JTRISTE, Vol.9, No.1, Maret 2022, pp. 46~55
ISSN: **2355-3677 | e-ISSN: 2460-8548**

ANALISIS KERENTANAN PADA WEBSITE SERVIO MENGGUNAKAN ACUNETIX WEB VULNERABILITY

Frenly Kristianto[1], Syaiful Rahman[2*], Syamsul Bahri[3]
[1,2,3]Program Studi Informatika, STIMIK KHARISMA Makassar
e-mail: [1]frenlykristianto_18@kharisma.ac.id, [2]syaifulrahman@kharisma.ac.id,
[3]syamsulbahri@kharisma.ac.id

Abstrak

Website Servio digunakan untuk layanan perbaikan elektronik berbasis digital. Keamanan website tersebut merupakan hal yang sangat krusial untuk menjamin layanan terbaik kepada pelanggan. Dibutuhkan analisis keamanan yang bertujuan untuk mengetahui tingkat kerentanan Website Servio. Metode yang digunakan adalah Vulnerability Assessment (VA) yang menjadi kontrol preventif dengan tujuan mencegah terjadinya insiden pada sistem berbasis teknologi informasi. Secara teknis penelitian ini menggunakan tiga tahap inti dari proses Vulnerability Assessment yaitu Vulnerability Scanning, result analysis and report dengan dua kali pengujian untuk mendapatkan hasil yang valid. Teknik pengumpulan data dalam penelitian ini menggunakan teknik observasi non-partisipan yaitu teknik yang menempatkan peneliti sebagai pengamat terhadap objek yang diteliti tanpa terlibat secara langsung. Hasil dari dua pengujian diperoleh kerentanan 2 pada level low, 2 di level medium, dan 2 pada level informational dengan berbagai web alert yang ditemukan pada website berupa HTML form without anti-CSRF, clickjacking dan beberapa web informational yang harus diterapkan. Ini menunjukkan bahwa website Servio masih memiliki celah keamanan yang perlu diwaspadai oleh pengelola website agar bisa meminimalisir potensi kerentanan ke depannya.

Kata kunci: : *vulnerability, assessment, website, servio, acunetix*

Abstract

The Servio website is used for digital-based electronic repair services. The security of the website is very crucial to ensure the best service to customers. It takes a security analysis that aims to determine the level of vulnerability of Website Servio. The method used is Vulnerability Assessment (VA) which is a preventive control with the aim of preventing incidents from occurring in information technology-based systems.. Technically, this research uses three steps of the Vulnerability Assessment process. Steps Vulnerability Scanning, result analysis and report with two tests to get valid results. The data collection technique in this study uses non-participant observation techniques, namely techniques that place the researcher as an observer of the object under study without being directly involved. The results of the two tests obtained vulnerabilities 2 at the low level, 2 at the medium level, and 2 at the informational level with various web alerts found on the website in the form of HTML forms without anti-CSRF, clickjacking and several informational webs that must be implemented. This shows that the Servio website still has security holes that website managers need to be aware of in order to minimize potential vulnerabilities in the future.

Keywords: : *vulnerability, assessment, website, servio, acunetix*

[*] Corresponding author : Syaiful Rahman (syaiful@kharisma.ac.id)

Diterima : *Agustus, 2022* ***Disetujui :*** *Agustus, 2022* ***Dipublikasikan :*** *September, 2022*

1. PENDAHULUAN

Servio (Service Elektronik Online) adalah sebuah *Website* untuk memperbaiki barang elektronik yang dapat dipesan secara *online*. Tujuannya guna mempermudah masyarakat atau pengguna yang ingin memperbaiki barang elektroniknya, terutama di masa yang sekarang dengan keterbatasan jarak, waktu, hingga khawatir biaya yang tidak sesuai. Saat ini, Servio baru bisa beroperasi di dalam kota Makassar. Servio dapat diakses melalui *link* http://servio.store.

