JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 12 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v12i1.3882

PENETRATION TESTING KEAMANAN *WEBSITE* STIE SAMARINDA MENGGUNAKAN TEKNIK SQL *INJECTION* DAN XSS

Fisilmy Hayati[1], Muhammad Nizar Sya Bana[2], Toni Anugrah[3*], Muhammad Qomarul Huda[4]

[1,2,3,4]UIN Syarif Hidayatullah Jakarta; Jl. Ir. H. Djuanda No.95, Ciputat, Tangerang Selatan, Banten, Indonesia 15412; (021) 7401925

Riwayat artikel:

Received: 22 November 2022
Accepted: 29 Desember 2023
Published: 1 Januari 2024

Keywords:
Website;
Penetration Testing;
SQL Injection;
Cross Site Scripting;
Cybersecurity.

Corespondent Email:
toni.anugrah20@mhs.uinjkt.ac.id

Abstrak. Website universitas memiliki banyak data dan informasi yang disimpan di dalamnya seperti data mahasiswa, data dosen, data staff, kurikulum, dan yang lainnya. Website sebagai alat untuk menyebarkan data dan informasi tersebut, oleh karena itu penting untuk menguji keamanan suatu website universitas. Terdapat banyak teknik ancaman penetrasi ke dalam suatu website yaitu SQL *injection*, XSS, dan yang lainnya. Untuk mengatasi masalah tersebut, peneliti melakukan analisis kerentanan keamanan website STIE Samarinda dengan *Penetration Testing* yang berfokus kepada teknik SQL *Injection* dan XSS. Terdapat 14 fitur form yang memiliki kerentanan terhadap teknik penetrasi SQL *Injection* dan XSS. Analisis kerentanan keamanan dengan teknik lainnya diperlukan untuk memahami lebih lanjut mengenai keamanan website STIE Samarinda.

Abstract. *The university website contains a wealth of data and information, including student records, faculty information, staff data, curriculum details, and more. The website serves as a tool for disseminating this data and information, making it crucial to assess the security of a university website. Various penetration testing techniques, such as SQL injection, XSS, and others, pose potential threats to the website's security. In order to address these issues, researchers conducted a security vulnerability analysis of the STIE Samarinda website using Penetration Testing, focusing on SQL Injection and XSS techniques. Fourteen form features were identified as having vulnerabilities to SQL Injection and XSS penetration techniques. Further analysis of security vulnerabilities using additional techniques is necessary to gain a more comprehensive understanding of the security of the STIE Samarinda website.*

1.PENDAHULUAN

Website kampus/universitas merupakan sarana yang penting untuk menyampaikan informasi kepada masyarakat terkait dengan profil, pengumuman, kurikulum, data mahasiswa, data dosen, data staff, pendaftaran, dan galeri. Tujuannya adalah memastikan masyarakat dapat dengan mudah mengakses perkembangan informasi terkini.

Selain sebagai alat untuk menyebarkan informasi, website kampus juga berfungsi sebagai platform transaksi online, seperti pendaftaran mahasiswa baru atau pemesanan layanan akademik. Ini memudahkan masyarakat, terutama bagi mereka yang tinggal jauh dari kampus.

Keamanan website sangat penting mengingat website tersebut menyimpan data penting, termasuk data pribadi mahasiswa, data transaksi, dan informasi keuangan. Untuk itu, pengujian keamanan, seperti SQLI (Structured Query Language Injection) dan XSS (Cross Site

Scripting), dapat dilakukan untuk mengidentifikasi potensi celah keamanan [1].

SQLI adalah teknik untuk mengevaluasi kerentanan pada website yang dapat memungkinkan peretas memanipulasi query SQL yang dikirimkan ke database. Ini dapat berdampak serius, menyebabkan kehilangan data atau penyalahgunaan informasi [2].

XSS, di sisi lain, melibatkan penyisipan skrip khusus pada website untuk memungkinkan peretas mengakses informasi dari jarak jauh. Serangan ini dapat dicegah dengan menggunakan fungsi filter karakter dan menghapus tag HTML berbahaya [3].

