Buletin Sistem Informasi dan Teknologi Islam
Vol 5, No 3 (2024), pp 194-203
ISSN: 2721-0901
DOI: http://dx.doi.org/10.33096/busiti.v5i3.2116

Analisis Keamanan Website Digital School di SMAS Semen Tonasa Pangkep

Security Analysis of Digital School Website at SMAS Semen Tonasa Pangkep

Khayyirah Annisa Qurratu'ain[a,1*], Yulita Salim [a,2], Andi Widya Mufila Gaffar [a,3]

[a]*Fakultas Ilmu Komputer (Program Studi Teknik Informatika, Universitas Muslim Indonesia, Makassar, Indonesia)*
[1]*khayyirahannisaqurratuain@gmail.com;* [2]*yulita.salim@umi.ac.id;* [3]*widya.mufila@umi.ac.id;*
**corresponding author*

Informasi Artikel

Diserahkan : 20 Februari 2024
Diterima : 27 September 2024
Direvisi : 30 oktober 2024
Diterbitkan : 30 Oktober 2024

Kata Kunci:
Digitalisasi
Keamanan
Penetration Test
SQL Injection
Cross Side Scripting

ABSTRAK

Di era digitalisasi, isu terkait keamanan data dan informasi menjadi salah satu isu yang penting. Menurut data yang dihimpun oleh Badan Siber dan Sandi Negara (BSSN), menjelaskan bahwa dari bulan Januari sampai bulan Agustus 2020, menghasilkan sebanyak 190 juta upaya serangan terhadap web server yang ada di Indonesia. Karena maraknya kasus penyerangan, dibutuhkan upaya untuk mengetahui celah keamanan pada sebuah website untuk meminimalisir resiko penyerangan. Salah satunya pada website Digital School Database milik SMAS Semen Tonasa, yang menjadi objek penelitian ini. Pada penelitian ini, website SMAS Semen Tonasa diuji dengan menggunakan metode Penetration Test untuk menganalisis keamanan pada website. Khususnya menggunakan *SQL Injection* dan *Cross Side Scripting* (XSS) sebagai celah keamanan yang ditemukan melalui proses *scanning website*. Adapun hasil dari penelitian ini menunjukkan bahwa website discas.smasementonasa.sch.id rentan terhadap serangan *Cross Side Scripting* (XSS) dan *SQL Injection* yang dibuktikan dengan proses penetration testing yang dilakukan dengan menggunakan *tools nikto*, *acunetix*, dan sqlmap.Dari proses pengujian *Cross Site Scripting* (XSS), celah keamanan XSS website dapat diserang dengan menggunakan *script* yang dimasukkan ke database, sehingga dapat menyebabkan berubahnya tampilan website. Begitupun dengan pengujian celah keamanan SQL website menggunakan sqlmap, dimana database hingga tabel database website dapat ditemukan yang menyebabkan penyerang dapat melakukan pencurian ataupun pengrusakan database.

***Keywords*:**
Digitalization
Security
Penetration Test
SQL Injection
Cross Side Scripting

ABSTRACT

In the digital era, issues related to data and information security are one of the important issues. According to data collected by the National Cyber and Crypto Agency (BSSN), it explains that from January to August 2020, there were 190 million attacks on web servers in Indonesia. Due to the increasing number of attacks, efforts are needed to identify security gaps on a website to minimize the risk of attack. One of them is on the Digital School Database website owned by SMAS Semen Tonasa, which is the object of this study. In this study, the SMAS Semen Tonasa website was tested using the Penetration Test method to analyze security on the website. Specifically using SQL Injection and Cross Side Scripting (XSS) as security gaps found through the website scanning process. The results of this study indicate that the website discas.smasementonasa.sch.id is vulnerable to Cross Side Scripting (XSS) and SQL Injection attacks as evidenced by the penetration testing process carried out using the nikto, acunetix, and sqlmap tools. From the Cross Site Scripting (XSS) testing process, the XSS website security hole can be attacked using a script that is inserted into the database, which can cause the appearance of the website to change. Likewise with testing the SQL website security hole using sqlmap, where the database to the website database table can be found which causes attackers to steal or damage the database.

I. Pendahuluan

Di era digitalisasi, isu terkait keamanan data dan informasi menjadi salah satu isu yang penting [1]. Dengan semakin berkembangnya era digitalisasi, masyarakat semakin menggantungkan dirinya pada teknologi digital guna mempermudah pekerjaan/aktifitas keseharian. Hal ini dapat dilihat dengan semakin banyaknya pengguna media sosial dan layanan internet saat ini [2]. Dalam laporan bertajuk Profil Internet Indonesia 2022, Asosiasi Penyelenggara Internet Indonesia (APJII), menyatakan jumlah penduduk indonesia yang telah terkoneksi

dengan internet pada kurun waktu 2021-2022 mencapai 210 juta orang. Dimana sebelum pandemi, jumlah pengguna interet di Indonesia hanya mencapai175 juta orang. Laporan AAJI menunjukkan tingkat penetrasi internet pada periode ini mencapai 77,02 persen [3].

