Vol. 5, No. 1, April 2024, hal. 134-143

p-ISSN: 2723-567X
e-ISSN: 2723-5661

**Jurnal Computer Science and Information Technology (CoSciTech)**

**http://ejurnal.umri.ac.id/index.php/coscitech/index**

# Audit Keamanan Website Menggunakan Acunetix Web Vulnerability (Studi Kasus Di SMK Muhammadiyah 3 Terpadu Pekanbaru)

**Boby Supriyanto[1], Sumijan[2] , Yuhandri[3]**
Email: [1]bobby.supriantost@gmail.com, [2]sumijan@upiyptk.ac.id, [3]yuyu@upiyptk.ac.id

[123]Magister Teknik Informatika, Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK Padang

Diterima: 29 Januari 2024 | Direvisi: 28 April 2024 | Disetujui: 12 Mei 2024


**Abstrak**

Teknologi informasi mengalami evolusi yang cepat sejalan dengan pertumbuhan penggunaannya. Contoh konkret dari evolusi ini adalah pemanfaatan situs web sebagai sarana pendukung dalam proses pembelajaran. Situs web dapat didefinisikan sebagai kumpulan halaman web yang dapat diakses secara publik, yang dapat mencakup beragam jenis konten seperti teks, gambar, video, dan audio.Namun, sejalan dengan kemajuan teknologi, terjadi peningkatan dalam kerentanan atau ancaman terhadap teknologi tersebut. Berdasarkan laporan tahunan pemantauan keamanan siber tahun 2023 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), terdokumentasikan lebih dari 13 juta insiden anomali serangan siber yang terjadi di Indonesia. Studi ini akan memanfaatkan Acunetix Web Vulnerability Scanner (WVS) untuk melakukan audit terhadap keamanan situs *web* SMK Muhammadiyah 3 Terpadu Pekanbaru (SMK MUTI). Penelitian ini akan mengkaji kelemahan keamanan *website* SMK MUTI dan membahas bagaimana *Acunetix Web Vulnerability* dapat membantu dalam meningkatkan tingkat keamanan *website* tersebut. Metode Penilaian Kerentanan (Vulnerability Assessment) yang diterapkan menggunakan pendekatan analisis deskriptif, yang mana data yang dikumpulkan disusun dalam format tabel, dengan tujuan untuk menghasilkan pemahaman yang lebih jelas terhadap hasil analisis yang dilakukan dalam proses audit. Berdasarkan hasil scanning iterasi pertama, website SMK MUTI dikategorikan pada tingkat ancaman 3 yang termasuk tinggi, dengan terdapat 192 peringatan atau kerentanan yang teridentifikasi, di antaranya, 2 dianggap berada pada tingkat tinggi dan 11 berada pada tingkat sedang. Berdasarkan evaluasi yang telah dilakukan, tingkat keamanan yang tercapai berada pada level 1. Pada level ini, tidak terdapat kerentanan yang teridentifikasi (nol kerentanan) dan dukungan keamanan juga mencapai tingkat optimal (nol dukungan). Oleh karena itu, dapat disimpulkan bahwa situs web SMK MUTI saat ini, dengan status level 1, tidak memiliki kerentanan keamanan.

**Kata kunci**: *Audit*, *Vulnerability*, *Acunetix*, *Vulnerability Assessment*, SMK MUTI

## *Website Security Audit Using Acunetix Web Vulnerabilities (Case Study At Muhammadiyah 3 Terpadu Vocational School Pekanbaru)*

***Abstract***

*The information technology has undergone rapid evolution in line with its growing usage. A concrete example of this evolution is the utilization of websites as supporting tools in the learning process. A website can be defined as a collection of publicly accessible web pages that can contain various types of content such as text, images, videos, and audio. However, along with technological advancements, there has been an increase in vulnerabilities or threats to this technology. Based on the annual report on cybersecurity monitoring in 2023 published by the National Cyber and Crypto Agency (BSSN), more than 13 million incidents of anomalous cyber attacks have been documented in Indonesia. This study will utilize the Acunetix Web Vulnerability Scanner (WVS) to conduct a security audit of the SMK Muhammadiyah 3 Terpadu Pekanbaru (SMK MUTI) website. The research will examine the security weaknesses of the SMK MUTI website and discuss how Acunetix Web Vulnerability Scanner can help improve its security level. The Vulnerability Assessment method applied uses a descriptive analysis approach, where*

*collected data is organized in table format, aiming to provide a clearer understanding of the analysis results obtained during the audit process. Based on the results of the first iteration scanning, the SMK MUTI website is categorized at threat level 3, which is considered high, with 192 warnings or identified vulnerabilities, among which, 2 are categorized as high level and 11 are categorized as medium level. Based on the evaluation conducted, the achieved security level is at level 1. At this level, no vulnerabilities are identified (zero vulnerabilities), and security support has also reached an optimal level (zero support). Therefore, it can be concluded that the SMK MUTI website currently, with level 1 status, does not have any security vulnerabilities.*

**Keywords**: *Audit*, *Vulnerability*, *Acunetix*, *Vulnerability Assessment*, SMK MUTI

## 1. PENDAHULUAN

Teknologi informasi mengalami evolusi yang cepat sejalan dengan pertumbuhan penggunaannya. Contoh konkret dari evolusi ini adalah pemanfaatan situs web sebagai sarana pendukung dalam proses pembelajaran. Seiring dengan perkembangan teknologi, pertumbuhan kerentanan atau serangan terhadap teknologi tersebut juga meningkat. Sejalan dengan pertumbuhan jumlah pengguna internet di Indonesia yang terus meningkat secara signifikan [1]. Situs web merupakan suatu layanan web yang menyajikan berbagai informasi dan berita [2]. Berdasarkan laporan tahunan pemantauan keamanan siber tahun 2023 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), tercatat lebih dari 13 juta anomali serangan siber yang terjadi di Indonesia [3].

