JURNAL INFORMATIKA
Volume 2, Nomor 2, September 2023 ISSN 2809-3704

Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)

Muhammad Nur Fikri[1], Bita Parga Zen[2]*, Rifki Adhitama[3], Eryan Ahmad Firdaus[4]
[1,2,3]Program Studi Teknik Informatika, Fakultas Informatika, Institut Teknologi Telkom Purwokerto
[4]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Galuh Ciamis
Email: [1]18102098@ittelkom-pwt.ac.id, [2]bita@ittelkom-pwt.ac.id, [3]rifki@ittelkom-pwt.ac.id,
[4]eryan.ahmad.firdaus@unigal.ac.id

ABSTRAK – Perkembangan teknologi di dunia terus maju seiring dengan perkembangan zaman pada masa sekarang. Selaras juga dengan perkembangan internet pada masa sekarang yang semakin lama semakin meningkat penggunanya. Dengan begitu maka akan sangat rentan terjadinya serangan hacker. Serangan yang sering digunakan oleh para hacker untuk membobol sebuah database dengan menggunakan teknik SQL Injection. SQL Injection merupakan salah satu teknik hacking yang digunakan untuk masuk ataupun menyusup kedalam sistem database website, yang bertujuan untuk mengetahui isi database dan informasi-informasi yang terdapat di situs tersebut. Dalam penelitian ini peneliti menggunakan metode Penetration Testing Execution Standard (PTES) untuk menganalisis kerentanan dan juga melakukan penetrasi terhadap website SMA Negeri 1 Sokaraja. Pada metode Penetration Testing Execution Standard (PTES) memiliki 7 tahapan. Hasil analisis keamanan website SMA Negeri 1 Sokaraja, Ditemukan 11 kerentanan yang berhasil discanning dengan menggunakan tools OWASP ZAP. Dari 11 kerentanan yang berhasil discanning ada 1 kerentanan yang paling berisko tinggi. Kerentanan tersebut terdapat pada serangan SQL Injection, pada penelitian ini peneliti berhasil masuk kedalam sistem database MySQL website SMA Negeri 1 Sokaraja menggunakan teknik serangan SQL Injection. Pada database website SMA Negeri 1 Sokaraja peneliti berhasil menemukan data-data penting seperti username dan password admin website SMA Negeri 1 Sokaraja.

Kata Kunci: Database, SQL Injection, Website, PTES.

ABSTRACT – *Technological developments in the world continue to advance along with current developments. It is also in line with the development of the internet today, where users are increasingly increasing. That way, it will be very vulnerable to hacker attacks. An attack that is often used by hackers to break into a database using SQL Injection techniques. SQL Injection is a hacking technique used to enter or infiltrate a website's database system, which aims to find out the contents of the database and the information contained on the site. In this research, researchers used the Penetration Testing Execution Standard (PTES) method to analyze vulnerabilities and also penetrate the SMA Negeri 1 Sokaraja website. The Penetraton Testing Execution Standard (PTES) method has 7 stages. The results of the security analysis of the SMA Negeri 1 Sokaraja website, found 11 vulnerabilities which were successfully scanned using the OWASP ZAP tool. Of the 11 vulnerabilities that were successfully scanned, there was 1 vulnerability that had the highest risk. This vulnerability is found in SQL Injection attacks. In this study, researchers managed to enter the MySQL database system of the SMA Negeri 1 Sokaraja website using the SQL Injection attack technique. In the SMA Negeri 1 Sokaraja website database, researchers managed to find important data such as the SMA Negeri 1 Sokaraja website admin username and password.*

Keywords: *Database, SQL Injection, Website, PTES.*

PENDAHULUAN

Perkembangan teknologi di dunia terus maju seiring dengan perkembangan zaman pada masa sekarang. Selaras juga dengan perkembangan internet pada masa sekarang yang semakin lama semakin meningkat penggunanya [1]. Dengan begitu maka akan sangat rentan terjadinya serangan hacker. Bentuk ancaman yang dilakukan hacker yang terjadi saat ini diantaranya Denial of Service (DoS) dan Distributed Denial of Service (DDoS) [2], Serangan Defacement, Serangan Phishing, Serangan Malware, Trojan Horse, dan Cracking Password [3]. Serangan yang sering digunakan oleh para hacker untuk membobol

sebuah database dengan menggunakan teknik SQL Injection [4]. SQL Injection merupakan salah satu teknik hacking yang digunakan untuk masuk ataupun menyusup kedalam sistem database website, yang bertujuan untuk mengetahui isi database dan informasi-informasi yang terdapat di situs tersebut [5]. Penetration Test Execution Standar (PTES) suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi atau perusahaan tertentu untuk menemukan kelemahan yang ada dengan cara mempraktekkan serangan melalui celah keamanan maupun kerentanan dan melakukan analisa keamanan sistem [6]. Ada beberapa penelitian sebelumnya yang membahas tentang PTES yang sudah dilakukan, pada penelitian yang dilakukan oleh Bita Parga Zen, Rudy A.G Gultom, dan Agus H.S Reksoprodjo pada tahun 2020. Penelitian ini bertujuan untuk memahami risiko keamanan sistem dari serangan siber.

