

Pemindaian Kerentanan Web Profil Sekolah Menggunakan RedHawk di Kali Linux

Vulnerability Scanning Web Profile School Using RedHawk on Kali Linux

Andria^{*1}, Silvy Ananta Dewi², Muchammad Rizqi Wisnu Nor Rohman³

^{1,3}Program Studi Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun

²SDN Simbatan 3 Magetan

e-mail: ^{*1}andria@unipma.ac.id

Abstrak – Situs web profil sekolah dalam pemanfaatannya tidak terlepas dari adanya potensi celah kerentanan. Adanya celah kerentanan pada sebuah situs web dapat berdampak pada akses yang tidak sah pada sistem yang mengakibatkan kebocoran data dan juga kerusakan situs web. Serangan siber yang semakin masif menunjukkan bahwa pentingnya pengelola web untuk lebih menyadari tentang kesadaran keamanan diantaranya yang dapat diwujudkan dengan melakukan pemindaian kerentanan situs web. SDN Simbatan 3 memiliki web profil sekolah namun selama pemanfaatannya belum pernah dilakukan pengujian keamanan seperti pemindaian kerentanan. Penelitian ini bertujuan untuk melakukan analisis kerentanan pada situs web profil sekolah dengan menggunakan RedHawk yang merupakan alat bantu untuk melakukan pemindaian, dan memanfaatkan Kali Linux sebagai sistem operasi yang digunakan untuk menjalankan RedHawk. Metode penelitian ini menggunakan metode Systematic Literature Review (SLR) yang merupakan metode untuk mengidentifikasi, menilai, dan menginterpretasi temuan pada suatu topik penelitian. Hasil penelitian menunjukkan bahwa situs web profil SDN Simbatan 3 berdasarkan hasil pemindaian saat ini belum ditemukan adanya celah kerentanan sehingga dapat disimpulkan bahwa situs web profil sekolah tersebut memiliki tingkat keamanan yang baik.

Kata kunci: Kerentanan; Pemindaian; RedHawk; Web

Abstract - The use of school profile websites cannot be separated from potential vulnerabilities. The existence of vulnerabilities on a website can result in unauthorized access to the system resulting in data leaks and website damage. Increasingly massive cyber attacks show that it is important for web managers to be more aware of security awareness, which can be achieved by scanning website vulnerabilities. SDN Simbatan 3 has a school profile website but during its use it has never carried out security testing such as vulnerability scanning. This research aims to carry out vulnerability analysis on school profile websites using RedHawk, which is a tool for scanning, and utilizing Kali Linux as the operating system used to run RedHawk. This research method uses the Systematic Literature Review (SLR) method, which is a method for identifying, assessing and interpreting findings on a research topic. The results of the research show that based on the results of the current scan, no vulnerabilities have been found on the SDN Simbatan 3 profile website, so it can be concluded that the school profile website has a good level of security.

Keywords: RedHawk; Scanning; Vulnerability; Web

I. PENDAHULUAN

Pesatnya perkembangan teknologi informasi sejalan dengan perkembangan aplikasi berbasis web, hal tersebut meningkatkan potensi serangan keamanan dan berbagai teknik ancaman yang dapat menyerang sebuah situs web [1]. Situs web sebagai media informasi dan komunikasi tentu memiliki peranan yang sangat penting. Tidak dapat dipungkiri bahwa terdapat risiko berupa ancaman yang berkaitan dengan celah keamanan dari sebuah situs web. Adanya celah kerentanan atau yang biasa dikenal istilah *bug* pada suatu website tersebut, tentu memerlukan perhatian serius agar tidak mudah dieksploitasi oleh pihak yang tidak memiliki kewenangan. Berdasarkan hal tersebut, diperlukan adanya upaya pencegahan diantaranya dengan melakukan analisis terhadap kemungkinan adanya celah kerentanan pada suatu website [2].

Mengingat adanya data-data penting yang tersimpan, dan diproses di sebuah aplikasi web tersebut, maka pengujian terhadap kerentanan situs web perlu dilakukan. Dari adanya temuan celah kerentanan, selanjutnya dilakukan antisipasi serta perbaikan oleh pengembang situ web sehingga dapat menjamin keamanannya [3]. Pengujian keamanan informasi atau *pentesting* merupakan sebuah teknik evaluasi terhadap keamanan pada suatu sistem, dan jaringan komputer dengan melaksanakan suatu pengujian [4].

