Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux

Andria
Universitas PGRI Madiun; Jl Setia Budi No. 85, Madiun
Program Studi Sistem Informasi, Fakultas Teknik, UNIPMA, Madiun
e-mail: andria@unipma.ac.id

Abstrak— *Website sebagai media informasi dan komunikasi tentunya memiliki peran yang sangat penting. Seiring perkembangannya, tidak bisa dipungkiri bahwa terdapat ancaman terkait dengan celah keamanan dari suatu website. Adanya celah keamanan (bug) pada suatu website tentu memerlukan perhatian serius agar tidak dieksploitasi oleh pihak yang tidak bertanggung jawab. Berdasarkan hal tersebut, tentunya diperlukan adanya upaya preventif diantaranya dengan melakukan analisis terhadap kemungkinan adanya celah keamanan pada suatu website. Pada penelitian ini, tools yang digunakan adalah WEBPWN3R yang merupakan Web Applications Security Scanner, tool open source ini dapat menganalisa, mendeteksi adanya bug dari suatu website. Pengujian dilakukan menggunakan perangkat komputer bersistem operasi Kali Linux. Penelitian ini bertujuan untuk menganalisa adanya celah keamanan pada suatu website dan membantu administrator atau pengelola web untuk dapat mengetahui adanya kemungkinan celah keamanan pada suatu website, sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada website tersebut.*

Kata kunci : *Analisis, Celah Keamanan, Kali Linux, WEBPWN3R, Website*

1. PENDAHULUAN

Perkembangan Teknologi Informasi dan Sistem Informasi yang semakin pesat membawa perubahan besar dalam dunia usaha atau organisasi. Pemanfaatan Teknologi Informasi dan Sistem Informasi (TI/SI) dapat menjadi bagian yang sangat penting bagi keberlangsungan suatu organisasi dalam menjalankan kegiatan operasionalnya [1]. Penerapan teknologi informasi dan sistem informasi diantaranya dengan pengembangan aplikasi berbasis website.

Website sebagai media informasi dan komunikasi tentunya memiliki peran yang sangat penting. Seiring perkembangannya, tidak bisa dipungkiri bahwa terdapat ancaman terkait dengan celah keamanan dari suatu website. Adanya celah keamanan (bug) pada suatu website tentu memerlukan perhatian serius agar tidak dieksploitasi oleh pihak yang tidak bertanggung jawab hingga menimbulkan kerugian.

Berdasarkan hal tersebut, tentunya diperlukan adanya upaya preventif diantaranya dengan melakukan analisis terhadap kemungkinan adanya celah keamanan pada suatu website. Pada penelitian ini, *tool* yang digunakan adalah WEBPWN3R yang merupakan *Web Applications Security Scanner, tool open source* ini dapat menganalisa, mendeteksi adanya bug dari suatu website.

Pengujian dilakukan menggunakan perangkat komputer bersistem operasi Kali Linux. Mengutip dari situs resminya, *"Kali Linux, Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments."* [2]. Kali Linux merupakan sistem operasi *open source* yang dapat dimanfaatkan untuk melakukan *penetration testing* terhadap suatu sistem dan jaringan komputer. Terdapat lebih dari 300 *tools* dengan fungsi masing-masing yang dapat digunakan untuk melakukan pengujian keamanan terhadap suatu sistem.

Pada penelitian sebelumnya [3], analisis sistem keamanan web server dan database server dilakukan menggunakan tool Suricata. Suricata merupakan perangkat lunak pendeteksi dan sekaligus pencegah gangguan atau Intrusion Detection and Prevention System (IDPS) open source yang merupakan generasi lanjutan dari IDS/IPS.

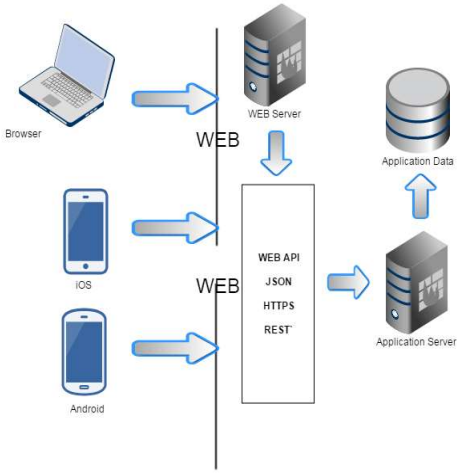
Perbedaan mendasar dengan penelitian ini yaitu pada tool dan jenis analisa yang dilakukan. Bila pada penelitian sebelumnya tool yang dipakai menggunakan Suricata dengan analisa yang mengarah pada pendeteksi dan sekaligus pencegah gangguan atau Intrusion Detection and Prevention System (IDPS), pada penelitian ini tool yang dipakai yaitu WEBPWN3R dengan beragam analisa celah keamanan seperti: Remote Code/Command Execution, Cross-Site Scripting (XSS) dan SQL Injection.