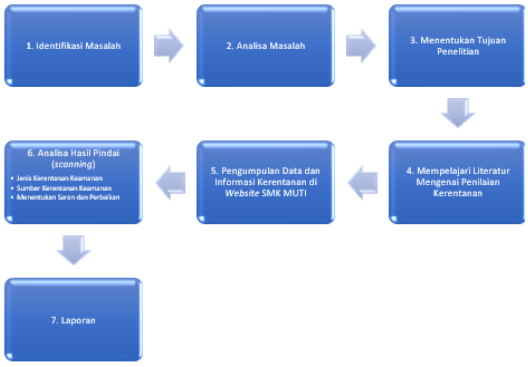
SQL Injection merupakan teknik yang sering dilakukan oleh seorang Hacker yang dimaksudkan untuk menyerang database dari targetnya, seorang Hacker akan mendapatkan banyak informasi yang terdapat pada database targetnya [4]. Selain itu, serangan Cross-Site Scripting (XSS) juga biasa digunakan untuk mengubah situs web. Dalam serangan ini, pelaku menyisipkan kode skrip berbahaya ke dalam halaman web, yang kemudian dijalankan oleh browser pengguna. Ini memungkinkan pelaku mencuri informasi sensitif, mengarahkan pengguna ke halaman palsu, atau mengubah tampilan dan nuansa situs [5].

Penerapan teknik-teknik keamanan sistem informasi, seperti pemindaian kerentanan, pengujian penetrasi, WAF, IDS dan IPS, enkripsi data, dan peningkatan keamanan fisik server, seperti instalasi CCTV dan penerapan pengendalian akses menggunakan kartu akses atau sidik jari, dapat diimplementasikan untuk memastikan kepatuhan terhadap standar keamanan informasi yang berlaku terjaga [6]. Diperlukan analisis keamanan yang bertujuan untuk menilai tingkat kerentanan situs web yang difokuskan pada ranah Vulnerability atau kerentanan menggunakan metode Vulnerability Assessment dengan menggunakan perangkat lunak Acunetix Web Vulnerability [7].

Berdasarkan uraian latar belakang tersebut, penelitian dilaksanakan untuk melakukan Pengujian dan Audit Keamanan pada Situs Web SMK Muhammadiyah 3 Terpadu Pekanbaru menggunakan Acunetix. Pemilihan aplikasi Acunetix Web Vulnerability Scanner sebagai alat penelitian didasari oleh reputasinya sebagai salah satu solusi terkemuka dalam menangani masalah keamanan situs web.

## 2. METODE PENELITIAN

Proses sistematis dalam memperoleh dan mengevaluasi bukti secara objektif mengenai asersi-asersi aktivitas dan peristiwa ekonomi, dengan tujuan untuk menentukan tingkat kesesuaian antara asersi tersebut dengan kriteria yang telah ditetapkan sebelumnya, serta mengkomunikasikan hasilnya kepada para pemangku kepentingan [8]. Kerangka kerja digunakan sebagai landasan untuk merumuskan serangkaian tahapan yang akan dilakukan dalam rangka penelitian. Hal ini memastikan bahwa setiap tahap memiliki dampak terhadap pencapaian tujuan penelitian [9]. Dimana representasi variabel yang satu dengan variabel yang lain dapat dihubungkan secara detail dan sistematis. Selain itu, kerangka penelitian perlu dikembangkan dan diterapkan agar penelitian dapat lebih mudah dipahami. Berikut ini adalah susunan kerangka kerja penelitian:




Gambar 1. Kerangka Penelitian

Kerangka penelitian merupakan suatu konsep penelitian yang saling berkaitan. Dimana representasi variabel yang satu dengan variabel yang lain dapat dihubungkan secara detail dan sistematis. Selain itu, kerangka penelitian perlu dikembangkan dan diterapkan untuk memudahkan pemahaman penelitian, berikut adalah penjelasan langkah-langkah yang akan digunakan dalam penelitian ini:

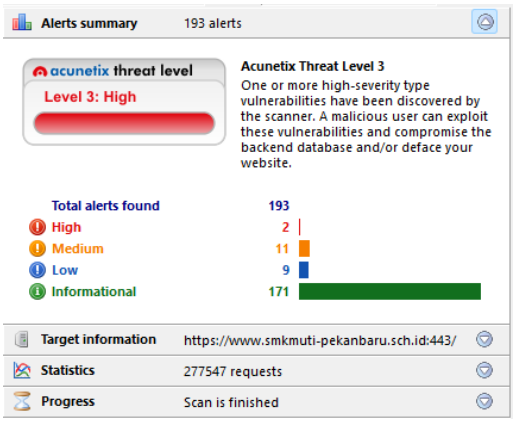
1. Identifikasi Masalah
   Pada tahap awal pelaksanaan penelitian, terlibat dalam identifikasi masalah yang akan diselidiki. Identifikasi masalah merupakan proses untuk menemukan permasalahan yang akan menjadi fokus perhatian penelitian [10]. Langkah ini merupakan langkah awal yang memungkinkan dalam melakukan penelitian dan meninjau informasi yang berkaitan dengan aspek apa pun yang relevan dengan keamanan website, untuk mengaudit celah keamanan website SMK Muhammadiyah 3 Terpadu Pekanbaru dalam penelitian ini. Langkah awal identifikasi masalah dilakukan dengan memanfaatkan data dari berbagai sumber atau melakukan komunikasi secara langsung dengan administrator situs web.
2. Analisa Masalah
   Pada fase ini, peneliti akan menjalankan proses analisis permasalahan. Kemajuan Analisis ini memungkinkan untuk lebih memahami permasalahan yang muncul ditentukan pada langkah sebelumnya. Penilaian Kerentanan (VA) merupakan evaluasi keamanan menyeluruh dan mendalam, meliputi aspek keamanan informasi, hasil pemindaian jaringan, pengelolaan sistem, konfigurasi, kesadaran keamanan pelaku yang terlibat, serta keamanan fisik, guna mengidentifikasi seluruh potensi kerentanan kritis yang ada [11].
3. Menentukan Tujuan Penelitian
   Tahap penetapan Tujuan ini merupakan fase di mana peneliti secara tegas menyatakan tujuan penelitian untuk menghindari deviasi dari hasil yang diinginkan. Tujuan penelitian ini adalah untuk mengaudit kerentanan atau kelemahan keamanan yang ada pada situs web SMK Muhammadiyah 3 Terpadu Pekanbaru dan menyajikan solusi untuk masalah yang dihadapi. Hal ini bertujuan agar hasil penelitian ini dapat dilaporkan sebagai referensi bagi pengembang atau administrator sistem guna meningkatkan dan mengembangkan sistem.
4. Mengkaji Literatur tentang Evaluasi Kerentanan
   Fase studi literatur ini bertujuan untuk mengeksplorasi metode dan dasar-dasar yang mendukung pemahaman peneliti. Sumber literatur dapat berupa artikel dan jurnal ilmiah yang membahas tentang evaluasi kerentanan serta referensi yang relevan dengan penelitian.
   Literatur merupakan salah satu tahapan dalam menemukan penilaian kerentanan (*vulnerability Assessment*) dan kerentanan (*vulnerability*), karena metode yang digunakan dalam penelitian. Literatur yang dipelajari akan dibandingkan dengan apa yang akan digunakan dalam penelitian.
5. Pengumpulan Data dan Informasi Kerentanan di Website SMK Muhammadiyah 3 Terpadu Pekanbaru
   Menganalisis data yang telah terkumpul dari berbagai sumber untuk mengidentifikasi kelemahan sistem serta menilai tingkat kesiapan serta efektivitas keamanan [12]. Saat ini, pemindaian situs web SMK MUTI diinterpretasikan menggunakan alat pemindaian kerentanan *web Acunetix*. Data yang terkumpul akan dikumpulkan dalam bentuk tabel agar mudah dilihat suatu analisis dapat dilakukan. Alat ini juga akan bertindak sebagai tes penetrasi akan diuji langsung dengan sistem. Misalnya; Untuk pengujian SQL injection, Acunetix akan melakukan serangkaian upaya untuk mengeksplorasi berbagai potensi kerentanan dalam sistem yang diuji. Alat Acunetix WVS akan menghasilkan laporan dan hasil dalam bentuk tingkat atau tingkat peringatan. Selain itu, Acunetix juga memberikan laporan umum mengenai masalah yang terdeteksi setelah proses pemindaian.
6. Analisis Hasil Pemindaian
   Pada fase berikut, data yang dihasilkan dari analisis akan mengalami pengujian terhadap kerentanan keamanan yang teridentifikasi sesuai dengan jenisnya. Dengan mengklasifikasikan jenis kerentanan keamanan, analisis akan menjadi lebih terstruktur. Hasil analisis akan didukung oleh referensi literatur yang relevan.
   a. Analisa Jenis Kerentanan Keamanan
      Analisis dilakukan dalam tahap akuisisi data, berkaitan dengan beragam jenis kerentanan keamanan seperti: Injeksi SQL, XSS, CSRF, dan lain-lain. Dengan pengelompokan ini, analisis terhadap langkah-langkah yang diperlukan untuk menangani kerentanan dapat dilakukan secara lebih efisien.
   b. Analisa Sumber Kerentanan Keamanan
      Setelah jenis kerentanan dikelompokkan, sumber kerentanan akan diidentifikasi berdasarkan kasus masing-masing. Tindakan ini dilakukan dengan tujuan memberikan solusi dan perbaikan yang sesuai dengan karakteristik kasus yang bersangkutan. Sumber-sumber kerentanan keamanan umumnya dapat dikategorikan menjadi dua, yaitu yang timbul akibat kesalahan dalam penulisan kode program dan yang muncul sebagai akibat dari kelalaian atau kesalahan konfigurasi pada infrastruktur (server), seperti pengaturan izin akses direktori. Pembagian ini memfasilitasi analisis terhadap asal-usul kerentanan keamanan tersebut.
   c. Penentuan Rekomendasi dan Perbaikan
      Setelah mengetahui jenis dan sumber kerentanan, langkah berikutnya adalah menentukan rekomendasi dan perbaikan yang sesuai. Meskipun kasus yang serupa, namun penanganannya dapat berbeda karena beberapa faktor seperti keberulangan skrip atau penggunaan fitur yang berbeda. Perbaikan tidak dapat dilakukan secara seragam karena belum dilakukan analisis yang mendalam, yang dapat mengakibatkan tumpang tindih dalam perbaikan sistem. Dalam penelitian ini, telah diidentifikasi beberapa kerentanan pada tingkat tinggi, sedang, dan rendah pada

situs web target. Sebagai hasilnya, pengujian dan perbaikan dilakukan pada situs web tersebut untuk meningkatkan keamanan layanan yang akan digunakan oleh sekolah [13].

