Jurnal Sistim Informasi dan Teknologi
https://jsisfotek.org/index.php
2021 Vol. 3 No. 4 Hal: 215-220 e-ISSN: 2686-3154

Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS

Muhammad Arif Zikir Risky[1]✉, Yuhandri [2]
[1]Independent Researcher
[2]Universitas Putra Indonesia YPTK Padang
arifzikir66@gmail.com

Abstract

SQLI (SQL Injection) and XSS are hacking techniques that are often used by hackers. This technique can find out the contents of the database by inserting a script on the website. This technique can be a threat if a website does not have security that can ward off such attacks. Hackers will look for loopholes using this technique in a login menu, searching, upload menu, input menu and URLs that have parameters ending in numbers, but not all websites that can be attacked use this technique if you don't limit the use of characters. This research was conducted to find out the gaps in a website that can be attacked with SQLI and XSS techniques and help optimize website security to avoid these attacks. Penetration testing will be carried out on a CV car rental website. Merdeka Auto Rental which is located in Padang City. This penetration testing uses SQLI and XSS techniques to find security holes in a website. The result of this test is that on the car rental website there are 12 gaps that are vulnerable to SQLI and XSS attacks, based on the results of these tests, a PHP script function is made that can remove all dangerous special characters. The script function is inserted in the PHP input, process and output files. The use of this script function does not apply to attacks other than SQLI and XSS so that if hackers use attack techniques other than that, this website is vulnerable to these attacks. After the script is inserted in the source code of the website, it can be concluded that the 12 known loopholes in the previous test without using the script function have changed status to not vuln or not vulnerable to SQLI and XSS attacks.

Keywords: Penetration Testing, SQLI, XSS, Function Script, Filter Character.

Abstrak

SQLI (SQL Injection) dan XSS merupakan salah satu teknik hacking yang sering digunakan oleh seorang hacker. Teknik ini bisa mengetahui isi yang ada pada database dengan menyisipkan script pada website. Teknik ini bisa menjadi sebuah ancaman jika sebuah website tidak memiliki keamanan yang dapat menangkal serangan tersebut. Hacker akan mencari celah dengan menggunakan teknik tersebut pada sebuah menu login, searching, menu upload, menu input dan URL yang memiliki parameter berakhiran dengan angka, tetapi tidak semua website yang bisa diserang menggunakan teknik ini jika tidak membatasi penggunaan karakter. Penelitian ini dilakukan untuk mengetahui celah pada sebuah website yang dapat diserang dengan teknik SQLI dan XSS serta membantu mengoptimalisasikan keamanan website agar terhindar dari serangan tersebut. Penetrasi testing akan dilakukan pada sebuah website rental mobil CV. Merdeka Auto Rental yang beralamat di Kota Padang. Penetrasi testing ini menggunakan teknik SQLI dan XSS untuk menemukan celah keamanan sebuah website. Hasil dari pengujian ini adalah pada website rental mobil terdapat 12 celah yang rentan terhadap serangan SQLI dan XSS, berdasarkan hasil pengujian tersebut maka dibuatlah sebuah script function PHP yang dapat membuang semua karakter spesial yang berbahaya. Script function tersebut disisipkan pada file PHP input, proses dan output. Penggunaan script function ini tidak berlaku untuk serangan selain SQLI dan XSS sehingga jika hacker menggunakan teknik serangan selain itu maka website ini rentan terhadap serangan tersebut. Setelah script tersebut disisipkan pada source code website maka dapat disimpulkan bahwa 12 celah yang sudah diketahui pada pengujian sebelumnya yang tanpa menggunakan script function, sudah berubah status menjadi tidak vuln atau tidak rentan terhadap serangan SQLI dan XSS.

Kata kunci: Penetrasi Testing, SQLI, XSS, Script Function, Filter Karakter.

