Jurnal KomtekInfo

https://jkomtekinfo.org/ojs

2024 Vol. 11 No. 3 Hal: 173-180 e-ISSN: 2502-8758

# Penerapan Acunetix Vulnerability Scanner dari Serangan Siber pada Keamanan Website Kampus

Rezki Rusydi✉, Yuhandri, Syafri Arlis

Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK, Padang, 25221, Indonesia

rezkirusydi1@gmail.com

**Abstract**

Website security is an important aspect in maintaining integrity, confidentiality, and data from cyber attacks. This is a significant challenge for institutions in ensuring that their websites are protected from increasingly complex and sophisticated security threats. This study focuses on the analysis and improvement of the security system of the Faculty of Engineering website of UM West Sumatra using the Acunetix Vulnerability Scanner. Acunetix allows for fast and comprehensive vulnerability detection, thus providing a clear picture of the risks that may be faced by the website. The research method applied in this study involves penetration testing using Acunetix to detect website security gaps. This testing includes identifying gaps that may be exploited by irresponsible parties, including cross-site scripting (XSS) attacks, SQL injection, etc. The results of the analysis show several vulnerabilities that must be addressed immediately to prevent exploitation. Based on the findings, the researcher recommends improvements aimed at reducing the risk of attacks. Based on literacy scanning, the Faculty of Engineering website of UM West Sumatra is categorized at a high threat level of 3, there are 245 identified warnings, of which, 8 are considered at the high level, 2 are at the medium level, 13 are at the low level and the rest are Informational Based on the evaluation that has been carried out, the level of security achieved is at level 0. At this level, there are no identified vulnerabilities (zero vulnerabilities) and security support also reaches the optimal level (zero support). Therefore, it can be concluded that the current Faculty of Engineering website of UM West Sumatra, with level 0 status, has no vulnerabilities. The results of the study can be a reference for website managers in academic environments in protecting websites from cyber threats.

Keywords: Cyber Attacks, Acunetix Vulnerability Scanner, Security Website

**Abstrak**

Keamanan website menjadi satu aspek yang penting dalam menjaga integritas, kerahasiaan, dan data dari ancaman serangan siber. Hal ini merupakan tantangan signifikan oleh institusi dalam memastikan bahwa website mereka terlindungi dari berbagai ancaman keamanan yang semakin kompleks dan canggih. Penelitian ini berfokus pada analisis dan peningkatan sistem keamanan website Fakultas Teknik UM Sumatera Barat dengan menggunakan Acunetix Vulnerability Scanner. Acunetix memungkinkan pendeteksian kerentanan secara cepat dan menyeluruh, sehingga memberikan gambaran yang jelas mengenai risiko yang mungkin dihadapi oleh website. Metode penelitian yang diterapkan dalam studi ini melibatkan pengujian penetrasi menggunakan Acunetix untuk mendeteksi celah keamanan website. Pengujian ini mencakup identifikasi celah yang mungkin dieksploitasi oleh pihak tidak bertanggung jawab, termasuk serangan cross-site scripting (XSS), SQL injection, dll. Hasil analisis menunjukkan beberapa kerentanan yang segera diatasi untuk mencegah eksploitasi. Berdasarkan temuan, peneliti merekomendasi perbaikan yang bertujuan mengurangi risiko serangan. Berdasarkan scanning literasi, website Fakultas Teknik UM Sumatera Barat dikategorikan pada tingkat ancaman 3 yang tinggi, terdapat 245 peringatan yang teridentifikasi, di antaranya, 8 dianggap berada pada tingkat high, 2 berada pada tingkat medium, 13 berada ditingkat Low dan selebihnya Informational Berdasarkan evaluasi yang telah dilakukan, tingkat keamanan yang tercapai berada pada level 0. 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 Fakultas Teknik UM Sumatera Barat saat ini, dengan status level 0, tidak memiliki kerentanan. Hasil penelitian bisa menjadi acuan pengelola website di lingkungan akademis dalam melindungi website dari ancaman siber.

Kata kunci: Serangan Siber, Acunetix Vulnerability Scanner, Keamanan Website.



## 1. Pendahuluan

Perkembangan ilmu pengetahuan khususnya pada bidang teknologi informasi (IT), sangat membantu setiap orang mencapai tujuan hidupnya dalam waktu yang singkat, baik secara legal maupun ilegal. Banyak industri, bank serta Perguruan tinggi mendapat manfaat dari kemajuan teknologi informasi dan komunikasi global. Tetapi perubahan ini membawa masalah baru dengan munculnya berbagai pelanggaran internet oleh individu yang mencoba memanfaatkan kelemahan sistem dan ketidaktahuan pengguna tentang sistem informas dan 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

Diterima: 21-09-2024 | Revisi: 17-08-2024 | Diterbitkan: 30-09-2024 | doi: 10.35134/komtekinfo.v11i3.569

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].

Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum [8]. Teknologi informasi yang semakin berkembang pesat dapat menjadi suatu ancaman ketika disalahgunakan seperti untuk aktivitas peretasan yang tentunya dapat merugikan. Manajemen keamanan sistem informasi dapat mengurangi terjadinya penyimpangan hak akses oleh pihak tertentu dan pernyalahgunaan data dan informasi sebuah organisasi atau perusahaan [9]

Ancaman keamanan terhadap sistem dan risiko serangan dapat berasal dari tiga aspek: integritas, kerahasiaan, dan ketersediaan [10]. Kejahatan siber atau yang dikenal dengan istilah cybercrime tentu menjadi suatu ancaman serius yang perlu diantisipasi dan ditangani dengan tepat, sebagai contoh dalam penerapan sistem informasi berbasis web tidak sedikit ditemukan kasus peretasan sehingga dari hal tersebut tentu perlu adanya suatu tindakan pengungkapan pelaku yaitu dengan dilakukannya forensik digital atau digital forensic yang merupakan suatu ilmu pengetahuan dan keahlian dalam melakukan identifikasi, analisa dan pemetaan jaringan komunikasi pada suatu sistem informasi serta mengumpulkan bukti-bukti digital yang terkait dengan tindakan cybercrime tersebut. Beberapa teknologi tersebut antara lain deteksi spam, phishing deteksi, pemfilteran konten, dan pemfilteran lampiran [11]. Badan Siber dan Sandi Negara (BSSN) memprediksi peningkatan tren serangan siber, termasuk ransomware, kebocoran data, phising, dan social engineering pada tahun 2023 [12].

Bersumber dari penelitian yang Berjudul "Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID" Terdapat tujuh kerentanan yang diberikan ID A1 – A7. Kerentanan dengan ID A1 merupakan kelemahan sistem autentikasi yang membuat akses pengguna mudah diambil alih. selanjutnya, kerentanan dengan ID A2 merupakan Kelemahan pada Control Security Policy (CSP) membuat website rentan dimasukkan script berbahaya. Kemudian, kerentanan dengan ID A3 adalah Kelemahan pada konfigurasi header X-Frame-Options sehingga website utama mudah disematkan iframe berbahaya [13].

Adapun penelitian lainnya yang berjudul "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)", penelitian ini membahas perbandingan terkait tool Forensik yang digunakan untuk proses eksaminasi dan analisa. Pengambilan salinan bukti digital dilakukan dengan metode forensik statik, sedangkan tahapan penelitian dan analisa mengadaptasi dan mengimplementasikan metode forensik dari National Institute of Justice (NIJ) untuk mendapatkan bukti digital. Software pembeku drive seperti Shadow Defender terbukti berpengaruh terhadap praktik eksaminasi forensik digital terhadap didapatkannya bukti-bukti digital, dengan kondisi tersebut prosentase keberhasilannya merestorasi file hanya 28,7% sehingga dapat menjadi hambatan dalam proses forensik digital [14].

Adapula penelitian dengan judul ""Investigasi Forensik Pada E-Mail Spoofing Menggunakan Metode Header Analysis", menjelaskan bahwa Email merupakan salah satu fasilitas internet yang banyak digunakan untuk komunikasi dan bertukar informasi. Hal ini memungkinkan pihak ketiga menyalahgunakan email untuk mendapatkan informasi secara ilegal dengan mengubah identitas pengirim email dan menjadikannya seperti email yang berasal dari email yang sah (legitimate email), aktivitas tersebut biasa dikenal dengan istilah email spoofing. Untuk dapat mendeteksi adanya email spoofing, maka perlu adanya investigasi forensik email terhadap email spoofing. Salah satu teknik investigasi forensik email adalah menggunakan analisis header email (header analysis method) [15].

Begitu juga dengan Fakultas Teknik Universitas Muhammadiyah Sumatera Barat, dari penelitian-peneltian yang telah ada belum ada satupun peneliti yang pernah melakukan vulnerability terhada website

ft.umsb,ac,id punya Fakultas Teknik Universitas Muhamadiyah Sumatera Barat. Alasan Fakultas Teknik Universitas Muhammadiyah Sumatera Barat membuat web ini untuk mempermudah proses pekerjaan dalam urusan administrasi Fakultas Teknik Universitas Muhammadiyah Sumatera Barat namum perlu dilakukan pemeriksaan terhadap web tersebut untuk menutupi celah keamanan dimana rentan menjadi target serangan oleh attacker karena dari observasi dengan pengguna website Fakultas Tenkik Universitas Muhammadiyah menyampaikan ada beberapa kejangkalan seperti ada beberapa link yang kadang bisa dibukak terkadang tidak.