Penelitian ini dilakukan dengan menggunakan metode Penetration Testing untuk mengetahui kerentanan (vulnerability) yang ada pada website teknologi informasi Pertahanan Negara. Penelitian ini berhasil menemukan beberapa kerentanan dan serangan siber seperti Brute Force Password [6]. Pada penelitian sebelumnya yang dilakukan oleh Setyo Utoro, Bayu Andi Nugroho, Meinawati, dan Septian Rheno Widianto pada tahun 2020 dengan judul Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. Analisis ini dapat mengetahui beberapa celah keamanan yang ada di website E-Learning SMKN 1 Cibatu diantaranya berupa Web Server Transmits Cleartext Credential, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF). Hasil penelitian analisis dengan menggunakan tool Open Web Application Security Project (OWASP) ditemukan beberapa kerentanan salah satunya Clickjacking dimana kerentanan tersebut memudahkan penyerang untuk menipu user agar menghapus akun nya dengan cara mengklik tombol yang sudah dimanipulasi oleh penyerang [7]. Berdasarkan penelitian sebelumnya yang sudah dilakukan tersebut, maka penelitian ini akan melakukan analisis keamanan sistem informasi website SMA Negeri 1 Sokaraja menggunakan metode Penetration Testing Execution Standard (PTES). Penelitian ini berbeda pada penelitian sebelumnya, yang menjadi perbedaan adalah tools yang digunakan dalam melakukan serangan terhadap target. Untuk penelitian terdahulu tools yang digunakan masih menggunakan versi yang lama sedangkan tools yang digunakan peneliti untuk melakukan penelitian sudah menggunakan tools yang terbaru. Pada penelitian kali ini ditujukan untuk menguji kerentanan dan keamanan yang ada di dalam sistem informasi website SMA Negeri 1 Sokaraja.

METODE

2.1. Implementasi Metode PTES

Pada tahap ini peneliti mulai melakukan pengujian dengan menggunakan metode Penetration Testing Execution Standard (PTES). Metode tersebut menggunakan 7 tahapan yang nantinya akan dilakukan oleh peneliti seperti Pre-engagement Interaction, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting [4]. Berikut kerangka kerja dari PTES.

Gambar 1. Kerangka Kerja PTES

Pada tahapan Pre-engagement Interaction peneliti melakukan beberapa kegiatan seperti identifikasi masalah yang terdapat pada sistem informasi website SMA Negeri 1 Sokaraja [8]. Selanjutnya peneliti melakukan konfirmasi terhadap pihak SMA Negeri 1 Sokaraja dengan membuat surat izin penelitian. Setelah itu peneliti menyiapkan alat dan bahan yang diperlukan untuk melakukan PTES terhadap sistem informasi website SMA Negeri 1 Sokaraja. Selanjutnya pada tahapan Intelligence Gathering peneliti mengumpulkan beberapa informasi yang dibutuhkan pada saat melakukan PTES [9]. Informasi yang dibutuhkan seperti nama domain dan subdomain, alamat IP, domain info, alamat email serta DNS. Selanjutnya pada tahapan Threat Modeling peneliti melakukan tahapan untuk pendekatan pemodelan dari pengujian yang akan dilakukan. Pemodelan ini digunakan untuk memudahkan peneliti untuk memahami kerentanan keamanan yang akan ditemukan pada

pengujian dalam penelitian ini [10]. Selanjutnya pada tahapan Vulnerability Analysis peneliti mulai melakukan analisa kerentanan keamanan sistem informasi website SMA Negeri 1 Sokaraja dengan menggunakan tool OWASP ZAP [11]. Tool ini dapat memberikan informasi mengenai kerentanan (vulnerability) yang ada di dalam website. Selanjutnya pada tahapan Exploitation dilakukan penetrasi serangan menggunakan teknik SQL Injection terhadap sistem informasi website SMA Negeri 1 Sokaraja [12]. Tool yang digunakan peneliti dalam melakukan penetrasi serangan yaitu dengan menggunakan bantuan SQL MAP [13].

Teknik tersebut dilakukan untuk menguji keamanan pada sistem informasi website SMA Negeri 1 Sokaraja. Selanjutnya pada tahapan Post Exploitation dilakukan penilaian tingkat risiko terhadap sistem yang memiliki celah keamanan setelah dilakukan pengujian pada tahapan sebelumnya [14]. Dengan ini peneliti membuat tabel untuk memberikan penilaian untuk melihat risiko serangan yang telah ditemukan pada tahapan sebelumnya. Setelah dilakukan pengujian, tahapan terakhir yang peneliti lakukan adalah Reporting. Tahapan tersebut dilakukan dengan menuliskan laporan hasil analisis dan pengujian yang sudah dilakukan sebelumnya [15].