Salah satu aturan dasar dalam menentukan keamanan suatu jaringan ada 3 yaitu *Confidentiality* (kerahasiaan) menjaga kerhasiaan infomarsi dari orang-orang yang tidak berhak, *Integrity* (integritas) menjaga perubahan informasi dari orang yang tidak berhak dan *Availability* (ketersediaan) menjaga informasi selalu ada untuk diakses atau disingkat sebagai CIA TRIAD. Jika 3 faktor dasar dalam keamanan jaringan itu tidak dapat terpenuhi maka suatu jaringan dapat dikategorikan tidak aman dan rawan tersusupi oleh pihak yang tidak bertanggung jawab [4].

Menurut data yang dihimpun oleh Badan Siber dan Sandi Negara (BSSN), menjelaskan bahwa dari mulai bulan Januari sampai bulan Agustus 2020, menghasilkan sebanyak 190 juta dalam upaya serangan terhadap web server yang ada di Indonesia, data ini menunjukan bahwa ada kenaikan lebih dari lima kali lipat dibanding jumlah data yang sama pada tahun lalu yang tercatat di kisaran 39 juta [5]. Angka paling banyak tercatat pada bulan Agustus 2020, bahwa Badan Siber dan Sandi Negara (BSSN) mencatat jumlah serangan siber di kisaran 63 juta, jauh lebih tinggi dibandingkan Agustus 2019 yang hanya di kisaran 5 juta [6]. Data diatas menunjukan bahwa keadaan web server yang ada di indonesia masih jauh dari keadaan aman dari ancaman dan serangan [7]. Data lain yang dikumpulkan oleh POLRI, pada tahun 2020 sampai saat ini, setidaknya ada 937 kasus yang dilaporkan. Dari 937 kasus tersebut ada tiga kasus dengan angka tertinggi yaitu kasus *provocative, hate content and hate speech* yang paling banyak dilaporkan, sekitar 473 kasus. Kemudian disusul oleh penipuan online dengan 259 kasus dan konten porno dengan 82 kasus [8].

SMAS Semen Tonasa sebagai salah satu institusi pendidikan, ikut memanfaatkan perkembangan internet dengan mengembangkan website digital school. Website ini dimanfaatkan menjadi pusat informasi seputar SMA Semen Tonasa, seperti profil sekolah, staff, fasilitas, data guru dan siswa evaluasi hasil belajar, jadwal penerimaan siswa baru, hingga monitoring kehadiran guru dan siswa. Untuk website SMAS Semen Tonasa, dapat di akses melalui https://discas.smassementonasa.sch.id/. Website ini dikembangkan dengan menggunakan domain milik pemerintah yang merupakan bagian dari upaya meningkatkan mutu pendidikan dengan cara penerapan sistem digitalisasi sekolah. Sedangkan untuk *content managament system* (CMS) website ini, masih menggunakan versi balitbang.

Meskipun domain yang digunakan adalah domain resmi pemerintah yang di khususkan untuk sekolah-sekolah, tidak dipungkiri bahwa tidak hanya pihak yang memiliki akses saja yang dapat mengakses informasi yang ada di dalamnya, terdapat pihak-pihak lain yang tidak bertanggung jawab dapat mengaksesnya dan menyalahgunakan informasi yang ada hingga menyebabkan kerugian bagi sekolah.

Berdasarkan hasil observasi yang dilakukan di SMAS Semen Tonasa, website ini pernah mengalami pembobolan oleh pihak yang tidak bertanggung jawab. Karena hal tersebut, mengakibatkan tampilan website berubah. Meskipun menurut pengelola tidak ada data sekolah yang hilang, namun data-data yang ada di dalam website telah di akses oleh pihak yang membobol, apalagi di dalamya tersimpan data-data pribadi siswa dan staff sekolah, seperti NIK.

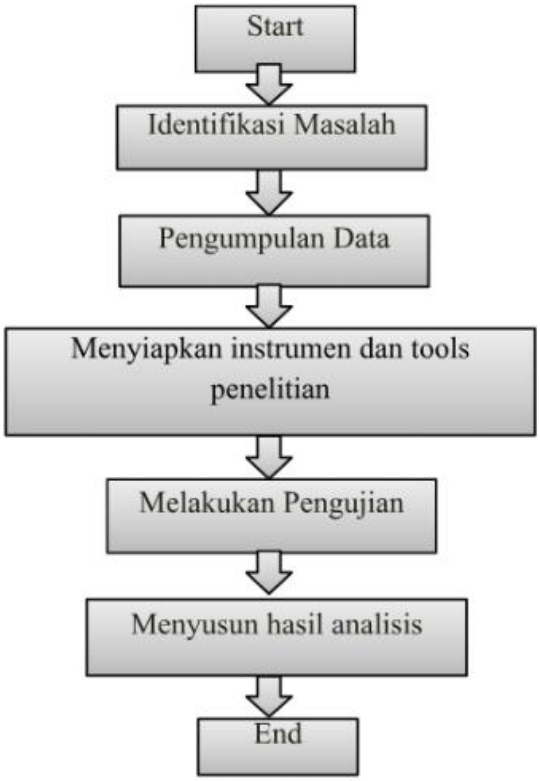
Menurut keterangan pengelola website, pasca pembobolan, pengelola membenahi kembali tampilan website kemudian mengeluarkan beberapa data-data penting. Setelah itu, tidak ada upaya perbaikan keamanan pada website. Sehingga belum diketahui dengan pasti letak celah kerentanan untuk pencegahan serangan yang bisa dilakukan kapan saja. Hal ini dikarenakan tidak adanya SDM yang mampu melakukan uji keamanan jaringan tersebut.

