesan terkait pelecahan di dalam website tersebut [2].

Hal tersebut dapat terjadi karena masih kurangnya keamanan pada website yang digunakan sebagai sarana informasi di dunia pendidikan, salah satunya adalah SDN 9 Bantan yang menggunakan teknologi informasi seperti website, website SDN 9 Bantan adalah sebuah website yang menyajikan informasi seputar kegiatan belajar-mengajar di SDN 9 Bantan.

Beberapa penelitian sebelumnya telah mengamati lemahnya keamanan di berbagai jenis website. Penelitian terhadap Website Sistem Informasi Administrasi Kependudukan mengungkap adanya 14 kerentanan, termasuk celah CSRF dan cookie tanpa atribut keamanan [3]. Website SMA Negeri 2 Sumbawa Besar juga diketahui memiliki 13 kerentanan yang berisiko menyebabkan XSS dan kebocoran informasi [4]. Audit terhadap website E-Government menemukan 148 kerentanan berisiko tinggi, termasuk SQL Injection dan XSS [5]. Penelitian lain pada aplikasi pelaporan pajak daerah mendeteksi tujuh jenis kerentanan seperti DDoS dan open port, dengan sebagian besar berada pada kategori risiko sedang [6]. Analisis pada website instansi pemerintah lainnya seperti Dinas Penanaman Modal juga menunjukkan keberadaan kerentanan tingkat tinggi dan sedang [7].

Walaupun demikian, terdapat hasil penelitian yang menunjukkan keadaan yang baik. Aplikasi Dapodik misalnya, dinyatakan dalam kondisi aman tanpa celah yang berbahaya [8]. Namun, website absensi tetap ditemukan memiliki kerentanan kritis seperti data exposure, SQL injection, dan komponen rentan [9]. Dan juga pada dan lembaga lainnya tetap ditemukan memiliki kerentanan kritis seperti data exposure, SQL injection, dan komponen rentan [10] Sedangkan pada Website Tapanuli Tengah bahkan ditemukan memiliki puluhan ribu timestamp disclosure, meskipun berisiko rendah [11]. Analisis terakhir terhadap website Universitas Singaperbangsa Karawang ditemukan 12 kerentanan, termasuk XSS dan header keamanan yang hilang [12].

Berdasarkan penelitian yang telah dilakukan sebelumnya masih banyak website khususnya website instansi pendidikan, yang masih memiliki beberapa celah keamanan yang belum di perbaiki, penelitian yang telah dilakukan sebelumnya hanya melakukan identifikasi dari celah keeamanan yang ditemukan, hal tersebut dapat berbahaya jika tidak segera dilakukan perbaikan. Berdasarkan hal tersebut, penelitian ini bertujuan untuk menganalisa dan memperbaiki celah keamanan dengan metode *Vulnerability Assessment* menggunakan *OWASP ZAP* dan *Mozilla Observatory*.

II. LANDASAN TEORI

2.1 *Vulnerability Assessment*

Vulnerability Assessment adalah sebuah metode yang digunakan untuk melakukan analisa yang mendalam untuk mengetahui keamanan informasi, konfigurasi pada sistem, yang dapat dijadikan sebagai informasi dalam melakukan perbaikan [13]. metode Vulnerability Assessment diterapkan untuk menganalisis kondisi keamanan website SDN 9 Bantan, yang berfungsi sebagai media informasi sekolah. Dengan penilaian ini, dapat diketahui seberapa besar risiko yang ditimbulkan oleh celah keamanan yang ada.

2.2 *Vulnerability scanning*

Vulnerability scanning digunakan untuk mengetahui informasi tentang kerentanan dengan menggunakan alat atau *tools* pemindaian [14]. Hal tersebut dapat berguna untuk memindai website SDN 9 Bantan sebagai langkah awal identifikasi potensi celah keamanan yang ditemukan.

2.3 *OWASP ZAP*

OWASP ZAP digunakan untuk menemukan kerentanan dengan cara yang mudah, alat ini menyediakan *scanner automatis* untuk menemukan kerentanan dan terdapat juga fitur manual [15]. Hal tersebut dapat berguna untuk mengetahui apakah terdapat kerentanan dari sisi struktur HTML, parameter input, atau konfigurasi *server* pada website SDN 9 Bantan dalam proses *scanning*.

2.4 *Mozilla Observatory*

Mozilla Observatory adalah alat untuk menguji konfigurasi HTTPS server, dan beberapa konfigurasi lainnya properti keamanan [16]. Proses *scanning* menggunakan Mozilla Observatory pada website SDN 9 Bantan bertujuan untuk mengidentifikasi kekurangan konfigurasi pada sisi server dari website.