SDN Simbatan 3 memiliki web profil sekolah yang sejauh pemanfaatannya belum pernah dilakukan pengujian keamanan berupa pemindaian kerentanan. Potensi serangan siber yang semakin masif tentunya menjadi peringatan bagi pengelola web untuk dapat meningkatkan sistem keamanan agar tidak sampai terjadi peretasan situs web yang berdampak pada akses yang tidak sah sehingga mengakibatkan pada kebocoran data dan kerusakan situs web. Tujuan penelitian ini yaitu melakukan pemindaian kerentanan situs web profil sekolah dengan menggunakan alat bantu yang disebut dengan RedHawk yang merupakan *tools* gratis untuk *Information Gathering*, dan *Vulnerability Scanning*. Dalam penelitian ini RedHawk dijalankan melalui sistem operasi Kali Linux.

Linux yang merupakan diantara dari sedikit pilihan sistem operasi komputer yang bersifat *opensource* (dapat digunakan secara bebas tanpa biaya dan dapat dimodifikasi), artinya Linux berlisensi gratis. Linux mengambil kendali infrastruktur perangkat keras ketika pertama kali sistem tersebut dijalankan. Selain itu Linux mendukung berbagai platform perangkat keras mulai dari PC berbasis Intel, Macintosh, Amiga, Silicon Graphics, Digital Alpha, sampai dengan perangkat mini computer seperti PDA dan pocket PC [5].

Adanya pengujian keamanan berupa pemindaian kerentanan situs web profil sekolah tersebut menjadi bagian dari upaya preventif dari potensi serangan siber. Diharapkan keamanan situs web beserta aset digitalnya tersebut dapat semakin terjaga dengan baik sehingga potensi kebocoran data maupun kerusakan web dapat diminimalisir secara optimal.

Penelitian sebelumnya yang berjudul “Audit Keamanan Website Menggunakan Uniscan di Kali Linux” bertujuan untuk menganalisis adanya kerentanan pada suatu website sehingga dapat membantu para pengelola web dalam mengaudit sistem keamanan pada websitenya menggunakan *Uniscan Tools* yang merupakan alat *scanner* kerentanan aplikasi web yang tersedia pada sistem operasi Kali Linux [6].

Sedangkan penelitian yang berjudul “Pengujian Keamanan Basis Data Sistem Informasi Berbasis Web”, menjelaskan bahwa pada pengujian keamanan basis data sistem informasi

berbasis web ditemukan adanya celah kerentanan pada lapisan basis data. Terjadinya kesalahan atau kekurangan dalam pengembangan sistem informasi pada aspek keamanan data dapat berpotensi adanya serangan *SQL Injection* yang memungkinkan peretas dapat mengakses basis data pada suatu web server, sehingga privasi data pengguna atau informasi sensitif didalamnya sangat beresiko untuk disalahgunakan sehingga perlu adanya upaya preventif sebagai langkah antisipasi dalam mengamankan suatu sistem informasi. Upaya yang dapat dilakukan untuk pencegahan maupun perbaikan terhadap *Bug SQL Injection* diantaranya memberikan enkripsi pada lapisan basis data, melakukan validasi terhadap input, menyembunyikan notifikasi kesalahan atau pesan *error* dan melakukan manipulasi *URL Web* [7].

Penelitian lainnya yang berjudul “Analisis Kerentanan XSS dan Rate Limiting Pada Website SMAN 8 Denpasar Menggunakan Framework OWASP ZAP”, menjelaskan bahwa website yang memiliki sistem keamanan yang lemah akan rentan terhadap serangan atau ancaman siber yang dapat terjadi setiap saat. Kasus kerentanan yang sering ditemui yakni *Cross Site Scripting (XSS)* dan *Rate Limiting*. Untuk mengantisipasi hal tersebut, aplikasi OWASP ZAP dapat dimanfaatkan untuk menguji kerentanan XSS yang ada pada sebuah website [8].