Karenanya, untuk kasus SMAS Semen Tonasa, peneliti akan coba melakukan uji keamanan jaringan website menggunakan metode penetration testing. Untuk uji keamanan jaringan website sendiri, ada beberapa metode yang dapat digunakan. Dari penelitian-penelitian yang telah dilakukan, pengujian keamanan sistem informasi menggunakan metode PTES mampu memberikan hasil analisis yang komprehensif terhadap para penggunanya serta mudah untuk dilakukan.

Ada beberapa contoh metode yang umumnya digunakan untuk menguji keamanan jaringan website, misalnya suricata [9] SSE-CMM ISO 27002: 2013 [10] dan bot telegram [11]. Selain itu terdapat pula riset yang menggunakan metode penetatrion testing [12],[13].Tujuan penelitian dengan judul "Analisis Keamanan Website Digital School di SMAS Semen Tonasa Pangkep" yang akan dilakukan oleh penulis adalah menguji keamanan sistem aplikasi berbasis website SMAS Semen Tonasa dengan menggunakan metode PTES yang terdiri dari tujuh tahapan dengan menggunakan alat pengujian yang telah ditentukan di setiap tahapannya dan pada akhir penelitian dibuat laporan berupa rekomendasi dan saran perbaikan yang akan di informasikan kepada pihak SMAS Semen Tonasa. Melalui laporan tersebut diharapkan SMAS Semen Tonasa dapat meningkatkan keamanan sistem informasinya secara lebih efektif.

II. Metode

A. Tahap Penelitian

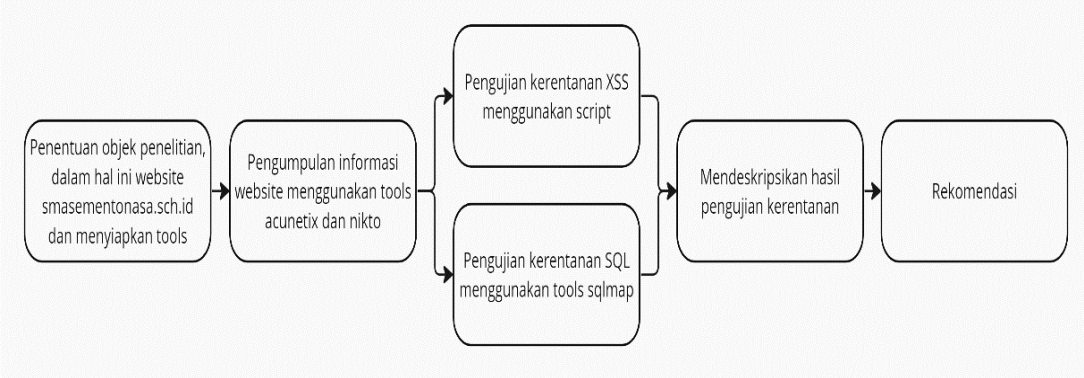


Gambar 1.Tahapan Penelitian

Tahapan penelitian terdiri atas 5 tahapan yaitu Identifikasi Masalah (Mengidentifikasi masalah dari objek penelitian), pengumpulan data (observasi, wawancara dan studi pustaka), Menyiapkan instrumen dan tools penelitian (Menyiapkan kebutuhan-kebutuhan untuk melakukan *penetration testing*), Melakukan Pengujian (Menyusun hasil analisis untuk menghasilkan rekomendasi), kemudian Menyusun hasil analisis.

B. Desain Penelitian

1) Analisis Sistem Berjalan



Gambar 2. Bagan Desain Penelitian

Gambar 2 Menentukan objek penelitian dalam hal ini website smassementonasa.sch.id. Penentuan objek penelitian, berdasarkan permasalahan yang pernah dialami oleh website tersebut, yang didapatkan melalui wawancara kepada admin website dan pengamatan langsung. Setelah itu merumuskan permasalahan, pertanyaan penelitian, lalu mengumpulkan data terkait seperti alamat IP, jenis server dan script yang digunakan dari objek yang akan di teliti.

a) Penentuan Objek Penelitian

Menentukan objek penelitian dalam hal ini website smassementonasa.sch.id. Penentuan objek penelitian, berdasarkan permasalahan yang pernah dialami oleh website tersebut, yang didapatkan melalui wawancara kepada admin website dan pengamatan langsung.

b) Identifikasi *(CollitionI)*

Pada tahap ini, akan dilakukan pengidentifikasian kebutuhan penelitian berupa instrumen dan tools untuk melakukan *penetration testing*. Adapun tools yang digunakan yaitu:

- Kali Linux
- *Waapalayzer*
- Nikto
- *Acunetix*
- Sqlmaps

c) Pengujian (*Examinition*)

Peneliti mulai melakukan *SQL Injection* terhadap website SMAS Semen Tonasa. Serangan disini hanya dilakukan untuk melihat apakah penyerang dapat memasuki database website tanpa melakukan manipulasi terhadap database yang ada, sehingga tidak akan mengganggu kondisi website yang sedang berjalan.