1. Pendahuluan

Website merupakan sebuah wadah untuk menginformasikan kepada masyarakat tentang hasil produk pada perusahaan atau pelayanan jasa pada instansi-instansi pemerintah dimana tujuannya adalah agar masyarakat dapat mengetahui perkembangan informasi yang ada pada saat ini. Selain sebagai media untuk menyebarkan informasi, *website* juga digunakan sebagai media transaksi berbasis online seperti transaksi pembelian, transaksi penjualan, transaksi pemesanan dll sehingga dapat membantu masyarakat untuk bertransaksi khususnya untuk masyarakat yang lokasi tempat tinggalnya jauh dari toko. *Website* harus memiliki tampilan yang bagus dan mudah digunakan oleh masyarakat, selain itu *website* harus memiliki keamanan dari serangan *hacker* karena *website* tersebut memiliki sebuah *database* untuk menyimpan data-data penting pelanggan. Sebagai contoh data pribadi pelanggan, data transaksi, data keuangan dll. Oleh sebab itu penting adanya keamanan pada *website* dimana nanti bisa diketahui celah yang dapat masuk ke

Diterima: 17-08-2021 | Revisi: 01-09-2021 | Diterbitkan: 31-12-2021 | doi: 10.37034/jsisfotek.v3i4.68

dalam *website* tersebut. Ada beberapa teknik untuk menguji keamanan *website*, salah satunya yaitu SQLI (*Structured Query Language Injection*) dan XSS (*Cross Site Scripting*).

SQLI dan XSS merupakan salah satu teknik *hacking* yang sering digunakan oleh seorang *hacker*. Teknik ini bisa mengetahui isi dari tabel-tabel pada *database*, *session*, *cookies*, *user*, tipe *database* dan versi *database* dengan mencantumkan *script* atau *payload* pada sebuah *website* [1]. SQLI adalah sebuah teknik untuk mengetahui kerentanan pada website yang menyebabkan seorang hacker bisa untuk mempengaruhi *query SQL* yang dikirimkan melalui website *database* [2]. SQLI bukan suatu serangan yang eksklusif untuk mempengaruhi website, melainkan menyisipkan kode untuk menerima masukan dari sumber yang tidak diketahui dan kemudian menggunakan input script SQL dinamis yang bisa menyebabkan website rentan [3]. Serangan ini sangat berisiko karena bisa menyebabkan hilangnya data, informasi atau menyalahgunakan data oleh orang yang tidak bertanggunjawab serta mempunyai akibatnya fungsi fungsi kerahasiaannya menjadi rusak [4].

SQLI merupakan serangan website yang menggunakan query SQL dimana query tersebut disisipkan dengan karakter-karakter spesial yaitu karakter selain huruf dan angka. Dalam melakukan serangan SQLI biasanya menggunakan single quote character (‘) atau double quote character (“) atau tanda pagar (#) di akhir parameter angka untuk mengetahui website tersebut rentan atau tidak [5]. Peretas dengan kemampuan tinggi dapat melakukan control pada website setelah mendapatkan sebuah celah dengan serangan SQLI atau XSS, dimana peretas dapat mengirimkan sebuah script menggunakan payload ke website dengan melakukan rekayasa sistem [6]. Berdasarkan uraian di atas maka SQLI adalah suatu teknik untuk menguji keamanan *website* menggunakan *tag HyperText Markup Language* (HTML) atau karakter spesial yang bertujuan untuk merekayasa *query* SQL pada *database*.

Melepaskan karakter atau escape character adalah sebuah fungsi tag HTML yang dapat membuang karakter-karakter yang menyebabkan terjadinya serangan SQLI sehingga jika pada input variabel dari URL atau dari form input dengan menyisipkan perintah SQL, maka sistem website tidak akan mengeksekusi karena akan terbaca sebagai input variabel bukan query SQL [7]. Fungsi htmlentities merupakan salah satu dari tag HTML dimana fungsi ini akan merubah karakter spesial pada string menjadi entity sedangkan fungsi strip_tags juga termasuk bagian dari tag HTML dimana fungsi ini akan menghapus semua tag HTML yang dapat dianggap berbahaya serta merubah tag tersebut menjadi input biasa yang tidak memiliki dampak terhadap website [8].

