UNIVERSITAS MUHAMMADIYAH SIDOARJO

IMPLEMENTASI METODE HONEYPOT DALAM PENGAMANAN FORM INPUT TERHADAP SERANGAN SQL-INJECTION

Oleh:

Adam Putra Erriyanto

Ade Eviyanti

Progam Studi Teknik Informatika

Universitas Muhammadiyah Sidoarjo

Februari, 2023

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

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. 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

Pertanyaan Penelitian (Rumusan Masalah)

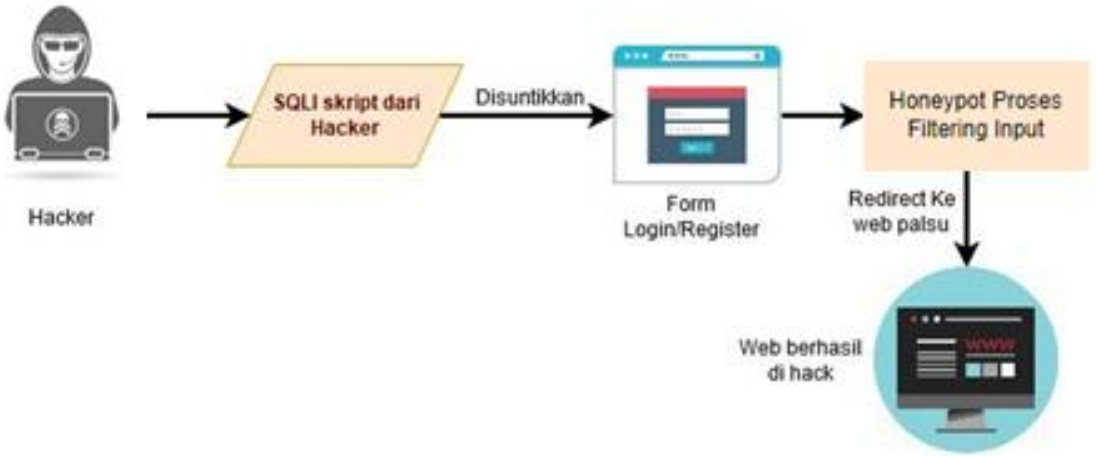
Berdasarkan latar belakang yang ditulis sebagai berikut :

1. Pada penelitian ini memiliki perhatian permasalahan utama ialah “Bagaimana cara implementasi form input terhadap serangan SQL Injecton?”

Metode

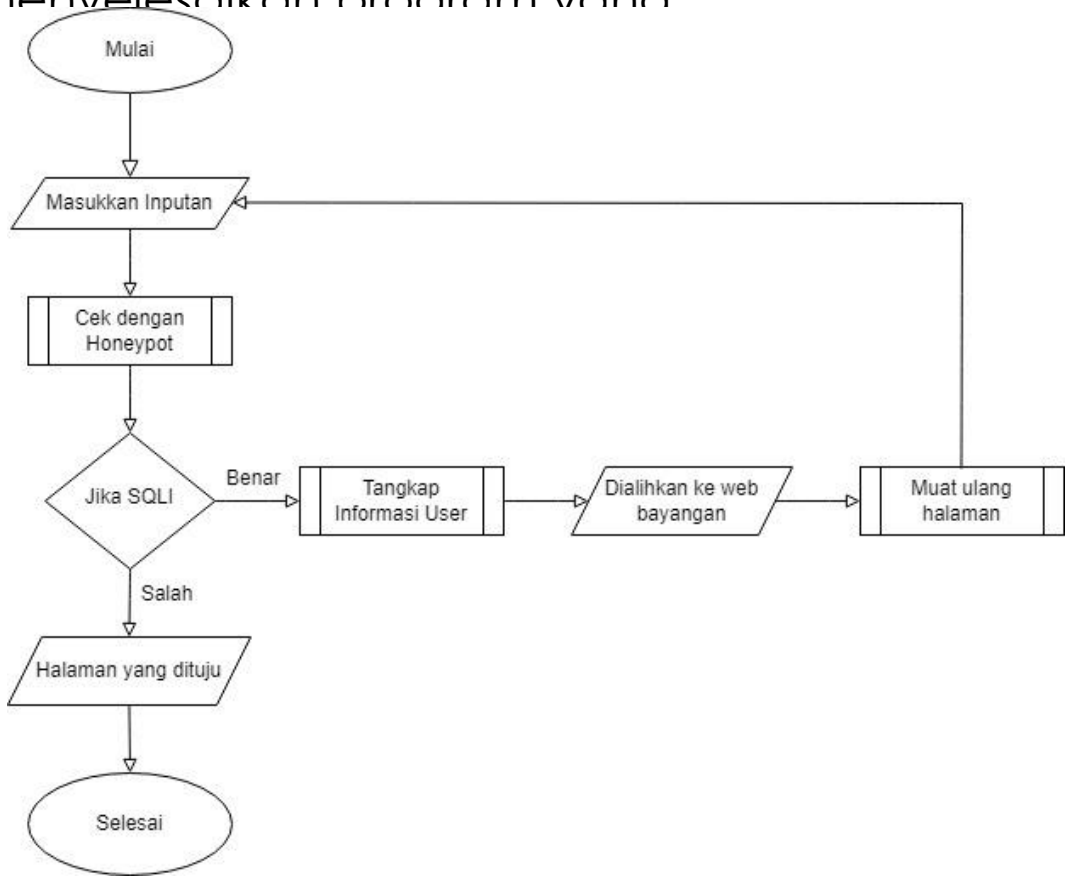
- Honeypot

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. 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.