Penelitian yang dilakukan oleh Gede et al. (2020) menyimpulkan bahwa evaluasi keamanan website suatu lembaga menggunakan framework ISSAF dengan metode penetrasi testing. Hasilnya menunjukkan bahwa serangan XSS dan SQLI dapat dihindari dengan menerapkan fungsi filter karakter pada form input, form pencarian, dan login [4].

Studi yang dilakukan oleh Kusdikdoyodkk (2019) pada website E-CRM toko pelangi menekankan perlunya aspek keamanan pada database untuk mengatasi serangan SQLI dan XSS. Metode studi kasus ini menghasilkan temuan bahwa penggunaan fungsi filter karakter seperti mysql_real_escape_string dapat mencegah injeksi SQL. Selain itu, password dienkripsi dengan MD5, sedangkan pada menu input, filter karakter htmlspecialchars digabungkan dengan enkripsi ent_quotes untuk sejumlah parameter, termasuk nama, tempat lahir, dan kota [5]

Penelitian Kumardkk (2017) juga menggunakan metode studi kasus untuk mendeteksi kerentanan pada keamanan website. Temuan dari penelitian ini menunjukkan bahwa penggunaan bind_param pada menu login dan input, bersama dengan enkripsi password MD5, efektif mencegah serangan SQLI dan XSS [1].

Dhivya et al. (2019) menghasilkan studi tentang pencegahan serangan SQLI dan XSS dengan menggunakan EVENT tools pada menu input, login, dan URL. EVA Itools, sebuah fungsi coding PHP, digunakan untuk membatasi karakter yang diizinkan dan mengubah karakter yang tidak diizinkan menjadi string [3].

Liu & Wang (2018) meneliti metode penetrasi testing untuk mengidentifikasi kerentanan website terhadap serangan SQLI dan XSS. Temuan penelitian menunjukkan bahwa fungsi filter karakter dasar, seperti mysqli_real_escape_string, dan penggantian URL menjadi URLS dapat mencegah serangan [6].

Sitorus dkk (2020) menemukan bahwa serangan SQLI dapat dicegah dengan menerapkan coding anti-injeksi pada query database dan melakukan validasi karakter dengan membatasi jumlah inputan karakter serta mengubah jenis inputan pada form login [7].

Penelitian Gunadhi & Nugraha (2016) menyarankan penggunaan URL dinamis, enkripsi URL, atau penggunaan URL SEO untuk mencegah serangan SQLI dan XSS pada website [8].

Berdasarkan studi yang dilakukan oleh Nurbojatmiko et al. (2022), disimpulkan bahwa pengujian penetrasi dengan menggunakan OWASP-ZAP dapat mengungkap berbagai tingkat kerentanan keamanan pada situs web, termasuk tetapi tidak terbatas pada SQL injection, XSS, dan kerentanan lainnya. Hasil pengujian menunjukkan variasi tingkat kerentanan, dengan solusi yang telah diusulkan untuk meningkatkan keamanan situs web. Penelitian ini menggunakan metode pengujian keamanan, alat-alat, dan fokus pada kerentanan khusus seperti SQL injection dan XSS, serta memanfaatkan kerangka kerja untuk mendeteksi dan mencegah kerentanan dalam perangkat lunak sistem [13].

Beberapa penelitian tersebut menunjukkan bahwa pencegahan serangan SQLI dan XSS dapat dilakukan dengan menggunakan berbagai metode, seperti filter karakter, enkripsi password, dan validasi input [4]. Penggunaan URL dinamis atau enkripsi URL juga dapat membantu mencegah serangan.

Penting untuk menerapkan langkah-langkah keamanan ini pada website kampus/universitas untuk melindungi data sensitif dan memastikan kelancaran operasional. Dengan demikian, masyarakat dapat dengan aman dan nyaman mengakses informasi serta melakukan transaksi secara online.

Dalam penelitian ini dilakukan sebuah analisis kerentanan keamanan website STIE Samarinda dengan menggunakan metode SQLI dan XSS. Penelitian ini bertujuan untuk menganalisa kerentanan atas penyerangan hacking dari website STIE Samarinda dan

mengidentifikasi dan memberikan saran terhadap keamanan website STIE Samarinda khususnya pada teknik SQL Injection dan XSS.