Sedangkan penelitian sebelumnya yang berjudul “Analisis Keamanan Website Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan Comprehensive Website Security Assessment”, bertujuan untuk mengidentifikasi risiko keamanan yang dapat membahayakan data sensitif yang tersimpan dan untuk menganalisis hasil Penilaian Keamanan Situs Web Komprehensif dalam menilai keamanan situs web Sekolah Menengah Atas Negeri 1 Surade. Hasil dari penelitian ini akan berkontribusi untuk meningkatkan kesadaran akan keamanan situs web dan membantu lembaga pendidikan lainnya dan pemerintah dalam memperkuat keamanan situs web untuk mengurangi ancaman siber di Indonesia [9].

Penelitian terkait yang berjudul “Diagnosis Keamanan Web Menggunakan Metode Uji Penetrasi Website Sekolah”, menunjukkan bahwa keamanan dari website Sekolah SMK Negeri 13 Medan perlu dilakukan pengujian untuk mengetahui bagian-bagian yang memiliki kelemahan dan rentan akan serangan para hacker. Serangan para hacker ini dapat menyusahkan pihak sekolah karena serangan para hacker ini berpotensi untuk merubah isi dari konten website sekolah tersebut dan memberikan informasi yang salah kepada masyarakat. Permasalahan yang telah dijabarkan tersebut dapat diselesaikan dengan melakukan Penetration testing terhadap website sekolah SMK Negeri 13 Medan. Hasil dari penelitian ini ialah melakukan analisis terhadap keamanan web sekolah SMK Negeri 13 Medan dan memberikan rekomendasi terhadap keamanan web tersebut [10].

II. METODE

Pada penelitian ini menggunakan metode *Systematic Literature Review (SLR)* yang merupakan metode *literature review* yang mengidentifikasi, menilai, dan menginterpretasi seluruh temuan pada suatu topik penelitian [4]. *Systematic Literature Review (SLR)* dapat dikaitkan dengan keamanan sistem informasi dalam melindungi kepentingan bisnis dan informasi pada sebuah sistem. Data yang dikumpulkan dan diidentifikasi menggunakan metode SLR adalah jurnal yang membahas mengenai keamanan dalam sistem informasi dan bagaimana cara mengatasinya. Dengan metode SLR, memungkinkan untuk meninjau dan mengidentifikasi jurnal secara sistematis yang setiap prosesnya mengikuti langkah atau protokol yang telah ditentukan sebelumnya [11]. Adapun alat dan bahan yang digunakan

pada penelitian ini seperti yang ditunjukkan pada tabel 1 sebagai berikut.

Tabel 1. Alat dan Bahan Pemindaian Kerentanan Situs Web

Nama	Keterangan	
	Kuantitas	Kegunaan
Laptop/PC	1	Akses ke sistem / perangkat lunak
Kali Linux	1	Sistem operasi untuk menjalankan RedHawk Tools
RedHawk	1	Perangkat lunak atau alat bantu (<i>tools</i>) untuk pemindaian kerentanan situs web
Internet	1	Agar dapat terkoneksi ke web server situs web
VirtualBox (Opsional)	1	Untuk menjalankan Kali Linux secara virtual, apabila sistem operasi di install secara langsung melalui Bootable maka tidak perlu VirtualBox / Virtual Machine
Situs Web	1	Target atau objek untuk dilakukan pemindaian kerentanan

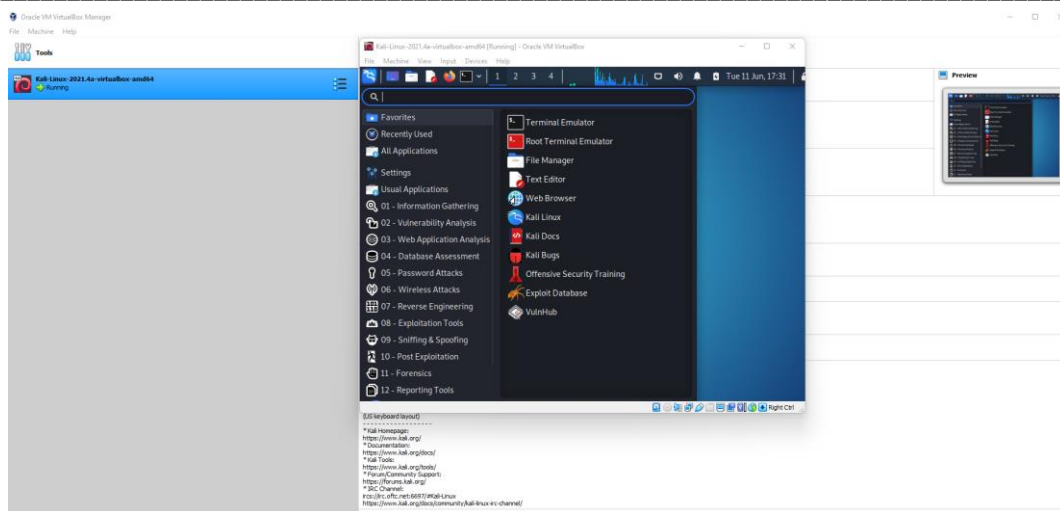
Pada penelitian ini, pengumpulan data berupa data utama yang didapat dari studi lapangan yang terdiri dari hasil observasi terhadap situs web target. Selain itu pengumpulan data yang diperoleh dari penelitian sebelumnya berupa jurnal dan sumber referensi lain seperti buku. Pemindaian kerentanan pada situs web profil dilakukan dengan eksperimen atau uji coba secara langsung ke web server target dengan memasukkan *URL Address* situs web. Adapun alur penelitian lebih jelasnya dapat ditunjukkan pada gambar 1 sebagai berikut.