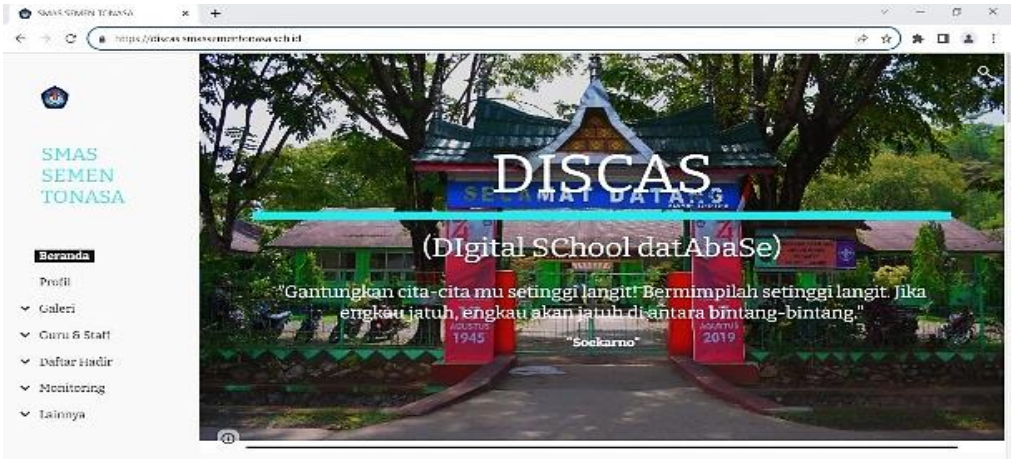
- Pengujian kerentanan XSS
- Pengujian kerentanan *SQL Injection*
- Deskripsi
- Rekomendasi

III.Hasil dan Pembahasan

Proses yang dilakukan untuk menemukan celah keamanan pada website meliputi *scope, reconnaissance, vulnerability detection, information analysis & planning,* dan *penetration testing*. Pada proses *vulnerability detection* di dalamnya terdapat metode DAST (*Dynamic Application Security Testing*) dalam menemukan celah keamanan pada website dengan bantuan aplikasi, misalnya *Acunetix*. Sehingga, dalam melakukan penetrasi pada website discas.smassementonasa.sch.id menggabungkan metode *penetration test* dan DAST.

1) Scope

a) Halaman Kerja



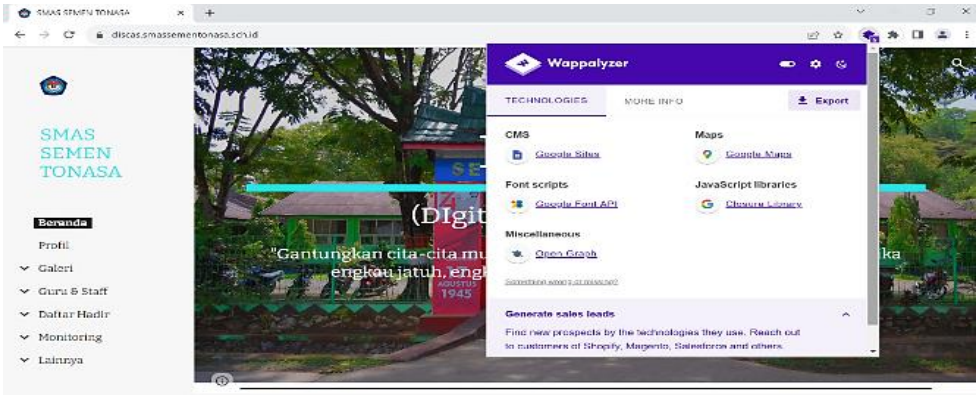
Gambar 3. Dashboard website SMA Semen Tonasa

Gambar 3 *Scope* yang dipilih adalah website discas.smassementonasa.sch.id berfungsi sebagai objek pengujian *penetration test*. Informasi secara singkat,discas.smassementonasa.sch.id adalah sebuah website yang menyediakan layanan informasi staff sekolah, kurikulum, data siswa, dan jadwal belajar. Data itu diinput dan diproses oleh admin.