Tujuan yang ingin diperoleh dari penelitian ini agar lebih bermanfaat kedepannya dalam melakukan pengujian terhadap keamanan website Fakultas Teknik Universitas Muhammadiyah Sumatera Barat dengan menggunakan tools Acunetix WVS serta memberikan saran peningkatan keamanan dan perbaikan website Fakultas Teknik Universitas Muhammadiyah Sumatera Barat sehingga diharapkan memberikan manfaat kedepannya kepada Fakultas Teknik Universitas Muhammadiyah Sumatera Barat dapat mengetahui celah keamanan yang terdapat pada website serta memberikan saran peningkatan keamanan dan perbaikan website Fakultas Teknik Universitas Muhammadiyah Sumatera Barat.

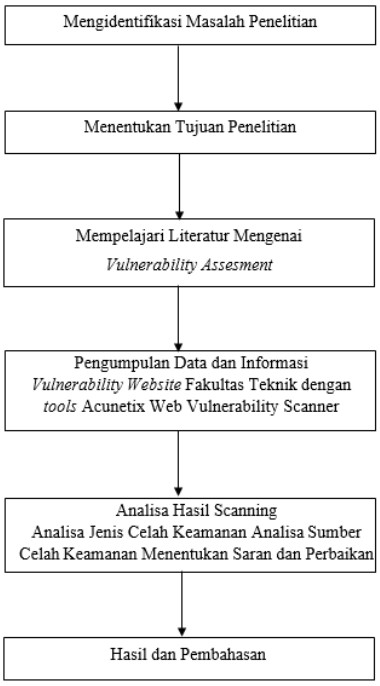
## 2. Metodologi Penelitian

Metodologi penelitian merupakan Esperimen Penetration Testing dengan bantuan Alat Acunetix Vulnerability, dan Peneliti melakuakn suatu pendekatan yang meninjau beberapa bagian dalam menemukan masalah dan menanganinya menggunakan teknik yang logis yang sesuai dengan kebenaran yang sedang dipertimbangkan. Metodologi penelitian memiliki tiga komponen yang harus dipertimbangkan secara tepat, khusunya komponen tujuan penyelidikan, komponen tenaga yang akan diselesaikan untuk mencapai tujuan,dan teknik ilmiah.

Metodologi penelitian mengidentifikasi semua tahapan yang digunakan dalam pembuatan struktur kerja atau biasa dikenal dengan kerangka kerja. Kerangka kerja digunakan untuk membuat tahapan – tahapan yang akan diselesaikan dalam penelitian, sehingga tahapan tersebut mempengaruhi setiap tahapan dalam mencapai tujuan penelitian.

Tujuan penelitian ini adalah untuk menganalisis vulnerability yang terdapat pada website Fakultas Teknik Universitas Muhammadiyah Sumatera Baratdengan menggunakan tools Acunetix Web vulnerability scanner. Data yang sudah diperoleh akan ditelaah celah keamanan yang ditemukan satu persatu berdasarkan jenis celah keamanan. Dengan mengelompokkan jenis celah keamanan memudahkan untuk menganalisi. Informasi ini dijadikan landasan untuk mengetahui apa yang menjadi penyebab dan pemberian solusi untuk masalah celah keamanan ini.

Berikut kerangka kerja penelitian adalah suatu tahapan dalam menyelesaikan suatu permasalahan yang akan diteliti. Kerangka kerja penelitian dilihat pada Gambar 1.




Gambar 1.Kerangka Kerja Penelitian

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.

### 2.1. Midentifikasi Masalah

Identifikasi masalah adalah tahapan untuk menemukan masalah sebelum melakukan penelitian. Permasalahan yang dihadapi adalah Vulnerability Assesment yang seharusnya dilakukan sebelum release dianggap tidak terlalu penting dan hanya berpedoman pada black box test atau uji fungsionalitas sistem.

### 2.2. Menetapkan Tujuan Peneltian

Tahapan penentuan tujuan ini merupakan tahapan di mana peneliti mengemukakan tujuan dari penelitian agar tidak keluar dari hasil yang ingin diperoleh. Tujuan penelitian ini adalah untuk menganalisa vulnerability atau celah keamanan yang ada pada website Fakultas Teknik UM Sumatera Barat dan memberikan solusi terhadap masalah yang ditemukan,

dengan tujuan laporan dari hasil penelitian ini dapat menjadi acuan bagi pengembang atau administrator sistem untuk melakukan perbaikan dan pengembangan sistem.

### 2.3. Mempelajari Literatur Vulnerability Assesmant

Mempelajari literatur merupakan fase dalam mencari tahu tentang vulnerabilty dan vulnerabilty assesment. Sebagai metode yang digunakan dalam penelitian, akan digunakan untuk menganalisis vulnerability yang terdapat pada website Fakultas Teknik UM Sumatera Barat, literatur yang sudah didapatkan akan dipilih dan dicocokan dengan apa aja yang akan dipakai di dalam penelitian. Sumber dari literatur ini dapat berasal dari artikel, jurnal ilmiah mengenai vulnerability assesment, serta referensi-referensi yang berhubungan dengan penelitian.