Gambar 1. Alur Penelitian

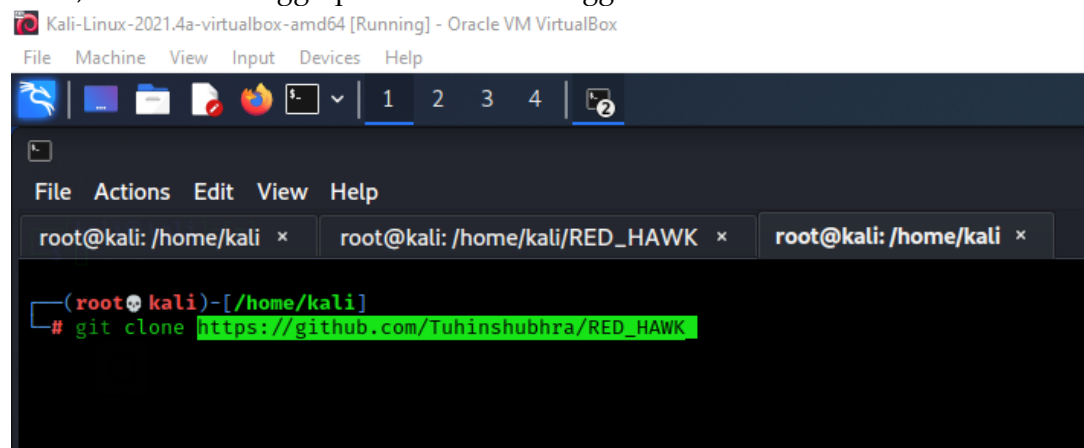
III. HASIL DAN PEMBAHASAN

Langkah pertama yang perlu dilakukan dalam melakukan pemindaian kerentanan situs web yaitu dengan menjalankan sistem operasi Kali Linux. Pada penelitian ini penulis menggunakan bantuan aplikasi *VirtualBox* untuk dapat menjalankan Kali Linux secara virtual. Lebih jelasnya dapat ditampilkan pada gambar 2 sebagai berikut.



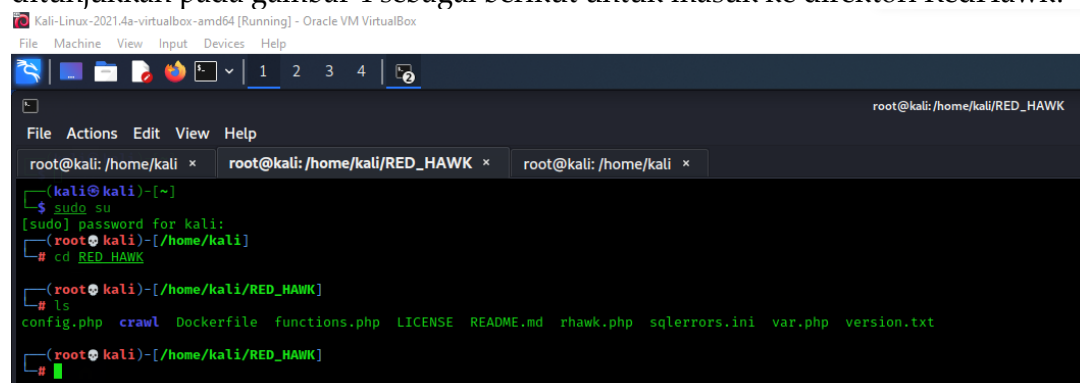
Gambar 2. Tampilan Sistem Operasi Kali Linux di VirtualBox