Menurut data dari Internetlivestats.com [1], terdapat lebih dari 5 miliar pengguna *internet* saat ini. Bertambahnya jumlah pengguna *internet* maka akan semakin banyak pula pihak-pihak yang terlibat dalam penyalahgunaan layanan *internet*, sehingga pembobolan data seringkali disebabkan oleh para *hacker* [2]. *Hacker* dapat dengan mudah mengambil alih sistem yang telah dibangun. Ini membuat permasalahan di data yang sifatnya pribadi, ataupun data yang penting bagi sebuah perusahaan maupun lembaga yang semestinya orang lain tidak mengetahui hal tersebut, namun dapat diakses oleh *hacker*. *Hacker* ialah seseorang dengan kemampuan tinggi pada bidang teknologi informasi [3].

Diperlukan adanya analisis keamanan yang bertujuan untuk mengetahui seberapa jauh tingkat kerentanan *Website* Servio yang berfokus pada *Vulnerability* atau kerentanan dengan metode *Vulnerability Assessment* menggunakan *software Acunetix web vulnerability.* Rumusan masalah dalam penelitian ini adalah bagaimana mengetahui kerentanan pada *website* Servio menggunakan *Acunetix web vulnerability* dengan tujuan mengetahui kerentanan pada Servio menggunakan *Acunetix web vulnerability.* Metode penelitian yang digunakan adalah *Vulnerability Assessment (VA)* dengan 2 kali pengujian guna mendapatkan hasil yang valid. *Vulnerability assessment* memberikan wawasan kepada *website* / perusahaan tentang kemungkinan kerentanan yang dapat dieksploitasi oleh peretas. Penelitian ini menggunakan *tools Acunetix web vulnerability*, yaitu perangkat lunak yang dikembangkan untuk melakukan *Scanning Website*. Kelebihannya adalah kemampuan untuk menemukan kelemahan dan kerentanan *Website*. *Acunetix* dapat menemukan semua kerentanan umum, kesalahan konfigurasi, dan kelemahan yang diabaikan dan memverifikasi kerentanan mana yang berbahaya dan tidak [4]. Berikut beberapa tinjauan pustaka yang peneliti gunakan sebagai acuan dalam penelitian ini:

Mia Zattu Maharani, Henry Rossi Adrian S.T., M.T., Setia Juli Irzal Ismail S.T., M.T. "Analisis Keamanan *Website* Menggunakan Metode *Scanning* dan Perhitungan Metriks".[5] Penelitian ini tentang analisis *Vulnerability* pada *Website* igracias.telkomuniversity.ac.id,ppdu.telkomuniversity.ac.id menggunakan metode *Scanning* dan hasil *scan* yaitu perhitungan metrik keamanan yang dimana hasil akhirnya berupa hasil *Vulnerability Assessments*.

Febri Al Fajar pada penelitiannya yang berjudul "Analisis Keamanan Aplikasi *Web* Prodi Teknik Informatika UIKA menggunakan *Acunetix web vulnerability*" [6]. Dengan tujuan penelitian yaitu melakukan audit serta menganalisis aspek keamanan pada Aplikasi Web

Prodi Teknik Informatika UIKA. Dilakukannya audit dan juga analisis keamanan adalah sebuah langkah mencegah terjadinya kerentanan sehingga dapat segera diperbaiki.

Feri Wibowo, Harjono dan Agung Purwo Wicaksono melakukan penelitian yang berjudul "Uji Vulnerability pada *Website* Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan *OpenVAS* dan *Acunetix WVS"* [7], menurut penelitian tersebut perlu diperkuat nya keamanan pada sistem operasi. Cara yang efektif yang bisa dilakukan yaitu dengan *Vulnerability Assessment (VA)* yang bertujuan sebagai kontrol preventif sehingga mencegah terjadinya kesalahan pada sistem berbasis teknologi informasi.

Md. Abdur Rahman, Mahfida Amjad, Byezid Ahmed dan Md. Saeed Siddik melakukan penelitian dengan judul *"Analyzing Web Application Vulnerabilities: An Empirical Study on E-Commerce Sector in Bangladesh"* [8] yang menyebutkan bahwa analisis empiris untuk mengevaluasi kerentanan aplikasi web berbasis e-di Bangladesh dapat menggunakan metode *Acunetix* dan Nikto.