### 2.4. Pengumpulan Data dan Informasi

Tujuan dari pengumpulan data adalah untuk mendapatkan suatu informasi dari data-data yang dibutuhkan untuk penelitian agar mencapai tujuan yang diharapkan. Pada tahapan ini dijelaskan berupa kegiatan scanning dari website Fakultas Teknik Universitas Muhammadiyah Sumatera Baratdengan menggunakan tools acunetix web vulnerability Scanner. Dari data yang didapat akan dihimpun dalam bentuk tabulasi agar mudah dilakukan analisa. Tools ini akan bekerja juga sebagai penetration testing yang akan lansung diujikan dengan sistem. Sebagai contoh; untuk pengujian SQL injection maka acunetix akan bekerja meng-inject dengan berbagai macam kemungkinan untuk mendapatkan titik lemah dari sistem yang diuji. Pada tools acunetix WVS ini menghasilkan report dan keluaran berupa tingkatan atau level alert. selain itu acunetix juga memberikan report secara umum masalah yang didapat setelah dilakukan scanning.

### 2.5. Analisa Hasil Scanning

Pada tahapan ini, data yang didapatkan dari hasil scanning akan ditelaah celah keamanan yang ditemukan satu berdasarkan jenis celah keamanan. Dengan mengelompokkan jenis celah keamanan memudahkan untuk menganalisis. Hasil analisa akan di tunjang dengan beberapa literatur yang sudah dibaca.

#### 2.5.1. Analisa Jenis Celah Kemanan

Analisa yang dilakukan pada tahapan ini, adalah mengelompokkan jenis celah keamanan, seperti; SQL Injection, XSS, CSRF dan lain- lain. Dengan adanya pengelompokan ini memudahkan untuk menganalisa apa yang harus dilakukan untuk menangani celah dengan tipe ini.

#### 2.5.2. Analisa Sumber Celah Keamanan

Setelah mengelompokkan jenis celah, maka akan diturunkan case by case dari mana sumber celah tersebut. Kenapa hal ini dilakukan karena untuk memberikan solusi dan perbaikan yang tepat sasaran untuk perbaikan. Analisa sumber celah kemanan ini juga dapat dibagi menjadi 2 yaitu; bersumber dari kesalahan penulisan syntax program (coding); dan bersumber dari kekurangan atau kesalahan konfigurasi di sisi infrastrukur (server) seperti pengaturan hak akses direktori (directory level acces control), yang bisa menyebabkan client atau attacker bisa mengakases ke root folder.

#### 2.5.3. Menentukan Saran Perbaikan

Setelah jenis dan sumber telah di temukan, maka tahapan ini adalah tahapan yang paling penting, karena walaupun satu case dengan case yang lain sama, namun perbaikan atau treatment yang dilakukan berbeda-beda. Hal ini karena beberapa faktor seperti penulisan script yang berulang atau tidak menggunakan fungsi yang dipakai bersama, ataupun perbaikan yang tidak dilakukan merataa karena belum dilakukan scanning, yang menyebabkan tumpeng tindih pada perbaikan sistem.

## 3. Hasil dan Pembahasan

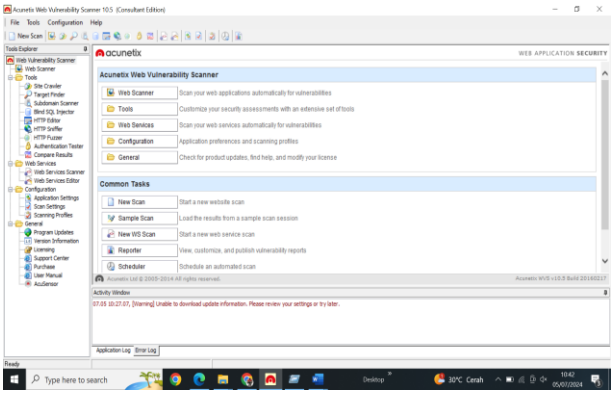
Pada tahapan ini data yang didapat dari proses scanning menggunakan acunetix web vulnerability scanner terhdapa website ft.umsb.ac.id punya Fakultas Teknik Universitas Muhammadiyah Sumatera Barat disajikan pada Gambar 2.