2.5 *Vulnerability Analysis*

Vulnerability Analysis adalah proses yang mendefinisikan, mengidentifikasi, mengklasifikasika kerentanan keamanan (*vulnerabilities*) [17]. Hal tersebut dapat menjadi landasan dalam memberikan mitigasi dan perbaikan keamanan yang ditemukan dari celah keamanan dari website SDN 9 Bantan.

2.6 OWASP TOP 10

OWASP Top 10 adalah sebuah panduan bagi para developers dan security team tentang kelemahan-kelemahan pada web apps yang mudah diserang dan harus segera disiasati. *Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, dan Server-Side Request Forgery (SSRF)* [18]. Hal ini dapat membantu dalam menyusun langkah mitigasi dan perbaikan keamanan yang ditemukan dari celah keamanan dari website SDN 9 Bantan sesuai dengan standar keamanan.

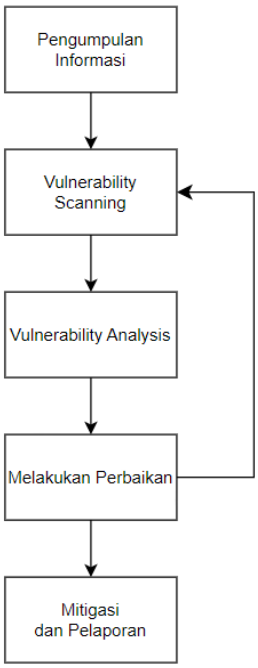
2.6 Perbandingan *Tools* Yang Digunakan

Tools	Kelebihan	Kekurangan
OWASP ZAP	Hasil Scanning yang didapatkan sangat bervariasi karena proses scanning dilakukan pada struktur HTML, parameter input, atau konfigurasi *server*	Beberapa konfigurasi di OWASP ZAP sulit dipahami dengan cepat.
Mozilla Observatory	Cara menggunakan tools ini tergolong mudah karena hanya memasukan url dari website dan dapat di akses di *browser*	Hasil scanning tergolong kurang lengkap karena proses *scanning* hanya dilakukan pada konfigurasi pada sisi server dari website

Tabel 1. Perbandingan *Tools* Yang Digunakan

III. METODE PENELITIAN

Dalam melakukan analisa dan perbaikan keamanan website SDN 9 Bantan menggunakan metode *Vulnerability Assessment*. *Vulnerability Assessment* terdapat beberapa langkah langkah yaitu:



Gambar 1 Langkah-langkah penelitian

3.1. Pengumpulan Informasi

Pada tahapan ini peneilti melakukan analisa dan perbaikan keamanan website SDN 9 Bantan sebagai objek penelitian. Penelitian ini menggunakan metode *Vulnerability Assessment (VA)* dan menggunakan *tools OWASP ZAP* versi 2.16.0 dan *Mozilla Observatory* versi terbaru yaitu HTTP Observatory untuk menganalisa tingkat keamanan website.

3.2. *Vulnerability Scanning*

Pada proses ini akan dilakukan pemindaian kerentanan pada tanggal 17 Februari 2025 di dalam website SDN 9 Bantan menggunakan *tools* pemindain kerentanan berupa *OWASP ZAP* dan *Mozilla Observatory, tools* tersebut di pilih dalam proses *scanning* karena *OWASP ZAP* memiliki hasil *scanning* yang cukup lengkap, sedangkan *Mozilla Observatory* digunakan karena mudah dan cepat saat ingin mengetahui celah keamanan dari website.

3.3. *Vulnerability Analysis*

Pada tahapan ini peneliti melakukan analisa kerentanan dari hasil pemindaian sebelumnya, pada proses ini peneliti akan mengelompokkan celah berdasarkan tingkat resikonya.

3.4. Melakukan Perbaikan

Pada tahapan ini peneliti melakukan perbaikan terhadap celah-celah keamanan yang celah keamanannya berisiko terjadinya serangan pada SDN 9 Bantan yang terdapat pada *OWASP ZAP* dan *Mozilla Observatory*.