Penelitian ini bertujuan untuk menganalisa adanya celah keamanan pada suatu website dan membantu administrator atau pengelola web untuk dapat mengetahui adanya kemungkinan celah keamanan pada suatu website, sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada website tersebut.

2. METODE PENELTIAN

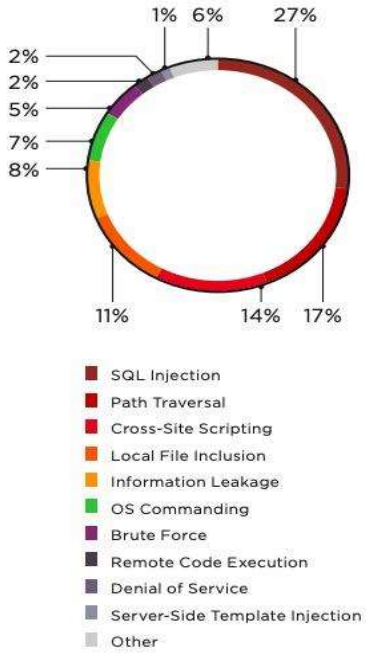
WEBPWN3R merupakan tool yang ditulis dengan bahasa Python. Fitur yang disediakan oleh tool ini meliputi pendeteksian *remote command execution vulnerability, cross site scripting attacks* dan kelemahan basis data dalam aplikasi web.

Belakangan ini berkembang berbagai cara untuk menghack suatu web server tergantung dengan kelemahan dari web server tersebut. Salah satu dengan cara hacking web server dengan SQL Injection. SQL Injection merupakan sebuah teknik hacking dimana seorang penyerang dapat memasukkan perintah-perintah SQL melalui URL untuk dieksekusi oleh database. Penyebab utama dari celah ini adalah variable yang kurang di filter, jadi hacker dapat dengan mudah mendapatkan data dari web server targetnya [4].



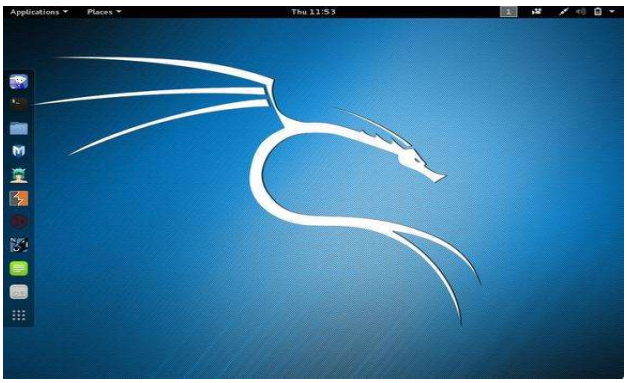
Gambar 1. Application Server
(*http://www.starrybyte.com*)

Keamanan data pada suatu web server dapat dijadikan salah satu indikator kualitas website. Menurut Endang Supriyati, kualitas *website* dipengaruhi tiga hal yaitu kulitas system (*system quality*),kualitas layanan(*service quality*) dan kualitas informasi (*information quality*) [5]. Kualitas *website* dipengaruhi oleh beberapa faktor kualitas, kualitas informasi dapat mendiskripsikan mengenai kualitas konten dari suatu *website* [6].



Gambar 2. Top 10 Web Application Attacks
(*https://ptsecurity.com*)

Berdasarkan survei yang ditunjukkan pada gambar 2, serangan *SQL Injection* paling mendominasi disusul dengan serangan lain seperti *Path Traversal, Cross-Site Scripting* dan lain sebagainya. Serangan menggunakan SQL injeksi memungkinkan seseorang dapat login ke dalam sistem tanpa harus memiliki account serta mendapatkan hak akses pada web secara jarak jauh. Selain itu SQL injeksi juga memungkinkan penyerang untuk merubah, menghapus, maupun menambahkan data–data yang berada di dalam database. Bahkan penyerang bisa mematikan database web tersebut, sehingga tidak bisa memberi layanan kepada web server. Dari menginjeksi web kita bisa mendapatkan data-data yang bersifat sensitif seperti email dan password serta data pribadi yang terdapat pada database web target yang kita injeksi. [7].

