Laporan Praktikum: Keamanan Aplikasi Laravel 9

Laporan Praktikum : Keamanan Aplikasi Laravel 9

Nama Mahasiswa : Ahmad Farieq
NIM : 231240001397
Tanggal Praktikum : 27 Juni 2025

Pendahuluan

Pada praktikum ini, tujuan utama adalah untuk menguji keamanan aplikasi Laravel 9 terhadap tiga jenis serangan umum pada aplikasi web, yaitu:

1. **CSRF (Cross-Site Request Forgery)**
2. **XSS (Cross-Site Scripting)**
3. **SQL Injection**

Setiap jenis serangan diuji melalui beberapa langkah simulasi dan diamati hasilnya, untuk memastikan bahwa fitur keamanan Laravel bekerja sebagaimana mestinya.

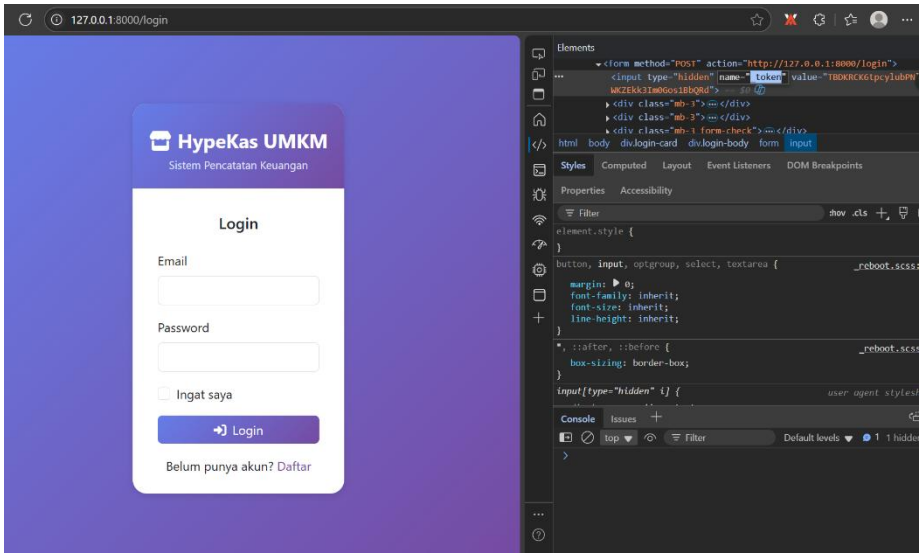
1. Uji Keamanan Terhadap Serangan CSRF

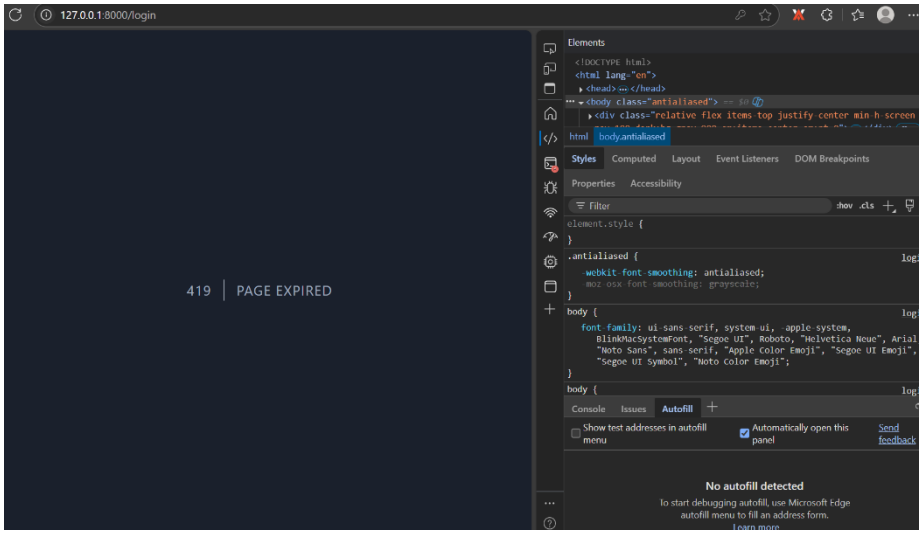
1.1. Pengertian CSRF

CSRF adalah serangan yang menipu pengguna agar melakukan tindakan yang tidak diinginkan pada aplikasi web tempat mereka saat ini sedang login (terautentikasi), seperti mengirim data tanpa izin.

1.2. Langkah-langkah Pengujian

- Buka halaman login di aplikasi Laravel (/login).
- Gunakan fitur *Inspect Element* pada browser untuk melihat elemen form.
- Temukan field tersembunyi dengan nama _token (token CSRF).
- Hapus atau ubah nilai _token, lalu kirim form login.





1.3. Hasil Pengujian

Setelah menghapus input _token dan mencoba login, aplikasi menampilkan halaman error 419 | PAGE EXPIRED.

Kesimpulan: Laravel berhasil menolak request tanpa token CSRF. Aplikasi aman dari CSRF.

2. Uji Keamanan Terhadap Serangan XSS

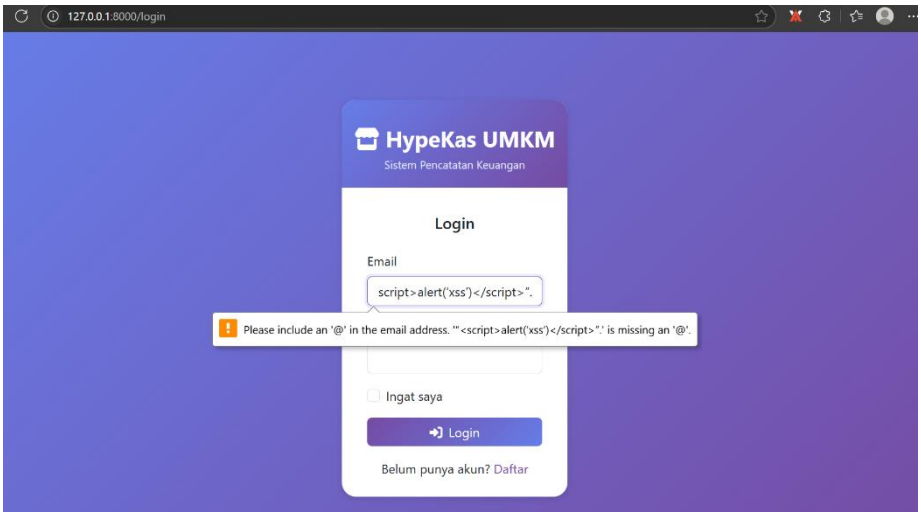
2.1. Pengertian XSS

XSS adalah serangan di mana penyerang menyisipkan skrip berbahaya ke dalam konten aplikasi. Skrip ini bisa dijalankan di browser pengguna lain tanpa sepengetahuan mereka.

2.2. Langkah-langkah Pengujian

- Pada form registrasi, di field nama/email/password, masukkan payload:

- <script>alert('xss')</script>
- Submit form dan perhatikan apakah skrip dieksekusi (muncul popup alert).



2.3. Hasil Pengujian

Setelah mengisi nama dengan skrip di atas dan menyimpan data, **tidak muncul popup alert** saat data ditampilkan kembali. Teks skrip ditampilkan sebagai teks biasa.

Kesimpulan: Laravel secara default melakukan escaping terhadap output. Aplikasi aman dari XSS.

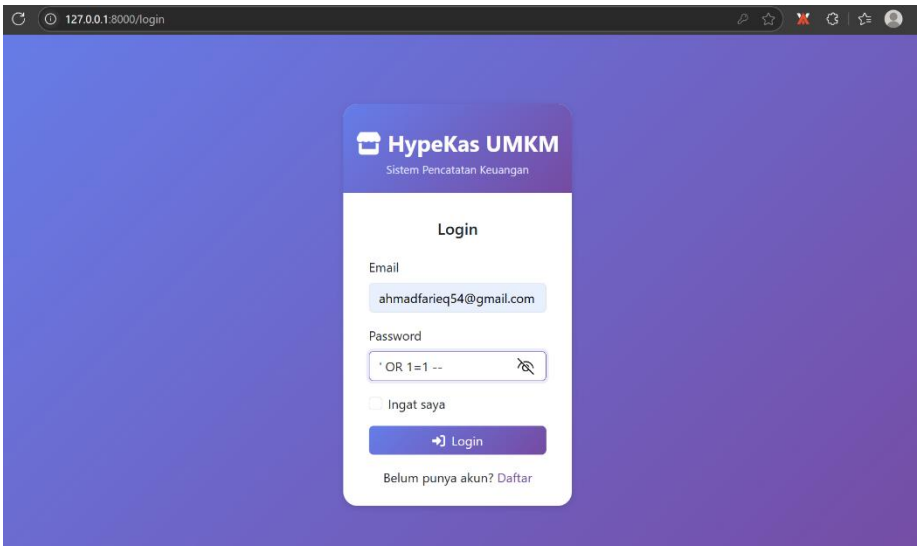
3. Uji Keamanan Terhadap Serangan SQL Injection

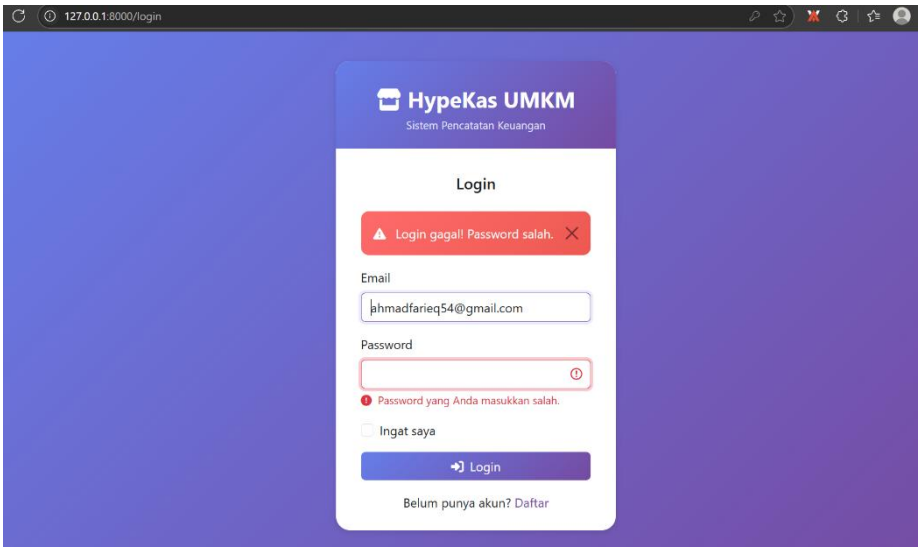
3.1. Pengertian SQL Injection

SQL Injection adalah teknik di mana penyerang memasukkan sintaks SQL berbahaya ke dalam input aplikasi, untuk memanipulasi query database.

3.2. Langkah-langkah Pengujian

- Akses halaman login aplikasi.
- Di field **email** masukkan:
- ' OR 1=1 --
- Masukkan password sembarang.
- Klik login dan amati hasilnya.





3.3. Hasil Pengujian

Setelah mencoba payload tersebut, login gagal dan tidak ada user lain yang bisa diakses.

Kesimpulan: Laravel menggunakan query builder/Eloquent ORM yang secara otomatis melindungi aplikasi dari SQL Injection. Aplikasi aman.

Kesimpulan Umum

Dari hasil pengujian yang dilakukan, aplikasi Laravel 9 terbukti **memiliki sistem keamanan default yang kuat** terhadap:

- Serangan CSRF melalui middleware VerifyCsrfToken.
- Serangan XSS melalui fitur blade templating ({{ }}).
- Serangan SQL Injection melalui penggunaan Eloquent ORM dan query builder.