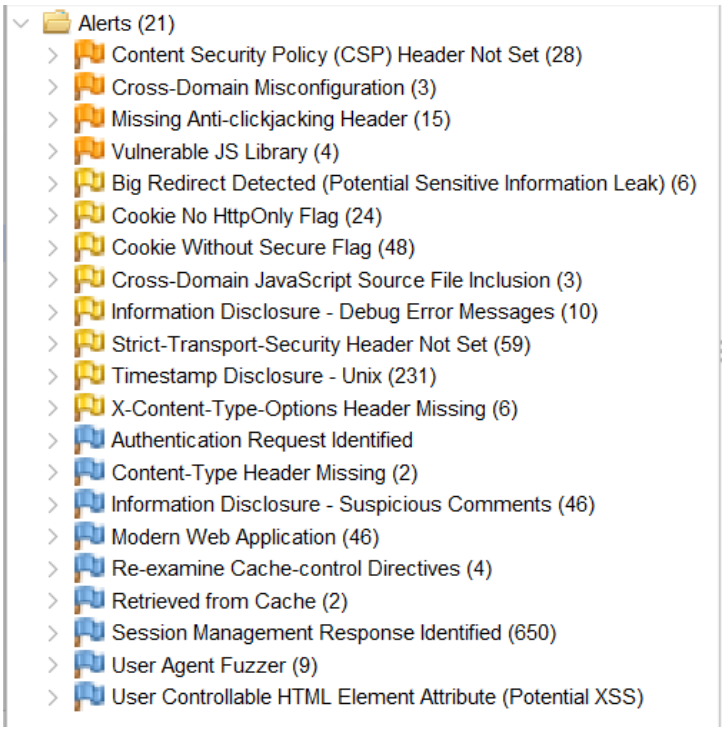
3.5 Pelaporan dan Mitigasi

Pada tahapan ini memberikan laporan dari hasil penelitian yang telah dilakukan dan memberikan rekomendasi tambahan jika diperlukan untuk meingkatkan keamanaan.