- Flowchart System

Sebelum peneliti memulai pembuatan program, terlebih dahulu Peneliti menggambarkan sebuah flowchart untuk membantu peneliti menjelaskan proses yang dilakukan oleh program saat dijalankan. Sehingga membantu peneliti dalam menyelesaikan program yang akan diharapkan.



Hasil

Terkait Pada pengujian metode Honeypot adalah melakukan testing (uji coba) pada website yang akan dijadikan target. Langkah selanjutnya adalah melakukan pengamanan pada file login.php dan ceklogin.php terlebih dahulu dengan cara memberikan filtering berupa preg_match() pada file yang terdapat form input username dan password.

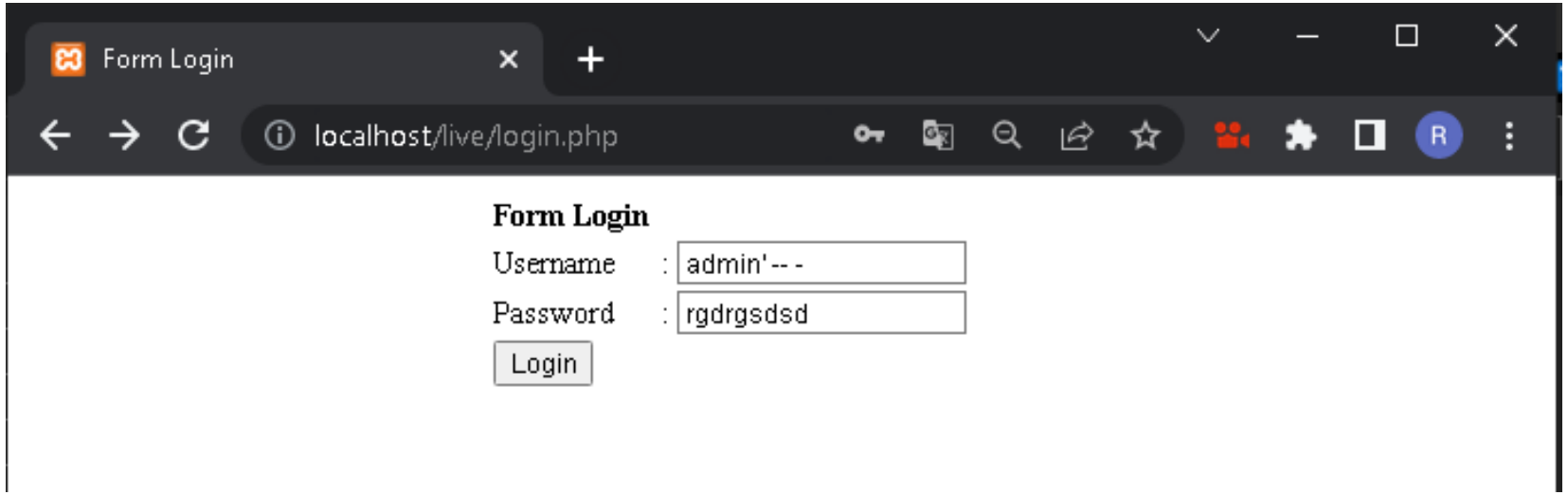
Hal ini digunakan untuk memfilter setiap inputan yang dimasukkan oleh user. Kemudian fungsi preg_match() diberikan pada inputan tersebut adalah untuk membatasi inputan agar terhindar dari serangan sql injection yang berasal dari form input username dan password yang menggunakan method $_POSE seperti pada ceklogin.php.

Pada saat website sudah diamankan maka website pada lapis pertama atau form login akan teramankan, jika tahapan awal atau pintu masuk website gambang ditembus semakin rentan website tersebut akan diambil datanya oleh paraperetas.

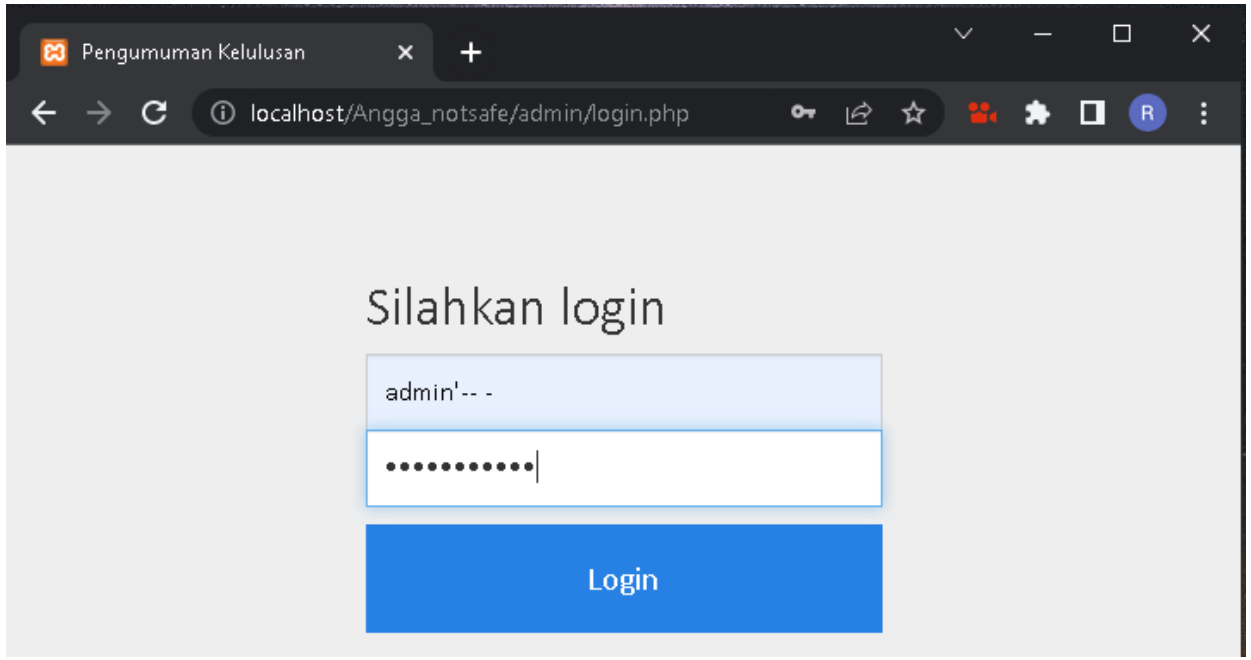
Pembahasan

1. Tahap Eksploitasi

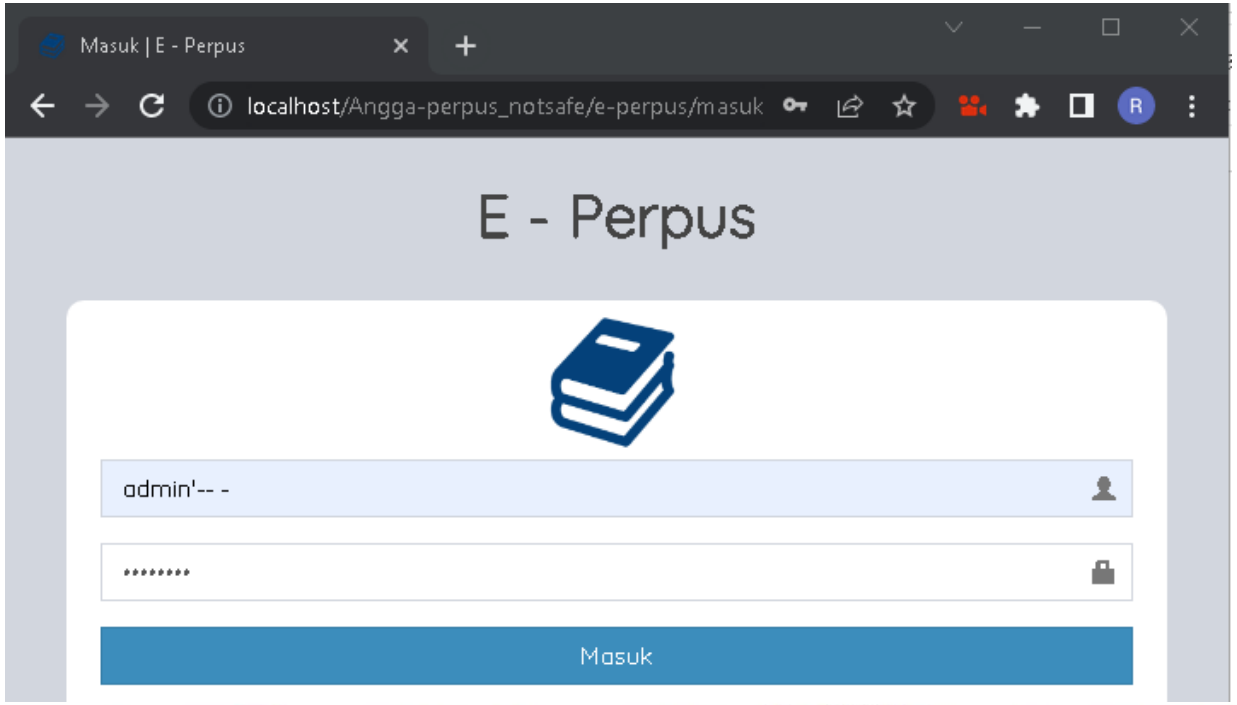
- Langkah selanjutnya adalah melakukan pengujian terhadapkarakter khusus. Dimulai dari karakter *sql injection* yang berupa tandakutip satu, maupun dengan menggunakan payload admin'-- - yang akandiuji apakah dengan menginputkan payload tersebut peretas dapatmenerobos masuk (*bypass login*). Jika peretas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



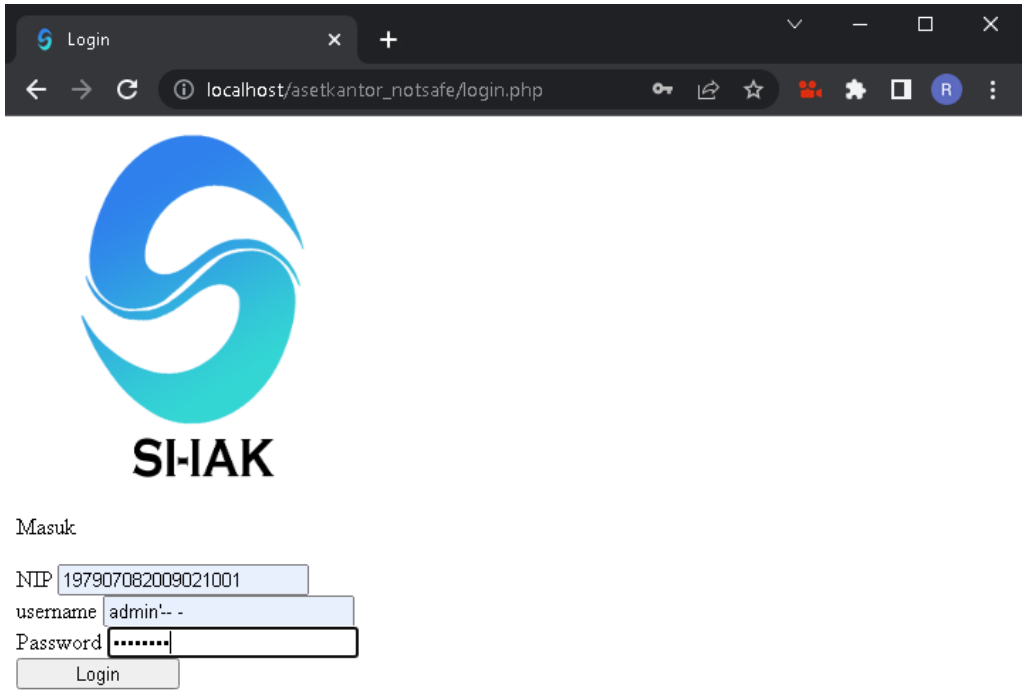
- Interface pada gambar 4.2 berisi form tampilan pertama atau form login website SMKN-1 Nganjuk yang diinject atau diserang dengan payload SQL-Injection tersebut yang dapat dapat menerobos masuk (bypass login).



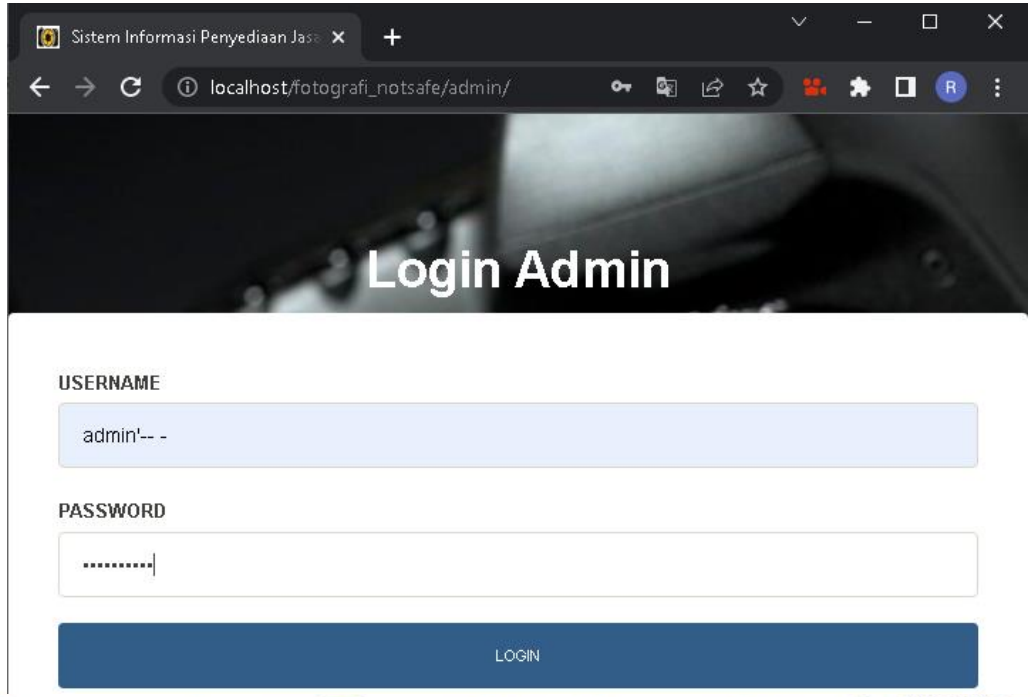
- Interface pada gambar 4.3 berisi form tampilan pertama atau form login website E-Perpus yang diinject atau diserang dengan payload SQL-Injection tersebut yang dapat dapat menerobos masuk (bypass login).



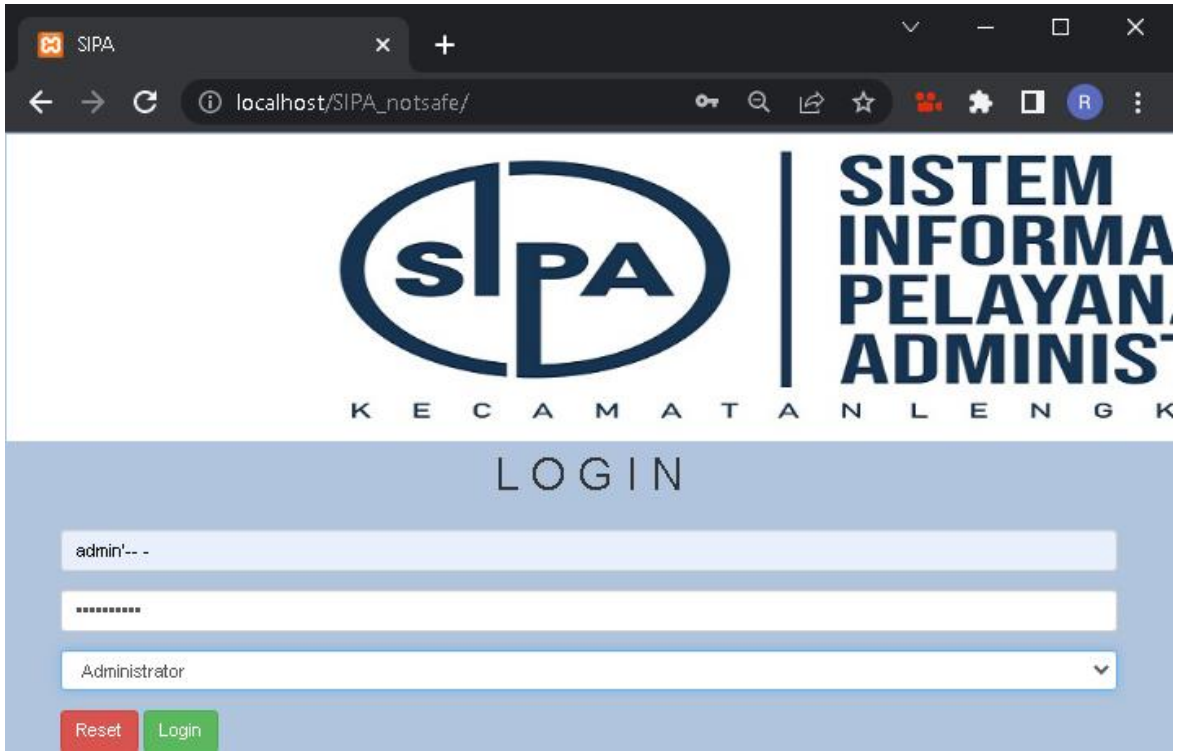
- Interface pada gambar 4.4 berisi form tampilan pertama atau form login website SI-IAK yang diinject atau diserang dengan payload SQL-Injection tersebut yang dapat dapat menerobos masuk (bypass login).



- Interface pada gambar 4.5 berisi form tampilan pertama atau form login website Sistem informasi penyedia jasa fotografi yang diinject atau diserang dengan payload SQL-Injection tersebut yang dapat dapat menerobos masuk (bypass login).



- Interface pada gambar 4.6 berisi form tampilan pertama atau form login website SIPA yang diinject atau diserang dengan payload SQL-Injection tersebut yang dapat dapat menerobos masuk (bypass login).

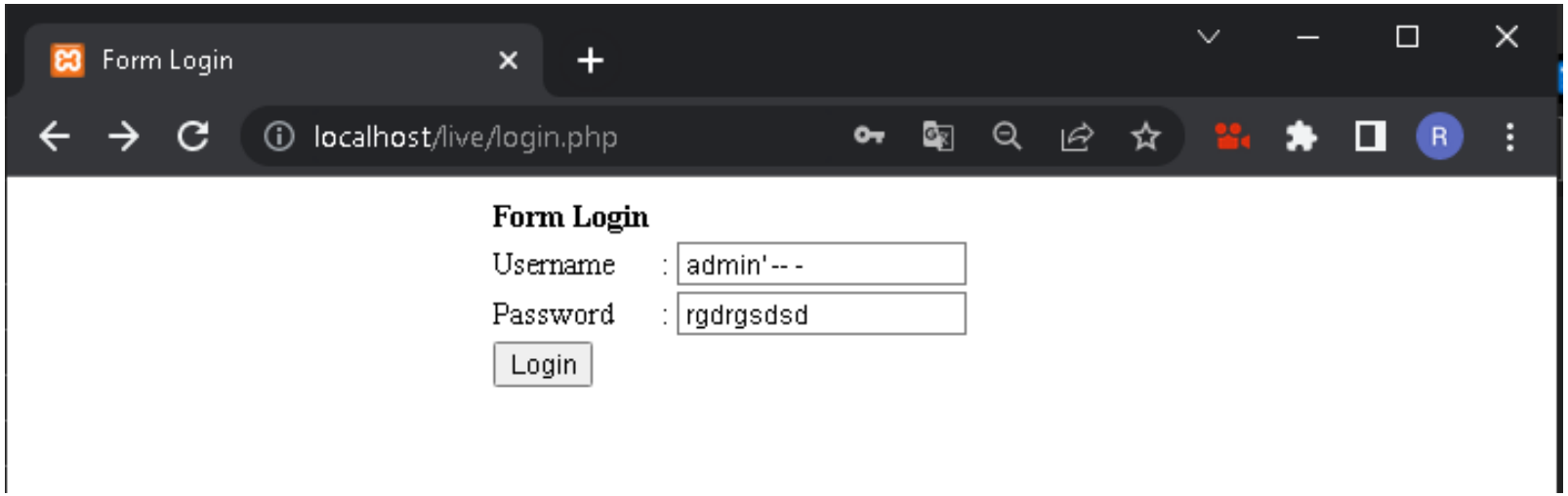


- Seperti yang bisa dilihat pada gambar-gambar diatas perintah sql injection yang telah diinjek dengan menggunakan sqlmap dan nantinya akan dijalankan pada website yang belum terfilter oleh fungsi Honeypot preg_match() . Akan tetapi pada studi kasus sql injection ini banyak orang tidak sadar bahwasanya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

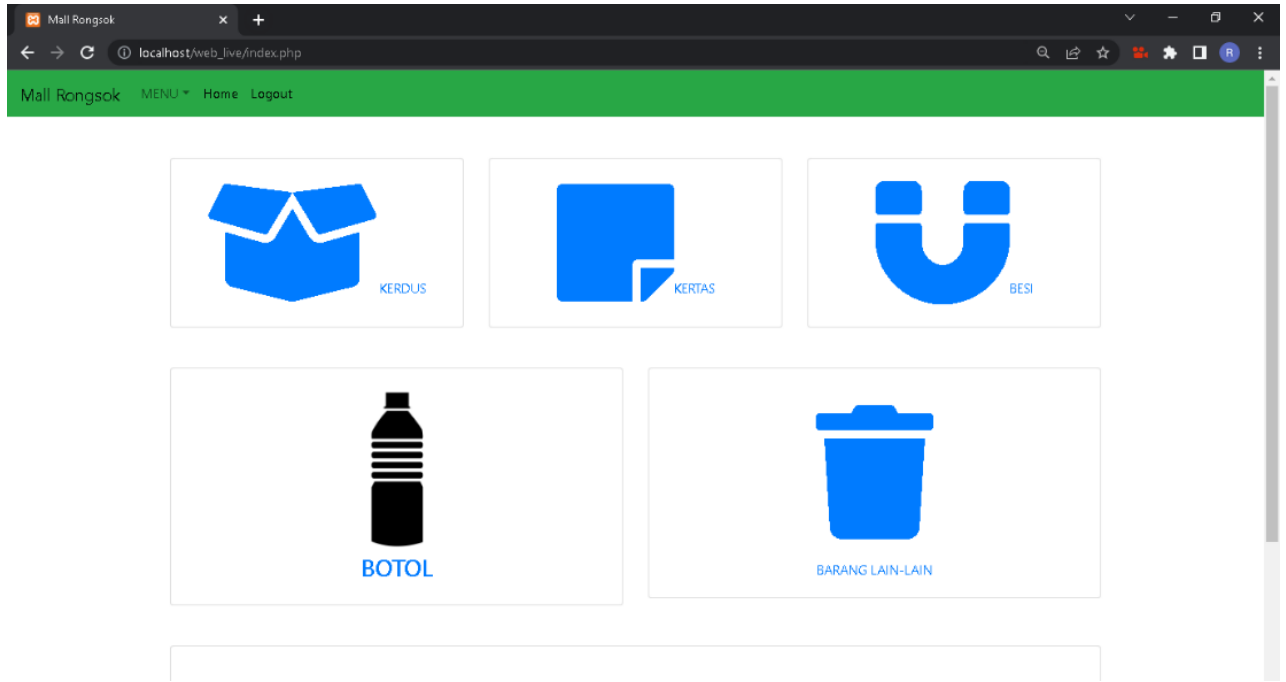
- Tahap penggunaan Honeypot

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.

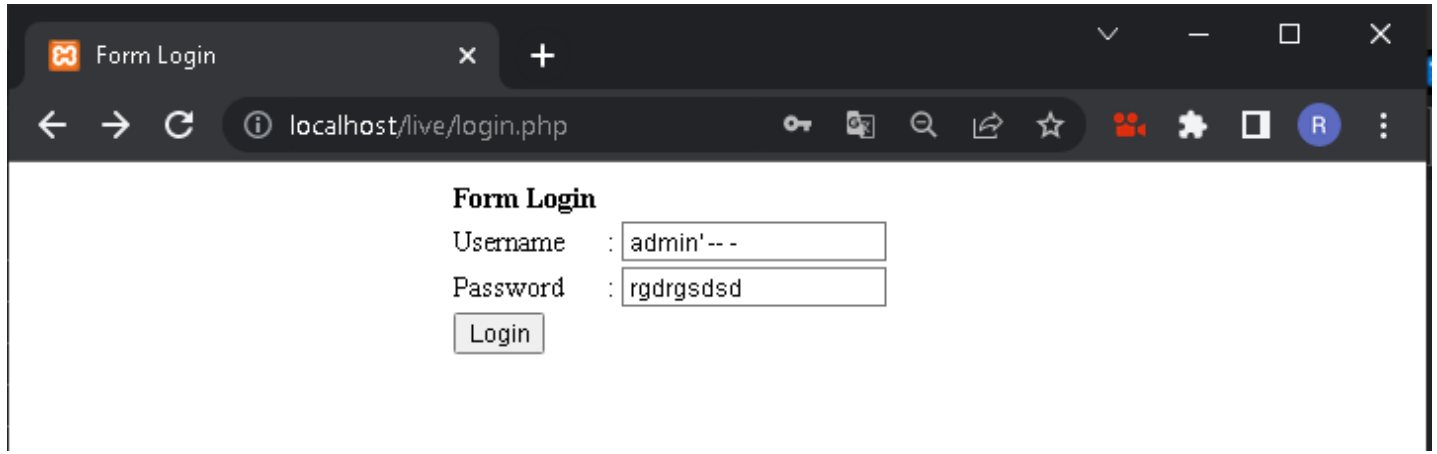
- Interface pada gambar 4.7 berisi form tampilan pertama atau form login website bank sampah yang belum diamankan menggunakan metode Honeypot dengan fungsi preg_match()



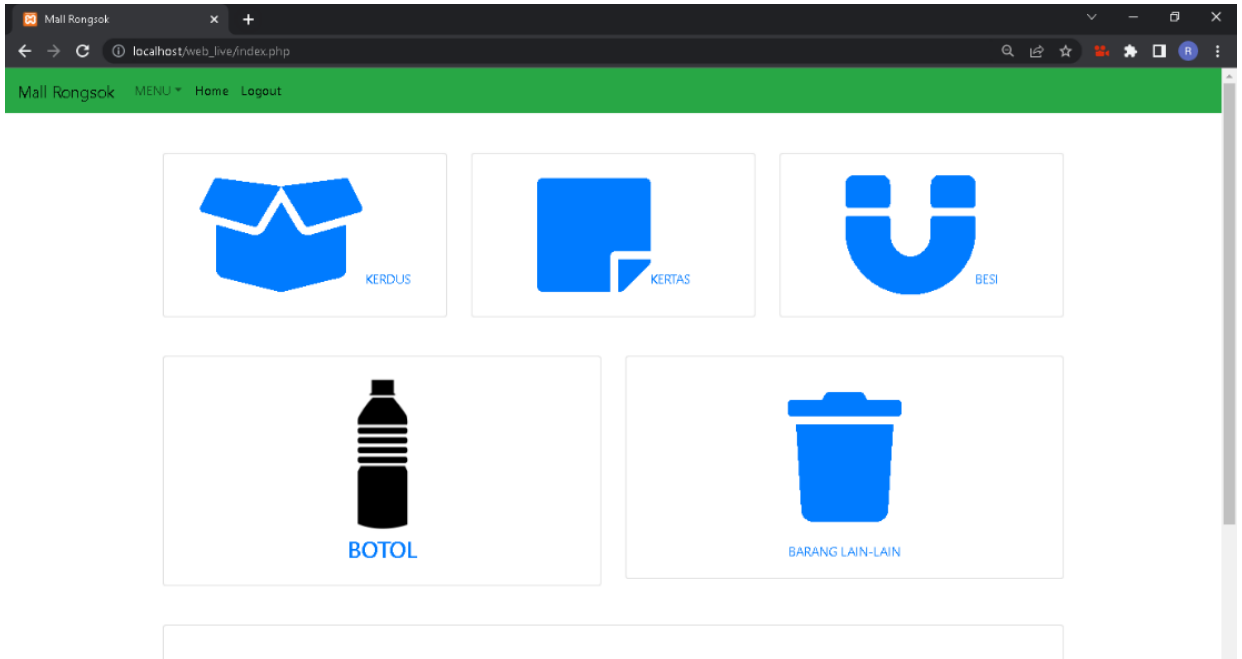
- Interface pada gambar 4.8 maka user dapat menggunakan fitur yang ada dalam halaman dashboard. Yang didalam website terisi beberapa menu yaitu : Kardus Kertas Besi Botol Barang Lain lain.



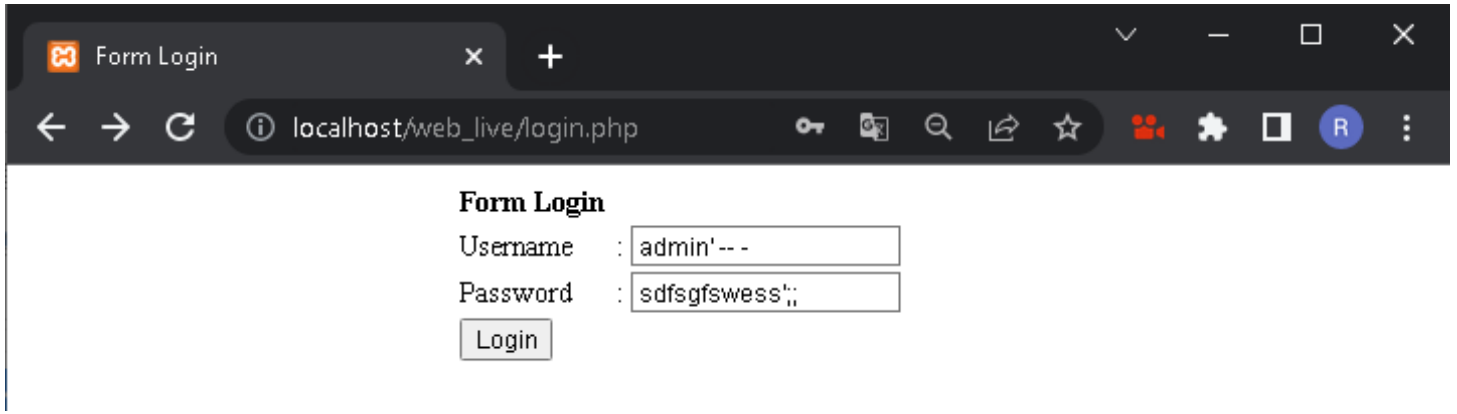
- Berikut ini adalah hasil proses pengecekan dan pengaman pada website Bank Sampah menggunakan metode Honeypot menggunakan fungsi preg_match().
- Interface pada gambar 4.7 berisi form tampilan pertama atau form login website bank sampah yang belum diamankan menggunakan metode Honeypot dengan fungsi preg_match()



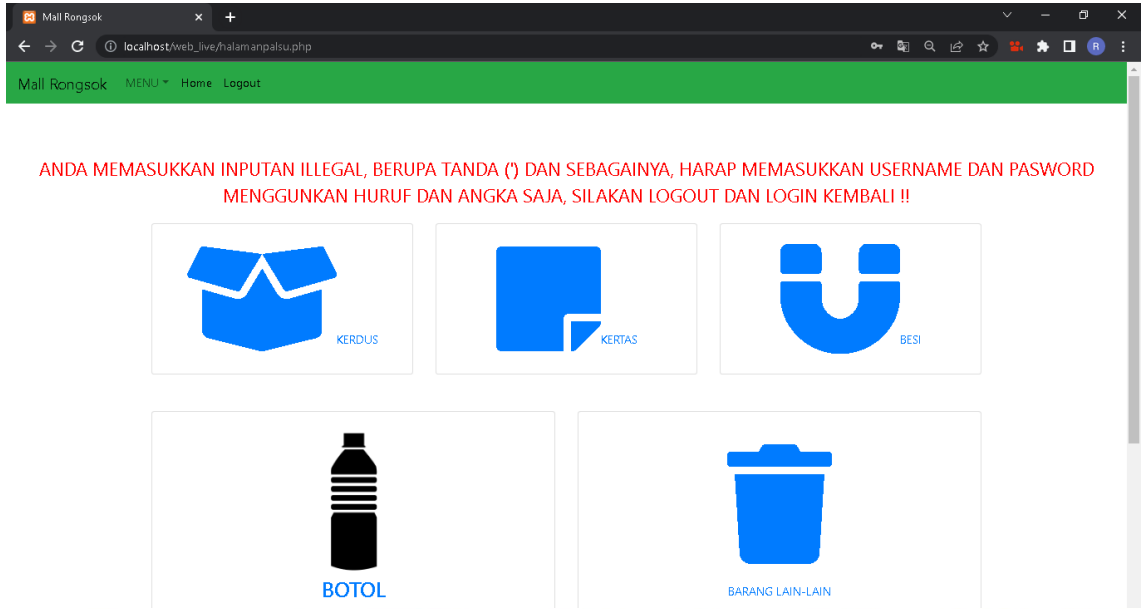
- Interface pada gambar 4.8 maka user dapat menggunakan fitur yang ada dalam halaman dashboard. Yang didalam website terisi beberapa menu yaitu : Kardus Kertas Besi Botol Barang Lain lain.



- Pada gambar 4.9 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 4.10, 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



Kesimpulan

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 pada form login.

Referensi

- Fatma, Weni Dwi. 2018. “Analisa Keamanan Server Pada Login Page Webserver Dengan Enkripsi Sha 1 Dari Serangan Sql Injection Menggunakansystemoperasi Kali Linux Di Lkp Multi Logika Binjai.”
- Irawan, Alex Sandro, Eko Sakti Pramukantoro, and Ari Kusyanti. 2018. “Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization.” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya* 2(6): 2295–2301.
- Patah, Herwanto, and Mustofa Zaid. *Perancangan Aplikasi Deteksi Kerentanan Sql Injection Dan Cross-Site Script Pada Aplikasi Berbasis Website Menggunakan Metode Waterfall*.
- Pemula, Penelitian Dosen. 2018. “RANCANG BANGUN APLIKASI KASIR TIKET NONTON BOLA BARENG PADA X KASIR DI SUATU LOKASI X DENGAN VISUAL BASIC 2010 DAN MYSQL Ninuk.” 110265(2): 110493.
- Ramadhan, Rizky Fajar, and Riki Mukhaiyar. 2020. “Penggunaan Database Mysql Dengan Interface PhpMyAdmin Sebagai Pengontrolan Smarthome Berbasis Raspberry Pi.” *JTEIN: Jurnal Teknik Elektro Indonesia* 1(2): 129–34.
- Riadi, Imam, Rusydi Umar, and Wasito Sukarno. 2019. *ANALISIS FORENSIK SERANGAN SQL INJECTION MENGGUNAKAN METODE STATIS FORENSIK*.

- Romadhon, M Hamdan, and Yusuf Yudhistira. 2021. “Sistem Informasi Rental Mobil Berbsasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri.” 2(1): 30–36.
- Soepomo, Prof. 2019. “Penerapan Sistem Keamanan Honeypot Dan Ids Pada Jaringan Nirkabel (Hotspot).” *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)* 1(1): 111–18.
- Wasis Wicaksono, Galih, and Andi Al-Rizki. 2016. “Peningkatan Kualitas Evaluasi Mutu Akademik Universitas Muhammadiyah Malang Melalui Sistem Informasi Mutu (SIMUTU).” *KINETIK* 1(1): 1–8.
- Wiguna, Bangkit et al. 2019. “Wiguna, Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website.” https://doi.org/10.31849/digitalzone.v11i2.4867ICCS.
- Yudantoro, Tri Raharjo. 2018. “Adoc.Pub_sql-Injection-Pada-Sistem-Keamanan-Database.”
- Yulianingsih, Jalan Nangka, Tanjung Barat, and Jagakarsa Jakarta Selatan. 2018. 2 Jurnal Edukasi dan Penelitian Informatika (JEPIN) *Menangkal Serangan SQL Injection Dengan Parameterized Query*.


UMSIDA
DARI SINI PENCERAHAN BERSEMI