2. TINJAUAN PUSTAKA

Serangan XSS dan SQL *injection* termasuk diantara serangan yang paling berbahaya, dimana salah satu teknik dalam pencegahannya yaitu dengan pencocokan *string* dari *input* pengguna dengan pola *string injection* yang telah disimpan untuk mendeteksi adanya *malicious code* yang dimasukkan [9].

SQL *injection* dimaksudkan sebagai serangan dengan menggunakan suatu *class* dari injeksi kode dimana data yang disediakan *user* termasuk dalam bentuk SQL *Query* sedemikian rupa sehingga input dari pengguna dapat diartikan sebagai kode SQL, hal ini memungkinkan penyerang untuk memanfaatkan kelemahan tersebut dan memasukkan perintah SQL langsung pada *database* dimana *input* tersebut langsung digabungkan dalam SQL *queries* di dalam *database* [10]. Teknik untuk mendeteksi serangan ini diantaranya seperti *log analysis*, deteksi intrusi pada sistem, dan *honeypots* [12].

Serangan XSS (*Cross Site Scripting*) dideskripsikan sebagai serangan injeksi kode pada lapisan aplikasi di sisi klien dimana penyerang memasukkan *malicious scripts* ke dalam aplikasi web yang *vulnerable* karena memiliki kelemahan dalam validasi *input*, sehingga menjadikan *malicious code* tersebut dapat dijalankan pada *browser* pengguna yang tidak bersalah [11].

3.METODE PENELITIAN

Metodologi penelitian merujuk pada suatu rangkaian prosedur sistematis yang diterapkan dalam penelitian untuk memastikan bahwa penelitian tersebut terstruktur dengan baik dan dapat diterima oleh semua pihak terkait. Struktur penelitian yang akan diimplementasikan dalam penelitian ini dapat ditemukan pada gambar berikut.

Gambar 1. Metodologi Penelitian

3.1. Tahapan Review (Review Steps)

Langkah ini merupakan fase permulaan dalam pelaksanaan penelitian, di mana peneliti akan merumuskan masalah yang teridentifikasi pada objek penelitian dan mengukuhkan batasan permasalahan yang diinvestigasi untuk memberikan arah yang lebih jelas

3.2. Menentukan Tujuan

Tahapan ini penting dalam upaya memastikan bahwa peneliti tidak menyimpang dari sasaran yang ingin dicapai dalam penelitian. Pada tahap ini peneliti akan merinci dengan jelas tujuan-tujuan yang ingin dicapai melalui penelitian.

3.3. Mempelajari Studi Literatur

Pada tahapan ini peneliti akan mencari dan memahami bahan-bahan terkait dengan topik penelitian yang bersumber dari artikel jurnal.

3.4. Penentuan Target

Pada tahap ini peneliti menentukan target (*website*) *penetration testing* melalui Google Dorking. Setelah itu setiap *website* dari hasil Google Dorking akan dievaluasi kerentanan *website* mereka terhadap SQL Injection. *Website* yang memiliki kerentanan tersebut akan dipilih sebagai target *penetration testing*.

3.5. Analisis Kerentanan

Pada tahapan ini peneliti akan menguji dan menganalisis keamanan *website* STIE Samarinda menggunakan teknik SQL Injection dan XSS.

1. Peneliti akan mencoba menyisipkan perintah SQL yang tidak sah dan manipulatif ke dalam formulir input di

website. Tujuan dari pengujian ini adalah untuk mengidentifikasi apakah *website* rentan terhadap serangan SQL Injection, yang dapat menyebabkan akses tidak sah.

2. Peneliti akan mencoba menyisipkan skrip XSS ke dalam halaman web, melalui input formulir yang menerima input dari pengguna. Pengujian ini bertujuan untuk menentukan apakah website rentan terhadap serangan XSS, yang dapat memungkinkan penyerang untuk menjalankan skrip pada peramban pengguna akhir.