IV. ANALISIS DAN HASIL PERANCANGAN

4.1 *Vulnerability Scanning*

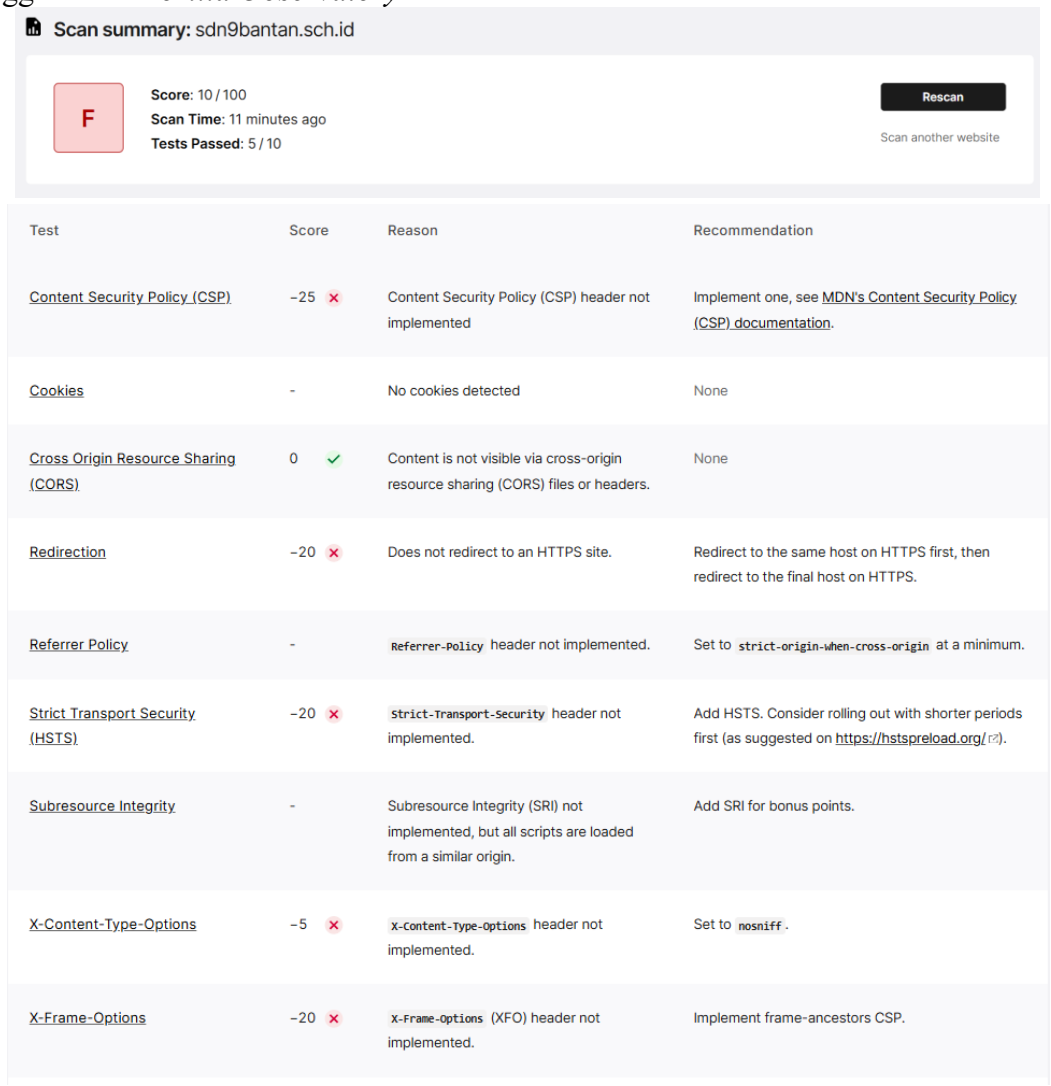
1. Menggunakan *OWASP ZAP*



Gambar 2 *Scanning OWASP ZAP*

Berdarkan gambar hasil scanning tersebut ditemukan 21 celah yaitu*: Content Security Policy Header Not Set, Cross-Domain Misconfiguration, Missing Anti-clickjacking Header, Vulnerable JavaScript Library, Big Redirect Detected, Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cross-Domain JavaScript Source File Inclusion, Information Disclosure - Debug Error Messages, Strict-Transport-Security Header Not Set, Timestamp Disclosure (Unix), X-Content-Type-Options Header Missing, Authentication Request Identified, Content-Type Header Missing, Information Disclosure - Suspicious Comments, Modern Web Application Identified, Re-examine Cache-control Directives, Retrieved from Cache, Session Management Response Identified, User Agent Fuzzer Detection, dan User Controllable HTML Element Attribute.*

2. Menggunakan *Mozilla Observatory*



Gambar 3 *Scanning Mozilla Observatory*

Dari gambar hasil scanning tersebut ditemukan 5 celah yaitu: *Missing Content Security Policy (CSP), Missing HTTPS Redirection, Missing Strict Transport Security (HSTS), Missing X-Content-Type-Options, Missing X-Frame-Options (Clickjacking Vulnerability).*

4.2 *Vulnerability Analysis*

Tools	Celah Keamanan	Tingkat Resiko
	Big Redirect Detected (Potential Sensitive Information Leak)	Low
	Cross-Domain Misconfiguration	Medium
	Information Disclosure - Debug Error Messages	Low
	Timestamp Disclosure - Unix	Medium

OWASP ZAP	Timestamp Disclosure - Unix	Low
	Cookie No HttpOnly Flag	Low
	Cookie Without Secure Flag	Low
	X-Content-Type-Options Header Missing	Low
	Missing Anti-clickjacking Header	Medium
	Strict-Transport-Security Header Not Set	Low
	Content Security Policy (CSP) Header Not Set	Medium
	Vulnerable JS Library	Medium
Mozilla Observatory	X-Frame-Options	Medium
	Redirection	Medium
	Strict Transport Security (HSTS)	Medium
	Content Security Policy (CSP)	Medium
	X-Content-Type-Options	Low

Tabel 2. *Vulnerability Analysis*

4.3 Melakukan Perbaikan

4.3.1 Menentukan Celah Keamanan

Pada tahap ini bertujuan untuk menentukan celah keamanan untuk diperbaiki berdasarkan hasil dari Vulnerability Analysis sebelumnya yang berasal dari *tools scanning* menggunakan *OWASP ZAP* dan *Mozilla Observatory.*

Tools	Celah Keamanan	Tingkat Resiko
OWASP ZAP	Content Security Policy (CSP) Header Not Set	Medium
	Missing Anti-clickjacking Header	Medium
Mozilla Observatory	Content Security Policy	Medium
	Redirection	Medium

	Strict Transport Security (HSTS)	Medium
	X-Frame-Options	Medium

Tabel 3. Menentukan Celah Keamanan

4.3.2. Backup Data

Pada tahap ini dilakukan backup data-data berupa database maupun script dari website SDN 9 Bantan.

4.3.3. Implementasi Perbaikan

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

```
<IfModule mod_headers.c>
# Menerapkan CSP Header
Header set Content-Security-Policy "default-src 'self';
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline';
img-src 'self' data:; font-src 'self'; connect-src 'self'; frame-src 'self'; object-src 'none';"
</IfModule>
```

Gambar 4 Penerapan CSP di *file* .htacess

Berdasarkan gambar tersebut digunakan untuk menambahkan perintah pada file .htaccess, agar semua konten dari luar tidak dapat di akses seperti *script, style, image,* maupun *font.*

```
$csp = "default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:;
font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src 'none'; object-src 'none';
frame-ancestors 'none'; form-action 'self'; upgrade-insecure-requests";
header(header: "Content-Security-Policy: $csp");
```

Gambar 5 Penerapan CSP di *file layout*

Berdasarkan penerapan *script* dari gambar tersebut, membuat sumber daya secara default hanya bisa berasal dari *domain* sendiri, baik berupa *script, style, image,* maupun *font* hanya dapat berasal dari domain SDN 9 Bantan.