Prof. Sangeeta Nagpure dan Sonal Kurkure melakukan penelitian dengan judul "*Vulnerability Assessment and Penetration Testing of Web Application"* [9] pada penelitian ini menyebutkan bahwa *"Acunetix web vulnerability scanner"* adalah salah satu alat pengujian yang sangat aman untuk menemukan semua kerentanan system seperti jenis injeksi SQL dan *Script* lintas situs yang dapat ditemukan dalam suatu sistem.

David Harjowinoto, Agustinus Noertjahyana, Justinus Andjarwirawan pada penelitiannya yang berjudul "*Vulnerability Testing* pada Sistem Administrasi Rumah Sakit X" [10] menyampaikan bahwa untuk menemukan kelemahan sistem administrasi pada Rumah Sakit X dapat menggunakan standar *acunetix* dan CISSP.

Kotim Subandi dan Victor Ilyas Sugara melakukan penelitian dengan judul "Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemic Covid-19 Sebagai Prosedur Mitigasi" [11]yang menyebutkan bahwa pendeteksian kelemahan pada server dengan menggunakan *acunetix* dapat memberikan informasi secara lengkap. Penelitian tersebut menggunakan *penetration testing* sebagai metode penelitiannya sedangkan pada penelitian ini menggunakan *vulnerability assessment.*

2. METODE PENELITIAN

Penelitian ini menggunakan metode *Vulnerability Assessment* dimana terjadi proses identifikasi, penilaian, serta pengklasifikasian pada tingkat keparahan, kerentanan dan keamanan pada jaringan komputer, sistem, aplikasi, atau bagian lain dari ekosistem IT. Kerentanan tersebut dapat menimbulkan risiko bagi *Website*. VA akan mencari kerentanan dan melaporkan potensi eksposur yang ada. Menurut Priandoyo [12], Vulnerability assessment bertujuan meningkatkan kesadaran pada pentingnya keamanan informasi yang sering menjadi prioritas yang kesekian di dalam institusi.

Tools yang digunakan adalah *Acunetix web vulnerability* dengan dua kali pengujian untuk mendapatkan hasil yang valid. Terdapat 4 kategori tingkat keparahan pada *acunetix* yaitu:

1. *Information Alert*

   kerentanan ini merupakan sebuah informasi keamanan yang dianggap menarik berupa kemungkinan celah-celah yang perlu diwaspadai seperti kemungkinan alamat internal IP yang terungkap maupun alamat pada email, atau bisa menjadi saran keamanan tambahan pada *website.*

2. *Low Risk Alert level 1:*

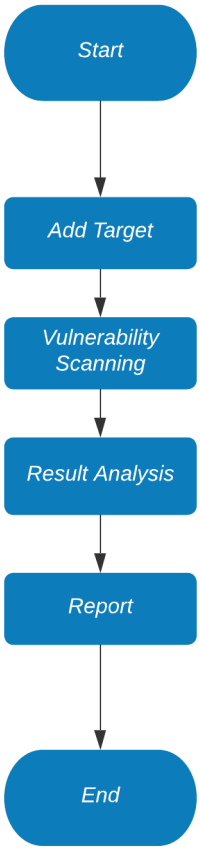
   Kerentanan yang disebabkan kurangnya enkripsi traffic data.

3. *Medium Risk Alert Level 2:*

   Terjadinya kerentanan yang dikarenakan kesalahan konfigurasi pada server serta *site coding* yang lemah, dimana memfasilitasi gangguan pada *server* dan instruksi.

4. *High Risk Alert Level 3:*

   Kerentanan termasuk kategori yang sangat berbahaya, dimana menempatkan target yang beresiko maksimum terjadinya maupun pencurian data.



Gambar 1. *Flowchart* pengujian

Berdasarkan Gambar 1, Langkah pertama adalah menambahkan target *website* dengan pengaturan tipe *full scan*. Setelah itu dilakukan *Scanning* pada *website* untuk mendapatkan hasil *vulnerability*. Setelah itu dilakukan analisis terhadap hasil *vulnerability* yang ditemukan. Terakhir tahap *report* yang bertujuan untuk membuat dokumentasi dalam