7. Laporan
   Pada tahap ini, data yang diperoleh selama proses pemindaian dengan menggunakan Acunetix Web Vulnerability Scanner dianalisis guna menghasilkan kesimpulan terkait keadaan objek penelitian [14]. Data tersebut kemudian dijabarkan dengan menggunakan data yang terkumpul untuk menghasilkan informasi atau laporan yang dapat menjadi rekomendasi perbaikan bagi pengelola situs web. Analisis dilakukan dengan menjelaskan jenis kerentanan keamanan, sumber kerentanan, dan solusi perbaikan terhadap celah keamanan. Selain menggunakan metode tabulasi, proses penyusunan laporan juga harus disajikan dalam bahasa teknis, mengingat laporan ini akan ditujukan kepada pengembang atau administrator sistem. Meskipun demikian, untuk memudahkan pemahaman kepala sekolah, direkomendasikan untuk menyusun kesimpulan dengan menggunakan bahasa yang lebih mudah dipahami.

## 3. ANALISA DAN PERBAIKAN

Dari hasil Skrining yang dilakukan, situs web SMK MUTI memperoleh skor pada tingkat 3, Menunjukkan bahwa situs web tersebut dalam kondisi yang tidak aman. Durasi skrining dilakukan selama 2 jam 5 menit dengan 2 iterasi. Penelitian ini menemukan total 192 peringatan atau kerentanan, terdiri dari 2 tingkat Tinggi, 11 tingkat Menengah, 9 tingkat Rendah, dan 171 tingkat Informasional. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan situs hingga mencapai tingkat 1. Oleh karena itu, penjelasan perbaikan hanya difokuskan pada peringatan tingkat Tinggi dan Menengah.




Gambar 2. **Hasil *Scanning* awal *Website***

Menurut prosedur investigasi yang ditetapkan, hasil pemindaian mengalami pengelompokan terhadap jenis kerentanan, menjelaskan asal mula serta karakteristik kerentanan tersebut, dan menetapkan batasan investigasi, yakni penyusunan laporan hasil. Subsekuensinya memaparkan langkah-langkah yang diambil untuk meningkatkan aplikasi ke tingkat ancaman level 1. Berikut ini adalah penjelasan terkait peringatan dan kerentanan yang terdeteksi selama proses pemindaian situs web, serta tindakan perbaikan yang diimplementasikan.

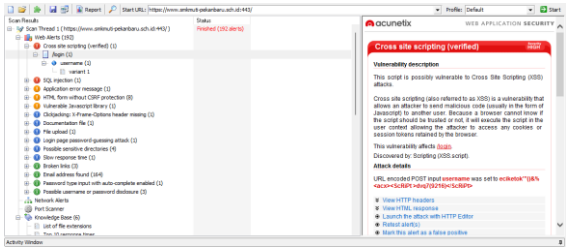
### 3.1 *Cross Site Scripting* (XSS)

Seperti yang telah dibahas pada bab sebelumnya, serangan cross-site scripting (XSS) adalah serangan siber berbahaya yang memungkinkan penyerang mencuri data berharga pada sistem informasi target. Berikut adalah langkah-langkah penyelesaiannya:

1. Membuka aplikasi Acunetix WVS dan mengakses file bug login.php.
2. Melokasikan penyimpanan file login.php.
3. Mengidentifikasi kerentanan Cross Site Scripting (XSS).
4. Melakukan perbaikan terhadap kerentanan tersebut.

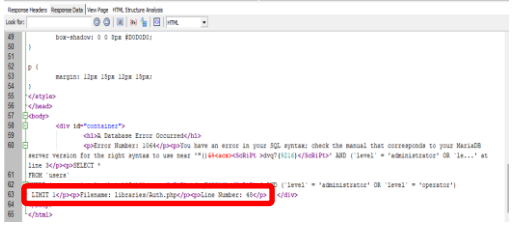
Berikut penjelasan dari langkah-langkah diatas:

1. Membuka aplikasi Acunetix WVS dan membuka bug file login.php
   Pada tahap ini, akan dilakukan pencarian file yang menjadi sumber kerentanan keamanan XSS menggunakan Acunetix. Berdasarkan temuan bug, lokasi injeksi yang terjadi terletak pada file login.php.