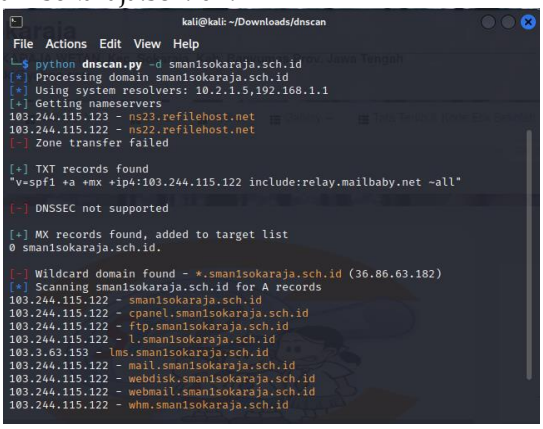
HASIL DAN PEMBAHASAN

3.1. Pre-Engagement Interaction

Pada tahap pertama peneliti melakukan pre-engagement interaction yang diantaranya mengidentifikasi suatu permasalahan yang ada di website SMA Negeri 1 Sokaraja yang dimana peneliti menemukan sebuah masalah kerentanan di dalam website tersebut. Kemudian peneliti melakukan konfirmasi ruang lingkup dengan tim IT SMA Negeri 1 Sokaraja bahwasanya akan melakukan kegiatan analisis keamanan terhadap website SMA Negeri 1 Sokaraja.

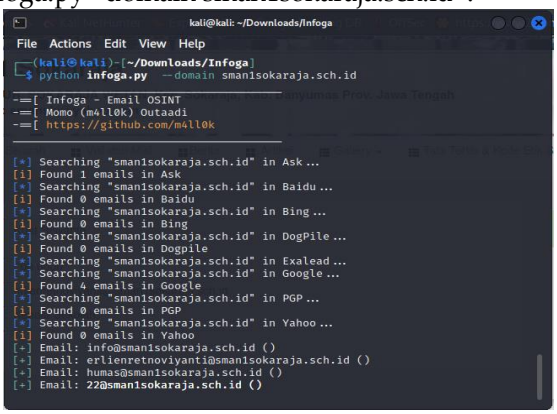
3.2. Intelligence Gathering

Pada tahapan selanjutnya adalah melakukan Intelligence Gathering atau melakukan pengintaian terhadap target dan mengumpulkan informasi penting sebanyak mungkin untuk digunakan untuk menembus target selama fase pentesting. Informasi yang peneliti kumpulkan seperti informasi alamat domain dan subdomain website, alamat email, alamat IP, alamat name server, dan port apa saja yang terbuka pada SMA Negeri 1 Sokaraja. Terdapat beberapa tools yang peneliti gunakan dalam melakukan tahap Intelligence Gathering. Untuk mengumpulkan informasi alamat domain dan subdomain serta informasi alamat ip address, alamat name server pada website SMA Negeri 1 Sokaraja peneliti menggunakan tools DNS Scan, dengan perintah" "python dnscan.py -d sman1sokaraja.sch.id".



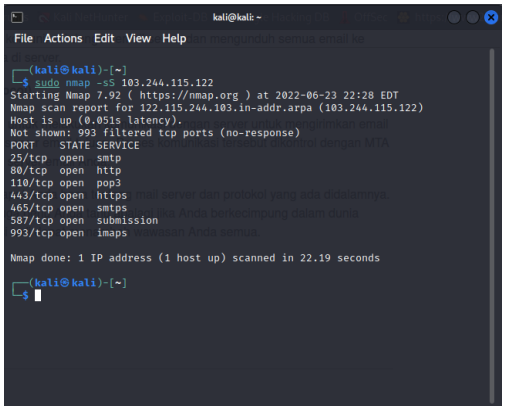
Gambar 2. Proses Identifikasi Alamat Domain dan Subdomain

Perintah tersebut digunakan untuk mengetahui informasi tentang domain yang diberikan. Informasi yang diberikan oleh tools DNS Scan seperti alamat IP address, alamat server hosting. Selain alamat IP, tools DNS Scan juga memberikan informasi untuk alamat Subdomain dari website SMA Negeri 1 Sokaraja. Selanjutnya untuk mendapatkan informasi sebuah alamat email peneliti menggunakan tools open source dari github yaitu Infoga, dengan perintah "python infoga.py –domain sman1sokaraja.sch.id".



Gambar 3. Proses Identifikasi Alamat Email

Perintah tersebut digunakan untuk mencari informasi alamat email yang ada di website SMA Negeri 1 Sokaraja. Ada 4 email yang berhasil ditemukan dengan menggunakan tools Infoga. Langkah selanjutnya untuk mengetahui port-port apa saja yang sedang terbuka pada alamat domain sman1sokaraja.sch.id peneliti menggunakan bantuan tools NMAP, dengan perintah "sudo nmap -sS 103.244.155.122".

