Implementasi Metode Honeypot Dalam Pengamanan Form Input Terhadap Serangan Sql-Injection
Implementation of the Honeypot Method in Form Input Security Against Sql-Injection Attacks

Adam Putra Erriyanto[1], Ade Eviyanti[2].
{raregar77@gmail.com[1], adeeviyanti@umsida.ac.id[2]}

Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Sidoarjo

Abstract*. At this time the internet is something that can not be separated in the life of modern society. For this reason, fast, safe and reliable internet is very important. To achieve this on the internet there are various kinds of technology that make it very influential in our lives. In the scope of security for safe and smooth internet web surfing, we need security, especially in the excess part of the website. One way to do this is to commit website crimes, namely Sql Injection. Sql injection is a hacking action that is carried out in the client application by modifying the SQL commands that are in the client application memory. SQL Injection is a technique for exploiting web applications, commands can be entered as desired by the user even though the user is not authorized to do so. The damage done by the user that can lead to fatal consequences can be done by using SQL injection. One of the methods used to prevent website security attacks is Honeypot. Honeypot is a system or computer that is deliberately used as bait to become a target for attacks from attackers.*
Keywords *- website security, honeypot, sql-injection.*

Abstrak*. Pada masa ini internet merupakan hal yang tak dapat dipisahan dalam kehidupan masyarakat modern. Untuk itu internet yang cepat, aman dan dapat diandalkan menjadi sangat penting. Untuk mencapai hal tersebut dalam internet terdapat berbagai macam teknologi yang menjadikannya sangan berpengaruh besar dalam kehidupan kita. dalam lingkup keamanan berselancar web internet yang aman dan lancar, kita membutuhkan keamanan khususnya di bagian website yang belebih. salah satu cara dilakukan untuk melakukan kejahtan website yaitu Sql Injection. Sql injection adalah sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah SQL yang ada di memori aplikasi client. SQL Injection merupakan teknik mengeksploitasi web aplikasi, perintah-perintah dapat dimasukkan sesuai yang diinginkan oleh pengguna walaupun pengguna tersebut bukan yang berwenang akan hal itu.Perusakkan yang dilakukan oleh pengguna tersebut yang bisa menimbulkan akibat fatal dapat dilakukan dengan menggunakan SQL injection. salah satu metode yang digunakan untuk menangkalnya serangan keamanan website yaitu Honeypot. Honeypot merupakan sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (attacker).Jadi Honeypot seolah-olah menjadi website yang berhasil disusupi oleh attacker, padahal penyerang tidak masuk ke website sebenarnya, tetapi masuk ke website yang palsu..*
Kata Kunci *– keamanan website, honeypot, sql-injection*

I. PENDAHULUAN

Website adalah kumpulan halaman dalam suatu domain yang memuat tentang berbagai informasi agar dapat dibaca dan dilihat oleh pengguna internet melalui sebuah mesin pencari. Informasi yang dapat dimuat dalam sebuah website umumnya berisi mengenai konten gambar, ilustrasi, video, dan teks untuk berbagai macam kepentingan. Menjelaskan dengan perkembangan teknologi internet saat ini memungkinkan pertukaran informasi seperti ilmu pengetahuan, hiburan, berita dan jenis informasi lain secara real-time. Faktor kemudahan dan kenyamanan ini menyebabkan internet menjadi media informasi yang paling banyak digunakan saat ini [1].

Semakin meningkat pertumbuhan layanan informasi maka semakin tinggi pula tingkat kerentanan keamanan dari suatu sumber informasi. Salah satu cara untuk mengakses internet adalah menggunakan aplikasi web. Tampilan web yang interaktif menyebabkan pengguna dapat memakai web dengan mudah. Namun dibalik kemudahan penggunaan web, ada faktor lain yang kurang diperhatikan yaitu keamanan yang merupakan aspek penting dalam aplikasi web. Ancaman yang menempati urutan teratas yang dapat dilakukan pada aplikasi web adalah injection. Salah satu injection yang paling umum dilakukan adalah pada databaseSQL [2]. SQL injection merupakan salah satu tindakan yang mencurigakan yang memanfaatkan celah keamanan pada database SQL dengan menyisipkan query ilegal yang bertujuan untuk bypass login, memanipulasidata dan merusak database [3]. Meningkatnya kerentanan keamanan dari suatu sumber informasi. Melalui tulisan ini disajikan penelitian yang dilakukan secara eksperimen yang membahas tentang kejahatan penyerangan database secara SQL Injection. Penyerangan dilakukan melalui halaman autentikasi dikarenakan halaman ini merupakan pintu pertama akses yang seharusnya memiliki pertahanan yang cukup [4].

A. Sql-injection

SQL injection adalah sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah SQL yang ada di memori aplikasi client. SQL Injection merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan database untuk penyimpanan data. Pada sistem database dengan menggunakan SQL, perintah-perintah dapat dimasukkan sesuai yang diinginkan oleh pengguna walaupun pengguna tersebut bukan yang berwenang akan hal itu.Perusakkan yang dilakukan oleh pengguna tersebut yang bisa menimbulkan akibat fatal dapat dilakukan dengan menggunakan SQL injection [5].

B. Flowchart

Flowchart merupakan bentuk diagram yang memperlihatkan arus kerja suatu sistem secara grafik dari langkah yang bertahap dalam gambaran simbol yang sudah ditetapkan. Apabila dibahasakan ke Bahasa Indonesia, yaitu menjadi diagram alir yang di artikan mengarahkan atau mewakili sketsa penuntasan sebuah masalah. Pada proses pembuatan flowchart, akan disimpan pada antrian dari setiap hasil token kemudian setelah semua selesai dalam pembuatannya barulah dilakukan pembuatan gambar semuannya. Sehingga gambar-gambar yang akan dibuat dilakukan penampungan terlebih dahulu [6].

C. Website

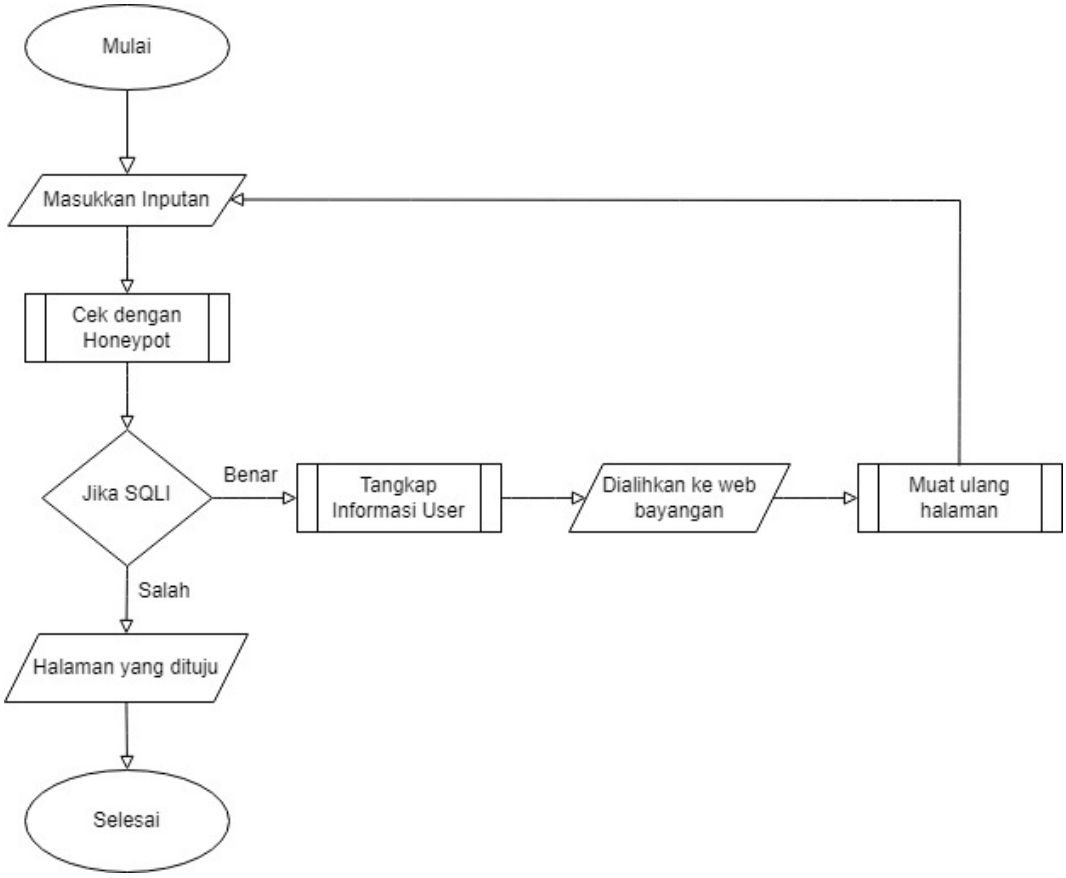
Website adalah kumpulan informasi/kumpulan page yang biasa diakses lewat jlur internet. Setiap orang di berbagai tempat dan segala waktu bisa menggunakannya selama terhubung secara online di jaringan internet. Secara teknis, website adalah kumpulan dari page, yang tergabung kedalam suatu domain atau subdomain tertentu. halaman informasi yang disediakan melalui jalur internet sehingga bisa diakses di seluruh dunia selama terkoneksi dengan jaringan internet juga disebut dengan Website [7].

D. Honeypot

Honeypot merupakan sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (attacker). Komputer tersebut melayani serangan yang dilakukan oleh attacker dalam melakukan penetrasi terhadap server tersebut. Honeypot akan memberikan data palsu apabila ada hal aneh yang yang akan masuk ke dalam sistem atau server [8]. Secara teori Honeypot tidak akan mencatat trafik yang legal. Sehingga dapat dilihat bahwa yang berinteraksi dengan Honeypot adalah user yang menggunakan sumber daya sistem yang digunakan secara ilegal. Jadi Honeypot seolah-olah menjadi sistem yang berhasil disusupi oleh attacker, padahal penyerang tidak masuk ke sistem sebenarnya, tetapi masuk ke sistem yang palsu [9].

E. Flowchart

Flowchart merupakan gambaran jalannya sebuah program dari satu proses ke proses lainnya. Sehingga, alur dari system menjadi simple dan mudah dipahami oleh semua orang. Selain itu, fungsi lain flowchart adalah menyederhanakan rangkaian prosedur pemahaman terhadap informasi tersebut [10]. Flowchart metode honeypot dapat dilihat pada Gambar 1. dibawah ini.

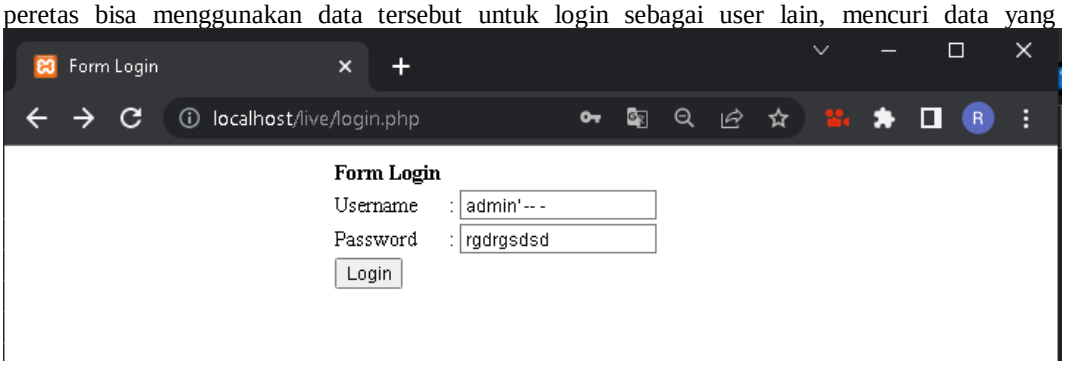


Gambar 1. Flowchart Sistem

III. HASIL DAN PEMBAHASAN

A. Tahap Percobaan

Langkah selanjutnya adalah melakukan pengujian terhadap karakter khusus. Dimulai dari karakter *sql injection* yang berupa tanda kutip satu, maupun dengan menggunakan payload admin'-- - yang akan diuji apakah dengan menginputkan payload tersebut peretas dapat menerobos masuk (*bypass login*). Jika peretas dapat masuk secara paksa ke admin maka peretas dapat mencuri data dari user lain dan jika jatuh ke tangan yang tidak bertanggung jawab, maka peretas bisa menggunakan data tersebut untuk login sebagai user lain, mencuri data yang bersifat sensitif.



Gambar 2. Proses eksploitasi dengan menggunakan perintah SQL-Injection

Seperti yang bisa dilihat pada gambar 2 perintah *sql injection* yang telah diinjek dengan menggunakan sqlmap dan nantinya akan dijalankan pada website yang belum terfilter oleh fungsi Honeypot *preg_match()* . Akan tetapi pada studi kasus *sql injection* ini banyak orang tidak sadar bahwasanya peretas seakan – akan hanya dapat melakukan penerobosan masuk (*bypass login*). Hal inilah yang membuat serangan *sql injection* dihiraukan oleh sebagian pihak.

B. Tahap Penggunaan Honeypot

Untuk menghindari user menginput script sql-injection kembali pada website, maka inputan – inputan yang sering terdapat celah kerentanan sql injection akan diberi funsi Honeypot preg_match(), begitu juga dengan request $_POST pada kolom inputan username dan password. Maka kegiatan injection akan otomatis terbatasi dan otomatis teralihkan ke halaman palsu.

Script ceklogin.php

```
<?php include "inc/koneksi.php"; ?>
<?php
$username= $_POST['username'];
$password= $_POST['password'];


$query = "SELECT * FROM user WHERE username='$username' and
password='$password'";
$result = $sql->query($query);
   if($result->num_rows > 0) {
  $_SESSION["login"] = true;
// echo "anda berhasil login.";
header("location: index.php");
}
else {
echo '<script>alert("username/password yang anda masukkan salah.
Silahkan ulang kembali"); </script>';
}
?>
```

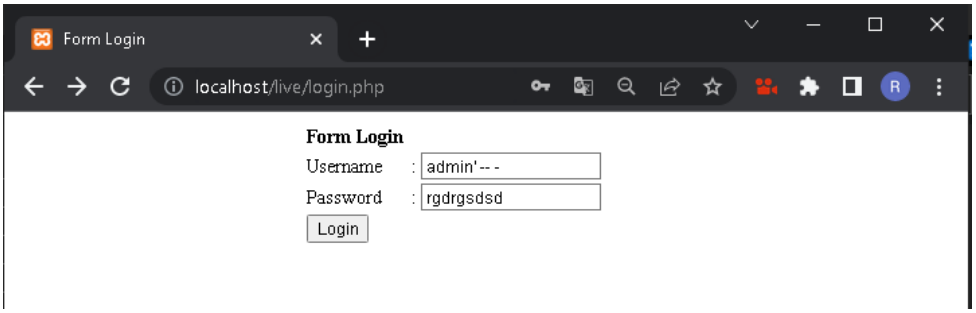
Pada file script ceklogin.php menjelaskan tentang form login yang menggunakan method $_POST untuk diterima dan diproses ke database untuk mencocokkan data yang diinputkan. Pada form username_user dan password_user, sangat rawan terjadinya serangan sql injection, maka dari itu peneliti akan mengamankan variabel

$username_user dan $password_user yang akan menerima inputan user dan meneruskan request dari user menuju $_POST dari serangan sql injection dengan cara membatasi inputan dengan fungsi Honeypot preg_match().

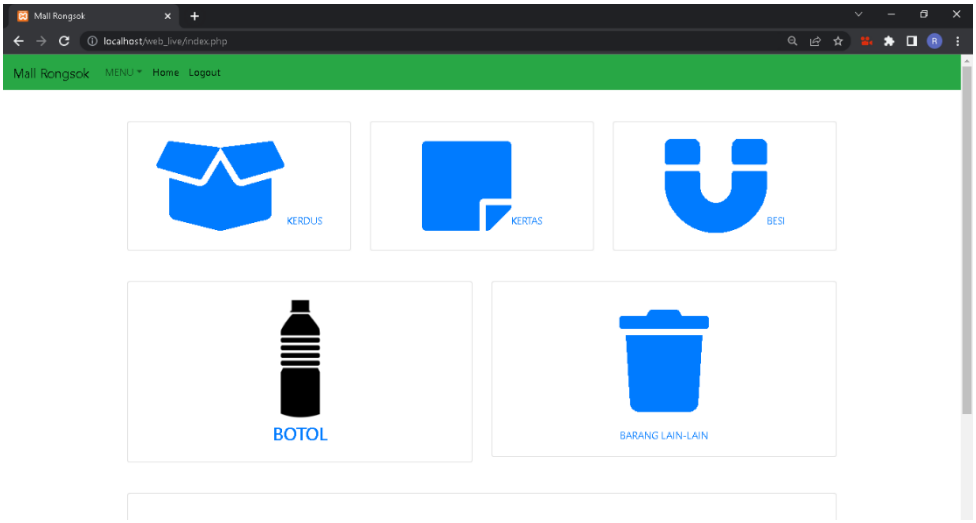
Script ceklogin.php

Pada file script ceklogin.php menjelaskan tentang bagaimana proses request data dari $username_user dan $password_user yang menggunakan method $_POST diterima dan diproses ke database untuk mencocokkan data yang diinputkan di kolom login. Untuk menghindari serangan sql injection diinjekkan di kolom login, maka peneliti akan mengamankan variable $username_user dan $password_user yang membawa sekaligus mengalihkan request dari login.php menuju halamanpalsu.php dengan cara membatasi inputan dengan fungsi Honeypot preg_match().

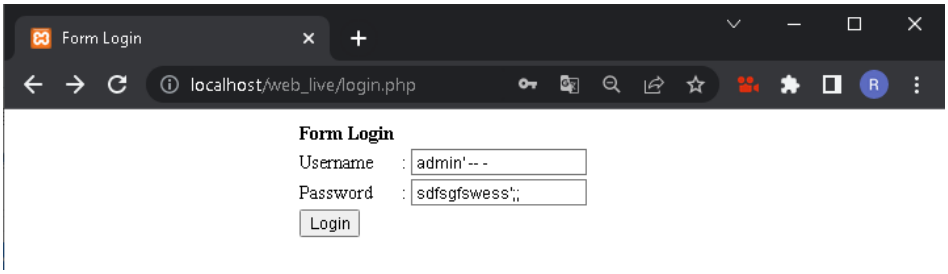
```
<?php include "inc/koneksi.php"; ?>
<?php
$username= $_POST['username'];
$password= $_POST['password'];

$query = "SELECT * FROM user WHERE username='$username' and
password='$password'";
$result = $sql->query($query);
   if(!preg_match("/^[a-zA-Z0-9]*$/", $username)){
         header("location: halamanpalsu.php");
            //echo "Input hanya huruf dan angka yang diijinkan, dan tidak boleh
menggunakan spasi ...!<br>";
          }
else if($result->num_rows > 0) {
         $_SESSION["login"] = true;
// echo "anda berhasil login.";
header("location: index.php");
}
else {
echo '<script>alert("username/password yang anda masukkan salah. Silahkan
ulang kembali"); </script>';
}
?>
```



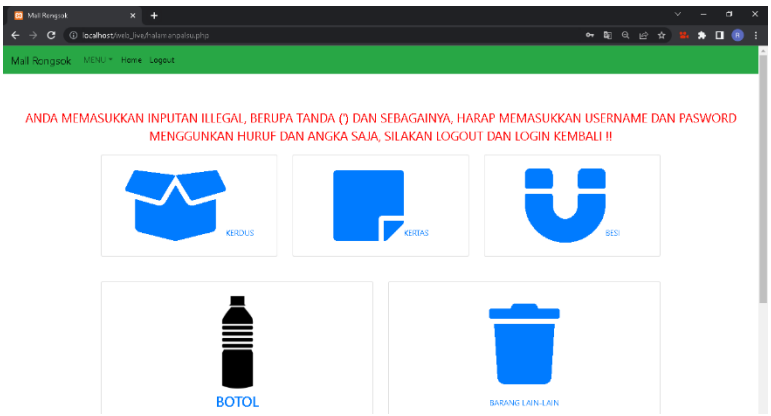
Gambar 3. Tampilan form login sebelum ada Honeypot



Gambar 4. Halaman login sebelum ada Honeypot dan menerima serangan sql injection.



Gambar 5. form login setelah ada Honeypot



Gambar 6. Halaman login setelah menggunakan Honeypot dan menerima serangan sql injection

Pada gambar 3 dan 4 menjelaskan bahwa ketika perintah sql injection dimasukkan lewat form input username dan password, dengan tidak adanya fungsi honeypot preg_match() maka website tidak akan melakukan validasi pada inputan sehingga website akan menjalankan perintah sql injection yang diinputkan oleh user.

Begitu juga halnya pada gambar 5 dan 6, ketika user mencoba memasukkan perintah sql injection lewat form input username dan password maka fungsi honeypot preg_match() akan dialihkan ke halaman palsu. Sehingga karakter unik atau karakter khusus yang diinputkan pada form username tidak diperbolehkan .

IV. KESIMPULAN

Akhir dari pengujian dan analisa yang telah dilaksanakan pada bab sebelumnya dapat disimpulkan sebagai berikut:

Dengan melakukan pengujian metode Honeypot pada suatu website, kita bisa mengetahui dan menentukan kelemahan dan serangan yang dapat terjadi terhadap celah kerentanan suatu sistem sejak dini dan dapat langsung memperbaikinya sebelum terjadi serangan terhadap sistem. Salah satu cara pencegahan serangan sql injection adalah dengan memfilter kata dan karakter yang masuk karena selalu ada celah kerentanan selama ada inputan user.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih yang sebesar besarnya kepada pihak-pihak yang berkontribusi dalan penelitian ini. Terimakasih kami sampaikan kepada :

1. Laboratorium Informatika Fakultas Sains dan Teknologi Universitas Muhammadiyah Sidoarjo.
2. Rekan mahasiswa Universitas Muhammadiyah Sidoarjo

REFERENSI

[1] A. S. Irawan, E. S. Pramukantoro, and A. Kusyanti, "Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2295–2301, 2018.

[2] I. Riadi, R. Umar, and W. Sukarno, *ANALISIS FORENSIK SERANGAN SQL INJECTION MENGGUNAKAN METODE STATIS FORENSIK*. 2019.

[3] W. D. Fatma, "Analisa Keamanan Server Pada Login Page Webserver Dengan Enkripsi Sha 1 Dari Serangan Sql Injection Menggunakansystemoperasi Kali Linux Di Lkp Multi Logika Binjai," 2018.

[4] Yulianingsih, J. Nangka, T. Barat, and J. J. Selatan, "Menangkal Serangan SQL Injection dengan Parameterized Query," 2018.

[5] T. R. Yudantoro, "Sql Injection Pada Sistem Keamanan Database," 2018.

[6] P. Soepomo, "Penerapan Sistem Keamanan Honeypot dan Ids pada Jaringan Nirkabel (Hotspot)," *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 1, no. 1, pp. 111–118, 2019, doi: 10.12928/jstie.v1i1.2512.

[7] M. H. Romadhon and Y. Yudhistira, "Sistem Informasi Rental Mobil Berbsasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri," vol. 2, no. 1, pp. 30–36, 2021.

[8] R. F. Ramadhan and R. Mukhaiyar, "Penggunaan Database Mysql dengan Interface PhpMyAdmin sebagai Pengontrolan Smarthome Berbasis Raspberry Pi," *JTEIN J. Tek. Elektro Indones.*, vol. 1, no. 2, pp. 129–134, 2020, doi: 10.24036/jtein.v1i2.55.

[9] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[10] B. Wiguna *et al.*, "Wiguna, Implementasi Web Application Firewall dalam Mencegah Serangan SQL Injection pada Website Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website," 2019, doi: 10.31849/digitalzone.v11i2.4867ICCS.