Gambar 2. Tampilan Awal Website

Gambar 2 terhadap website diatas kita melakukan target scanning pada website Fakultas Teknik Universitas Muhammadiyah Sumatera Barat. Versi dari Acunetix yang digunakan adalah versi 10.5. Acunetix mengelompokkan hasil VA menjadi 4, yaitu High Risk Alert (sangat rentan), Medium Risk Alert Level 2 (disebabkan oleh kesalahan konfigurasi server dan kelemahan pengkodean situs), Low Risk Alert Level 1 (berasal dari kurangnya enkripsi lalu lintas data atau keamanan direktori), Informational Alert (bersifat informasi yang dianggap bisa menjadi celah seperti IP address, alamat email dan lain lain). Proses

mendapatkan data dengan menggunakan tools Acunetix WVS dilakukan dengan tahapan berikut:

1.Untuk memulai scan wizard di Acunetix WVS, klik "File" lalu pilih "New" dan "New Website Scan." Kita juga bisa memulai scan dengan mengklik "New Scan" di sisi kiri atas menu bar. Kedua opsi tersebut akan membuka wizard untuk memulai pemindaian situs web.

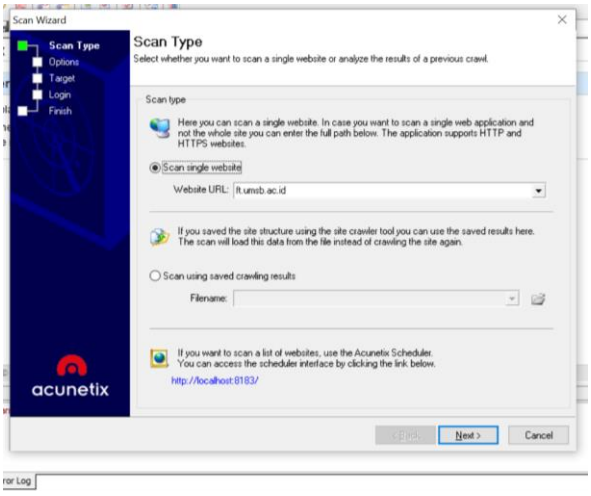


Gambar 3. Tampilan New Website Scan

Gambar 3 menunjukkan tampilan Pemilihan saat memulai proses scanning di Acunetix Web Vulnerability Scanner. Pada tahap ini, pengguna dapat memilih opsi untuk memulai scan baru. Pilihan ini memungkinkan pengguna untuk menentukan website baru yang akan dipindai.

2. Tentukan jenis scanning yang akan digunakan

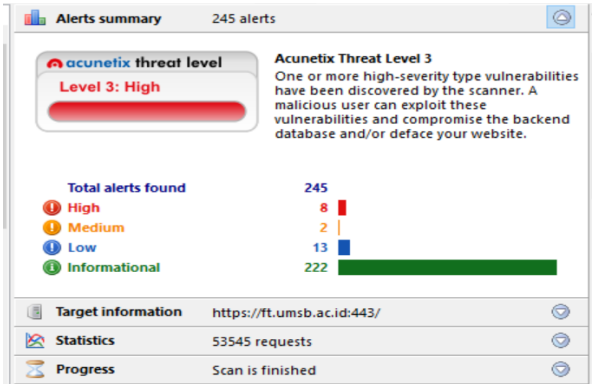
Pada tahap ini, terdapat dua opsi scan yang tersedia: Scan Single Website dan Scan Using Saved Crawling Result. Opsi pertama memungkinkan pengguna melakukan scanning secara langsung dari URL atau aplikasi yang sedang berjalan. Sedangkan opsi kedua menggunakan hasil crawling yang telah disimpan sebelumnya untuk melakukan pemindaian.




Gambar 3. Tampilan masukan target scaning

Gambar 3 di atas menunjukkan pemilihan jenis scan yang akan digunakan. Setelah itu, dari gambar tersebut kita juga dapat melihat tampilan target web yang akan discan. Target ini akan diperiksa untuk mengidentifikasi sisi kerentanannya terhadap ancaman keamanan.

3.Tahapan terakhir adalah tampilan dari Alert Summary. Tampilan ini digunakan dengan hasil pemindaian Acunetix. Hasilnya menunjukkan Threat Level (High).




Gambar 4. Tampilan Hasil Scaning Web ft.umsb.ac.id

Gambar 4 di atas menunjukkan hasil analisis lengkap dari aplikasi Acunetix Web Vulnerability Scanner. Hasil tersebut menampilkan warna dan jumlah web alert berdasarkan tingkat ancaman yang terdeteksi. Masing-masing threat level ditampilkan dengan jelas untuk memudahkan identifikasi risiko keamanan.

### 3.1 Analisa Sistem dan Perbaikan

Pada tahap analisa dan perbaikan hasil Assesment awal yang ditemukan akan diuraikan case by case menjadi informasi acuan perbaikan yang akan dilakukan tetutama untuk Level High, Medium, dan low. Serta Terdapat beberapa tahapan proses yang dilakukan sehingga muncullah beberapa kerentanan yang ditampilkan pada flowchart disajikan pada Tabel 1.