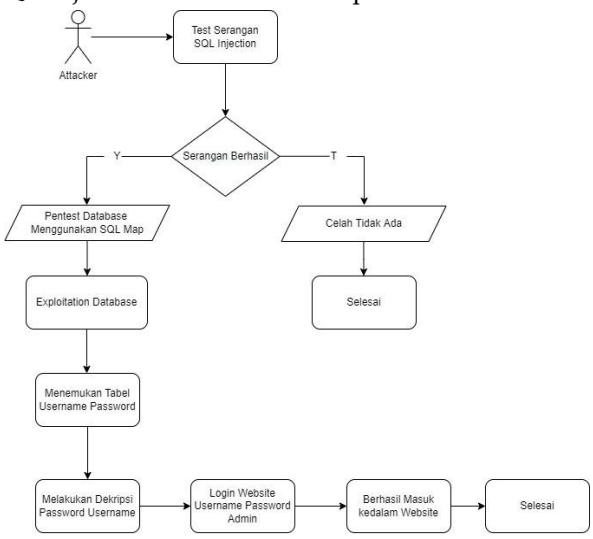


Gambar 4. Proses Identifikasi Port

Perintah diatas digunakan untuk mengetahui port apa saja yang terbuka pada website SMA Negeri 1 Sokaraja, tools NMAP berhasil mendapatkan informasi port yang terbuka dari alamat IP address 103.244.155.122.

3.3. Threat Modeling

Pada tahapan berikutnya peneliti melakukan Threat Modeling atau Pemodelan Ancaman merupakan tahapan untuk pendekatan pemodelan dari pengujian yang akan dilakukan. Pemodelan ini digunakan untuk memudahkan peneliti untuk memahami kerentanan keamanan yang akan ditemukan pada pengujian dalam penelitian ini. Gambar 5 menunjukkan pemodelan ancaman yang dilakukan untuk ancaman SQL Injection. Langkah pertama untuk memodelkan ancaman SQL Injection adalah penyerang mengirimkan perintah SQL Injection ke sebuah web aplikasi.

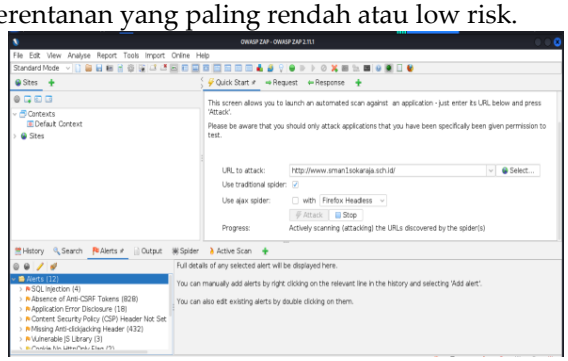


Gambar 5. Skema Threat Modeling

Setelah itu database web aplikasi yang telah dimasukan perintah SQL Injection memberikan akses kepada penyerang. Selanjutnya penyerang mendapatkan sebuah password user dari database tersebut. Setelah password user telah didapatkan oleh penyerang, langkah selanjutnya penyerang melakukan dekripsi pada password user yang telah di enkripsi. Setelah itu penyerang melakukan login ke website dengan memasukkan user admin dan password. Dan akhirnya penyerang dapat mengakses server web aplikasi dan melihat data-data pribadi yang ada di sebuah web aplikasi.

3.4. Vulnerability Analysis

Tahapan selanjutnya adalah melakukan tahap Vulnerability Analysis atau Analisis Kerentanan, pada tahapan ini peneliti melakukan analisis kerentanan yang terdapat pada website SMA Negeri 1 Sokaraja. Dalam penelitian ini, analisis kerentanan akan menggunakan bantuan tools OWASP ZAP. Pada tools OWASP ZAP digunakan untuk melakukan analisis celah kerentanan pada suatu website SMA Negeri 1 Sokaraja. OWASP ZAP yang peneliti gunakan sudah menggunakan versi yang terbaru yaitu OWASP ZAP Version 2.11.1. Dalam tahap ini tools OWASP ZAP sangat diperlukan, karena tools tersebut gratis dan mudah digunakan. Selain itu tools OWASP ZAP juga dapat memberikan informasi tingkat kerentanan mulai dari tingkat kerentanan yang paling rendah atau low dan tingkat kerentanan yang paling tinggi atau high. Dalam website SMA Negeri 1 Sokaraja ditemukan beberapa kerentanan dari risiko yang paling tinggi atau high risk sampai risiko kerentanan yang paling rendah atau low risk.