2) Reconnaissance

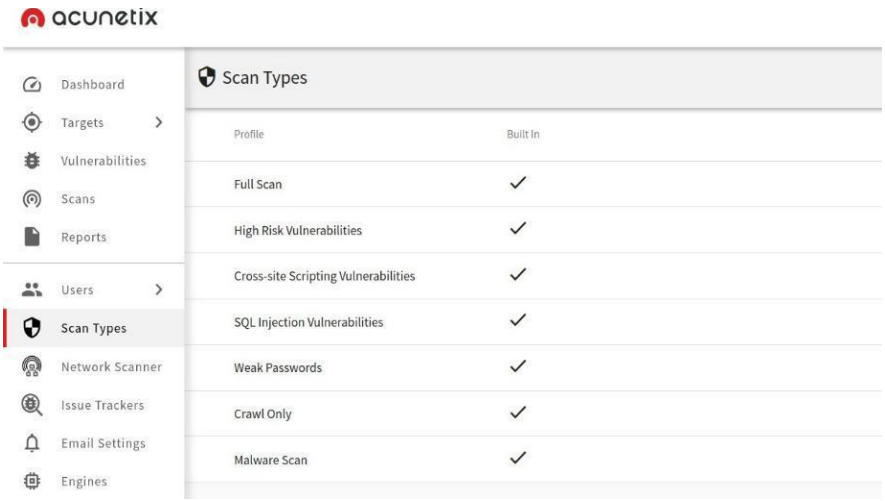
Maksudanya adalah mengumpulkan informasi sebanyak mungkin dari website discas.smassementonasa.sch.id untuk mengumpulkan informasi pada website.

3) Wappalyzer



Gambar 4. Sub kriteria

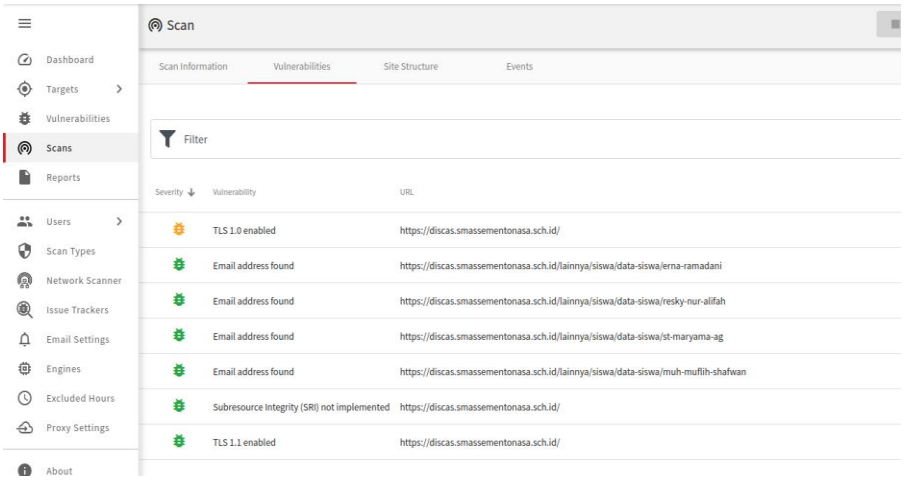
4) Vulnerability Detection



Gambar 5. Keterangan Jenis Kerentan Yang Akan di Scan Menggunakan Acunetix 13

Gambar 5, ditunjukkan jenis kerentanan apa saja yang akan di scan. Dari keterangan itu, diperlihatkan bahwa tipe scan yang digunakan akan mencari kerentanan *Cross-Site Scripting* dan *SQL*.

5) Injection



Gambar 6. Hasil Scanning Dengan Acunetix 13

Gambar 6 merupakan salah satu hasil *scanning*. Ketika di klik, akan memberikan deskripsi kerentanan (*Vulnerability Description*).

6) Information Analysis & Planning

Hasil dari *vulnerability detection* manampilkan celah keamanan pada website discas.smassementonasa.sch.id. Pada proses Information *Analysis & Planning* akan mengambil celah keamanan yang digunakan sebagai bahan penetration testing.

Tabel 1. Model Tabel yang digunakan pada BUSITI

No	Jenis Kerentanan
1	SQL Injection
2	XSS

7) Penetration Testing

Penetration testing yang dilakukan pada website discas.smassementonasa.sch.id memanfaatkan celah keamanan pada gambar 8. Hasil pengujiannya adalah sebagai berikut:

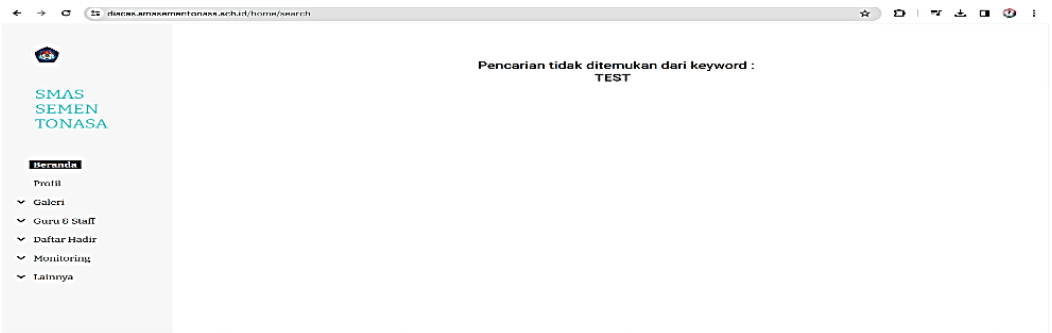
a) XSS

Cross Side Scripting (XSS) memanfaatkan celah keamanan yang salah satunya dengan menginputkan *script javascript*, maka pengujian *penetration testing* dilakukan dengan memasukan informasi, yang salah satunya bisa dilakukan melalui kolom pencarian (*search*) website yang disediakan oleh website smasementonasa.sch.id.