3.6. Kesimpulan dan Saran

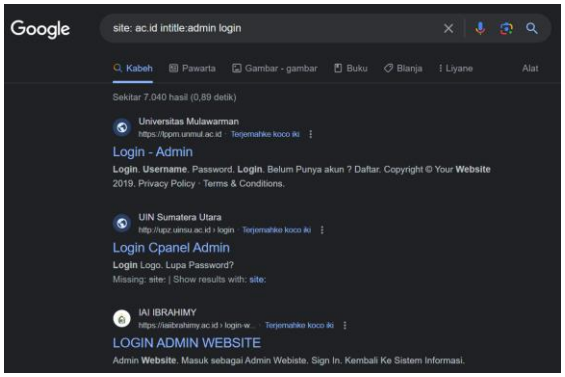
Pada tahapan ini, peneliti akan merangkum temuan-temuan utama yang ditemukan selama penelitian. Ini mencakup jawaban terhadap rumusan masalah atau tujuan penelitian yang telah ditetapkan sebelumnya. Bagian saran akan memberikan rekomendasi kepada pihak terkait, baik praktisi maupun peneliti di masa mendatang. Saran ini bisa berkaitan dengan perbaikan, pengembangan lebih lanjut, atau langkah-langkah pencegahan yang direkomendasikan berdasarkan temuan penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Penentuan Target

Penentuan target dengan teknik dorking Google adalah langkah awal yang dilakukan oleh peneliti untuk mengidentifikasi potensi sasaran atau celah keamanan pada suatu domain atau website. Teknik ini dijalankan melalui input Google Search dengan nilai berikut:

“site: ac.id intitle:admin login”



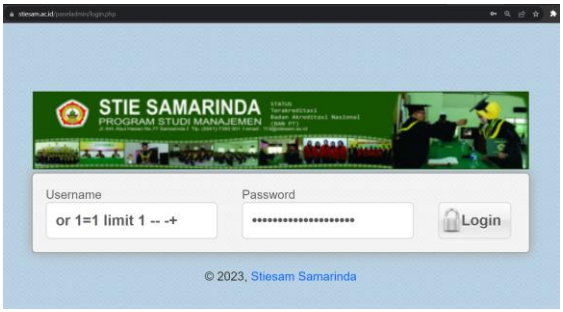
Gambar 2. Dorking melalui Google Search

Berikut adalah penjabaran yang dimaksud dari pencarian yang dilakukan:

1. “site: ac.id”: Operator "site:" digunakan untuk membatasi pencarian pada domain tertentu. Dalam hal ini, pencarian dibatasi pada domain yang memiliki ekstensi ".ac.id", yang sering digunakan oleh lembaga pendidikan di Indonesia.
2. “intitle:admin login”: Operator "intitle:" digunakan untuk membatasi pencarian pada halaman web yang memiliki judul tertentu. Dalam contoh ini, pencarian difokuskan pada halaman web yang judulnya mengandung kata "admin login". Hal ini dapat mengindikasikan bahwa peneliti atau penyerang mencari halaman login admin pada website dengan domain ".ac.id".

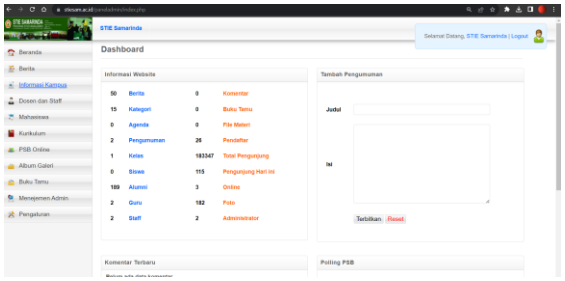
Berdasarkan hasil pencarian tersebut peneliti mencari website yang rentan terhadap SQL Injection. Hal ini dilakukan dengan memasukkan input SQL yang tidak sah ke dalam input untuk memperoleh akses yang sah. Berikut adalah query SQL yang dimasukkan ke dalam input form login website:

“' OR 1 -- -”



Gambar 3. SQL Injection

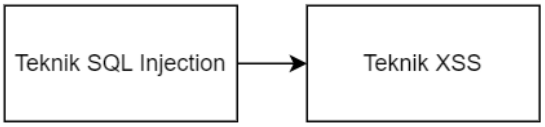
Berdasarkan pencarian peneliti, peneliti menemukan *website https://stiesam.ac.id/paneladmin/login.php* yang rentan terhadap SQL Injection. Hal ini ditunjukkan oleh pemberian akses yang tidak sah kepada peneliti melalui input SQL Query peneliti. Website ini akan dijadikan target *penetration testing* menggunakan teknik XSS dan SQL Injection.



