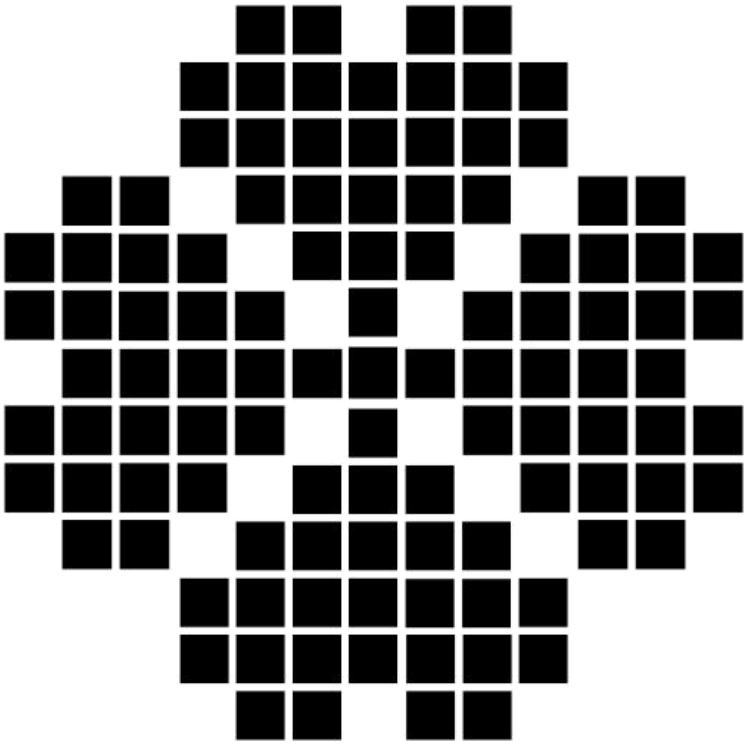

Reporter

Name	Kadek Dwi Wardana Saputra
Email	sapu2776@gmail.com

REPORT

Vulnerability Name **:**Business Logic (RCE).

Level **:** Critical

Vulnerability Description **:**

Business logic vulnerabilities adalah sebuah alur pada aplikasi yang dapat dimanfaatkan seseorang yang dapat merugikan pihak pemilik. Disini permasalahannya berada pada form edit profile dimana user jika memiliki akses login, user dapat memasukan kode kode *“critical”* pada *form update user*.

Vulnerability Impact **:**

Dampak vunerability ini saat seseorang memasukan php syntax pada form, seseorang ini dapat mengeksekusi critical syntax, dan syntax yang dimasukan akan tampil sebagai nama dari user, dan memungkinkan terjadinya kebocoran data yang bisa membuat “*hacker*” dapat mengakses data-data sensitif, bahkan melakukan perusakan website (*defacing*).

Vulnerability URL **:**

http://siska.primakara.ac.id/users/user/profile.html

Tahapan **:**

1. Login https://siska.primakara.ac.id
2. Ganti nam http://siska.primakara.ac.id/users/profile.html
3. Masukan critical syntax pada form

POC **:**

<?php system(“critical syntax”); ?> -> Masukan pada form nama

Gambar contoh injection.