**TUGAS 1**

**SQL INJECTION**



Nama: I Gusti Putu Arya Zaki Yoga Pratama  
NIM: 220010117

**LINK CODE:** [**lLINK CODE**](https://github.com/aryazaki052/secureweb/tree/34ffd33ea53cef5eb8f712b57772ec8d751860db/tugas_pert_8)

|  |
| --- |
|  |
| Ini adalah tampilan awal dari aplikasi yang saya buat. Yang dimana ada beberapa menu yang dapat diakses. Untuk menu client saya menggunakan port 3001 yang akan mengakses halaman html nya yang dimana halaman client pertama kali akan masuk ke halaman index.html.  Di halaman index.html ini akan memunculkan data – data produk yang sudah di masukan oleh user sebelumnya.  Ada menu create, edit dan delete yang bisa digunakan dalam halaman ini. |
|  |
| Jika user meng-klik tombol create maka user diminta untuk memasukan name dan price. Masalahnya disini adalah code belum diberikan perlindungan terhadap serangan sql injection yang berarti hacker dapat memasukan script – script sql untuk memanipulasi data. |
|  |
| Lalu masuk ke tampilan edit, yang dimana user bisa mengedit data sesuai dengan id data yang telah dipilih oleh user. Bisa dilihat pada url nya itu menunjukan Id 17. |
|  |
| Ini adalah tampilan delete nya yang bisa digunakan untuk menghapus product. Disaat user klik button delete maka akan muncul alert untuk konfirmasi seperti yang terlihat pada gambar diatas. |
|  |
| Ini adalah pengujian form untuk create nya. Saya memasukan script sql untuk mengambil semua data dari tabel produk. Karena ini tidak menggunakan prepare statement untuk mencegah serangan sql injection maka script yang saya masuka di form product itu akan di jalankan oleh browser. |
|  |
| Lalu hasilnya akan seprti ini, script itu berhasil dimasukan ke dalam database. |
|  |
| Ini adalah app yang sudah ditambahkan prepare statement, terlihat perbedaan nya jika menggunakan prepare statemant maka input yang dimasukan oleh user tidak akan di respon oleh server karena tidak sesuai dengan validasi data nya. |
|  |
| Lalu selanjutnya saya akan mencoba edit nya. Ini adalah code yang belum diberikan prepare statement. |
|  |
| Disaat saya mencoba mengedit nya di aplikasi postman dengan menggunakan ednpoint edit/18 OR 1=1, maka yang terjadi adalah semua produk itu diedit dan dimasukan nilai tes edit sql. Ini terjadi karena server merespon OR 1=1 ini adalah semua nilai bernilai true. Jadi semua product nya berubah menjadi tes edit sql. |
|  |
| Ini setelah code dijalankan akan menjadi seperti ini. Semua produk aka berubah nama nya. |
|  |
| Namun setelah diberikan prepare statement jika saya memasukan url yang sama, maka server akan merespon error. |
|  |
| Lau selanjutnya saya akan testing delete nya. Jika saya memberikan perintah yang sama dengan endpoint edit pada endpoint delete maka akan menghapus semua produk yang ada di dalam table. Ini terjadi karena OR 1=1 akan menghasikan nilai true untuk semua id nya. |
|  |
| Sehingga semua produk akan terhapus |
|  |
| setelah diberikan prepare statement script tidak akan bisa dijalankan oleh server. |