Selanjutnya instalasi *Redhawk Tools* melalui terminal di sistem operasi Kali Linux dengan mengetikkan: `git clone https://github.com/Tuhinshubhra/RED_HAWK` dan tekan tombol enter, kemudian tunggu proses instalasi hingga selesai.



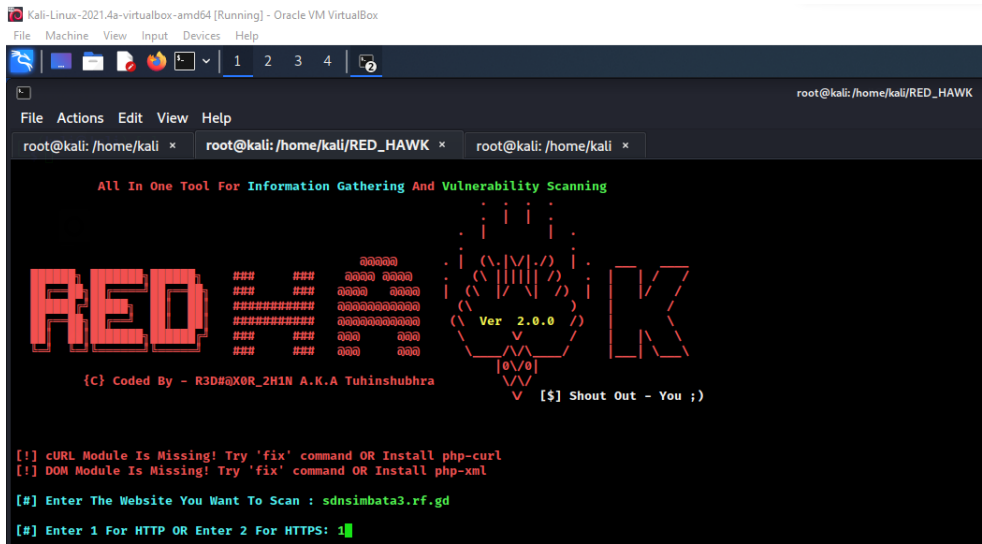
Gambar 3. Instalasi RedHawk Tools

Apabila instalasi sudah selesai, kemudian jalankan perintah atau *command* seperti yang ditunjukkan pada gambar 4 sebagai berikut untuk masuk ke direktori RedHawk.