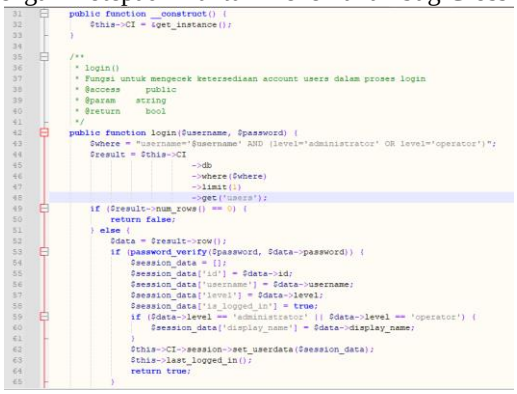
Gambar 3. Aplikasi Acunetix WVS

2. Melihat dimana file tersebut disimpan
   Menggunakan HTTP Editor di Acunetix dan melihat file yang teridentifikasi XSS tersimpan.



Gambar 4. *HTTP Editor* di Acunetix

3. Menemukan bug Cross Site Scripting (XSS)
   Membuka file libraries/Auth.php dengan Notepad++ untuk menemukan bug Cross Site Scripting (XSS).



Gambar 5. Skrip File libraries/Auth.php

4. Perbaikan Kerentanan
   Untuk mengatasi dan melindungi dari serangan XSS, beberapa langkah berikut dapat diambil:
   a. Untuk memastikan keamanan pada input data, serangan ini dapat ditangani dengan mengaktifkan filtrasi XSS dan menggunakan regular expression (regex) atau karakter yang diizinkan dalam proses skrip PHP. Dalam kasus ini, serangan XSS diperlakukan dengan melakukan filtrasi pada input dari semua metode menggunakan fungsi berikut.

```
$this->security->xss_clean(preg_replace("/[^a-zA-Z0-9\ ]/",
```

   Dalam skrip di atas, digunakan fungsi xss_clean yang merupakan bagian bawaan dari framework CodeIgniter untuk melakukan filtrasi karakter pada inputan. Sementara itu, fungsi preg_replace digunakan untuk menggunakan fungsi REGEX atau regular expression dalam membatasi jenis karakter yang dapat diterima dari inputan. Pada kasus ini, penggunaan REGEX terbatas hanya pada karakter a-z, A-Z, dan 0-9. Di sisi konfigurasi aplikasi, cukup dengan mengaktifkan pengaturan global xss filtering pada nilai true dalam file config.php.

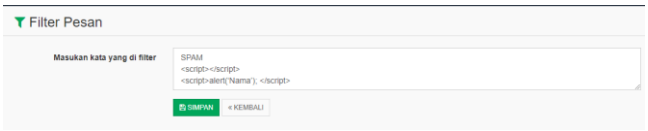
```
$config['global xss filtering'] = true;
```

   b. Pada bagian header halaman di mana injeksi XSS terjadi, terdapat kesalahan dalam skrip di mana pengambilan parameter URL tidak memerlukan penggunaan skrip $_SERVER['REQUEST_URI'], yang akan menangkap semua inputan metode GET pada URL, menyebabkan seluruh inputan tersebut terinjeksi ke dalam HTML. Seharusnya, untuk mendapatkan URL aktif, cukup menggunakan fungsi current_url() seperti berikut ini:

```
content="https://<?= $_SERVER['SERVER_NAME'].$_SERVER['REQUEST_URI'] ?>">
content="<?= current url() ?>">
```

Optimalisasi terhadap serangan *cross-site scripting* (XSS) dapat dicapai dengan mengkodekan banyak karakter. Dalam pemrograman PHP, metode ini dapat diimplementasikan menggunakan *htmlspecialchars()* yang mengkodekan semua tag HTML dan karakter khusus.

Selain itu, juga dapat mengisi celah ini dengan menambahkan filter pesan menggunakan *str_replace*. Proses optimasi *cross-site scripting (XSS)* pada website CMS SMK MUTI dilakukan dengan mengganti fungsi tersebut dengan skrip lain. Skrip terhubung dengan aplikasi kotak masuk di sistem operasi dan memerlukan filter pesan, sehingga penggunaannya lebih tervalidasi. Hal ini ditunjukkan pada Gambar 4.




Gambar 4. Implementasi *Script* pada *Filter* Pesan

Optimalisasi celah Cross Site Scripting (XSS) dengan mem-filter yaitu menggunakan filter pesan pada CMS, dimana filter ini nantinya akan melakukan redirect pada aplikasi kotak masuk yang ada pada sistem CMS sehingga user mengirimkan pesan masuk melalui halaman hubungi kami di website CMS SMK MUTI tidak dapat mengirimkan pesan yang mengandung skrip apapun. Dan peneliti juga memasukkan filter CMS ke sumber program, yaitu:

```
<!-- [Attributes by Finsweet] CMS Filter -->
<script async src="https://cdn.jsdelivr.net/npm/@finsweet/attributes-cmsfilter@1
    /cmsfilter.js"></script>
```

Gambar 5. Hasil Optimalisasi *Cross-Site Scripting* (XSS)

3.2 SQL Injection

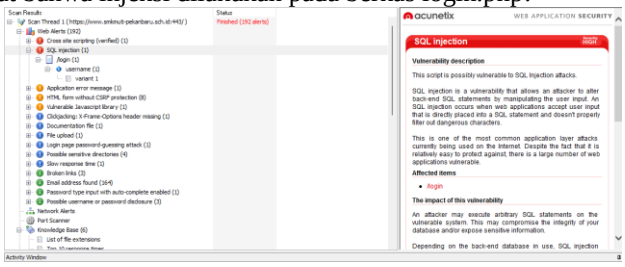
Serangan yang dilakukan melalui SQL Injection yaitu melalui modifikasi perintah SQL pada form input yang ada di Website CMS atau aplikasi, sehingga penyerang bisa mengirimkan sintaks ke database Website atau aplikasi.

