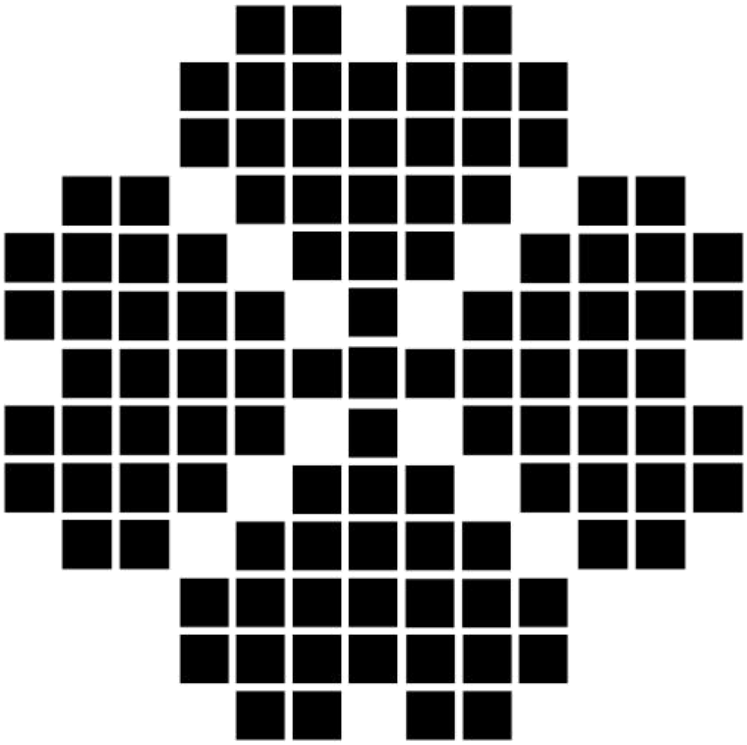


Reporter

Name	Kadek Dwi Wardana Saputra
Email	sapu2776@gmail.com

REPORT

Vulnerability Name **:**Sql Injection.

Level **: Critical**

Vulnerability Description :

Sql Injection vulnerability adalah sebuah kerentanan yang memanfaatkan pengkoneksian yang kurang baik pada database, pada kasus ini saat *user/attacker* membuka http://sigmal.id/data/posko/6/detail dan menambahkan ‘ (koma) pada akhir “6”, dan melakukan akses http://sigmal.id/data/posko/6'/detail, akan menampilkan *“SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1 (SQL: SELECT * from posko where id =6')”* yang mengidentifikasi kerentanan terhadap *Sql Injection,* dan saat *user/attacker* menambahkan “--” pada posisi yang sama dan menghapus ‘ (koma) maka akan menampilkan tampilan yang normal, ini sekaligus mengkonfirmasi kerentanan, pada saat web menampilkan *error,* web sekaligus menampilkan informasi yang sangat penting, hanya dengan kesalahan kecil *user/attacker* dapat membuat,menghapus, menampilkan dan merubah data/file.

Vulnerability Impact :

Dampak vulnerability ini akan sangat merugikan pihak pemilik maupun user lain karena data primadi mereka dapat dimanipulasi/diketahui *user/attacker*, yang dimana bukan hanya berpengaruh pada pihak pemilik dan user, tapi juga akan sangat merugikan pihak yang berbagi server/koneksi database.

Vulnerability URL :

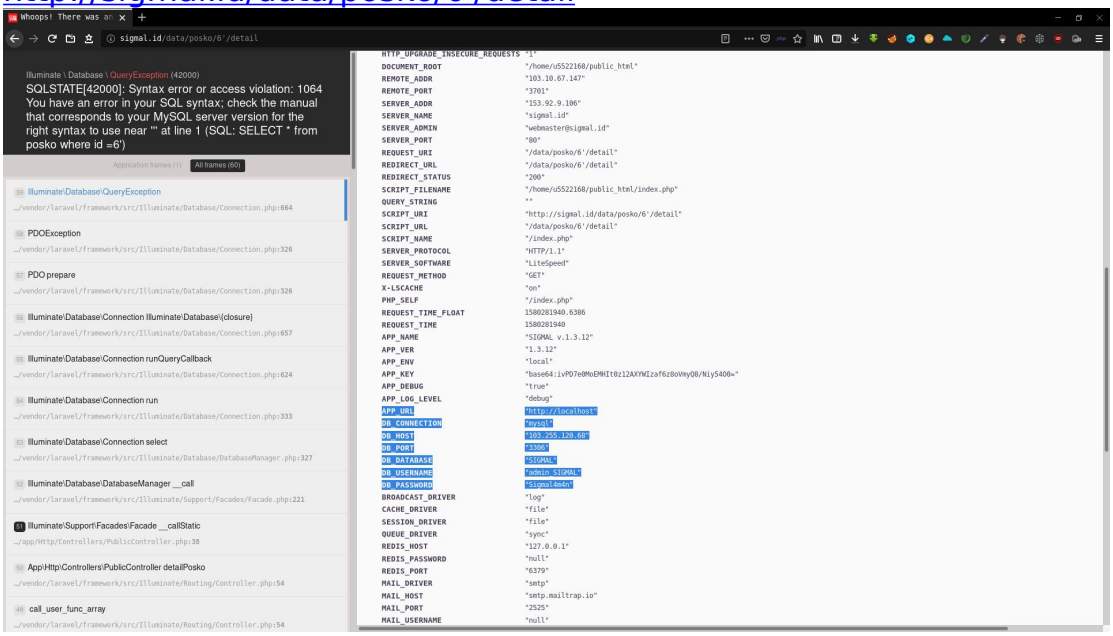
http://sigmal.id/data/*

Tahapan :

1. Melakukan aksess http://sigmal.id/data/posko/6/detail
2. Tambahkan ‘ (koma) http://sigmal.id/data/posko/6'/detail (disini *user/attacker* mendapatkan informasi yang cukup untuk mendapatkan akses lebih)
3. Tambahkan -- untuk mengkonfirmasi kerentanan http://sigmal.id/data/posko/6--/detail

POC :

http://sigmal.id/data/posko/6'/detail



http://sigmal.id/data/logistik?kabupaten=Karangasem%27&submit=Submit