Gambar 7. Script yang dimasukkan ke kolom pencarian website

Kemudian, pada gambar 7, diperlihatkan bahwa HTML yang dimasukkan pada website kemudian tampil pada halaman website. Ini menunjukkan bahwa sistem berhasil terserang pada celah keamanan *Cross Site Scripting* (XSS).

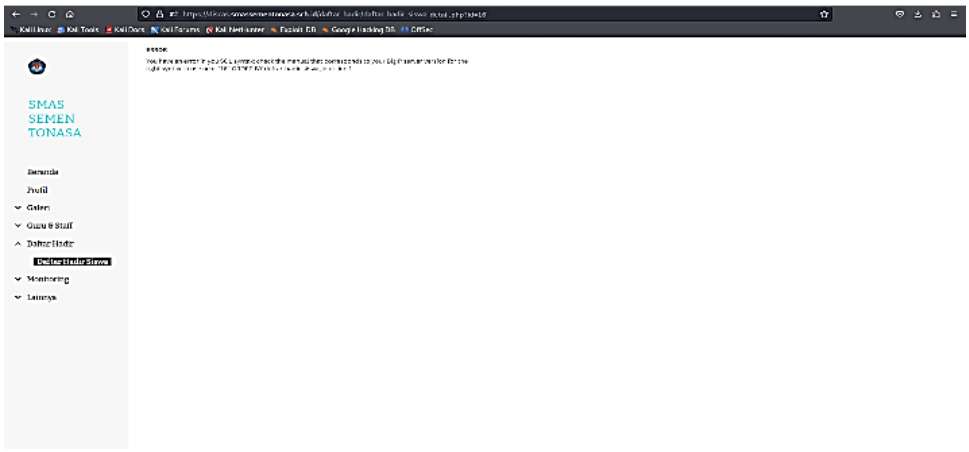
Gambar 8. HTML yang dimasukkan ke kolom pencarian website



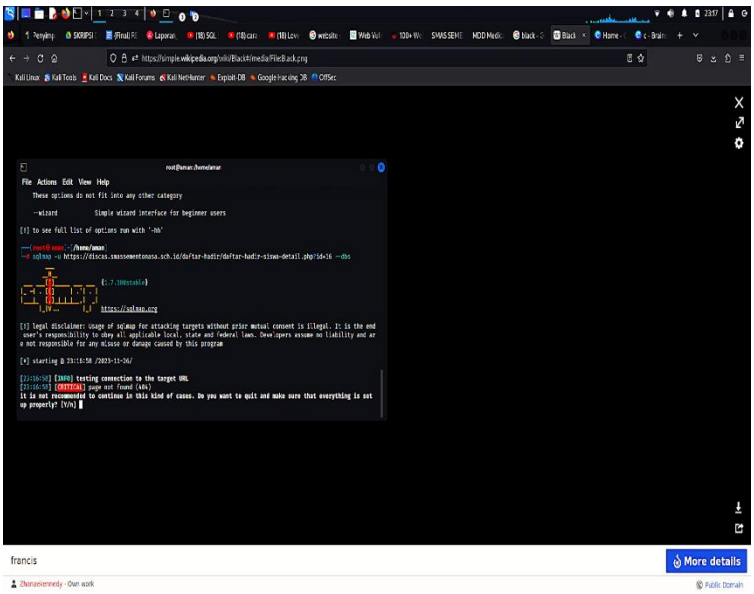
Gambar 9. Tampilan website ketika kode HTML dimasukkan

b) SQL Injection

SQL Injection adalah jenis serangan yang dilakukan oleh penyerang yang dapat menimbulkan banyak kerugian karena rusaknya database dari situs web. Teknik *sql injection* dapat mencuri informasi penting seperti *username* dan *password*, merubahkan database, dan memasukan konten berbahaya. Dalam melakukan penetration test terhadap celah *sql Injection* di lakukan dengan menggunakan *tools sqlmap* versi 1.3.11 yang di jalankan di Sistem Operasi Kali Linux.