Berdasarkan hasil eksploitasi kerentanan yang dilakukan oleh Acunetix Web Vulnerability Scanner, sistem yang terdampak oleh kerentanan ini adalah Website CMS SMK MUTI, dengan halaman yang menunjukkan adanya kerentanan SQL Injection adalah halaman sistem informasi status kelulusan siswa. Langkah-langkah penyelesaiannya adalah sebagai berikut:

1. Membuka aplikasi Acunetix WVS dan membuka bug file login.php
2. Melihat dimana file login.php tersebut disimpan
3. Menemukan bug SQL Injection
4. Memperbaiki bug

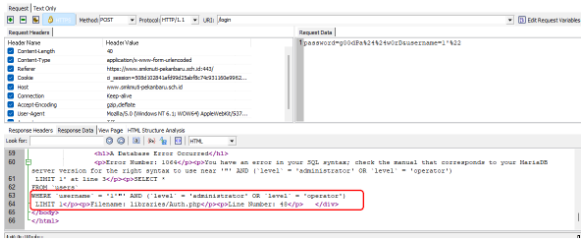
Berikut penjelasan dari langkah-langkah diatas:

1. Mengakses aplikasi Acunetix WVS dan mengakses berkas bug login.phpembuka aplikasi Acunetix WVS dan membuka bug file login.php
   Pada tahap ini, akan dilakukan pencarian berkas yang menjadi sumber kerentanan SQL Injection menggunakan Acunetix. Dari hasil temuan bug, terlihat bahwa injeksi dilakukan pada berkas login.php.




Gambar 8. Aplikasi Acunetix WVS

2. Melihat dimana file login.php tersebut disimpan
   Menggunakan fasilitas Launch the attack with HTTP Editor di Acunetix dan melihat file atau skrip yang teridentifikasi SQL Injection tersimpan.



Gambar 9. Fasilitas HTTP Editor di Acunetix

3. Menemukan Bug SQL Injection
   Membuka file libraries/Auth.php dengan aplikasi Notepad++ untuk menemukan bug SQL Injection.


Gambar 10. Skrip yang terdampak SQL Injection

4. Memperbaiki Bug

Pada kelas Auth, ada potensi celah SQL Injection di dalam metode login(). Ini terjadi karena nilai variabel $username langsung dimasukkan ke dalam string kueri tanpa sanitasi atau pengamanan.

```
$where = "username='$username' AND (level='administrator' OR level='operator')";
```

Untuk mengatasi celah ini, dapat menggunakan parameter binding atau metode aman lainnya yang disediakan oleh framework CodeIgniter. Sebagai contoh, bisa menggunakan fungsi where() bersama dengan array sebagai argumennya:

```
$where = array(
'username' => $username,
'level' => array('administrator', 'operator')
);
```

Ini akan memastikan bahwa nilai-nilai input pengguna di-sanitize sebelum dimasukkan ke dalam kueri SQL, mencegah celah SQL Injection.

3.3 Application Error Message

Kerentanan Application Error Message adalah kerentanan keamanan aplikasi yang terjadi ketika pesan kesalahan yang dihasilkan oleh aplikasi berisi informasi sensitif yang dapat dieksploitasi oleh penyerang untuk menyerang aplikasi. Umumnya, ketika terjadi kesalahan pada suatu aplikasi, pesan kesalahan ditampilkan untuk memberi tahu pengguna tentang kesalahan tersebut. Namun, jika pesan kesalahan berisi informasi sensitif seperti alamat IP, detail koneksi database, atau bahkan kata sandi, penyerang dapat menggunakannya untuk meretas atau menyerang aplikasi tersebut. Adapun langkah-langkah penyelesaiannya sebagai berikut:

1. Mengakses alamat web https://smkmuti-pekanbaru.sch.id/login
2. Membuka file login.php
3. Menemukan bug
4. Memperbaiki bug

Berikut penjelasan dari langkah-langkah diatas:

1. Mengakses alamat web https://smkmuti-pekanbaru.sch.id/login

Berdasarkan hasil scan dari Acunetix Web Vulnerability Scanner, kerentanan ini ditemukan dalam peringatan di website SMK MUTI. Elemen yang terkena kerentanan ini terdapat pada website seperti terlihat pada Gambar 11.

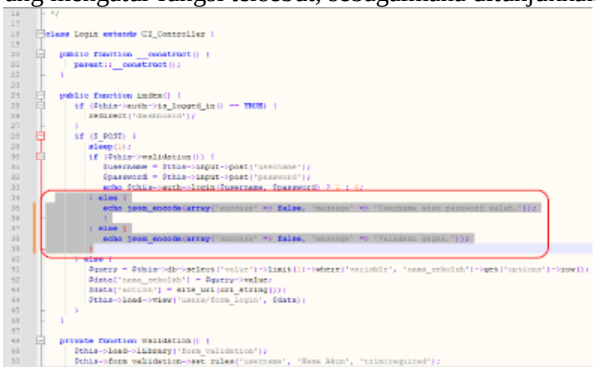

Gambar 11. Halaman Login Dashboard Admin yang terdampak

2. Membuka file login.php

Untuk melokasikan berkas Login.php, diperlukan navigasi ke dalam direktori aplikasi yang berada di root folder application\controllers\Login.php. Di dalam berkas ini, terdapat konfigurasi untuk mengatur fungsi pelaporan kesalahan (error reporting).