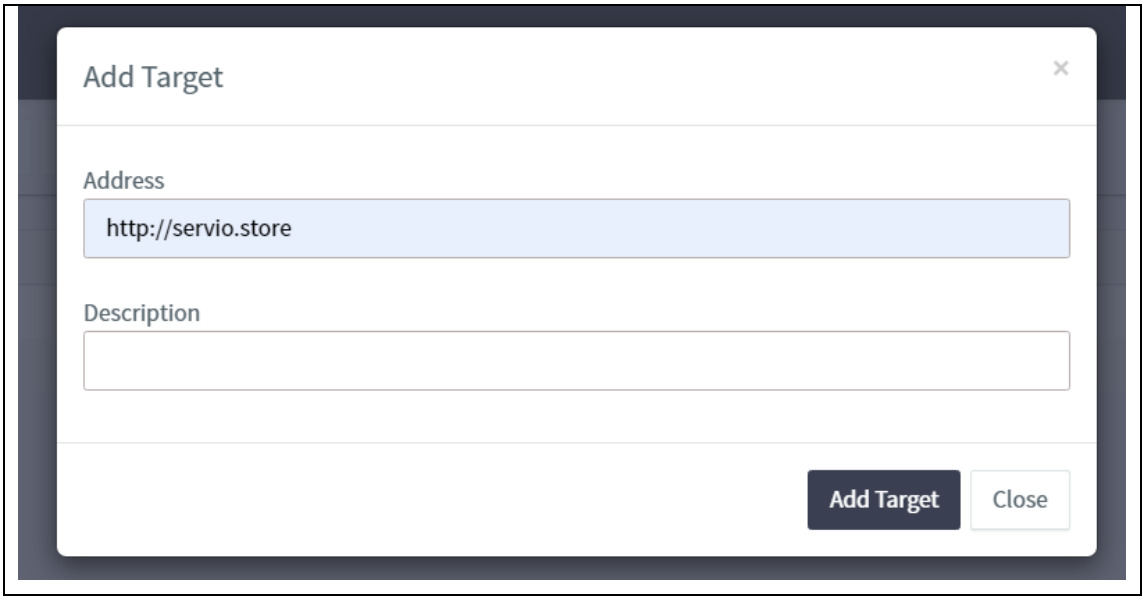
bentuk pdf atau html agar pengelola *website* dapat mengetahui kerentanan yang ada pada *website.*

3. HASIL DAN PEMBAHASAN

Keamanan *website* dianalisis menggunakan *software Acunetix web vulnerability* dengan tahapan sebagai berikut:

1. Add target

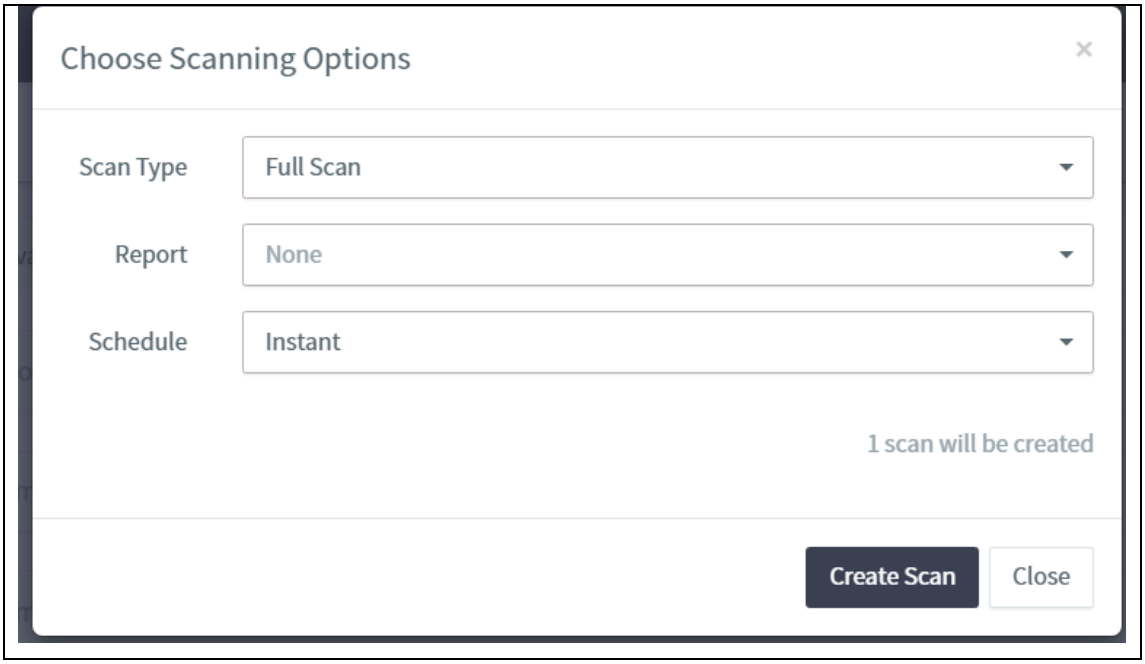
   Add target adalah input dari url target address dan description dengan memasukkan *address* http://servio.store/ seperti yang terlihat pada gambar 2:



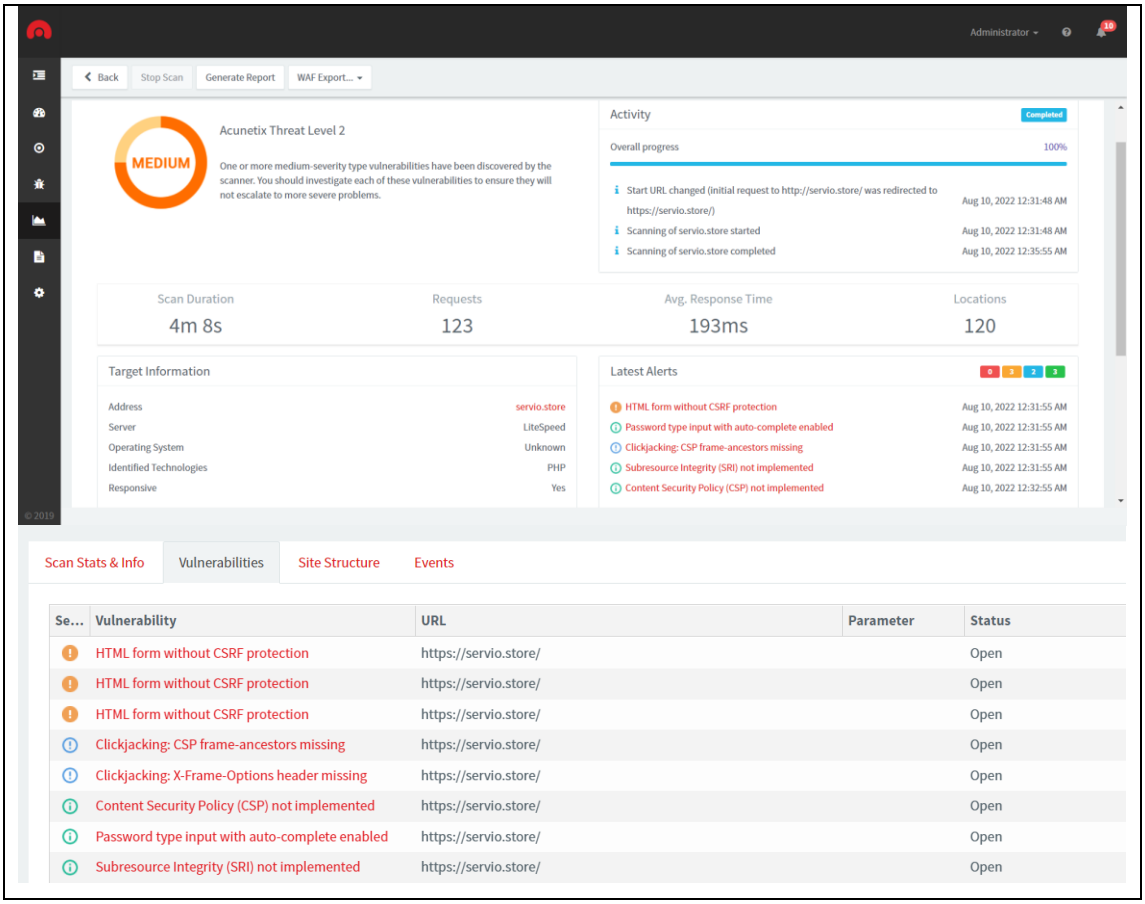
Gambar 2. *Add target*

2. Vulnerability Scanning

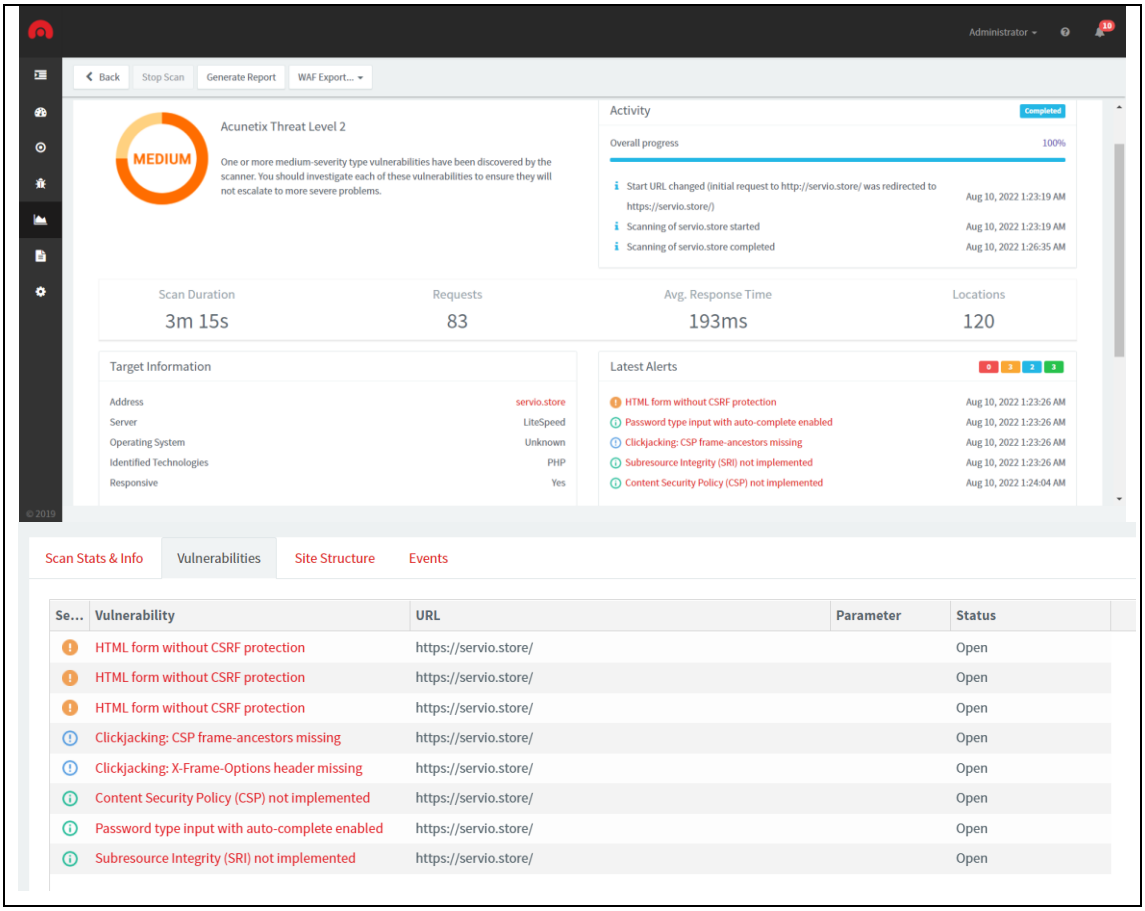
Terdapat 6 tipe scan pada Acunetix yaitu *full scan, high risk vulnerabilities, Cross-site scripting vulnerability, sql injection vulnerability, weak password, dan crawl only*. Peneliti menggunakan tipe *full scan* agar mendapatkan hasil kerentanan secara keseluruhan. Setelah itu klik *create scan* seperti pada Gambar 3:



Gambar 3. *Create scan*



Gambar 4. hasil *scan* pengujian 1



Gambar 5. hasil *scan* pengujian 2

3. Result Analysis

Seperti yang terlihat pada Gambar 4 dan Gambar 5, berdasarkan dari 2 pengujian yang telah dilakukan, terdapat hasil kerentanan yang sama pada pengujian 1 dan 2, dengan hasil 3 kerentanan dalam *level medium*, 2 di *level low* dan 2 pada *level informational*. Berikut penjelasan kerentanan dan rekomendasi penanganan dari kerantanan yang ditemukan :