XSS adalah salah satu teknik penetrasi testing dimana serangan yang dilakukan menggunakan kode atau script dengan menggunakan karakter spesial [9]. Serangan XSS dilakukan dengan menggunakan kode atau script yang memiliki karakter spesial dan kode tersebut diletakkan di akhir URL website dimana kode atau script yang dimaksud adalah kode javascript yang disisipkan pada website [10]. XSS juga dapat diartikan sebagai kelemahan yang terjadi karena web server tidak dapat memvalidasi data masukan yang diberikan oleh pengguna [11]. Dampak dari serangan menggunakan teknik XSS ini adalah seorang peretas dapat mengetahui isi dari database dan akan menjadi sangat berbahaya jika serangan itu terjadi [12]. Pada serangan XSS, peretas akan menggunakan payload untuk menyisipkan situs website dengan javascript sehingga hacker dapat mengakses korban dari jarak jauh, dan nantinya informasi penting dari korban akan dikaitkan ke website seperti xsshunter. Setelah terpancing, payload akan menampilkan pop di bawahnya yang akan membuat browser korban selalu online. Kemudian peretas akan mengarahkan korban ke situs web phishing [13].

Penelitian yang dilakukan oleh (Gede, 2020) menyatakan bahwa evaluasi yang dilakukan dalam keamanan website suatu lembaga X menggunakan framework ISSAF menggunakan metode penetrasi testing dimana memiliki hasil bahwa serangan XSS dan SQLI dapat dicegah dengan fungsi filter karakter pada form input, form pencarian dan login [14].

Penelitian yang dilakukan oleh (Kusdikdoyo dkk, 2019) menyatakan bahwa pada website E-CRM toko pelangi dalam mengatasi serangan SQLI dan XSS akan menerapkan aspek keamanan pada database. Penelitian ini menggunakan metode studi kasus dengan hasil penelitian yaitu dalam mencegah website E-CRM dari serangan hacker maka menggunakan fungsi filter karakter mysqli_real_escape_string untuk mencegah website dari injeksi SQL serta menggunakan password enkripsi MD5. Sedangkan pada menu input, penelitian ini menggunakan filter karakter htmlspecialchars dan digabungkan dengan enkripsi ent_quotes untuk form input namadepan, namabelakang, tempatlahir dan kota, sedangkan untuk tgllahir tidak menggunakan filter karakter karena berisi angka sedangkan untuk kolom input email menggunakan fungsi strip_tags.

Serangan SQLI dan XSS juga dapat dicegah dengan menggunakan fungsi bind_param yang disisipkan pada menu login dan menu input seperti pada penelitian yang dilakukan oleh Kumar dkk (2017) dimana penelitian ini menggunakan metode studi kasus untuk mendeteksi kerentanan pada keamanan website. Hasil dari penelitian ini menyatakan bahwa penggunaan bind_param pada menu login dan input, serta menggunakan enkripsi password MD5 dapat mencegah dari serangan SQLI dan XSS.

Penelitian yang dilakukan oleh Dhivya dkk (2019) menghasilkan sebuah studi mengenai pencegahan serangan SQLI dan XSS yaitu dengan menggunakan

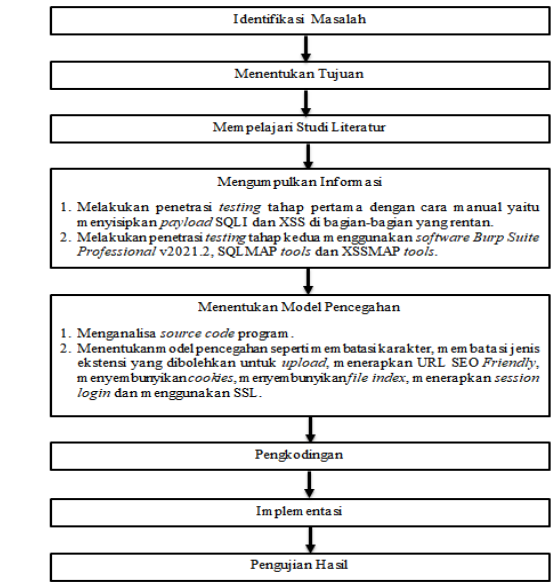
EVAIT tools untuk mengatasi serangan SQLI dan XSS pada menu input, login dan URL. EVAIT tools merupakan coding function PHP yang membatasi karakter apa saja yang diizinkan, sedangkan untuk karakter yang tidak diizinkan, akan dirubah menjadi bentuk string.