Gambar 4. Akses Admin

4.2 Analisis Kerentanan

Seperti yang telah dijelaskan dalam metodologi penelitian sistem dianalisis dengan menggunakan dua teknik serangan, sebagaimana terlihat pada gambar berikut:

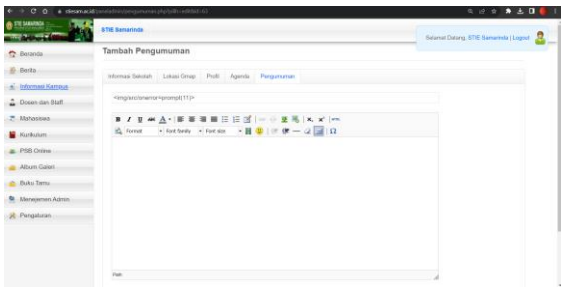


Gambar 5. Teknik Serangan

Langkah analisis, sebagaimana terlihat pada gambar tersebut, menjelaskan bahwa dalam melakukan uji penetrasi pada *website* STIE Samarinda dimulai dengan melaksanakan SQL Injection. Jika terdapat kerentanan, langkah selanjutnya akan melibatkan serangan *Cross-Site Scripting* (XSS), dan kesimpulan akan ditarik dari hasil kedua teknik serangan tersebut.

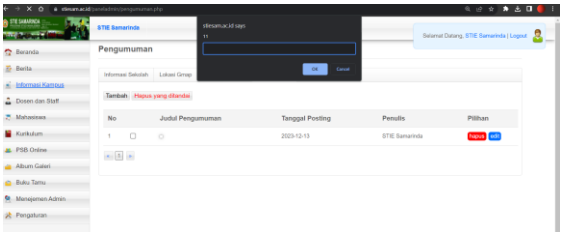
Teknik SQL Injection telah dilakukan pada halaman login sebagaimana yang telah dijelaskan. Selanjutnya peneliti menerapkan teknik XSS pada setiap form yang tersedia di setiap halaman *website https://stiesam.ac.id/* dengan input berikut:

“<img/src/onerror=prompt(11)>”



Gambar 6. Input XSS pada Halaman Tambah Pengumuman

Apabila input XSS berhasil pada formulir tersebut maka halaman yang menampilkan data tersebut akan menjalankan skrip yang telah diinput secara tidak wajar.



Gambar 7. Indikator Keberhasilan Input XSS

No	Keterangan	URL	Teknik	Hasil
1	Form Login	*https://stiesam.ac.id/paneladmin/login.php*	SQL Injection	Rentan
2	Form Tambah Pengumuman	*https://stiesam.ac.id/paneladmin/pengumuman.php?pilih=tambah*	XSS	Rentan
3	Form Tambah Agenda	*https://stiesam.ac.id/paneladmin/agenda.php?pilih=tambah*	XSS	Rentan
4	Form Tambah Profil	*https://stiesam.ac.id/paneladmin/profil.php?pilih=tambah*	XSS	Rentan
5	Form Informasi Kampus	*https://stiesam.ac.id/paneladmin/informasi_sekolah.php*	XSS	Rentan
6	Form Tambah Dosen	*https://stiesam.ac.id/paneladmin/guru_staff.php?pilih=tambah*	XSS	Rentan
7	Form Tambah Staff	*https://stiesam.ac.id/paneladmin/staff.php?pilih=tambah*	XSS	Rentan
8	Form Tambah Jabatan	*https://stiesam.ac.id/paneladmin/jabatan.php?pilih=tambah*	XSS	Rentan
9	Form Tambah Mahasiswa	*https://stiesam.ac.id/paneladmin/siswa.php?pilih=tambah*	XSS	Rentan

10	Form Tambah Alumni	*https://stiesam.ac.id/paneladmin/alumni.php?pilih=tambah*	XSS	Rentan
11	Form Tambah PSB Online	*https://stiesam.ac.id/paneladmin/psb_online.php?pilih=tambah*	XSS	Rentan
12	Form Tambah Album Galeri	*https://stiesam.ac.id/paneladmin/album_galeri.php?pilih=tambah*	XSS	Rentan
13	Form Tambah Buku Tamu	*https://stiesam.ac.id/paneladmin/buku_tamu.php?pilih=tambah*	XSS	Rentan
14	Form Manajemen Administrator	*https://stiesam.ac.id/paneladmin/admin.php*	XSS	Rentan

Tabel 1. Hasil Analisis Kerentanan

Hasil analisis menunjukkan bahwa website STIE Samarinda mengalami sejumlah kerentanan keamanan, terutama pada form yang terpengaruh oleh teknik XSS.