1. HTML form without CSRF protection

Cross-Site Request Forgery (CSRF, atau XSRF) merupakan kerentanan yang dilakukan penyerang dengan menipu korbannya agar membuat permintaan yang tidak diinginkan oleh korban. Oleh karenanya, dengan CSRF, penyerang melakukan kejahatannya dengan aplikasi *website* pada *browser* korban. Ditemukan HTML form tanpa adanya perlindungan anti-CSRF pada Servio. Direkomendasikan untuk menambahkan perlindungan anti-CSRF pada *website* dengan beberapa pengaturan tambahan berikut:

1) Keunikan token anti-*CSRF* pada setiap pengguna.

2) Berakhir dengan otomatisnya sesi setelah selang beberapa waktu (*request timeout)*.

3) Nilai acak kriptografis harus acak pada token *anti-CSRF* dengan panjang yang memungkinkan.

4) Secara kriptografis, token *anti-CSRF* haruslah aman dengan menggunakan algoritma *PRNG* yang kuat.

5) Penambahan token *anti-CSRF* di *field* yang tersembunyi pada *form* maupun dalam *URL*.

6) Ketika terjadinya kegagalan validasi pada token *anti-CSRF,* server harus segera menolak segala tindakan yang diminta.

2. Clickjacking: CSP frame-ancestors missing

Clickjacking ialah segala jenis serangan yang ditujukan pada aplikasi web dengan tujuan korban mengklik elemen pada halaman web dengan ketidak sengajaan dimana semestinya tidak diklik. Jenis dapat terjadi pada halaman *web* yang meletakkan konten-konten berbahaya di halaman *web* terpercaya. *CSP frame-ancestors* adalah sebuah fitur keamanan yang digunakan untuk memverifikasi sumber yang diizinkan untuk ditampilkan pada halaman. Direkomendasikan untuk menambahkan header *CSP frame-ancestors* menggunakan sintaks:

```
Content-Security-Policy: frame-ancestors <source1> <source2> ... <sourceN>;
```

3. Clickjacking: X-Frame-Options header missing

X-Frame Options ialah sebuah teknik yang tujuannya menampilkan sebuah *browser* apakah boleh atau tidak dapat menampilkan halaman yang ada dalam bingkai atau *frame*. Hal ini bertujuan agar dapat menghindari *visual clickjacking* dikarenakan halaman di mana *X-Frame Option* di *setting* agar tidak dapat disematkan di halaman lain. Direkomendasikan untuk menambahkan *header X-Frame-Options*:

```
x-frame-option: SAMEORIGIN
```

4. Content Security Policy (CSP) not implemented

Content Security Policy (CSP) adalah lapisan keamanan tambahan yang membantu mendeteksi dan mengurangi jenis serangan tertentu, termasuk *Cross Site Scripting (XSS)* dan serangan injeksi data. Disarankan untuk menerapkan *Content Security Policy (CSP)* atau kebijakan keamanan konten ke dalam *website*.

5. Password type input with auto-complete enabled

Ketika *username* serta kata sandi yang baru dimasukkan ke dalam formulir dan kemudian dikirim, *browser* menanyakan apakah kata sandi akan disimpan. Di saat formulir ditampilkan, *username* dan kata sandi akan terisi secara otomatis maupun terisi ketika *username* di input. *Hacker* dapat mengetahui kata sandi *cleartext* dari *cache browser* melalui akses lokal. Disarankan untuk menonaktifkan *Password auto-complete*, biasanya menggunakan sintaks:

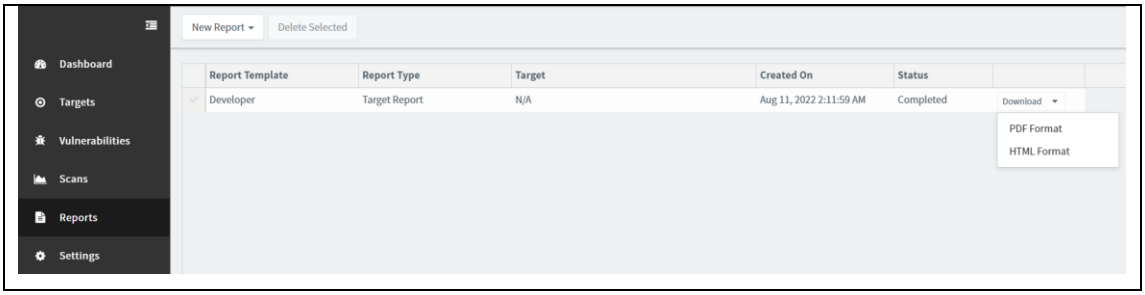
```
<INPUT TYPE=” password” AUTOCOMPLETE=” off”>
```

6. Subresource Integrity (SRI) not implemented

Terkhusus SRI, dapat memvalidasi aset yang telah tersedia, seperti jaringan pengiriman konten (CDN). Aset-aset tersebut dipastikan belum dikategorikan dengan tujuan baik serta dibuat menjadi *feedback* pada sejumlah serangan yang mana konten pada CDN berkemungkinan telah diinjeksi dengan kode yang berbahaya, serta dapat membahayakan berbagai situs web yang menggunakannya. *Browser* mengambil sejumlah data yang bersumber asal *resources* tersebut lalu mencocokkan dengan digit hash yang diambil dari sumber itu. Ketika terjadi ketidak cocokkan pada hash maka *resources* yang digunakan akan diblok. Disarankan untuk menerapkan *subresource integrity* pada *website* baik melalui *element script* atau menggunakan *tools* khusus dari *browser*.

4. Report

Tahap Terakhir adalah melakukan pelaporan hasil menggunakan fitur "*Reports*" yang ada pada *Acunetix*. Ini bertujuan agar pengelola *website* dapat melihat hasil *scan* langsung dari *Acunetix*. Hasil *report* dapat disimpan dalam bentuk pdf dan html. Bisa dilihat pada gambar 6:



Gambar 6. *Report* pada *Acunetix*

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan pada *website* servio diperoleh kerentanan – kerentanan seperti *HTML tanpa perlindungan CSRF, clickjacking,* dan beberapa *web alert informational.* Hasil yang ditemukan *Acunetix* berada pada *level medium,* yang berarti kerentanan terjadi karena kesalahan konfigurasi dan *site coding* yang lemah.

DAFTAR PUSTAKA

[1] "Number of Internet Users (2016) - Internet Live Stats." https://www.internetlivestats.com/internet-users/ (accessed Jan. 06, 2022).

[2] R. Mayasari, A. Ali Ridha, D. Juardi, and K. Ahmad Baihaqi, "Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability," *Systematics*, vol. 2, no. 1, p. 33, 2020, doi: 10.35706/sys.v2i1.3450.

[3] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System

Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, p. 853, 2020, doi: 10.25126/jtiik.2020701928.

[4] "Acunetix for IT & Telecom | Acunetix." https://www.acunetix.com/solutions/it-telecom/ (accessed Jan. 06, 2022).

[5] M. Z. Maharani, H. R. Andrian, and S. J. I. Ismail, "Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks," *e-Proceeding Appl. Sci.*, vol. 3, no. 3, pp. 1775–1782, 2017.

[6] U. I. Khaldun, "Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web," no. 2, pp. 110–120, 2020.

[7] F. Wibowo, H. Harjono, and A. P. Wicaksono, "Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS," *J. Inform.*, vol. 6, no. 2, pp. 212–217, 2019, doi: 10.31311/ji.v6i2.5925.

[8] A. Rahman and B. Ahmed, "Analyzing Web Application Vulnerabilities : An Empirical Study on E-Commerce Sector in Bangladesh," pp. 5–10, 2020.

[9] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 Int. Conf. Comput. Commun. Control Autom.*, pp. 1–6, 2017, doi: 10.1109/ICCUBEA.2017.8463920.

[10] D. Harjowinoto *et al.*, "Vulnerability Testing pada Sistem Administrasi Rumah Sakit X," pp. 2–7.

[11] K. Subandi and V. I. Sugara, "Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi," no. November, 2021.

[12] A. Priandoyo, "Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, 2006.