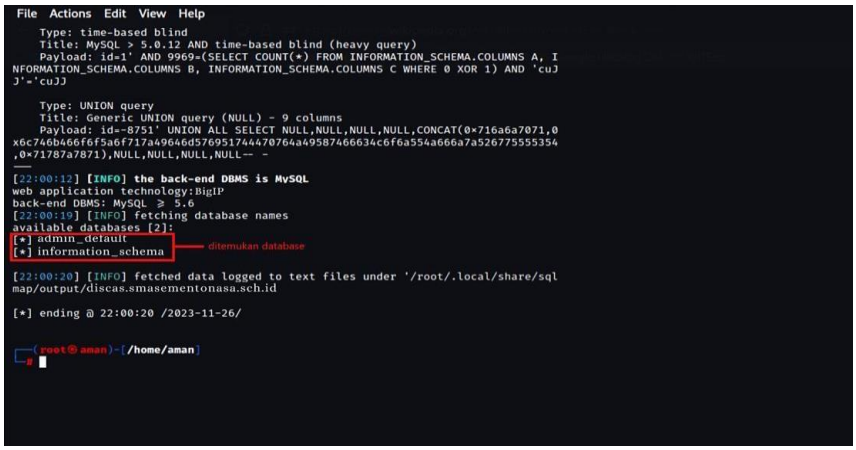


Gambar 10. Keterangan Status Attack Complexity Website



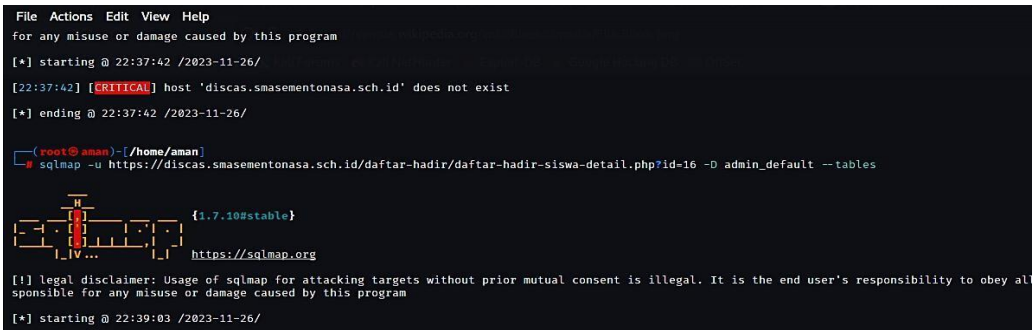
Gambar 11. Perintah SQL Map

Gambar 11 merupakan langkah penetration testing ke dalam database discas.smasementonasa.sch.id menggunakan tools sqlmap dengan memasukkan perintah "sqlmap -https://discas.smasementonasa.sch.id/daftar-hadir/daftar-hadir -siswa-detail.php?id=16 –dbs".



Gambar 12. Hasil penetration testing dengan Sqlmap

Gambar 12. merupakan hasil dari penetration testing dengan menggunakan sqlmap dan mendapatkan informasi database yang terdapat di server discas.smasementonasa.sch.id yang memiliki dua database, yaitu admin_default dan information_schema.



Gambar 13 Script Sqlmap untuk melihat tabel pada database admin_default

Gambar 13. merupakan script sqlmap yang digunakan untuk melihat tabel pada database admin_default di server discas.smasementonasa.sch.id. Perintah yang digunakan adalah "sqlmap -u https://discas.smasementonasa.sch.id/daftar-hadir /daftar-hadir-siswa-detail.php?id=16 –D admin_default –tables".

Gambar 14. Hasil penetration sqlmap untuk melihat table pada database admin_default

Penetrasi yang dilakukan pada website discas.smasementonasa.sch.id dilakukan dengan pertama-tama melakukan scanning untuk menemukan celah serangan. Kemudian celah itu coba diserang menggunakan XSS dan *SQl Injection*. Adapun hasilnya sebagai berikut:

1) Cross Site Scripting

Setelah dilakukan scanning menggunakan bantuan *software Acunetic* 13 dalam menemukan celah XSS, dan juga di lakukan dengan bantuan software nikto untuk menemukan informasi terkait website seperti server dan alamat IP, kemudian dilakukan penetrasi dengan cara memasukkan *script* ke kolom database website. Hasilnya terjadi eror pada website, dimana penyerang bisa mengubah tampilan website sesuai dengan isi script yang dimasukkan. Pada gambar 9, dapat dilihat teks bertuliskan 'TEST' yang dimasukkan menggunakan *script.*

2) SQL Injection

Di lakukan dengan menggunakan bantuan *software Acunetix* 13 dengan melakukan pemilihan konfigurasi *blind sql injection*. Setelah itu, untuk menguji apakah celah ini bisa diserang atau tidak, Di lakukan dengan menambahkan karakter pada url yang memungkinkan membuat *database error* seperti pada gambar 10. Dan di lakukan pentest dengan sqlmap dengan memasukan perintah seperti pada gambar 11. Hasilnya, jenis database yang ada dalam website ditampilan oleh sqlmap. Ada 2 jenis database yang ditampilkan, yaitu admin_default dan information_schema.

Setelah jenis database ditampilkan, penulis kemudian mencoba untuk mengetahui tabel yang terdapat dalam database. Gambar 14 merupakan hasil dari penetration testing. Informasi yang didapatkan adalah database *admin_default* di server discas.smasementonasa.sch.id terdapat *tabel admin, admin_token, message, resgistrant*, dan years yang tersimpan di dalamnya.