2. *Missing Anti-clickjacking Header*

```
<IfModule mod_headers.c>
# Menambah Header Anti Clickjacking
Header always set X-Frame-Options "DENY"
</IfModule>
```

Gambar 6 Penerapan *Missing Anti-clickjacking Header* di *file* .htacess

Berdasarkan gambar tersebut digunakan untuk mengaktifkan *X-Frame-Options* pada file *.htaccess*.

```
// Tambahkan Header Clickjacking Protection
$response->headers->set('X-Frame-Options', 'DENY');
```

Gambar 7 Penerapan *Missing Anti-clickjacking Header* di *file layout*

Berdasarkan penerapan *script* dari gambar tersebut, setelah menambahkan *X-Frame-Options* bertujuan agar situs website SDN 9 Bantan tidak dapat di muat dalam *iframe* atau *tag html* di situs website mana pun.

3. *Content Security Policy*

```
<IfModule mod_headers.c>
# Implementasi Header CSP
Header set Content-Security-Policy "default-src 'self';
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline';
img-src 'self' data:; font-src 'self'; connect-src 'self'; frame-src 'self'; object-src 'none';"
```

Gambar 8 Penerapan *Content Security Policy* di *file* .htacess

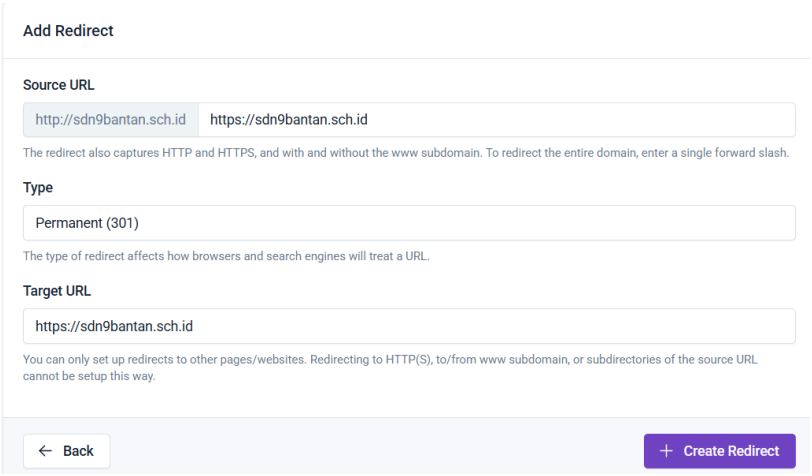
Berdasarkan penerapan *script* dari gambar tersebut, membuat sumber daya secara default hanya bisa berasal dari *domain* sendiri, baik berupa *script, style, image,* maupun *font* hanya dapat berasal dari domain SDN 9 Bantan.

4. *Redirection*

```
<IfModule mod_rewrite.c>
# Menerapkan Redirection hanya HTTPS
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^(.*)$ https://sdn9bantan.sch.id/$1 [R=301,L]
</IfModule>
```

Gambar 9 Penerapan *Redirection* di *file* .htacess

Berdasarkan penerapan *script* dari gambar tersebut, *Redirection* tersebut mengarahkan hanya ke https saja, Jika pengguna mengakses http://sdn9bantan.sch.id/home, mereka akan otomatis dialihkan ke https://sdn9bantan.sch.id/home.



Gambar 10 Penerapan *Redirection Hosting*

Gambar tersebut menunjukkan *Redirection* pada fitur di hosting yang berguna untuk mengarahkan pengguna saat akses dari http otomatis dipindahkan ke https.

5. *Strict Transport Security (HSTS)*

```
<IfModule mod_headers.c>
# Mengaktifkan HSTS untuk memastikan semua koneksi menggunakan HTTPS
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" env=HTTPS
</IfModule>
```

Gambar 11 Penerapan *Strict Transport Security (HSTS)* di *file* .htacess

Berdasarkan penerapan *script* dari gambar tersebut, *Strict Transport Security (HSTS)* tersebut digunakan untuk menginstruksikan browser agar selalu menggunakan HTTPS saat mengakses situs website.