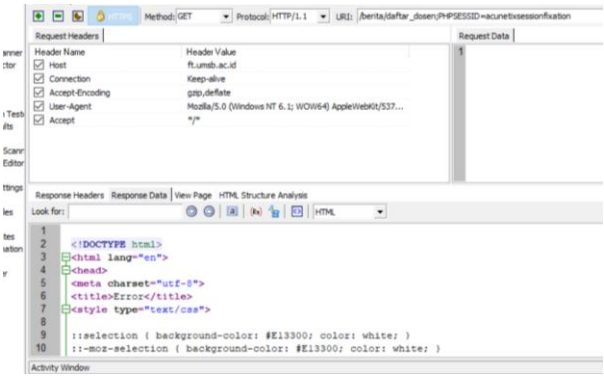
Tabel 1. Flowchart Web Alert Fakultas Teknik UM Sumbar

| No | Level | Jenis Web Alert | Level Severity | Jumlah Alert |
|---|---|---|---|---|
| 1 | 3 High | Sesion Fixation | High | 8 |
| 2 | | Development configuration file | Medium | 1 |
| 3 | | Slow HTTP Denial of Service Attack | Medium | 1 |
| 4 | | Clikjackiing :X-Frame-Options header missing | Low | 1 |
| 5 | | Cookie without Secure flag set | Low | 1 |
| 6 | | Documentation file | Low | 1 |
| 7 | | Slow respone time | Low | 10 |
| 8 | | Broken links | Informational | 6 |
| 9 | | Email Address Found | Informational | 216 |

Tabel 1, dijelaskan bahwa Sumatera Barat memiliki sembilan web alert yang ditampilkan. Dua di antaranya bersifat informational, yang artinya hanya memberikan informasi tanpa menunjukkan kerentanan. Dengan demikian, jumlah total web alert yang perlu diperhatikan terkait kerentanan ada tujuh.

a. Sesion Fixation

Session Fixation adalah teknik serangan yang digunakan untuk mencuri atau mengendalikan sesi pengguna yang sah di aplikasi web. Penyerang memaksa pengguna untuk menggunakan ID sesi yang telah ditentukan oleh penyerang sebelumnya. Dengan begitu, penyerang dapat mengambil alih sesi pengguna setelah login terjadi dapat dilihat pada Gambar 6.

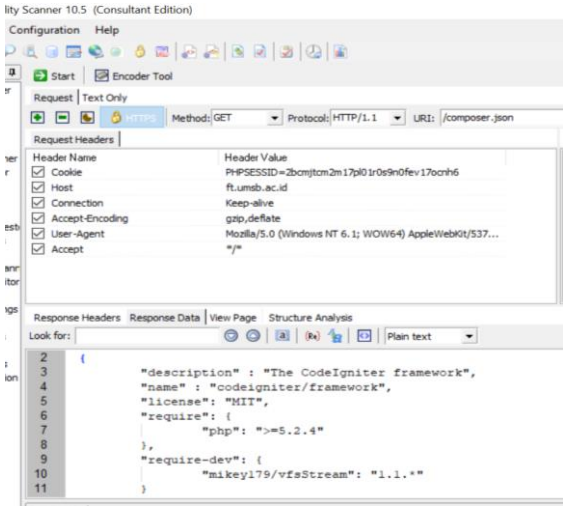


Gambar 6. Http Editor pada Sesion Fixation di Acunteix

Gambar 6 menampilkan hasil dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Pada gambar tersebut dijelaskan kemungkinan letak kerentanan yang terdeteksi pada Http Editor. Kerentanan ini terkait dengan teknik serangan Session Fixation.

b. Development Configuration

Development Configuration file ini biasanya ditemukan di dalam direktori instalasi Acunetix. File ini digunakan oleh pengembang atau administrator sistem untuk mengatur parameter dan opsi yang tidak dapat diakses melalui antarmuka pengguna grafis (GUI) standar. File ini memberikan fleksibilitas lebih dalam pengaturan aplikasi dapat dilihat pada Gambar 7.