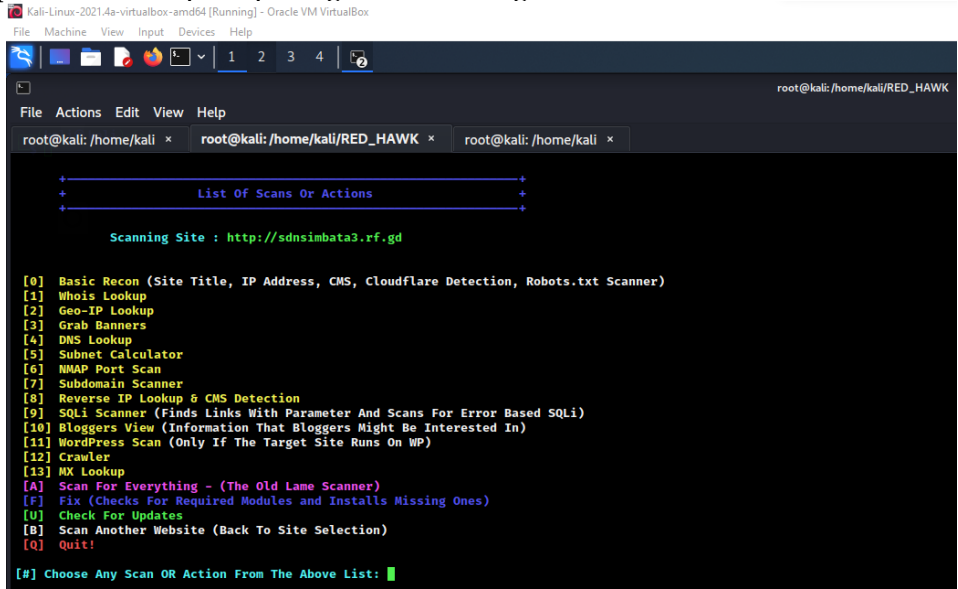
Gambar 4. Masuk ke Direktori RedHawk

Kemudian ketikkan perintah: `php rhawk.php` pada terminal untuk menjalankan programnya. Selanjutnya Redhawk tools akan terbuka seperti yang ditunjukkan pada gambar 5 sebagai berikut.



Gambar 5. Tampilan RedHawk Tool

Masukkan alamat situs web pada kolom yang tersedia, tekan tombol enter kemudian pilih jenis protokol. Pada penelitian ini situs web yang dipindai belum menggunakan SSL sehingga dipilih dengan mengetikkan angka 1, tekan enter sehingga akan ditampilkan pilihan pemindaian seperti pada gambar 6 sebagai berikut.



Gambar 6. Pilihan Pemindaian Kerentanan di RedHawk Tool

Berikut hasil dari pemindaian kerentanan situs web ditunjukkan pada tabel 2 sebagai berikut.

Tabel 2. Hasil Pemindaian Kerentanan Situs Web

Jenis Pemindaian	Hasil
Basic Recon	<pre>[#] Choose Any Scan OR Action From The Above List: 0 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbata3.rf.gd [S] Scan Type : BASIC SCAN [INFO] Site Title: [INFO] IP address: 199.59.243.225 [INFO] Web Server: Could Not Detect [INFO] CMS: Could Not Detect [INFO] Cloudflare: Not Detected [INFO] Robots File:</pre>

Whois Lookup	<pre>[#] Choose Any Scan OR Action From The Above List: 1 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : WHOIS Lookup [~] Whois Lookup Result: error valid key required [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Geo-IP Lookup	<pre>[#] Choose Any Scan OR Action From The Above List: 2 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : GEO-IP Lookup [GEO-IP] IP Address: 185.27.134.34 [GEO-IP] Country: United Kingdom [GEO-IP] State: [GEO-IP] City: [GEO-IP] Latitude: 51.4964 [GEO-IP] Longitude: -0.1224 [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Grab Banners	<pre>[#] Choose Any Scan OR Action From The Above List: 3 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : Banner Grabbing HTTP/1.1 200 OK Server: nginx Date: Tue, 11 Jun 2024 10:57:38 GMT Content-Type: text/html Content-Length: 829 Connection: close Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-cache [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
DNS Lookup	<pre>[#] Choose Any Scan OR Action From The Above List: 4 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : DNS Lookup [DNS Lookup] A : 185.27.134.34 [DNS Lookup] SOA : ns2.infinityfree.com. support.sdnsimbatan3.rf.gd. 2006112402 28800 7200 604800 86400 [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Subnet Calculator	<pre>[#] Choose Any Scan OR Action From The Above List: 5 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : SubNet Calculator [SubNet Calc] Address = 185.27.134.34 [SubNet Calc] Network = 185.27.134.34 / 32 [SubNet Calc] Netmask = 255.255.255.255 [SubNet Calc] Broadcast = not needed on Point-to-Point links [SubNet Calc] Wildcard Mask = 0.0.0.0 [SubNet Calc] Hosts Bits = 0 [SubNet Calc] Max. Hosts = 1 (2^0 - 0) [SubNet Calc] Host Range = { 185.27.134.34 - 185.27.134.34 } [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Nmap Port Scan	<pre>[#] Choose Any Scan OR Action From The Above List: 6 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : Nmap Port Scan [~] Port Scan Result: error valid key required [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Subdomain Scanner	<pre>[#] Choose Any Scan OR Action From The Above List: 7 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : Subdomain Scanner [i] Total Subdomains Found : 0 [*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop</pre>
Reverse IP Lookup	<pre>[#] Choose Any Scan OR Action From The Above List: 8 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : Reverse IP Lookup & CMS Detection (root@kali)~[/home/kali/RED_HAWK] #</pre>
SQLi Scanner	<pre>[#] Choose Any Scan OR Action From The Above List: 9 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : SQL Vulnerability Scanner (root@kali)~[/home/kali/RED_HAWK] #</pre>
Crawler	<pre>[#] Choose Any Scan OR Action From The Above List: 12 [+] Scanning Begins ... [i] Scanning Site: http://sdnsimbatan3.rf.gd [S] Scan Type : Crawling [i] Loading Crawler File [^_^] Admin Crawler File Found! Scanning For Admin Pannel [-] URLs Loaded: 817</pre>