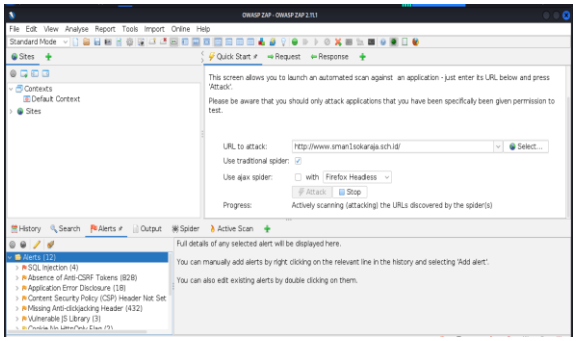
Gambar 6. Proses Analisis Kerentanan Web Menggunakan OWASP ZAP

Ada 11 celah kerentanan yang terdapat di dalam website SMA Negeri 1 Sokaraja menurut informasi. Namun celah kerentanan yang paling tinggi risikonya ada pada serangan SQL Injection, dengan ini peneliti mencoba melakukan simulasi serangan menggunakan teknik SQL Injection untuk melihat digunakan para attacker untuk membobol sebuah database yang ada di dalam sebuah website.

3.5. Exploitation

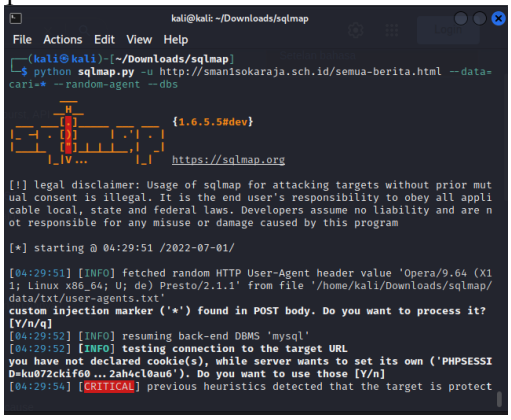
Exploitation merupakan tahapan yang dilakukan untuk menguji kerentanan yang telah ditemukan. Tahap ini akan menguji titik masuk pada kerentanan yang memiliki potensi serangan

tertinggi. Pada penelitian ini peneliti akan menguji kerentanan yang ada di dalam website SMA Negeri 1 Sokaraja dengan menggunakan teknik SQL Injection. Teknik tersebut memiliki risiko kerentanan yang paling tinggi saat melakukan analisis kerentanan website SMA Negeri 1 Sokaraja. Peneliti melakukan perintah SQL Injection dengan menambahkan tanda petik pada URL, yang terjadi adalah konten artikel yang ditampilkan jadi blank atau tidak ada.



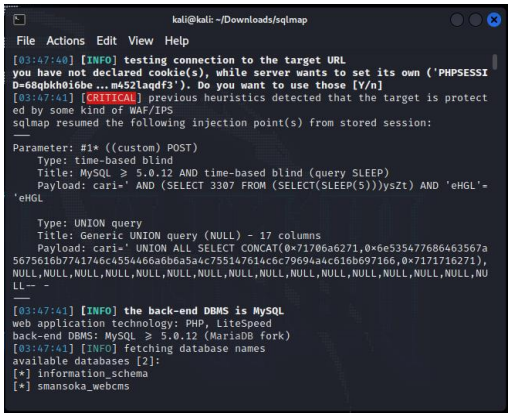
Gambar 7. Website SMA Negeri 1 Sokaraja Ketika Dimasukan Komen SQL Injection

Tanda petik tersebut biasanya digunakan untuk mengetes sebuah link URL yang rentan terhadap perintah SQL Injection atau tidak. Setelah melakukan pengecekan terhadap link url, peneliti melakukan step berikutnya yaitu melakukan pentest terhadap website SMA Negeri 1 Sokaraja. Pentest dilakukan peneliti untuk melakukan simulasi serangan terhadap website SMA Negeri 1 Sokaraja dengan menggunakan teknik SQL Injection. Tools yang digunakan peneliti dalam melakukan pentest ini yaitu menggunakan SQL Map. Tools tersebut sudah menggunakan versi terbaru yaitu versi 1.6.5.5, selain itu tools SQL Map bersifat open-source alias gratis. Untuk menyerang database website SMA Negeri 1 Sokaraja, peneliti melakukan perintah "python sqlmap.py -u http://sman1sokaraja.sch.id/semua-berita.html --data=cari=* --threads 10 --random-agent –dbs --dump".