SQLI dan XSS dapat dicegah dengan menggunakan fungsi filter karakter mysqli_real_escape_string dan mengganti URL menjadi URLS, seperti pada penelitian yang dilakukan oleh Liu & Wang (2018) yang menggunakan metode penetrasi testing untuk mengetahui kerentanan website. Penelitian ini mempunyai hasil yaitu SQLI dan XSS dapat dicegah dengan fungsi filter karakter dasar yaitu mysqli_real_escape_string serta merubah URL menjadi URLS [15] . Penelitian yang dilakukan oleh (Sitorus dkk, 2020) menghasilkan bahwa serangan SQLI dapat dicegah dengan cara menerapkan coding anti injeksi dibagian query database dan menerapkan validasi karakter seperti membatasi jumlah inputan karakter serta mengubah jenis inputan pada form login [16].

Penggunaan URL dinamis untuk mencegah website dari serangan SQLI dan XSS seperti pada penelitian Gunadhi & Nugraha (2017) menyatakan serangan SQLI dan XSS dapat dicegah dengan enkripsi URL atau penggunaan URL SEO [17].

2. Metodologi Penelitian

Kerangka kerja penelitian adalah suatu alur sistematis yang digunakan dalam penelitian supaya penelitian yang dilakukan dapat tersusun secara sistematis dan diterima oleh semua pihak. Adapun kerangka kerja penelitian yang akan dilakukan pada penelitian ini, dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Kerja Penelitian

Kerangka kerja penelitian seperti pada Gambar 1 dimana memiliki 8 tahap dalam melakukan penelitian ini, yaitu:

2.1. Identifikasi Masalah

Tahapan ini merupakan langkah awal dari penelitian yang akan dilakukan dimana peneliti akan membuat rumusan masalah yang ditemukan pada objek penelitian serta menentukan batasan dari permasalahan yang diteliti agar lebih terarah.

2.2. Menentukan Tujuan

Tahapan ini diperlukan agar peneliti tidak menyimpang dari tujuan yang ingin dicapai. Pada Tahapan ini akan memperjelas ruang lingkup dan batasan dari sebuah masalah.

2.3. Mempelajari Studi Literatur

Tahapan ini juga sangat penting dilakukan karena peneliti akan mencari dan memahami materi mengenai topik penelitian yang berasal dari jurnal periode 5 tahun ke belakang.

2.4. Mengumpulkan Informasi

Tahapan ini dilakukan untuk mencari informasi berupa celah kerentanan XSS dan SQLI pada website rental mobil CV. Merdeka Auto Rental dimana langkah-langkahnya yaitu:

a. Melakukan penetrasi testing tahap pertama dengan cara manual yaitu menyisipkan payload SQLI dan XSS di bagian-bagian yang rentan terhadap serangan tersebut seperti URL, form pencarian, form login, form input pendaftaran dan form input komentar/saran.

b. Melakukan penetrasi testing tahap kedua menggunakan software Burp Suite Professional v2021.2, SQLMAP tools dan XSSMAP tools.

2.5. Menentukan Model Pencegahan

Setelah informasi didapatkan pada tahapan sebelumnya, tahapan ini bertujuan untuk memberikan model pencegahan supaya website dapat terhindar dari serangan SQLI dan XSS, dimana untuk menentukan model pencegahan, langkah-langkahnya sebagai berikut:

a. Menganalisa source code program.

b. Menentukan model pencegahan seperti membatasi karakter, membatasi jenis ekstensi yang dibolehkan untuk upload, menerapkan URL SEO Friendly, menyembunyikan cookies, menyembunyikan file index, menerapkan session login dan menggunakan SSL.

2.6. Pengkodingan

Tahapan ini merupakan proses pengkodingan dari model pencegahan yang telah ditentukan pada tahapan sebelumnya, dimana model pencegahan tersebut akan

dibuat dalam bentuk script menggunakan bahasa pemograman PHP.

2.7. Implementasi

Implementasi dilakukan setelah tahapan pengkodingan selesai, dimana script PHP yang sudah dibuat, akan diimplementasikan pada source code program.

2.8. Pengujian Hasil

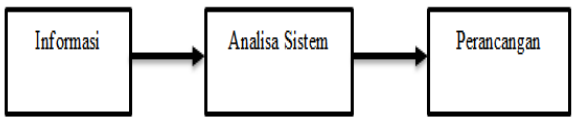
Tahapan ini merupakan tahapan terakhir dari penelitian, dimana setelah script diimplementasikan pada source code program, maka akan dilakukan kembali penetrasi testing dengan bantuan software maupun tools, dengan tujuan untuk mengetahui apakah script tersebut bisa menahan serangan SQLI dan XSS pada website.