Gambar 7. Http Editor pada Development Configuration file

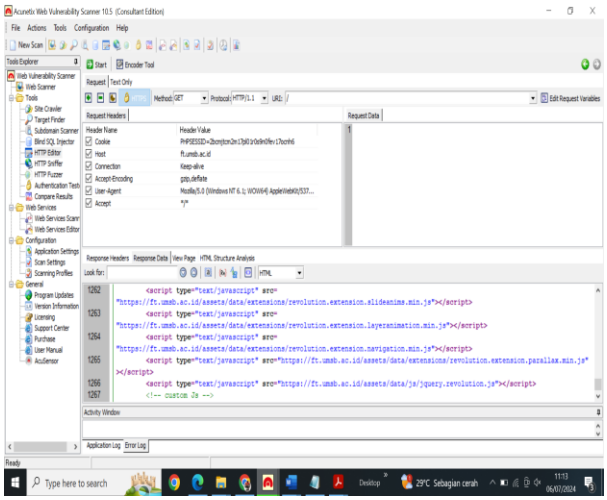
Gambar 7 ditampilkan dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Dalam gambar tersebut, dijelaskan kemungkinan letak kerentanan. Kerentanan ini terkait dengan Http Editor yang ada pada file konfigurasi.

c. Slow HTTP Deniel of Service j

Slow HTTP Denial of Service (DoS) adalah salah satu bentuk serangan DoS. Serangan ini mengandalkan kelambatan dalam proses komunikasi HTTP. Berbeda dengan serangan DoS lainnya, serangan ini tidak menggunakan volume tinggi permintaan secara instan.

d. Clikkjacking

Serangan X-Frame-Options header missing terjadi ketika situs web tidak menerapkan header keamanan. Header keamanan yang dimaksud adalah X-Frame-Options. Selain itu, pengaturan frame sejenis seperti Content Security Policy (CSP) juga dapat mencegah serangan ini dapat dilihat pada Gambar 8.



Gambar 8. Http Editor pada Clikkjacking: X-Frame-Options header missing di Acunetix

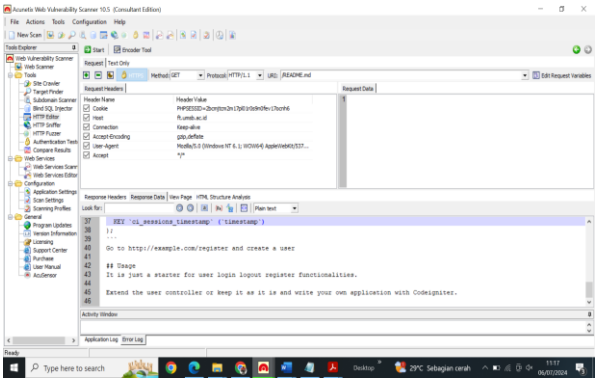
Gambar 8 ditampilkan dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Dalam gambar tersebut, dijelaskan kemungkinan kerentanan yang ada. Kerentanan ini terkait dengan Http Editor yang terdapat pada Clickjacking X-Frame Options.

e. Cookie without Secure flag set pada Acunetix

Tahapan ini menggunakan Flag Secure pada cookie. Flag ini menunjukkan bahwa cookie hanya akan dikirim ke server jika permintaan dilakukan melalui koneksi HTTPS. Dengan demikian, koneksi yang digunakan harus aman untuk mengirim cookie.

f. Documentation

File dapat merujuk pada berkas atau dokumen. Berkas ini berisi informasi penting terkait penggunaan alat keamanan. Selain itu, file juga mencakup pengaturan atau integrasi dengan alat keamanan tersebut dapat dilihat pada Gambar 9.

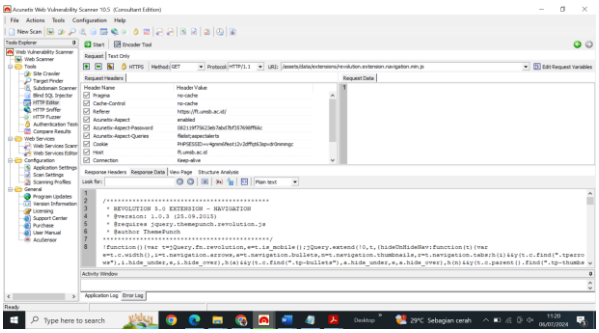


Gambar 9. Documentation File di Acunetix

Gambar 9 ditampilkan dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Dalam gambar tersebut, dijelaskan kemungkinan letak posisi kerentanan. Kerentanan ini terdapat pada Documentation File.

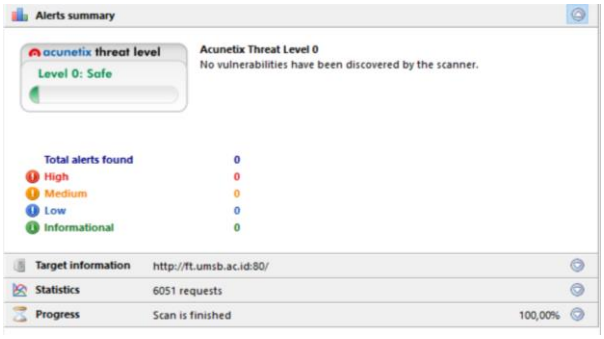
7. Slow Respone Time

Tahapan ini dapat menjadi masalah serius dalam pengujian keamanan. Masalah ini dapat mengganggu proses pemindaian yang sedang berlangsung. Selain itu, akurasi hasil yang diperoleh juga bisa terpengaruh dapat dilihat pada Gambar 10.