5.KESIMPULAN

Pada pengujian yang sudah dilakukan pada tahapan sebelumnya maka dapat disimpulkan bahwa website STIE Samarinda memiliki 14 tempat yang sering digunakan oleh pihak tidak sah (*hacker*) untuk melancarkan aksinya. Adapun berdasarkan pengujian tersebut disimpulkan bahwa *website* STIE Samarinda yang memiliki 14 celah kerentanan, semua jumlah celah kerentanan website STIE Samarinda tersebut disebut berstatus vulnerable atau rentan terhadap serangan SQL *Injection* dan XSS.

Berdasarkan hasil penetration testing pengembang situs web STIE Samarinda perlu melakukan aksi pencegahan terhadap penyerangan dengan teknik SQL *Injection* dan XSS. Berikut adalah beberapa saran yang dapat diterapkan untuk pengembangan situs web selanjutnya:

a. Validasi input dari pengguna dengan memastikan bahwa hanya data yang sesuai dengan format yang diharapkan yang diterima.
b. Validasi input dari pengguna dan tolak atau sanitasikan data yang mencurigakan atau tidak sah.
c. Selalu perbarui perangkat lunak serta framework yang digunakan untuk memastikan perlindungan terhadap kerentanan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Kumar, S., Mahajan, R., Kumar, N., & Khatri, S. K. (2018). A study on web application security and detecting security vulnerabilities. 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, 2018-Janua, 451–455. https://doi.org/10.1109/ICRITO.2017.8342469.

[2] Yulianingsih, Y. (2016). Menangkal Serangan SQL Injection Dengan Parameterized Query. Jurnal Edukasi Dan Penelitian Informatika (JEPIN), 2(1), 46–49. https://doi.org/10.26418/jp.v2i1.15507.

[3] Dhivya, Praveen Kumar, Saravanan, P. (2018). Evaluation Of Web Security Mechanisms Using Vulnerability & Sql Attack Injection. 119(14), 989–996.

[4] I Gede, Gusti Madi & Sri Arsa.(2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. Jurnal Ilmiah Merpati, 8(2), 113–124.

[5] Dwi Handoko Kusdikdoyo, T. W. (2019). Menerapkan Aspek Keamanan Database Pada Website E-CRM Toko Pelangi. 2, 419–430. https://doi.org/http://dx.doi.org/10.30700/.v2i1.871

[6] Liu, M., & Wang, B. (2018). A web second-order vulnerabilities detection method. IEEE Access, 6, 70983–70988. https://doi.org/10.1109/ACCESS.2018.2881070

[7] Sitorus, S. P., & Habibi, R. A. (2020). Teknik Pencegahan Penetrasi SQL Injeksi Dengan Pengaturan Input Type Number dan Batasan Input Pada Form Login Website. U-NET Jurnal Teknik Informatika, 4(2), 26–33. https://doi:10.52332/u-net.v4i2.303

[8] Gunadhi, E., & Nugraha, A. P. (2016). Penerapan Kriptografi Base64 Untuk

Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. Jurnal Algoritma, 13(2), 391–398. https://doi:10.33364/algoritma/v.13-2.39

[9] Abikoye, O. C., Abubakar, A., Dokoro, A. H., Akande, O. N., & Kayode, A. A. (2020). A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm. EURASIP Journal on Information Security, 2020, 1–14.

[10] Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering, 1, 13–15.

[11] Sarmah, U., Bhattacharyya, D. K., & Kalita, J. K. (2018). A survey of detection methods for XSS attacks. Journal of Network and Computer Applications, 118, 113–143.

[12] Abdullayev, V., & Chauhan, A. S. (2023). SQL Injection Attack: Quick View. Mesopotamian Journal of CyberSecurity, 2023, 30–34.

[13] Nurbojatmiko, Ari Lathifah, Faaza Bil Amri, Ani Rosidah (2022). Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP. The 10th International Conference on Cyber and IT Service Management., 2022,.