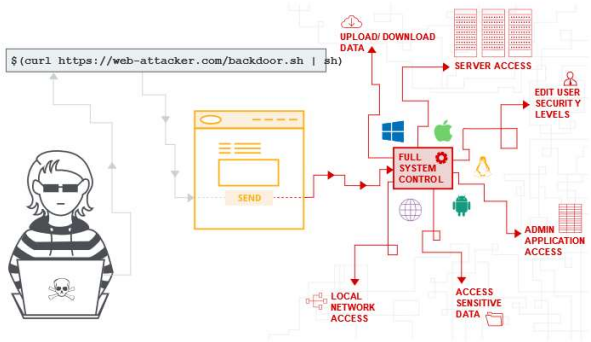


Gambar 3. Tampilan Desktop Kali Linux OS
(*http://pcworld.com*)

Kali Linux merupakan sistem operasi *open source* yang dapat digunakan untuk *penetration testing* terhadap suatu sistem dan jaringan komputer. Terdapat lebih dari 300 *tools* dengan fungsi masing-masing yang dapat digunakan untuk melakukan pengujian keamanan terhadap suatu sistem jaringan. Kali linux dikembangkan dan didanai oleh *Offensive Security.*

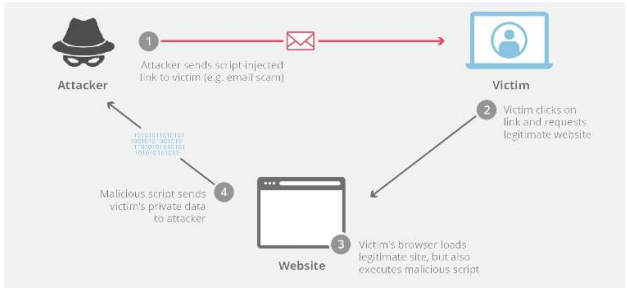
Gambar 4. WEBPWN3R Tool
(https://latesthackingnews.com)

WEBPWN3R merupakan *tool open source* untuk menganalisa keamanan aplikasi web. Fitur yang disediakan oleh tool ini meliputi pendeteksian *remote code/command execution vulnerability, cross site scripting attacks (XSS)* dan *SQL Injection*.



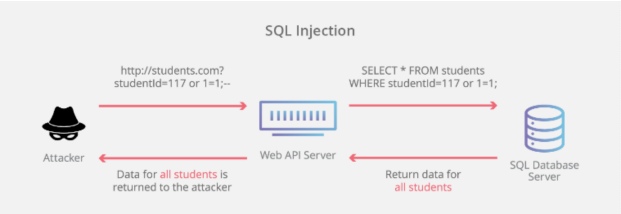
Gambar 5. *Remote Code/Command Execution*
(https://portswigger.net)

Remote Code/Command Execution merupakan jenis serangan dimana penyerang mengeksekusi kode jarak jauh menggunakan suatu kerentanan pada sistem. Kode tersebut dapat dijalankan dari server jarak jauh yang berarti bahwa serangan tersebut dapat memungkinkan berasal dari manapun selama diberikannya akses penyerang ke komputer.



Gambar 6. *Cross Site Scripting Attacks (XSS)*
(*https://cloudflare.com*)

Cross Site Scripting Attacks (XSS) merupakan jenis serangan dengan melakukan injeksi kode. XSS dilakukan oleh penyerang dengan cara memasukkan kode pemrograman tertentu ke suatu situs. Dampak dari serangan ini diantaranya penyerang dapat melakukan *bypass* keamanan pada sisi klien, memperoleh informasi sensitif dan bahkan penyerang dapat menyimpan atau menyusupkan program berbahaya pada sistem tersebut.



Gambar 7. *SQL Injection*
(*https://towardsdatascience.com*

SQL Injection merupakan jenis serangan dengan memanfaatkan celah keamanan yang ada pada lapisan database suatu aplikasi. *Database* merupakan suatu kumpulan data terhubung (*integrated*) yang disimpan secara bersama pada suatu media, data disimpan dengan cara tertentu sehingga mudah untuk digunakan sehingga proses modifikasi data dapat dilakukan dengan mudah dan terkontrol [8].