Gambar 10. Slow Respone di Acunetix

Gambar 10 ditampilkan dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Dalam gambar tersebut, dijelaskan letak kerentanan pada Slow Response. Setelah menganalisis dan memperbaiki 7 poin di flowchart, website ft.umsb.ac.id akan dipindai ulang untuk memastikan celah keamanan sudah tertutup dapat dilihat pada Gambar 11




Gambar 11. Hasil Terakhir Scanan Vulnerability

Gambar 11 ditampilkan dari aplikasi Acunetix Web Vulnerability Scanner versi 10.5. Dalam gambar tersebut, dijelaskan bahwa semua jenis kerentanan yang ditemukan pada web alert sebelumnya telah diperbaiki. Hasilnya, web alert menunjukkan nol, yang berarti tidak ada lagi kerentanan yang ditemukan pada website ft.umsb.ac.id.

## 4. Kesimpulan

Berdasarkan hasil analisis dan pengujian kerentanan website, tool Acunetix Web Vulnerability Scanner dapat mendukung proses audit website Fakultas Teknik Universitas Muhammadiyah serta melakukan evaluasi dan perbaikan hingga mengambil kesimpulan, yaitu Penilaian kerentanan awal menggunakan alat Acunetix WVS mengungkapkan bahwa situs web Fakultas Teknik Universitas Muhammadiyah terpapar ancaman pada level 3, yang termasuk dalam kategori tinggi. Dari dua iterasi pemindaian, terdeteksi 245 peringatan atau celah, di antaranya 8 di tingkat tinggi dan 2 di tingkat sedang. Berdasarkan analisis, peningkatan, dan uji coba yang dilakukan pada situs web Fakultas Teknik Universitas Muhammadiyah sebagai bagian dari penelitian ini, tingkat ancaman yang dihasilkan sudah mencapai level 2 (sedang), dengan kerentanan tingkat tinggi berkurang menjadi 0 dan jumlah kerentanan tingkat sedang juga berkurang menjadi 0. Dapat disimpulkan bahwa keamanan website Fakultas Teknik Universitas Muhammadiyah terhadap kerentanan telah mencapai tingkat yang aman dan juga Acunetix WVS dapat memfasilitasi evaluasi kerentanan serta melakukan tindakan perbaikan untuk mengurangi kerentanan yang teridentifikasi.

## Daftar Rujukan

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

[2] Andriansyah, Soni, Baidarus, and Rahmad Gunawan,. (2021). Implementasi Algoritma Brute Force Pada Pencarian Berita Berbasis Web. J. CoSciTech (Computer Sci. Inf. Technol., vol. 2, no. 2, pp. 120–127

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

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

[5] B. B. Aji. (2023). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. Cyber Secur. dan Forensik Digit., vol. 6, no. 1, pp. 25–29,

[6] A. Algiffary, M. Izman Herdiansyah, and Yesi Novaria Kunang. (2023). 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,

[7] F. Kristianto, S. Rahman, and S. Bahri. (2022). Analisis Kerentanan Pada Website Servio Menggunakan Acunetix Web Vulnerability. Jtriste, vol. 9, no. 1, pp. 46–55.

[8] Riskawati, Riskawati; Tahir, H. (2016). PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). Jurnal Tomalebbi, 2, 93–103.

[9] Adiyono, Soni, dkk. (2022). FRAMEWORK MANAGEMENT TO MINIMIZE RISK IN PROTECTING ENTERPRISE SYSTEMS: SYSTEMATIC LITERATURE REVIEW. Telematika: Jurnal Informatika dan Teknologi Informasi. Vol. 19(2), 159-172.

[10] Pratama, Tino Imam Maulana, Songida, Gunawan. (2022). Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik. JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu. Hal.28.

[11] Altulaihan, Esra, dkk. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. Sustainability. Jurnal Informatika dan Teknologi Informasi, 19(2), Hal 223.

[12] Putri, Nur Dwi, Dahliyusmanto. (2024). Analisis Keamanan Menggunakan Metode Live Forensic pada Web. Jurnal Teknlogi Informatika dan Komputer MH. Thamrin. Volume 10 No 1.

[13] Candra Darmawan, Putra Naibaho., & A, De.Kweldju. (2022).Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021. Jurnal Ilmiah EDUMATIC, 275

[14] Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). Evo (Electronics, Informatics, and Vocational Education), 3(1), 70–82

[15] Hoiriyah, H., Sugiantoro, B., & Prayudi, Y. (2016). Investigasi Forensik pada E-mail Spoofing menggunakan Metode Header Analysis. Data Manajemen Dan Teknologi Informasi,17(4), 20–25.