3. Hasil dan Pembahasan

3.1. Tahapan Analisa dan Perancangan

Pada bab ini akan membahas tentang analisa dan perancangan sistem untuk mengetahui celah kerentanan sistem keamanan sebuah website rental mobil dari serangan SQLI dan XSS. Sistem yang akan dirancang yaitu script function dengan bahasa pemograman PHP yang dapat membuang karakter-karakter spesial yang sering digunakan pada script payload SQLI dan XSS. Adapun script PHP ini nantinya akan disisipkan pada file proses dan file output. Proses kerja dari script ini adalah apabila diketahui sebuah input yang mengandung karakter spesial berupa script payload, maka function ini akan menghapus payload tersebut sehingga tidak tersimpan ke dalam database. Penghapusan ini disebabkan karena pada script function ini memiliki beberapa metode deteksi semua jenis karakter spesial maupun dalam bentuk encoding, sehingga dalam menggunakan script function ini harus disesuaikan dengan model input website.

Berdasarkan kerangka kerja penelitian yang terdapat pada metodologi penelitian yang terdiri dari identifikasi masalah, menentukan tujuan, mempelajari studi literatur, mengumpulkan informasi, menentukan model pencegahan, pengkodingan, implementasi dan pengujian hasil. Guna memudahkan dalam analisa dan perancangan sistem maka dibuat bagan alir analisa dan perancangan, dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Analisa dan Perancangan

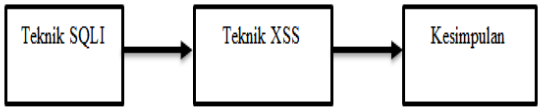
3.2. Informasi

Informasi yang diambil untuk penelitian ini bersumber dari website rental mobil CV. Merdeka Auto Rental. Adapun informasi yang diperoleh berupa nama website, domain, IP website, admin, form input, form proses dan output. Informasi ini diperoleh dengan cara bertanya secara langsung kepada pemilik perusahaan mengenai nama website, dari nama website tersebut dilakukan pengecekan dengan metode whitebox testing. Berdasarkan informasi yang didapatkan maka dilakukan sample testing guna mengetahui alur proses website tersebut.

Sample testing dimulai dari sisi user dimana user melakukan pendaftaran, melakukan login, melihat detail mobil, memilih mobil, melakukan pemesanan dan upload pembayaran. Sedangkan dari sisi admin dimulai dari pengecekan data pelanggan, pengecekan data rental, pengecekan data mobil, data sopir dan pembuatan laporan. Adapun informasi yang didapat berdasarkan informasi sample testing.

3.3. Analisa Sistem

Sebagaimana yang telah digambarkan pada bagan alir analisa dan perancangan, maka dalam menganalisa sistem mengunakan beberapa teknik serangan sebagai disajikan pada Gamabr 3.



Gambar 3. Tahapan Analisa Sistem

Tahapan analisa sistem seperti pada Gambar 3, menjelaskan bahwa dalam melakukan penetrasi testing di website rental mobil dimulai dengan melakukan SQLI, jika vuln maka akan lanjut dengan serangan XSS, dan nantinya akan ditarik kesimpulan dari hasil kedua teknik serangan tersebut.

3.3.1. Teknik SQLI

Proses awal penetrasi testing pada penelitian ini yaitu menggunakan teknik SQLI dengan cara menyisipkan karakter spesial di form login. Adapun pseudocode tahapan penetrasi testing menggunakan teknik SQLI di form login, dapat dilihat pada Gambar 4.

```
Tahapan SQLI Form Login

Begin

String (payload SQLI)

Input payload SQLI

Print
Payload SQLI;

Read 'payload SQLI'

Process
SQL check SELECT statement

IF (Website menggunakan filter karakter)
Then
Output (Kembali Ke Menu Login)
Else IF (Website tidak menggunakan filter karakter)
Then
Output (Tampil Hasil Query di Database)
End IF

Print Output

Stop
```

Gambar 4. Pseudocode SQLI Form Login

Pseudocode yang terlihat pada Gambar 4 merupakan tahapan proses penetrasi testing menggunakan teknik SQLI form login. Adapun implementasi dari tahapan tersebut adalah sebagai berikut:

a. Mencari target website

   Pencarian website yang memiliki celah SQLI ditandai dengan munculnya pesan eror ketika menyisipkan karakter single quote (‘) di akhir URL yang memiliki parameter. Jika website eror setelah disisipkan karakter single quote maka website tersebut rentan terhadap SQLI.

b. Mencari menu login

   Setelah website menampilkan pesan eror setelah disisipkan karakter single quote maka akan kita cari menu login untuk disisipkan payload SQLI.

c. Input payload SQLI form login

   Payload SQLI menggunakan logika OR seperti 1’ OR 1=1 LIMIT 1-- . Payload ini dimasukkan ke dalam form input berupa username dan password.

d. SQL memeriksa inputan

   Payload yang dimasukkan adalah 1’ OR 1=1 Limit 1— sehingga query SQL akan memeriksa apakah masukan tersebut tersedia atau tidak. Jika dalam proses pemeriksaan oleh SQL mengalami kegagalan karena website menggunakan filter karakter, maka akan dikembalikan ke menu login untuk memasukkan username dan password kembali dengan benar.

e. SQL menampilkan data di database

   Ketika payload tersebut diproses oleh database maka query select akan bernilai benar karena adanya logika or 1=1. Syntak SQL seterusnya seperti AND passpel='Kotasurabaya1995' tidak akan diproses karena SQL akan menganggap itu sebagai komentar.

f. SQL mengirimkan data ke website

   Ketika user memasukkan payload 1’ OR 1=1 LIMIT 1— pada form login dan menekan tombol login, maka secara otomatis SQL akan menerima masukan tersebut dan menampilkan data ke website dalam bentuk berhasil login dengan username dan password palsu.

g. Masuk halaman user

   Pada proses penetrasi testing menggunakan teknik SQLI di form login dikatakan berhasil, sehingga bisa masuk ke halaman user tanpa memasukkan username dan password yang sesungguhnya.

3.3.2. Teknik XSS

Penggunaan payload XSS bisa digunakan untuk mengambil cookie session serta menyimpan otomatis cookie session tersebut. Adapun pseudocode tahapan penetrasi testing menggunakan teknik XSS dapat dilihat pada Gambar 5.

```
Tahapan XSS di Form Pendaftaran

Begin

String (Payload XSS)

Input payload XSS di form pendaftaran;

Print
Payload XSS di form pendaftaran;

Read ‘payload XSS’ AS ‘output’

INSERT ‘output’

SELECT ‘output’

Print ‘output’

Stop
```

Gambar 5. Pseudocode XSS

3.3.3. Hasil

Setelah dilakukannya analisa menggunakan teknik SQLI dan XSS pada website rental mobil, maka didapatkan hasil analisa yang akan menjadi sumber untuk dilakukannya pengujian. hasil analisa dapat dilihat pada Tabel 1.

Tabel 1. Hasil Analisa

No	Keterangan	URL	Rencana Pengujian
1	Form Pendaftaran Personal	http://localhost/rentalmobil_kacau/daftarpersonal	Menggunakan payload XSS
2	Form Pendaftaran Kelompok	http://localhost/rentalmobil_kacau/daftarkelompok	Menggunakan payload XSS
3	Form Login Personal	http://localhost/rentalmobil_kacau/personal	Menggunakan payload SQLI
4	Form Login Kelompok	http://localhost/rentalmobil_kacau/kelompok	Menggunakan payload SQLI
5	Form Detail Mobil	http://localhost/rentalmobil_kacau/detail?merek=Daihatsu001	Menggunakan payload XSS dan SQLI
6	Form Pesan Mobil	http://localhost/rentalmobil_kacau/pesan?merek=Daihatsu001	Menggunakan payload XSS dan SQLI
7	Form Masukan/Saran	http://localhost/rentalmobil_kacau/saran	Menggunakan payload XSS
8	Form Login Admin	http://localhost/rentalmobil_kacau/admin/	Menggunakan payload SQLI
9	Menu Detail Data Pelanggan	http://localhost/rentalmobil_kacau/admin/detailpelanggan?noktp=1371063112950009	Menggunakan payload XSS dan SQLI
10	Menu Edit Data Mobil	http://localhost/rentalmobil_kacau/admin/editmobil?idkendaraan=113	Menggunakan payload XSS dan SQLI
11	Menu Input Data Mobil	http://localhost/rentalmobil_kacau/admin/inputmobil	Menggunakan payload XSS
12	Menu Detail Data Supir	http://localhost/rentalmobil_kacau/admin/detailsupir?ktp=1371103010820003	Menggunakan payload XSS dan SQLI