6. *X-Frames-Options*

```
<IfModule mod_headers.c>
# Menambah X-Frame-Options
Header always set X-Frame-Options "DENY"
</IfModule>
```

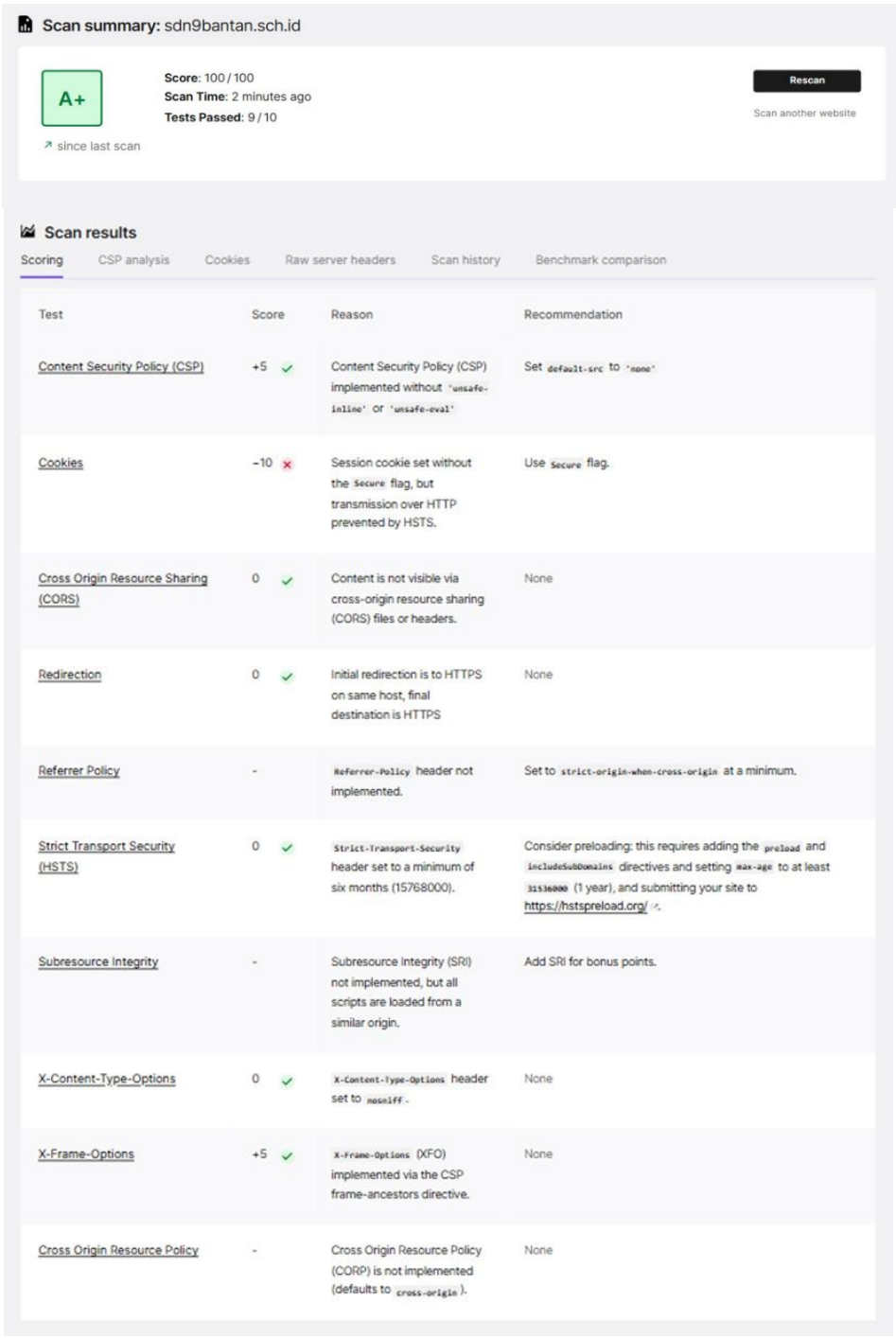
Gambar 12 Penerapan *X-Frames-Options* di *file* .htacess

Berdasarkan penerapan *script* dari gambar tersebut, penerapan *X-Frame-Options* bertujuan agar situs website SDN 9 Bantan tidak dapat di muat dalam *iframe* atau *tag html* di situs mana pun.