Gambar 8. Perintah SQL Map Untuk Menyerang Database

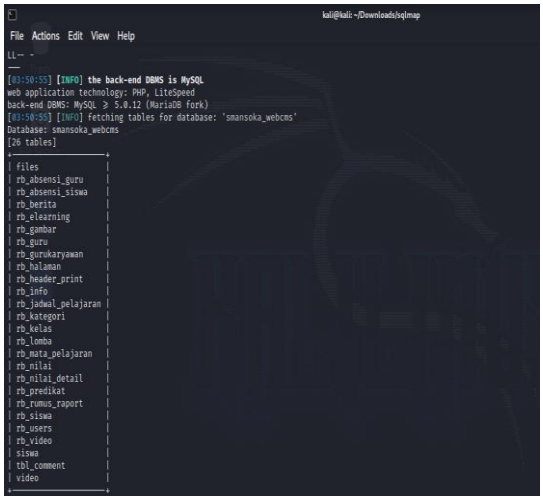
Perintah tersebut berfungsi untuk memerintahkan SQL Map untuk melakukan serangan terhadap database yang mengarahkan ke link http://sman1sokaraja.sch.id/semua-berita.html dengan menggunakan parameter –data=cari=*, parameter tersebut digunakan untuk mengirimkan data string (cari=*) melalui metode POST. Data string tersebut digunakan untuk menyerang website SMA Negeri 1 Sokaraja melalui celah kerentanan yang sudah ditemukan pada tahapan sebelumnya. Kemudian untuk –random-agent berfungsi untuk memerintahkan SQL Map untuk mengirimkan user agent secara acak ke URL yang dituju. Selanjutnya untuk –dbs berfungsi untuk memerintahkan SQL Map untuk mencari database dari target yang rentan terhadap SQL Injection. Setelah itu database website SMA Negeri 1 Sokaraja yang telah diserang akan menghasilkan informasi tentang nama database web SMA Negeri 1 Sokaraja. Informasi tersebut dapat dilihat pada Gambar 9 dibawah ini.



Gambar 9. Informasi nama database SMA Negeri 1 Sokaraja

Tools SQL Map berhasil melakukan injeksi terhadap sistem database SMA Negeri 1 Sokaraja, dan berhasil memberikan informasi nama database website SMA Negeri 1 Sokaraja. Seperti yang ditampilkan Gambar 10 bahwasanya nama database website SMA Negeri 1 Sokaraja adalah smansoka_webcms. Selain itu database smansoka_webcms menggunakan bahasa pemrograman MySQL pada website SMA Negeri 1 Sokaraja. Langkah selanjutnya peneliti menginjeksi informasi tabel yang ada di dalam database smansoka_webcms dengan perintah "python sqlmap.py -u http://sman1sokaraja.sch.id/semua-berita.html --data=cari=* --random-agent -`berfungsi untuk memerintahkan SQL Map untuk menginjeksi ke sebuah tabel yang ada didalam database smansoka_webcms, dengan menggunakan parameter -Dsmansoka_webcms -tables. Parameter tersebut digunakan untuk

memerintahkan SQL Map untuk mengakses isi table dari database smansoka_webcms. Isi table dari database smansoka_webcms dapat dilihat pada Gambar 10 dibawah ini.

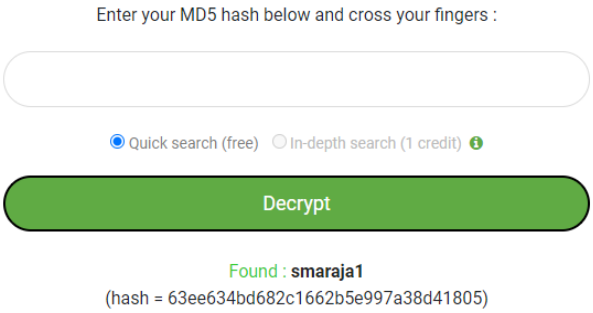


Gambar 10. Isi Table Database Smansoka_Webcms

Setelah berhasil menampilkan isi tabel dari database smansoka_webcms, langkah selanjutnya untuk melihat isi kolom yang terdapat pada setiap tables yang ada pada database website SMA Negeri 1 Sokaraja, tabel yang akan diserang pada penelitian ini yaitu pada tabel users yang berisi username dan password admin website SMA Negeri 1 Sokaraja, dengan menggunakan perintah "python sqlmap.py -u http://sman1sokaraja.sch.id/semua-berita.html --data=cari=* --random-agent -Dsmansoka_webcms -T rb_users –dump". Informasi tersebut dapat dilihat pada Gambar 11 yang ada dibawah ini.

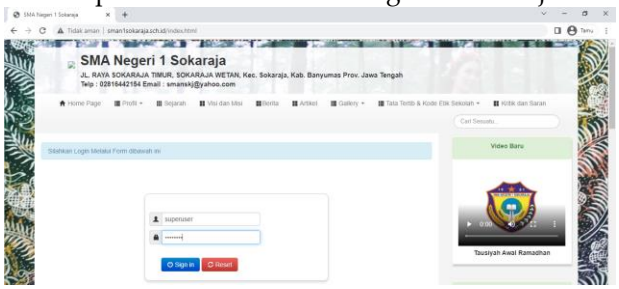
Gambar 11. Isi Table User Database Smansoka_Webcms

Setelah mengetahui isi kolom pada tabel yang ada di database smansoka_webcms, tabel rb_users akan menjadi target pada tahap pentest kali ini. Karena tabel tersebut berisi data-data penting seperti nama user dan password untuk masuk kedalam website SMA Negeri 1 Sokaraja. Password yang ada di dalam tabel rb_users masih di enkripsi seperti yang dilihat pada tabel, dimana password tersebut masih ter enkripsi oleh database MySQL. Untuk melihat password yang terenkripsi, peneliti harus menggunakan bantuan tools md5 decrypt untuk melihat password yang terenkripsi tersebut. Berikut hasil proses decrypt password superuser.



