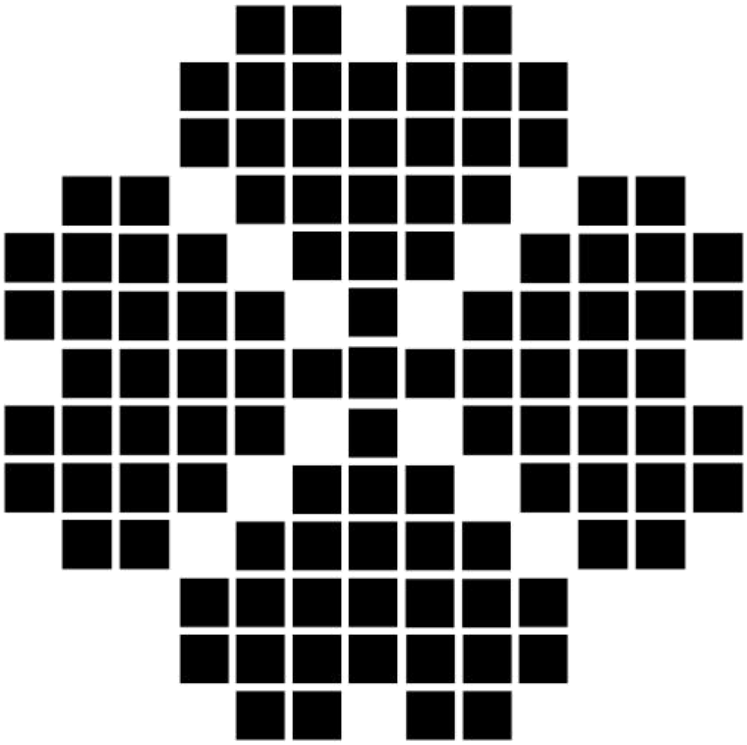

Reporter

Name	Kadek Dwi Wardana Saputra
Email	sapu2776@gmail.com
Ip	223.255.228.82

REPORT

Vulnerability Name **:**Sql Injection.

Level **:** Medium

Vulnerability Description **:**

Sql Injection vulnerabilities adalah sebuah kesalahan pada saat pengkoneksion pada database yang dapat dimanfaatkan seseorang yang dapat merugikan pihak pemilik. Disini permasalahannya berada pada parameter http get dimana user jika memasukan tanda Kutip (‘), user dapat memasukan kode kode *“critical”* pada parameter tesersebut.

Vulnerability Impact **:**

Dampak vunerability ini saat seseorang memasukan sql syntax pada parameter, seseorang ini dapat mengeksekusi critical syntax, dan dan terjadi kebocoran data yang bisa membuat “*hacker*” dapat mengakses data-data sensitif, bahkan melakukan perusakan website (*defacing*).

Vulnerability URL **:**

http://disdik.padang.go.id/mod.php?mod=gallery&op=gallery&id=12

Tahapan **:**

1. Cari parameter yang dapat di *inject*
2. Masukan tanda kutip dibelakang “id=12”
3. Setelah itu cari columns yang tersedia
4. Masukan syntax sql untuk menampilkan data-data sensitif

POC **:**

Gambar contoh injection.