4.4 Pelaporan dan Mitigasi

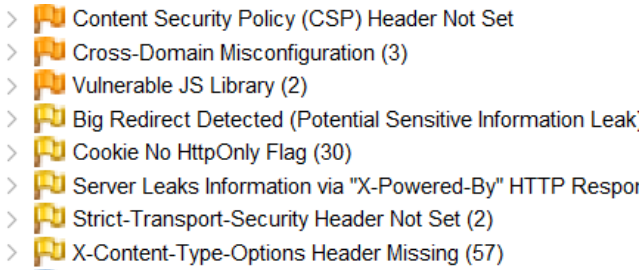
Setelah melakukan penelitian ini disimpulkan tingkat keamanan website SDN 9 Bantan pada *OWASP ZAP* berada pada tingkat sedang (*medium*) dikarenakan celah kerentanan yang di temukan beresiko *low – medium*, sedangkan tingkat keamanan website SDN 9 Bantan pada Mozilla Observatory berada pada tingkat sedang (medium) dikarenakan pada pengujian di Mozilla Observatory terdapat 10 aspek yang menjadi fokus utama yaitu*, X-Frame-Options, Cookies, Cross Origin Resource Sharing (CORS), Redirection, Referrer Policy, Content Security Policy (CSP), Subresource Integrity (SRI), X-Content-Type-Options, , Strict Transport Security (HSTS), , Cross Origin Resource Policy,* pada website SDN 9 Bantan berhasil melewati 5 dari 10 pengujian dan diberi nilai F yang berada pada tingkat rendah karena masih kurangnya konfigurasi keamanan pada website seperti belum terdapat *Content Security Policy (CSP), Redirection, Strict Transport Security (HSTS), X-Frame-Options, X-Content-Type-Options Header*. Dari hasil tersebut tingkat keamanan pada website SDN 9 Bantan berada pada tingkat sedang (*medium*).

Dalam tahap perbaikan, dilakukan identifikasi terhadap 6 celah keamanan yang berpotensi terjadinya serangan pada website. Langkah-langkah perbaikan dilakukan dengan menyesuaikan file konfigurasi server Apache. Setelah perbaikan diterapkan, dilakukan pengujian ulang untuk mengevaluasi efektivitas perubahan yang telah dilakukan, untuk memastikan bahwa risiko-risiko yang sebelumnya terdeteksi dapat diminimalkan agar tidak terjadinya serangan pada website SDN 9 Bantan dan meningkatkan tingkat keamanan sistem secara keseluruhan.



Gambar 13 Hasil Penelitian *Mozilla Observatory*

Gambar hasil penelitian ini memperlihatkan hasil berupa kenaikan tingkat keamanan pada *tools Mozilla Obsservatory* yaitu A+ yang berarti tinggi dan mendapatkan skor 100/100 karena telah menerapkan beberapa konfigurasi keamanan seperti *Cross Origin Resource Sharing (CORS), X-Content-Type-Options, Redirection, Referrer Policy, Strict Transport Security (HSTS), Subresource Integrity (SRI), Content Security Policy (CSP), X-Frame-Options, Cross Origin Resource Policy* pada website SDN 9 Bantan.



Gambar 14 Hasil Penelitian *Owasp ZAP*

Berdasarkan hasil tersebut peneltian ini berhasil *menerapkan Content Security Policy, Redirection, Strict Transport Security (HSTS), X-Frame-Options* untuk memperbaiki celah keamanan yang di temukan pada website SDN 9 Bantan. Sedangkan Pada Celah Keamanan *Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header* berhasil di aktifkan, namun pada *Content Security Policy (CSP) Header Not Set* masih terdeteksi pada *OWASP ZAP* hal tersebut dapat terjadi karena pada *file* sitemap.xml masih terdeteksi *CSP Header Not Set file* tersebut berisi daftar *URL* halaman *website* untuk membantu mesin pencari mencatat konten dengan lebih baik. *File* tersebut bukan *HTML,* sehingga tidak perlu menggunakan *CSP (Content-Security-Policy) header.*

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil analisa keamanan dapat di simpulkan bahwa tingkat keamanan website SDN 9 Bantan pada OWASP ZAP berada pada tingkat sedang (*medium*) dikarenakan celah kerentanan yang di temukan beresiko *low – medium*, sedangkan tingkat keamanan website SDN 9 Bantan *pada Mozilla Observatory* berada pada tingkat sedang (*medium*). Dari hasil tersebut tingkat keamanan pada website SDN 9 Bantan berada pada tingkat sedang (*medium*). Terdapat 6 celah keamanan yang dilakukan perbaikan, pada Celah Keamanan *Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header* berhasil di aktifkan, namun pada *Header* yang belum menereapkan *Content Security Policy* masih terdeteksi di *OWASP ZAP.* Sedangkan pada celah keamanan yang ditemukan di *Mozilla Observatory* berhasil meningkatkan tingkat keamanan dan mendapatkan skor A+ yang berarti tinggi dan mendapatkan poin 100 setelah menerapkan perbaikan keamanan website. Penelitian ini melakukan perbaikan melalui rekomendasi dari *tools* yang digunakan tanpa adanya proses *penetration testing* secara manual. Dengan demikian penelitian berfokus pada hasil konfigurasi keamanan yang ditemukan dan belum meliputi celah keamanan yang ditemukan pada proses *penetration testing* secara manual.