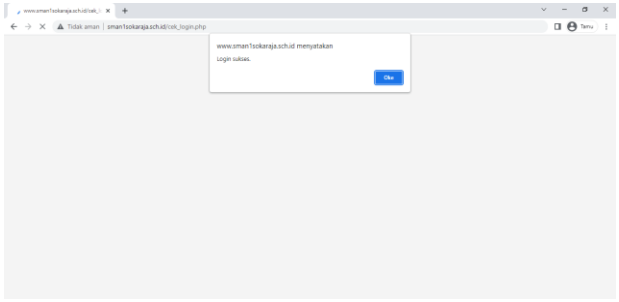
Gambar 12. Proses decrypt password

Gambar 12 berhasil mendecrypt password superuser yang telah di enkripsi oleh database MySQL. Setelah itu peneliti mencoba masuk kedalam website SMA Negeri 1 Sokaraja dengan menggunakan nama username: superuser dan password: smaraja1. Berikut hasil dari melakukan sebuah pentest website SMA Negeri 1 Sokaraja.



Gambar 13. Tampilan Halaman Login Web SMA Negeri 1 Sokaraja

Setelah itu peneliti mengklik tombol sign in yang ada ditampilkan form login website SMA Negeri 1 Sokaraja, setelah berhasil login nantinya akan muncul alert pesan seperti Gambar 14 dibawah ini.



Gambar 14. Tampilan Pesan Berhasil Login

Pesan tersebut menjelaskan bahwa peneliti berhasil memasukan username dan password dengan benar. Langkah selanjutnya peneliti mengklik tombol oke pada pesan yang muncul, nantinya peneliti akan diarahkan kedalam dashboard admin website SMA.

3.6. Post Exploitation

Tahapan selanjutnya yang peneliti lakukan adalah melakukan Post Exploitation, merupakan tahapan yang dilakukan setelah mengeksploitasi kerentanan yang ada pada target. Pada tahap ini dilakukan penilaian tingkat risiko terhadap sistem yang memiliki celah keamanan setelah dilakukan pengujian pada tahapan sebelumnya. Dengan ini peneliti membuat tabel untuk memberikan penilaian untuk melihat risiko serangan yang telah ditemukan pada tahapan sebelumnya.

Tabel 1. Tingkat Risiko Terhadap Celah Keamanan

Jenis Serangan	Tingkat Risiko	Tools
SQL Injection	Tinggi	OWASP ZAP, SQL Map

Berdasarkan hasil pengujian diatas, maka terdapat celah keamanan yang memiliki tingkat risiko tinggi. Untuk website SMA Negeri 1 Sokaraja terdapat celah keamanan berupa serangan SQL Injection. Serangan SQL Injection memiliki potensi serangan yang tinggi pada website SMA Negeri 1 Sokaraja.

3.7. Reporting

Tahapan terakhir pada metode PTES adalah membuat sebuah laporan atau reporting serta mendokumentasikan bagian-bagian penting yang terjadi selama pentest. Pada tahap ini peneliti melakukan pembuatan sebuah laporan dari hasil analisis dan hasil pentest terhadap sebuah website SMA Negeri 1 Sokaraja. Selain itu peneliti juga melakukan pendokumentasian yang sudah dilakukan pada tahap pentesting. Dari seluruh tahap pengujian yang telah dilakukan, maka penulis dapat menyimpulkan hasil pengujian menggunakan metode Penetration Testing Execution Standard (PTES) pada aplikasi website SMA Negeri 1 Sokaraja yang ditunjukkan sebagai hasil laporan pengujian keamanan pada Tabel 2.

Tabel 2. Hasil Penetration Testing

Jenis Serangan	Tools	Status
SQL Injection	SQL Map	Berhasil

Dari Tabel 2 dapat disimpulkan bahwa ada satu serangan yang berhasil menyerang dan mengeksploitasi website SMA Negeri 1 Sokaraja. Serangan tersebut adalah Serangan SQL Injection, serangan ini berhasil mengakses isi database yang ada di dalam website SMA Negeri 1 Sokaraja. Dalam tahap pengujian keamanan peneliti menggunakan bantuan tools SQL Map untuk melakukan simulasi serangan terhadap website tersebut. Berdasarkan hasil pengujian keamanan tersebut, maka rekomendasi perbaikan dari temuan celah keamanan pada website SMA Negeri 1 Sokaraja dapat dirangkum seperti pada Tabel 3.