IV.Kesimpulan dan saran

Berdasarkan penelitian yang sudah dilakukan, dapat diperoleh beberapa kesimpulan sebagai berikut: Pengujian celah keamanan pada website discas.smasementonasa.sch.id dapat dibuktikan melalui seperangkat tahapan *penetration testing*. Tahapan itu berupa, pengumpulan informasi dan data website berupa teknologi yang digunakan, alamat IP dan jenis kerentanan dengan cara *scanning website* menggunakan *tools Acunetix* 13. Setelah seluruh informasi terkumpul, kemudian dilakukan eksploitasi terhadap celah keamanan itu dengan memanfaatkan *script* dan *tools sqlmap.*

Adapun yang menjadi celah atau kelemahan dari website discas.smasementonasa.sch.id adalah celah keamanan *Cross Side Scripting* (XSS) dan *Sql Injection*. Dari hasil pengujian celah keamanan XSS, ditemukan bahwa website discas.smasementonasa dapat dijebol setelah memasukan inputan berupa *script* yang menyebabkan tampilan *website* menampilkan 'TEST'. Kemudian, pada celah keamanan *Sql Injection*, dilakukan dengan memasukan karakter (') pada akhir url yang ber id dan didapatkan *error* pada *query database* yang dapat dilihat di *browser.* Karenya, dengan memanfaatkan *tools sqlmap* yang di install di Kali Linux, database pada website discas.smasementonasa.sch.id dapat ditemukan.

Perlu diakukan perbaikan celah keamanan pada website ini, untuk menghindari pencurian dan penyalahgunaan data yang ada di dalam website. Kedua, dalam penelitian ini masih terdapat beberapa kelemahan yang dapat dikembangkan pada penelitian selanjutnya, antara lain : Melakukan pengujian celah keamanan website yang lain, dengan merujuk ke Top 10 OWASP & Melakukan pengujian dari sisi *Network*, seperi penyerangan ke port yang terbuka pada server..

Daftar Pustaka

[1] A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA J. Sist. Inf. Dan Inform.*, vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[2] S. M. Prasetiyo, R. Gustiawan, Faarhat, and F. R. Albani, "Analisis Pertumbuhan Pengguna Internet Di Indonesia," *J. Bul. Ilm. Ilmu Komput. dan Multimed.*, vol. 2, no. 1, pp. 65–71, 2024.

[3] A. P. J. I. Indonesia, "Pengguna Internet Indonesia Tembus 221 Juta Orang," Asosiasi Penyelenggara Jasa Internet Indonesia.

[4] J. Ginting and I. G. Suryantara, "Uji Penetrasi Sistem Keamanan Jaringan Universitas Gadjah Mada Dengan Information System Security Assesment Framework," *Infotech J. Technol. Inf.*, vol. 7, pp. 41–46, Jun. 2021, doi: 10.37365/jti.v7i1.105.

[5] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, pp. 183–190, Aug. 2021, doi: 10.31294/ji.v8i2.10854.

[6] I. G. B. Hengki and I. G. N. Anom, "Pembaruan Undang-Undang Cyber Crime Melalui Rancangan Undang-Undang Keamanan Kerahasiaan Data Diri Berbasis Digitalisasi," *Pros. Semin. Nas. ...*, pp. 144–159, 2021, [Online]. Available: https://e-journal.unmas.ac.id/index.php/psnfh/article/view/2397%0Ahttps://e-journal.unmas.ac.id/index.php/psnfh/article/download/2397/1823

[7] Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, "Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia," *J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 1135–1145, 2023.

[8] S. Situmeang, "Fenomena Kejahatan di Masa Pandemi Covid-19: Perspektif Kriminologi," *Maj. Ilm. UNIKOM*, vol. 19, pp. 35–43, Apr. 2021, doi: 10.34010/miu.v19i1.5067.

[9] E. Stephani, F. Nova, and E. Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[10] A. Rosadi and B. A. Wardijono, "Analysis of System Security Levels of Tax Payment and Regional Retribution Based on ISO / IEC27002: 2013 Standard Using SSE-CCM," *Int. Res. J. Adv. Eng. Sci.*, vol. 6, no. 1, pp. 205–211, 2021, [Online]. Available: https://irjaes.com/wp-content/uploads/2021/02/IRJAES-V6N1P175Y21.pdf

[11] D. Sandi and A. Tedyyana, "Implementasi dan Analisa Sistem Pencegahan Intrusi pada Aplikasi Web Menggunakan Web Application Firewall," *Repeater Publ. Tek. Inform. dan Jar.*, vol. 2, pp. 16–26,

Aug. 2024, doi: 10.62951/repeater.v2i4.196.

[12] E. Abdillah, R. Khoriyah, A. Abqariy, and P. Susilo, "Pengembangan Keamanan Website Menggunakan Teknik Penetration Testing dan DAST (Dynamic Application Security Testing)," *Media J. Inform.*, vol. 14, p. 112, Dec. 2022, doi: 10.35194/mji.v14i2.2546.

[13] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," *sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, 2022, doi: 10.56211/sudo.v1i4.160.