Gambar 12. File Login.php

3. Mengidentifikasi Bug
   Bug yang terdapat dalam kasus ini terkait dengan kesalahan pengaturan fungsi pelaporan kesalahan (error reporting). Oleh karena itu, dicari posisi skrip yang mengatur fungsi tersebut, sebagaimana ditunjukkan pada Gambar 13 berikut.



Gambar 13. Pesan error pada format JSON

Dalam kode di atas, penulis menambahkan pesan error dalam format JSON untuk menangani situasi login yang gagal. Pesan error ini akan memberi tahu pengguna bahwa username atau password yang mereka masukkan salah. Pesan error juga akan ditampilkan jika validasi formulir gagal.

3.4 Form HTML Tanpa Perlindungan CSRF
Adapun langkah-langkah penyelesaiannya sebagai berikut:
1. Mengakses alamat web https://smkmuti-pekanbaru.sch.id/home/alumni
2. Membuka file Home.php
3. Menemukan Bug
4. Memperbaiki Bug

Berikut penjelasan dari langkah-langkah diatas:

1. Mengakses alamat web https://smkmuti-pekanbaru.sch.id/home/alumni
   Halaman website yang terkena kerentanan Form HTML Tanpa Perlindungan CSRF. Berdasarkan hasil pemindaian dengan Acunetix WVS, kerentanan ini ditemukan di website SMK MUTI yaitu home/alumni.
2. Membuka file home.php
   Dalam kode program yang dibuat, tidak ada tanda-tanda penggunaan proteksi CSRF (Cross-Site Request Forgery) pada HTML form. CSRF protection biasanya diimplementasikan dengan menggunakan token CSRF yang disertakan dalam form HTML. Dapat dilihat pada Gambar 15.

Gambar 15. Kode program tidak ada CSRF Protection

3. Menemukan Bug

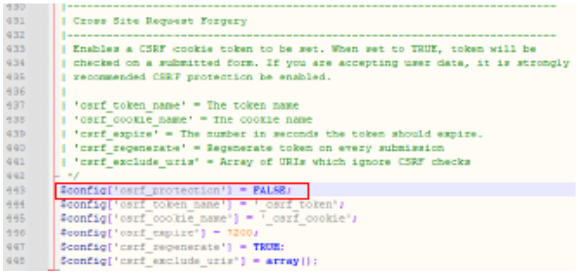
Berikut adalah contoh penggunaan form_open() untuk membuat form dengan proteksi CSRF:

```
echo form_open('controller/method');
```

Jika konfigurasi CSRF sudah diaktifkan, maka token CSRF akan otomatis disertakan dalam form yang dihasilkan oleh form_open(). Jadi, penggunaan form_open() adalah cara yang direkomendasikan untuk membuat form dengan proteksi CSRF di CodeIgniter.

4. Memperbaiki Bug

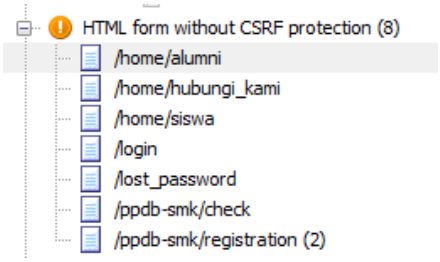
Kemudian dapat mengecek konfigurasi CSRF pada file config.php di folder application/config:




Gambar 16. Kode progam config.php

```
$config['csrf_protection'] = TRUE;
```

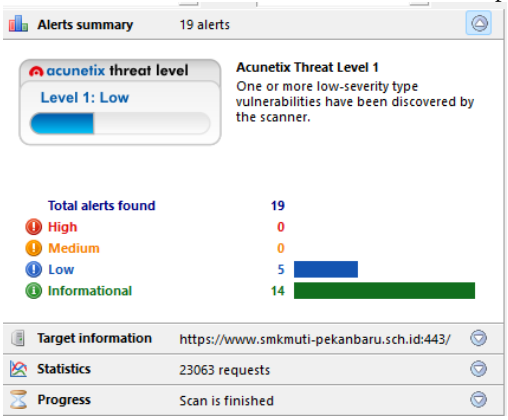
Pastikan konfigurasi ini diatur ke TRUE untuk mengaktifkan proteksi CSRF. Dan file-file yang masih terdampak HTML Form Without CSRF Protection dapat dilakukan sama pada tahapan dalam menyelesaikan, seperti pada semua tahapan pada direktori home/alumni diatas.




Gambar 17. Folder yang terdampak

## 5. HASIL

Berdasarkan proses optimalisasi yang diterapkan dalam pemindaian web, iterasi pemindaian dilakukan untuk memverifikasi apakah optimalisasi yang telah dilakukan telah menangani kerentanan keamanan yang diidentifikasi pada iterasi pemindaian sebelumnya. Langkah ini dilakukan untuk memastikan bahwa sistem beroperasi dengan aman.