5.2 Saran

Dari hasil penelitian yang telah di lakukan disarankan agar menggunakan metode lainnya untuk menambah proses penelitian menjadi lebih baik, serta lebih memperbanyak penggunaan *tools* untuk mendapatkan hasil yang lebih bervariasi pada proses *scanning.* Selain itu di sarankan untuk melakukan *monitoring* untuk kedepannya seperti melakukan audit keamanan secara berskala maupun melakukan integrasi sistem log untuk memantau potensi ancaman, sehingga dapat cepat memberikan tindakan pada website.

DAFTAR PUSTAKA

[1] R. A. Saepulloh, "Website SMAN 1 Kota Sukabumi Sempat Diretas, Jadi Iklan Judi Online," Kompas.com. [Online]. Available: https://bandung.kompas.com/read/2024/06/28/163947878/website-sman-1-kota-sukabumi-sempat-diretas-jadi-iklan-judi-online

[2] J. H. Wawan, "Website Sekolah Vokasi UGM Diretas, UGM Angkat Bicara," detik.com. [Online]. Available: https://www.detik.com/jateng/jogja/d-6369422/website-sekolah-vokasi-ugm-diretas-ugm-angkat-bicara

[3] T. R. Tara and Y. W, "Analisis Keamanan Website Sistem Informasi Administrasi Kependudukan Menggunakan Metode Vulnerability Assesment," *J. Teknol. Inform. Dan Komput.*, vol. 1, no. 1, pp. 1–9, 2023, doi: 10.51401/jurtikom.v1i1.3172.

[4] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 202–209, Oct. 2022, doi: 10.47065/josh.v4i1.2335.

[5] M. Dewi Puspa Khairani, "Audit Web E-Government Dengan Acunetix Web Vulnerability Guna Menganalisis Dan Perbaikan Celah Keamanan Website," *J. Ris. Sist. Inf. Dan Tek. Inform. (JURASIK*, vol. 9, no. 1, pp. 442–450, 2024, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[6] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, pp. 1–6, Mar. 2021, doi: 10.37034/jsisfotek.v3i1.36.

[7] D. N. Cunong, M. Saputra, and W. Puspitasari, "ANALYSIS OF OROS MODELER DATA REPORTING PROCESS TO SAP HANA IN ACTIVITY BASED COSTING FOR INDONESIA TELECOMMUNICATION INDUSTRY," vol. 7, no. 1, 2020.

[8] A. Bastian, H. Sujadi, and L. Abror, "ANALISIS KEAMANAN APLIKASI DATA POKOK PENDIDIKAN (DAPODIK) MENGGUNAKAN PENETRATION TESTING DAN SQL INJECTION", [Online]. Available: http://www.dapodik.com/contoh.php?id

[9] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, Oct. 2022, doi: 10.37034/jidt.v4i3.236.

[10] W. A. Nugraha, "Pengujian White Box Berbasis Path Pada Form Autentikasi Berbasis Mobile," *J. Siliwangi Seri Sains dan Teknol.*, vol. 8, no. 2, pp. 42–47, 2022, doi: 10.37058/jssainstek.v8i2.4098.

[11] K. Nisa, M. A. Putra, R. A. Siregar, and M. Dedi Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," *Bull. Inf. Technol.*, vol. 3, no. 4, pp. 308–216, 2022, doi: 10.47065/bit.v3i4.389.

[12] A. M. Akmal1, N. Heryana2, and Arip Solehudin3, "Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment," *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 6298–6309, 2022.

[13] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.

[14] A. Kendek Allo and I. R. Widiasari, "Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 8, no. 2, pp. 316–323, 2024, doi: 10.35870/jtik.v8i2.1723.

[15] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[16] USENIX Association., "Measuring HTTPS Adoption on the Web," p. 72, 2005.

[17] M. Muin Abdul, Kapti, and T. Yusnanto, "Campus Website Security Vulnerability Analysis Using Nessus," *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 03, no. 02, pp. 2745–9659, 2020, [Online]. Available: https://ijcis.net/index.php/ijcis/index

[18] R. R. Yusuf and T. N. Suharsono, "Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk," *Pros. Semin. Sos. Polit. Bisnis, Akunt. dan Tek.*, vol. 5, p. 402, 2023, doi: 10.32897/sobat.2023.5.0.3132.