Hasil pemindaian kerentanan situs web seperti yang ditunjukkan pada tabel 2 diatas menunjukkan bahwa tidak terdapat adanya temuan celah kerentanan sehingga situs web profil SDN Simbatan 3 dinyatakan aman. Pada RedHawk tools terdapat beragam jenis pengujian keamanan yang dapat memindai kerentanan situs web yang meliputi: *Basic Recon (Site Title, IP Address, CMS, Cloudflare Detection, Robots.txt Scanner)*, *Whois Lookup*, *Geo-IP Lookup*, *Grab Banners*, *DNS Lookup*, *Subnet Calculator*, *Nmap Port Scan*, *Sub-Domain Scanner*, *Reverse IP Lookup & CMS Detection*, *Error Based SQLi Scanner*, dan *Crawler*.

IV. KESIMPULAN

Berdasarkan pemindaian kerentanan situs web profil SDN Simbatan 3 menunjukkan bahwa dari hasil laporan RedHawk belum ditemukan adanya celah kerentanan, sehingga dapat disimpulkan bahwa situs web tersebut memiliki tingkat keamanan yang baik.

DAFTAR PUSTAKA

- [1] S. W. Ningsih, A. Almaarif, and A. Widjajarto, "Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1543–1556, 2021.
- [2] A. Andria, "Website Security Gap Analysis Using WEBPWN3R Tools at Kali Linux," *Gener. J.*, vol. 4, no. 2, pp. 69–76, 2020.
- [3] M. Wahidin, D. N. Rahayu, and R. M. Yulianto, "Analisis Kerentanan Situs Web KopKar Syariah PT BSIN menggunakan OWASP Zed Attack Proxy," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 18, no. 4, pp. 25–31, 2024.
- [4] A. Andria and R. Pamungkas, "Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux," *Indones. J. Appl. Informatics*, vol. 5, no. 1, pp. 1–10, 2020.
- [5] F. Burlian, I. Yani, I. Thamrin, M. Yanis, and Y. Resti, "PELATIHAN PENGINSTALAN DAN PENGGUNAAN OS LINUX YANG BERBIAYA MURAH DAN LEGAL BAGI GURU SMA DI KABUPATEN OGAN ILIR," *J. Pelita Sriwij.*, vol. 1, no. 1, pp. 21–27, 2022.
- [6] A. Andria, "Audit Keamanan Website Menggunakan Uniscan di Kali Linux," in *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, 2020, vol. 4, no. 3, pp. 323–328.
- [7] W. A. Andria;Ningrum and I. Mubarak, "PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB," *Pros. SNAST*, pp. 66–74, 2021.
- [8] G. A. Septiawan, K. W. S. Irawan, I. Mayasari, and I. M. E. Listartha, "Analisis Kerentanan XSS dan Rate Limiting Pada Website SMAN 8 Denpasar Menggunakan Framework OWASP ZAP," *J. Inform. Upgris*, vol. 8, no. 1, 2022.
- [9] S. Alhidamkara, I. L. Kharisma, and K. Kamdan, "Analisis Keamanan Website Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan Comprehensive Website Security Assessment," in *Prosiding SENDIKO (Seminar Nasional Hasil Penelitian & Pengabdian Masyarakat Bidang Ilmu Komputer)*, 2023, vol. 2.
- [10] M. Rozali and M. D. Sinaga, "DIAGNOSIS KEAMANAN WEB MENGGUNAKAN METODE UJI PENETRASI WEBSITE SEKOLAH," *J. Info Digit*, vol. 2, no. 1, pp. 246–262, 2024.
- [11] R. Soebiartika and I. Rindaningsih, "Systematic Literature Review (SLR): Implementasi Sistim Kompensasi dan Penghargaan Terhadap Kinerja Guru SD Muhammadiyah Sidoarjo," *MAMEN J. Manaj.*, vol. 2, no. 1, pp. 171–185, 2023.