Tabel 3. Rekomendasi Perbaikan

Jenis Serangan	Rekomendasi
SQL Injection	Sesuaikan kotak input yang akan digunakan, gunakan penghapusan file default di server web sehingga penyerang tidak dapat menggunakannya.
Anti-CSRF Tokens	Gunakan Anti-CSRF pada form login.
Application Error Disclosure	Tinjau kode sumber halaman ini. Terapkan halaman kesalahan khusus. Pertimbangkan untuk menerapkan mekanisme untuk memberikan referensi atau pengidentifikasian kesalahan unik ke klien (browser) saat mencatat detail di sisi server dan tidak memaparkannya kepada pengguna.
CSP Header Not Set	Menggunakan Content-Security-Policy: frame-ancestors 'none'; yang dapat mencegah domain apapun membuat framing.
Missing Anti-clickjacking Header	Browser Web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya disetel di semua halaman web yang ditampilkan oleh situs/aplikasi Anda. Jika Anda mengharapkan halaman dibingkai hanya oleh halaman di server Anda (mis. itu bagian dari FRAMESET) maka Anda akan ingin menggunakan SAMAORIGIN, jika tidak, jika Anda tidak pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Atau pertimbangkan untuk menerapkan arahan "frame-ancestor".
Vulnerable Js Library	Memperbaharui versi jQuery dengan versi yang terbaru.
Cookie No Http Only	Pastikan bahwa flag HTTP Only disetel untuk semua cookie.

Jenis Serangan	Rekomendasi
Flag	
Cookie Without Same Site Attribute	Gunakan atribut Same Site sehingga browser dapat memberitahukan kapan dan bagaimana mengaktifkan cookie dari pihak kedua atau pihak ketiga.
Cross Domain JavaScript Source File Inclusion	Pastikan file sumber JavaScript berasal dari sumber yang terpercaya dan sumber tidak dapat dikontrol oleh end-user application.
Timestamp Disclosure	Verifikasi secara manual bahwa data stempel waktu tidak sensitif dan bahwa data tidak dapat digabungkan untuk mengungkapkan pola yang disalahgunakan.
X Content Type Options Header Missing	Mengatur header X-Content-Type-Option Nosniff

KESIMPULAN

Dapat disimpulkan bahwa metode Penetration Testing Execution Standar (PTES) telah ditemukan kerentanan pada SQL Injection berupa database smansoka_webcms dengan jumlah 25 tabel dalam database yang mengakibatkan data mudah untuk diakses orang lain yang tidak memiliki kepentingan. Ketika melakukan pentest peneliti dapat masuk kedalam sistem dengan menggunakan teknik serangan SQL Injection sehingga peneliti bisa mengakses data-data yang dianggap penting oleh web SMA Negeri 1 Sokaraja dan dalam melakukan scanning diidentifikasi 11 celah yang memungkinkan dapat kembali diakses selain menggunakan tahapan SQL Injection.

REFERENSI

[1] "Top 20 Countries with The Highest Number of Internet Users". https://www.internetworldstats.com/top20.htm. (Diakses pada 18 Januari 2023).

[2] H. Alfidzar and B. Parga Zen, "Journal of Informatics, Information System, Software Engineering and Applications Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna Mendeteksi Serangan DOS Pada Server," vol. 4, no. 2, pp. 32–045, doi: 10.20895/INISTA.V4I2.

[3] "Honeynet Project Bssn-Ihp Laporan Tahunan," 2021. https://cloud.bssn.go.id/s/q5Hx6ifSj86cKnA#pdfviewer. (Diakses pada 18 Januari 2022).

[4] Y. Mulyanto and E. Haryanti, "Sumbawa Menggunakan Metode Vulnerability Asesement", JINTEKS, vol. 3, no. 3, 2021, doi: 10.51401.

[5] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website".

[6] B. P. Zen, R. A. G. Gultom, A. H. S. Reksoprodjo, P. T. Penginderaan, T. Pertahanan, and U. Pertahanan, "Analisis Security Assessment Menggunakan Metode Penetration Testing Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara Security Assessment Analysis Using Penetration Testing Methods In Maintaining The Security Capability Of National Defense Information Technology".

[7] S. Utoro et al., "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard".

[8] Zen, B. P., Gultom, R. A., & Reksoprodjo, A. H, "Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," Teknologi Penginderaan, vol 2, no. 1, pp. 105-122, 2020.

[9] A. Kerentanan Keamanan, W. Menggunakan, D. Aryanti, N. Dan, and J. N. Utamajaya, "Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja," 2021.

[10] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," Jurnal Ilmiah Informatika Komputer, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[11] I. Riadi, A. Yudhana, and P. Korspondensi, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," vol. 7, no. 4, 2020, doi: 10.25126/jtiik.202071928.

[12] A. Elanda and R. Lintang Buana, "Analisis Kualitas Keamanan Sistem Informasi E-

Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan Owasp Top 10," 2021.
[13] E. Irawadi Alwi and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," 2020.
[14] Purwanto Eko. "Keamanan Informasi". https://bpptik.kominfo.go.id/2014/03/24/404/ keamanan-informasi/. (Diakses pada 20 Desember 2022).
[15] D. Napitupulu and M. Kom, "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional".