JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

Penerapan Keamanan Login Admin Dan Filterisasi Input Untuk Mencegah Sql Injection

Yovie Ferdianto[1], Riska Nurtantyo[2], Iin Kurniasari[3]
[1]Teknik Komputer, Universitas Islam Kadiri, Indonesia
[1]yovieferdiantoo@gmail.com

Submitted : **1 July 2023** | **Accepted** : **10 September 2023** | **Published** : **15 September2023**

Abstrak: Dalam industri teknologi informasi, situs *web* sering menjadi sasaran serangan oleh peretas dengan berbagai macam cara untuk mengakali keamanan situs *web* tersebut. Serangan *SQL Injection* sering kali terjadi melalui *form login* dengan memasukkan *username* dan *password* yang telah dimodifikasi sedemikian rupa sehingga situs *web* tersebut dapat dengan mudah diakses oleh peretas. Sering kali kita mengabaikan keamananan pada *web*, Padahal para *hacker* bisa mengakses data kita itu dengan cara memasukan *sintax SQL Injection* pada *login*. Untuk mencegah serangan injeksi semacam ini, berbagai cara dilakukan, salah satunya adalah dengan menggunakan filterisasi input dengan teknik "*maxlength*" dan "*input type number*". Teknik ini ditanamkan ke dalam *source code php* atau *html* yang disisipkan pada *form login* di bagian input *username* dan *password*. Keuntungan dari teknik ini adalah dapat membuat batasan pada inputan *username* dan mengubah format inputan *password* hanya dalam bentuk angka. Bisa juga menggunakan teknik *addslashes() php* untuk mengembalikan nilai *string* dengan menambahkan karakter backslash terbalik (\) sebelum karakter-karakter tertentu seperti tanda kutip tunggal (') sehingga dapat mencegah peretas dalam melakukan serangan *SQL Injection* secara paksa pada situs *web* tersebut.

Kata Kunci: *SQL Injection*; Keamanan *Login*; Filterisasi *Input*; Teknik *addslashes*() *PHP;* Teknik *maxlength,* Teknik *Input type number.*

Abstract: In the information technology industry, websites are often the target of attacks by hackers in various ways to circumvent the website's security. SQL Injection attacks often occur through a login form by entering a username and password that has been modified in such a way that the website can be easily accessed by hackers. Often times we ignore security on the web, even though hackers can access our data by entering SQL Injection syntax at login. To prevent this kind of injection attack, various methods are used, one of which is to use input filtering with the "maxlength" and "input type number" techniques. This technique is embedded in the PHP or HTML source code which is inserted into the login form in the username and password input section. The advantage of this technique is that it can set limits on username input and change the format of input passwords to numbers only. You can also use the php addlashes() technique to return string values by adding an inverted backslash character (\) before certain characters such as single quotes (') so as to prevent hackers from carrying out SQL Injection attacks by force on the website.
Keywords: SQL injection; Security Login; Input Filterization; PHP's addlashes() technique; Maxlength technique, Input Engineering type number.

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

1. PENDAHULUAN

Perkembangan teknologi di bidang IT, khususnya dalam pengembangan website, terus meningkat seiring dengan berjalannya waktu. Namun, keamanan website menjadi hal yang sangat penting karena banyak terjadi kasus pembobolan website, baik itu website perusahaan maupun pemerintahan. Ada berbagai macam jenis serangan terhadap keamanan website, seperti serangan brute force dan SQL injection. Untuk mengamankan website, dapat dilakukan dengan menggunakan filterisasi input dengan menggunakan teknik maxlength dan input type number atau bisa juga mengunakan addslashes() PHP pada form login.

Pada filterisasi input fungsi dari Teknik maxlength dan input type number yakni akan membatasi jumlah karakter inputan username dan mengubah inputan password dari type text atau password menjadi type number, sehingga serangan SQL injection tidak dapat berjalan dan website menjadi aman dari serangan tersebut. Selain itu, teknik addslashes() pada PHP juga dapat membantu meningkatkan keamanan situs web dengan menambahkan karakter backslash terbalik pada karakter-karakter tertentu pada input form.

Penyelesaian untuk menghindari SQL injection dapat dilakukan baik secara client-side maupun server-side. Pada metode client-side, dilakukan pengecekan terhadap deviasi antara shadow query dengan query dinamis yang dibentuk oleh masukan pengguna. Dalam hal ini kita bisa menggunakan teknik maxlength pada form kita sebagai langkah awal guna mengamankan web. Sedangkan pada server-side, diperlukan sebuah metode yang mampu memberikan solusi tepat. Dalam hal ini kita bisa menggunakan teknik addslashes() php karena teknik ini mudah digunakan dan sangat efektif karena bekerja pada belakang web jadi tidak diketahui oleh peretas yang melakukan serangan SQL Injection.

Penyerangan SQL injection adalah salah satu jenis serangan yang sangat rentan terjadi, terutama di Indonesia. Para developer kadang lupa memberikan keamanan tambahan pada form login. Oleh karena itu, perlu dilakukan upaya untuk mengantisipasi serangan tersebut, seperti memberikan filter dari source code untuk query dan menggunakan verifikasi captca. Biasanya para peretas mencari letak form login dan mulai memasukan sintax SQL Injection yang dengan secara paksa login tanpa harus mengetahui username dan password. Pada dasarnya, serangan SQL Injection dilakukan melalui form login admin dengan melakukan injeksi menggunakan software khusus atau dengan cara paksa (penetrasi). Hacker akan mencoba untuk memasukkan username dan password khusus yang mengandung kolaborasi antara angka dan huruf dengan panjang karakter yang ditentukan. Seorang penyerang biasanya akan mencoba membajak field login yang tidak terlindungi untuk memperoleh akses database. Oleh karena itu, sangat penting untuk melindungi website dari serangan SQL Injection dengan menggunakan teknik-teknik yang efektif dalam pengamanan website.

Penelitian ini bertujuan untuk mempelajari teknik addslashes() dan filterisasi inputan dan penerapannya berfungsi untuk mencegah serangan SQL Injection pada situs web. Metode yang digunakan adalah eksperimental dengan membuat aplikasi web sederhana dan menerapkan kedua teknik ini pada form input. Hasil dari penelitian menunjukkan bahwa teknik addslashes() dapat membantu meningkatkan keamanan situs web dari serangan SQL Injection.

Diharapkan penelitian ini dapat memberikan kontribusi dalam pengembangan keamanan situs web dan dapat membantu mengurangi serangan cyber yang sering terjadi. Selain itu, hasil dari penelitian ini juga dapat menjadi referensi bagi pengembang aplikasi web dan pemilik situs web dalam memperkuat keamanan sistem mereka.

2. METODE PENELITIAN

Dalam penelitian ini, penulis mengadopsi metode SDLC Waterfall. Metode Waterfall atau Life Cycle Klasik digunakan secara luas dalam bidang Rekayasa Perangkat Lunak. Pendekatan ini mengikuti proses yang sistematis dan terurut dimulai dari pemahaman kebutuhan sistem, kemudian melalui tahap analisis, desain, implementasi, dan pengujian sistem. Metode ini dinamakan Waterfall karena setiap tahap harus menunggu selesainya tahap sebelumnya dan berlangsung secara berurutan. Berikut adalah langkah-langkah yang diambil dalam penelitian ini:

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

2.1 Analisis Sistem

Pada tahap analisis sistem, dilakukan analisis terhadap batasan lingkup sistem secara umum dari pengujian yang akan dilakukan. Untuk melihat proses filterisasi, pengujian akan melibatkan perangkat lunak (software), perangkat keras (hardware), dan form login (data sampel) yang akan digunakan dalam pengujian. Pengujian dilakukan pada ekstensi PHP dengan menggunakan database MySQL.

2.2 Identifikasi Kebutuhan Hardware dan Software

Dalam tahap ini dijalankan identifikasi perangkat keras serta perangkat lunak yang digunakan dalam proses pengujian terhadap form login.

Tabel 1. Spesifikasi Perangkat lunak yang Digunakan Peneliti

No	Software	Versi
1	Visual Studio Code	1.77.3
2	Google Chrome	112.0.5615.138
3	XAMPP	v3.3.0
4	MySQL	8.0.25

Tabel 2. Spesifikasi Perangkat Keras yang Digunakan Peneliti

No	Hardware	Spesifikasi
1	Memory	8, 00 GB
2	Processor	Intel Core i3-1005G1
3	VGA	Intel® UHD Graphics
4	Storage	

2.3 Pengujian Data (Sample Login)

Pada studi kasus ini peneliti membuat sebuah login page resposive dari situs https://codepen.io/SH20RAJ/pen/wvJzGxg dan kemudian membuat sebuah welcome page ketika berhasil login dari situs https://codepen.io/goodkatz/pen/LYPGxQz.

Tabel 1. Informasi sintaks SQL Injection yang biasa digunakan oleh peretas untuk membobol situs web

No	Sintax SQL Injection pada username	Sintax SQL Injection pada password
1	' or 1=1 limit 1 -- -+	' or 1=1 limit 1 -- -+
2	'='OR'	'='OR'
3	' or '1'='1	' or '1'='1
4	' or 'x'='x	' or 'x'='x
5	' or 0=0 --	' or 0=0 --
6	" or 0=0 --	" or 0=0 --
7	or 0=0 --	or 0=0 --
8	' or 0=0 #	' or 0=0 #
9	" or 0=0 #	" or 0=0 #
10	or 0=0 #	or 0=0 #
11	' or 'x'='x	' or 'x'='x
12	" or "x"="x	" or "x"="x
13	') or ('x'='x	') or ('x'='x

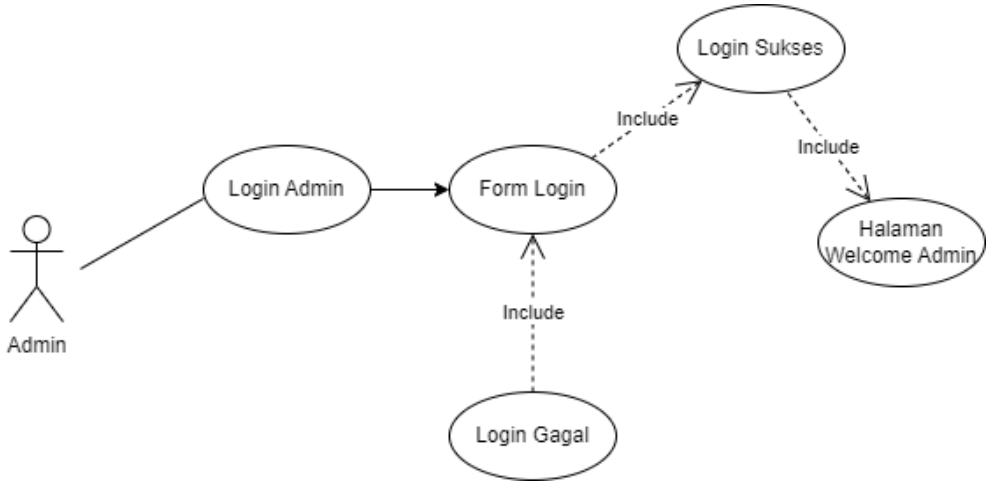
Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

14	` or 1=1--	` or 1=1--

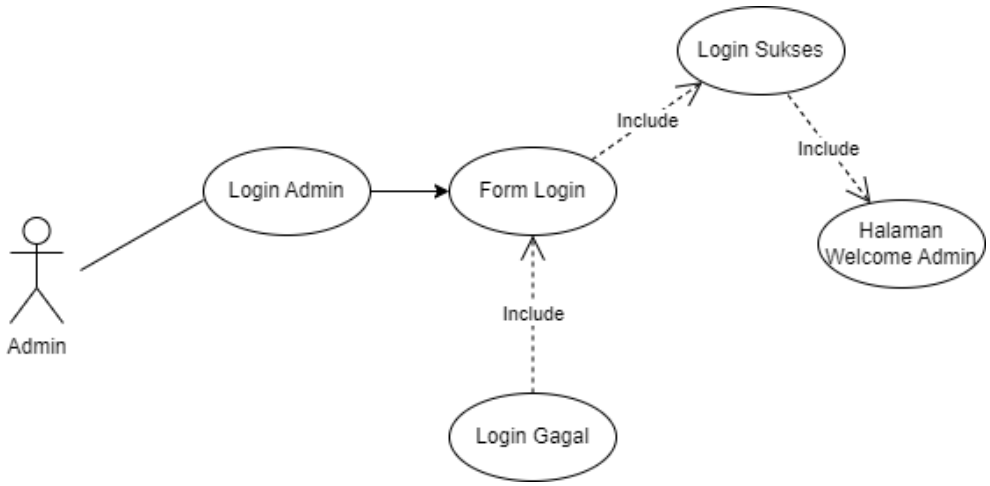
2.4 Analisis dan Desain Sistem

Rosa dan Shalahuddin (2015:137), UML adalah sebuah standarisasi bahasa pemodelan untuk pembangunan perangkat lunak yang dibangun dengan menggunakan teknik pemrograman berorientasi objek. UML dari login page yang dilakukan oleh peneliti dapat dilihat pada gambar berikut ini.



Gambar 1. Use Case Login Admin

Pada Gambar 2.1 di atas terdapat skenario admin dimana aktivitas login admin dilakukan dengan memasukkan username dan password. Jika autentikasi benar, administrator akan dapat masuk dan pergi ke halaman Welcome Admin, jika tidak, ia tidak akan dapat masuk.



Activity diagram menunjukkan proses di mana seorang admin melakukan login ke halaman operator dengan memasukkan informasi akun admin yang sah dan resmi. Jika informasi akun yang dimasukkan adalah benar, sistem akan melakukan validasi dan memungkinkan admin untuk mengakses halaman admin. Namun, jika informasi akun yang dimasukkan tidak valid, maka admin tidak akan bisa login kecuali melalui proses ilegal seperti aktivitas hacking.

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

3. HASIL DAN PEMBAHASAN

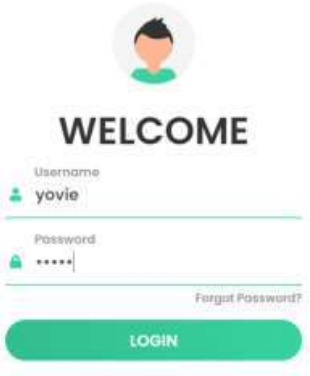
3.1. Penerapan SQL Injection pada Form Login Admin

Pada bagian ini akan dijelaskan proses pembobolan website dari login admin yang telah peneliti buat dengan melalui dua tahap, yaitu login page website dengan login biasa tanpa pengunaanya teknik filter inputan dan addslashes() dan strategi agar tidak terkena SQL Injection dengan menggunakan kedua teknik tersebut.

Untuk detail penjelasan dapat dilihat pada pembahasan berikuti ini :

- System login yang tidak menggunakan teknik maxlength, input type number,dan addslashes(). Disini peneliti akan menampilkan source code dari login.php yang telah dibuat dan menampilkan form login beserta pembahasanya sebagai berikut :

Gambar Form Login	Source Code

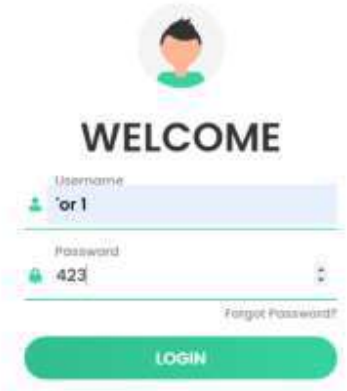
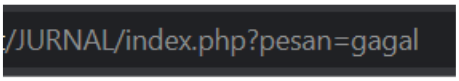

Hasil dapat login ke admin
 
	`<div class="div">`
	`<h5>Username</h5>`
	`<input`
	`type="text" class="input"`
	`name="username" />`
	`</div>`
	`</div>`
	`<div class="input-div pass">`
	`<div class="i">`
	`<i class="fas fa-lock"></i>`
	`</div>`
	`<div class="div">`
	`<h5>Password</h5>`
	`<input type="password"`
	`class="input"`
	`name="password" />`
	`</div>`
	`</div>`

Dari tabel di atas, terlihat bahwa pada bagian kode sumber yang ditandai dengan warna merah, tidak terdapat penggunaan atribut "maxlength" untuk membatasi panjang masukan pada bidang input "username". Hal ini dapat menyebabkan penyerang (hacker) dapat dengan mudah memasukkan sintax SQL Injection ke dalam bidang input "username" tersebut. Selanjutnya, pada bagian kode sumber yang ditandai dengan warna hijau, terlihat bahwa bidang input "password" menggunakan tipe "password" bukan "number". Hal ini berarti bahwa meskipun bidang input "password" tersebut diatur sebagai tipe "password", itu tidak akan efektif dalam mencegah serangan SQL Injection karena penyerang masih dapat memasukkan sintax Injection secara paksa, terlepas dari batasan panjang masukan.

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

❖ System Login mengunakan teknik filterisasi inputan dengan cara maxlength dan input type menjadi number.

Gambar Form Login	Source Code
Pada form dibawah ini peneliti ingin memasukan sql injection ' or 1=1 limit 1 -- -+ hasilnya seperti ini  dan ketika di Login 	 Username <input type="text" class="input" name="username" maxlength="5" /> <iclass="fas falock"></ i> Password <input type="number" class="input" name="password" />

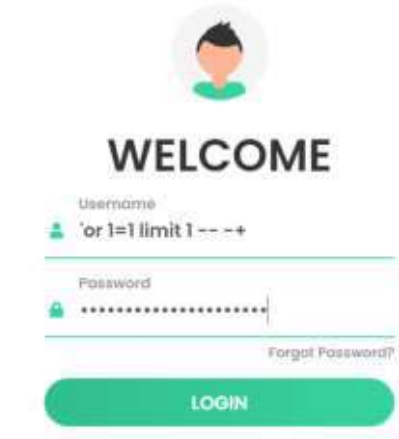
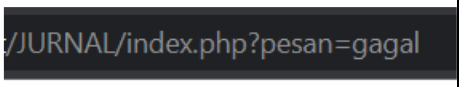
Tabel di atas menampilkan sebuah form login dan beberapa potongan source code login.php yang menggunakan teknik maxlength dan input type diubah ke number pada HTML. Dapat dilihat perbedaannya ketika seorang hacker mencoba melakukan serangan SQL injection pada inputan username menggunakan sintax (' or 1=1 limit 1 -- -+) dengan memasukkan teks sepanjang 21 karakter, namun serangan tersebut tidak berhasil karena inputan tersebut dibatasi oleh teknik yang telah dibuat oleh peneliti yakni maxlength menjadi 5 karakter saja. Sehingga, pada formulir login, inputan login yang masuk pada username hanya dapat tertulis beberapa teks (‘or) saja.

Selanjutnya, inputan pasword yang tipe inputnya password telah diubah oleh peneliti menjadi angka atau number. Hal ini menyebabkan sintax SQL injection yang seharusnya tertulis di inputan (' or 1=1 limit 1 -- -+) berubah menjadi (111--) karena mengikuti format angka. Selain itu, panjang karakter inputan juga dibatasi menjadi 5 karakter saja. Dengan demikian, proses penetrasi website dengan teknik paksa SQL injection menjadi tidak berfungsi karena karakter inputan yang terbatas sehingga semakin sulit bagi hacker untuk melakukan serangan SQL injection pada kolom password. Dengan kombinasi teknik maxlength dan input type number, maka sistem keamanan pada formulir login dapat menjadi lebih optimal dan dapat menghindari serangan SQL injection.

❖ System Login menggunakan teknik addslashes() PHP

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

Gambar Form Login	Source Code
 ketika di login hasilnya akan 	$username=addslashes(trim($_POST['username'])); $password =addslashes($_POST['password']);

Dari tabel diatas kita bisa melihat bahwa hacker menggunakan SQL Injection pada form input login, Akan tetapi peneliti telah menggunakan teknik addslashes() PHP, Dimana ketika kita menggunakan teknik ini maka Efek yang ditimbulkan adalah menambahkan simbol backslash (\). Fungsinya untuk mencegah hacker memasukan script yang mengandung kutip pada website kita. Seperti Contoh Gambar dibawah ini.

```php
<?php
$text = addslashes("Kursus di 'DUMET School' Grogol ");
echo($text);
?>
```

Maka akan jadi seperti ini inputanya

Kursus di \'DUMET School\' Grogol

4. KESIMPULAN

Teknologi informasi dan situs web memegang peranan penting dalam kehidupan sehari-hari, tetapi juga rentan terhadap serangan cyber seperti SQL Injection. Untuk mencegah serangan SQL Injection, teknik "maxlength" dan "input type number" dapat digunakan untuk membatasi inputan pada form login. Selain itu, teknik addslashes() pada PHP juga dapat membantu meningkatkan keamanan situs web

Yovie Ferdianto Korespondensi: *Penulis Korespondensi

JURNAL INFORMATIKA DAN REKAYASA PERANGKAT LUNAK (JATIKA)
Volume 4, Nomor 3, September 2023, Page 349-356
E-ISSN 2797-2011 P-ISSN 2797-3492
http://jim.teknokrat.ac.id/index.php/informatika/index
DOI: https://doi.org/10.33365/jatika.v4i3.3306

dengan menambahkan karakter backslash terbalik pada karakter-karakter tertentu pada input form. Penelitian eksperimental menunjukkan bahwa teknik addslashes() dan filterisasi inputan dapat efektif dalam mencegah serangan SQL Injection pada situs web. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan keamanan situs web dan dapat menjadi referensi bagi pengembang aplikasi web dan pemilik situs web untuk memperkuat keamanan sistem mereka. Kesimpulannya, penggunaan teknik-teknik seperti "maxlength", "input type number", dan addslashes() PHP sangat penting dalam mengamankan situs web dari serangan cyber seperti SQL Injection.

5. REFERENCES

[1] Zulkifli, Samsir, and Azrai Sirait, "Implementasi Max Length dan Input Type Number Pada Form Login Website Untuk Mencegah Penetrasi SQL Injeksi Secara Paksa," *U-NET J. Tek. Inform.*, vol. 4, no. 1, pp. 14–18, 2021, doi: 10.52332/u-net.v4i1.223.

[2] T. W. Harjanti and M. Fachri, "Perancangan Aplikasi Injeksi SQL dan Implementasi Terhadap Serangan Vulnerability Pada Website," *JI-Tech*, vol. 10, no. 2, pp. 1–5, 2014, [Online]. Available: https://jitech.i-tech.ac.id/index.php/jitech/article/view/10/8%0Ahttps://jitech.i-tech.ac.id/index.php/jitech/article/view/10

[3] S. P. Sitorus and R. A. Habibi, "Teknik Pencegahan Penetrasi SQL Injeksi Dengan Pengaturan Input Type Number dan Batasan Input Pada Form Login Website," *U-NET J. Tek. Inform.*, vol. 4, no. 2, pp. 26–33, 2020, doi: 10.52332/u-net.v4i2.303.

[4] M. S. Fathurrahman1, Yupi Kuspandi Putra2, "Jurnal Informatika dan Teknologi," *Teknol. infotek J. Inform. dan Teknol.*, vol. 3, no. 9, pp. 1689–1699, 2020.

[5] S. Lika, R. D. P. Halim, and I. Verdian, "Analisa Serangan Sql Injeksi Menggunakan Sqlmap," *POSITIF J. Sist. dan Teknol. Inf.*, vol. 4, no. 2, p. 88, 2018.

[6] V. Kumar Bohat, "Detection of SQL Injection Attack and Various Prevention Strategies," *Int. J. Eng. Adv. Technol.*, no. 2, pp. 2249–8958, 2013.

[7] M. M. Hassan *et al.*, "Broken Authentication and Session Management Vulnerability: A Case Study of Web Application," *Int. J. Simul. Syst. Sci. Technol.*, pp. 1–11, 2018, doi: 10.5013/ijssst.a.19.02.06.

[8] A. Iskandar *et al.*, "Web based testing application security system using semantic comparison method," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, 2018, doi: 10.1088/1757-899X/420/1/012122.

[9] E. Gunadhi and A. P. Nugraha, "Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection," *J. Algoritm.*, vol. 13, no. 2, pp. 391–398, 2017, doi: 10.33364/algoritma/v.13-2.391.

[10] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website," *Respati*, vol. 8, no. 22, pp. 111–124, 2017, doi: 10.35842/jtir.v8i22.53.

[11] A. Solichin, "Pemrograman Web dengan PHP dan MySQL - Achmad Solichin - Google Buku," *Univ. Budi Luhur*, p. 120, 2016, [Online]. Available: https://books.google.co.id/books?id=kcD4BQAAQBAJ&printsec=frontcover&dq=aplikasi+berbasis+web+dengan&hl=id&sa=X&ved=0ahUKEwib-fT80ITYAhVBrI8KHT9GD6QQ6AEIJzAA#v=onepage&q=aplikasi berbasis web dengan&f=false

[12] A. Krisharnomo, A. Sofwan, and R. R. Isnanto, "Sistem Informasi Kompetesi Sepakbola Liga Indonesia Berbasis Web Menggunakan PHP dan MYSQL," *Jur. Tek. Elektro Fak. Tek. UNDIP*, pp. 1–7, 2013.

[13] A. D. Praba, M. Safitri, and F. Faridi, "Implementasi Datatables Server-Side Untuk Mempercepat Load Halaman Pada Aplikasi E-Commerce," *JIKA (Jurnal Inform.*, vol. 5, no. 2, p. 139, 2021, doi: 10.31000/jika.v5i2.4339.

[14] T. F. Efendi and M. Krisanty, "Warehouse Data System Analysis PT. Kanaan Global Indonesia," *Int. J. Comput. Inf. Syst.*, vol. 1, no. 3, pp. 70–73, 2020, doi: 10.29040/ijcis.v1i2.26.

[15] M. A. Saputra, H. H. Kusuma, and A. Ibrahim, "Mengatasi Keamanan di dalam SQL Injection dan Cara Pencegahannya," *Pros. Annu. Res. Semin. 2017 Comput. Sci. ICT ISBN*, vol. 3, no. 1, pp. 105–108, 2017.

Yovie Ferdianto Korespondensi: *Penulis Korespondensi