Hasil analisa pada Tabel 1 menjelaskan bahwa website rental mobil memiliki banyak form input dan proses

sehingga ini akan dijadikan acuan dalam melakukan pengujian penetrasi testing.

Setelah dilakukan pengujian terhadap website rental mobil baik yang belum menggunakan script function maupun yang sudah menggunakan script function, maka didapatkan hasil status tidak vuln.

4. Kesimpulan

Pada pengujian yang sudah dilakukan pada tahapan sebelumnya maka dapat disimpulkan bahwa website rental mobil memiliki 12 tempat yang sering digunakan oleh hacker untuk melancarkan aksinya. Adapun berdasarkan pengujian tersebut disimpulkan bahwa website rental mobil yang memiliki 12 celah kerentanan, setelah dilakukan pengujian website sebelum diterapkan script function PHP, maka hasilnya semua lubang celah tersebut berstatus vuln atau rentan terhadap serangan SQLI dan XSS. Berdasarkan pada hasil pengujian tersebut maka dibuatlah sebuah script PHP dengan menggunakan function yang dapat membuang karakter-karakter spesial, sehingga ketika terdapat input data yang berisi payload maka sistem akan menolak dan membuat payload tersebut agar tidak tersimpan ke database. Adapun hasil dari penggunaan script function tersebut dimana lubang celah pada website rental mobil sudah berstatus tidak vuln terhadap serangan SQLI dan XSS.

Daftar Rujukan

[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] Zulkifli, & Samsir. (2020). Implementasi Sistem Keamanan SQL Injection Dalam berbasis web. U-NET Jurnal Teknik Informatika, 4(1), 8–13. https://doi:10.52332/u-net.v4i1.164.

[4] Halfond, W. G. J., & Orso, A. (2017). Detection and Prevention of SQL Injection Attacks. Advances in Information Security, 27(8), 85–109. https://doi.org/10.1007/978-0-387-44599-1_5.

[5] Bangkit Wiguna, Adi Prabowo, W., & Ananda, R. (2020). Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website. Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi, 11(2), 245–256. https://doi.org/10.31849/digitalzone.v11i2.4867.

[6] Sahren, Ashari Dalimuthe, R., & Amin, M. (2019). Prosiding Seminar Nasional Riset Information Science (SENARIS) Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus. September, 994–1001. https://doi.org/http://dx.doi.org/10.30645/senaris.v1i0.109

[7] 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

[8] Marashdih, A. W., & Zaaba, Z. F. (2017). Cross Site Scripting: Removing Approaches in Web Application. Procedia Computer Science, 124, 647–655. https://doi.org/10.1016/j.procs.2017.12.201

[9] Nagpal, B., Chauhan, N., & Singh, N. (2017). SECSIX: security engine for CSRF, SQL injection and XSS attacks. International Journal of Systems Assurance Engineering and Management, 8, 631–644. https://doi.org/10.1007/s13198-016-0489-0

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

[11] Setiawan, E. B., & Setiyadi, A. (2018). Web vulnerability analysis and implementation. IOP Conference Series: Materials Science and Engineering, 407(1). https://doi.org/10.1088/1757-899X/407/1/012081

[12] Aliero, M. S., Ghani, I., Qureshi, K. N., & Rohani, M. F. (2020). An algorithm for detecting SQL injection vulnerability using black-box testing. Journal of Ambient Intelligence and Humanized Computing, 11(1), 249–266. https://doi.org/10.1007/s12652-019-01235-z

[13] Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 729–737. https://doi.org/10.11591/ijeecs.v12.i2.pp729-737

[14] 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.

[15] 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

[16] 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

[17] 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.13-2.391