Celah keamanan pada database terjadi ketika input dari pengguna tidak di *filter* secara benar, misalnya terdapat kolom yang seharusnya hanya diisi dengan angka atau huruf, namun dapat diisi dengan karakter lain seperti symbol-simbol tertentu, sehingga penyerang menggunakan celah tersebut dengan cara memasukan *query* tertentu yang ditujukan pada *database server* dari aplikasi tersebut untuk mendapatkan akses ke basis data sehingga apabila teknik ini berhasil maka informasi sensitif yang terdapat pada *database* dapat diperoleh, hal ini tentu sangat berbahaya apabila data-data tersebut jatuh pada pihak yang tidak bertanggung jawab dan disalahgunakan.

Perancangan *database* difungsikan untuk menentukan struktur tabel dan relasi tabel yang akan diimplementasi ke dalam basis data MySQL [9]. Sehingga sangat diperlukan perancangan yang baik sebagai upaya preventif terkait dengan serangan SQL Injection.

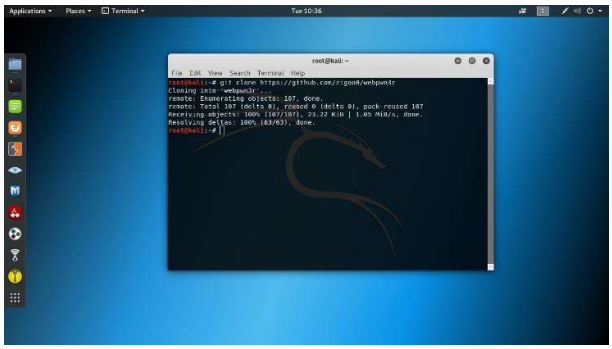
Metode penelitian ini menggunakan metode penelitian kuantitatif dengan melakukan uji coba atau eksperimen langsung ke server target dengan memasukkan *URL Address* suatu situs melalui link yang memungkinkan terdapat adanya suatu celah keamanan. Adapun pengumpulan data dengan dua cara yaitu: Studi pustaka dengan mempelajari laporan penelitian dan jurnal ilmiah Studi lapangan dengan melakukan pengujian secara langsung ke web target dengan tool WEBPWN3R

3. HASIL DAN PEMBAHASAN

Perangkat yang digunakan pada penelitian ini meliputi: komputer bersistem operasi Kali Linux dan tool WEBPWN3R untuk menganalisa adanya temuan celah keamanan pada web target.

Gambar 8. Tools Penetration Testing Kali Linux
(https://kali.training)

Pertama kali yang perlu dilakukan adalah membuka Terminal pada Kali Linux.



Gambar 9. Tampilan Terminal di Kali Linux

Kemudian ketikkan perintah-perintah berikut:

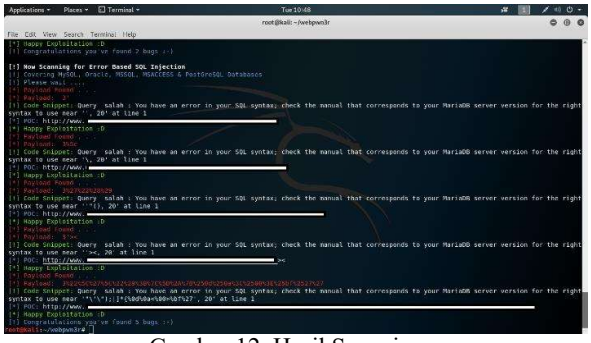
1. Perintah untuk mengeksekusi tool WEBPWN3R
   $git clone https://github.com/zigoo0/webpwn3r
2. Perintah untuk masuk ke directory tool
   $cd webpwn3r
3. Perintah untuk menjalankan tool WEBPWN3R
   $ chmod +x scan.py
   $ ./scan.py
4. Pilih kategori scanning dan masukkan URL Address dari web target
5. WEBPWN3R akan melakukan analisis

Gambar 10. Hasil Analisis Tool WEBPWN3R

Berdasarkan dari hasil analisis yang ditunjukkan pada gambar 10, dapat dijelaskan bahwa tidak terdapat adanya celah keamanan pada situs web target. Sehingga belum diperlukan adanya perbaikan secara serius pada web tersebut. Namun, tetap perlu dilakukan upaya preventif guna menghalau adanya kemungkinan ancaman atau serangan lainnya dengan melakukan pengecekan web secara berkala.