Gambar 18. Hasil Scan setelah dilakukan perbaikan

Tabel 1. Perbandingan Data Web Alert Setelah dioptimalisasi

| No. | Web Alert | Jumlah Case | |
|---|---|---|---|
| | | Sebelum Dioptimalisasi | Sesudah Dioptimalisasi |
| 1. | Cross-Site Scripting (XSS) | 1 | 0 |
| 2. | SQL Injection | 1 | 0 |
| 3. | Application error Message | 1 | 0 |

| | | | |
|---|---|---|---|
| 4. | Form HTML Tanpa Perlindungan CSRF | 8 | 0 |
| **Jumlah Case** | | **11** | **0** |

Pengembang tidak akan mendapatkan dukungan pengembangan keamanan kecuali jika mereka memperbarui versi Content Management System (CMS) sekolah, PHP, dan jQuery yang digunakan. Oleh karena itu, plugin, komponen, atau ekstensi yang terinstal di situs web tersebut dapat menjadi titik serangan untuk mengeksploitasi kerentanan keamanan yang ada di situs web CMS SMK MUTI.

Situasi ini akan diikuti dengan penyampaian laporan audit keamanan website kepada tim pengembang dan pengelola website CMS SMK MUTI untuk memberikan informasi yang komprehensif tentang kerentanan yang terdeteksi di situs web.

## 6. KESIMPULAN

Berdasarkan hasil analisis dan pengujian kerentanan *website*, *tool Acunetix Web Vulnerability Scanner* dapat mendukung proses audit *website* SMK Muhammadiyah 3 Terpadu Pekanbaru (SMK MUTI) serta melakukan evaluasi dan perbaikan hingga mengambil kesimpulan, yaitu:

1. Penilaian kerentanan awal menggunakan alat Acunetix WVS mengungkapkan bahwa situs web CMS SMK MUTI terpapar ancaman pada level 3, yang termasuk dalam kategori tinggi. Dari dua iterasi pemindaian, terdeteksi 192 peringatan atau celah, di antaranya 2 di tingkat tinggi dan 11 di tingkat sedang.
2. Berdasarkan analisis, peningkatan, dan uji coba yang dilakukan pada situs web CMS SMK MUTI sebagai bagian dari penelitian ini, tingkat ancaman yang dihasilkan sudah mencapai level 1 (rendah), dengan kerentanan tingkat tinggi berkurang menjadi 0 dan jumlah kerentanan tingkat sedang juga berkurang menjadi 0. Dapat disimpulkan bahwa keamanan website CMS SMK MUTI terhadap kerentanan telah mencapai tingkat yang aman..
3. *Acunetix WVS* dapat memfasilitasi evaluasi kerentanan serta melakukan tindakan perbaikan untuk mengurangi kerentanan yang teridentifikasi.

## DAFTAR PUSTAKA

[1] I. P. D. Suarnatha, I. M. Agus, and O. Gunawan, "Jurnal Computer Science and Information Technology ( CoSciTech ) manusia," *CoSciTech*, vol. 3, no. 2, pp. 73–80, 2022.

[2] Andriansyah, Soni, Baidarus, and Rahmad Gunawan, "Implementasi Algoritma Brute Force Pada Pencarian Berita Berbasis Web," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.37859/coscitech.v2i2.3342.

[3] S. A. Putra, A. Budiono, and U. Y. K. Septo, "Vulnerability Assesment Web ProposalTugas Akhir Mahasiswa MenggunakanAcunetix dan NMAP," vol. 10, no. 2, pp. 1615–1622, 2023.

[4] R. M. Ikhsanuddin, "Audit Kerentanan Menggunakan Sqlmap Dan Reserve Shell Pada Website Staff Bhakti Semesta," vol. 2, no. 1, pp. 33–44, 2023.

[5] B. B. Aji, "Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website," *Cyber Secur. dan Forensik Digit.*, vol. 6, no. 1, pp. 25–29, 2023, doi: 10.14421/csecurity.2023.6.1.4049.

[6] A. Algiffary, M. Izman Herdiansyah, and Yesi Novaria Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 19–26, 2023, doi: 10.52158/jacost.v4i1.505.

[7] F. Kristianto, S. Rahman, and S. Bahri, "Analisis Kerentanan Pada Website Servio Menggunakan Acunetix Web Vulnerability," *Jtriste*, vol. 9, no. 1, pp. 46–55, 2022, doi: 10.55645/jtriste.v9i1.363.

[8] E. Tripustikasari and A. D. Septiadi, "Audit Keamanan Sistem Informasi Perpustakaan: Studi Kasus Di Universitas Nahdlatul Ulama Al Ghazali Cilacap," *AKSELERASI J. Ilm. Nas.*, vol. 4, no. 2, pp. 139–145, 2022, doi: 10.54783/jin.v4i2.586.

[9] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[10] L. Kestina, Yuhandri and G. Widi Nurcahyo, "Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci)," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 4, pp. 9192–9203, 2023.

[11] 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.

[12] I. Dermawan, A. Baidawi, Iksan, and S. Mellyana Dewi, "Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia," *J. Inf. dan Teknol.*, vol. 5, no. 3, pp. 20–25, 2023, doi: 10.60083/jidt.v5i3.364.

[13] M. Adha, Z. D. KWA, and A. H. Muhammad, "Website Security Test At the University of Mataram Using Vulnerability Assessment," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 2, pp. 647–655, 2023, doi: 10.29100/jipi.v8i2.3830.

[14] U. Sangga, B. Sandy, and H. H. Solihin, "Jurnal Manajemen Informatika (JAMIKA) Audit Keamanan dan Manajemen Risiko pada e-Learning," *JAMIKA*, vol. 11, no. 1, 2021, doi: 10.34010/jamika.v11i1.