Kemudian pada eksperimen berikutnya, mencoba situs web lain dengan hasil seperti ditunjukkan pada gambar 11 dan gambar 12. Adapun langkah-langkah yang dilakukan sama dengan langkah sebelumnya, perbedaannya hanya pada URL Address web yang dimasukkan.

Gambar 11. Proses Scanning



Gambar 12. Hasil Scanning

Berdasarkan hasil analisis celah keamanan website dengan menggunakan tool WEBPWN3R seperti ditunjukkan pada gamabr 11 dan gambar 12, dapat dijelaskan bahwa terdapat celah keamanan website yang dapat dieksploitasi oleh peretas sehingga dapat memungkinkan terjadinya pengaksesan sistem secara tidak sah (illegal) yang ada pada suatu web server. Hal ini tentu sangat berbahaya mengingat terdapat informasi sensitif yang rawan untuk disalahgunakan. Sehingga perlu dilakukan upaya preventif berupa perbaikan sistem agar akses yang tidah sah (illegal) dapat diantisipasi dan tidak mengakibatkan dampak serius seperti penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

Tabel 1. Hasil Pengujian

No	Indikator	Hasil
1	Remote Code/Command Execution	Tidak terdapat bugs
2	Cross-Site Scripting (XSS)	Terdapat 2 bugs
3	SQL Injection	Terdapat 5 bugs

4. SIMPULAN

Pada penelitian ini, celah keamanan yang terdapat pada contoh situs web tersebut yaitu Cross-Site Scripting (XSS) dengan jumlah 2 bugs dan SQL Injection dengan jumlah 5 bugs. XSS merupakan salah satu jenis serangan dengan injeksi kode sedangkan SQL Injection merupakan suatu celah keamanan yang terdapat dalam lapisan basis data sebuah aplikasi web, sehingga memungkinkan peretas dapat mengakses database yang ada di server melalui kode tertentu pada URL.

Hasil analisa kerentanan web menggunakan tool WEBPWN3R tersebut didasarkan pada beragam analisa seperti: Remote Code/Command Execution, Cross-Site Scripting (XSS) dan SQL Injection. Sehingga hasil yang ditampilkan bisa dilihat secara spesifik dan akurat dengan mengacu pada bagian link atau kode tertentu yang berisikan celah kerentanan.

Dampak yang dirasakan bagi pengguna website setelah dilakukan analisa tentunya dapat lebih antasipatif terhadap adanya kemungkinan kerentanan website sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada website tersebut sehingga website yang dibangun dapat menjadi lebih aman dan terhindar dari ancaman serangan para peretas jahat *(blackhat)* yang dapat mengakibatkan kerugian.

DAFTAR PUSTAKA

[1] A. Andria , and Hani Atun Mumtahana, "Perancangan Sistem Informasi Prakerin Universitas PGRI Madiun Berbasis Web", *Generation Journal, Vol. 3 No.1, Januari 2019.*

[2] N. Nazwita dan S. Ramadhani. Analisis Sistem Keamanan, https://www.kali.org/

[3] Web Server dan Database Server Menggunakan Suricata. Seminar Nasional Teknologi Informasi , Komunikasi dan Industri (SNTIKI) 9 Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau Pekanbaru, 18-19 Mei 2017
H. B. Badaruddin. E Budiman and H. J. Setyadi, "Teknik Hacking Web Server Dengan SQLMap di Kali Linux", *JURTI, Vol 1 No. 1.2017*

[5] S, Endang, "Studi Empirik Social Commerce (S-Commerce) Dari Sudut Pandang Kualitas Website", *Jurnal SIMETRIS, 2015.*

[6] A. Andria, "Evaluasi Kualitas Web Portal Fakultas Teknik UNIPMA Dengan Metode McCall", *Jurnal Sistem Informasi Indonesia (JSII) Volume 3 Nomor 2. 2018.*

[7] L. Sudiharyanto, R. D. P. Halim, I. Verdian, "Analisa Serangan SQL Injeksi Menggunakan SQLMAP", *Positif: Jurnal Sistem dan Teknologi Informasi*, *Vol e 4, No. 2, pp. 88-94.2018*

[8] W. Worang and E. Sutanta, "Sistem Basis Data",*Yogyakarta: Graha Ilmu, 2004.*

[9] A. Andria, "Perancangan Sistem Informasi Administrasi Surat Desa Menggunakan Basis Data MySQL", *Research: Journal of Computer, Information System & Technology Management, Vol.1 No.2, pp 12 – 16. 2018*