前台结算处selcart参数存在SQL注入

Done #I15J32 Task 晓枫 Opened this issue 2019-11-23

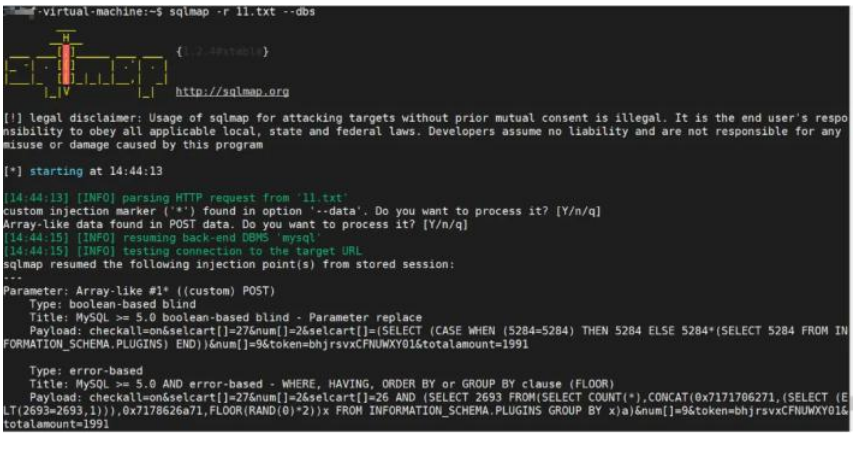
url链接：http://10.2.7.13/yun/index.php?m=shop&c=cart&a=pa
对此参数进行跟进

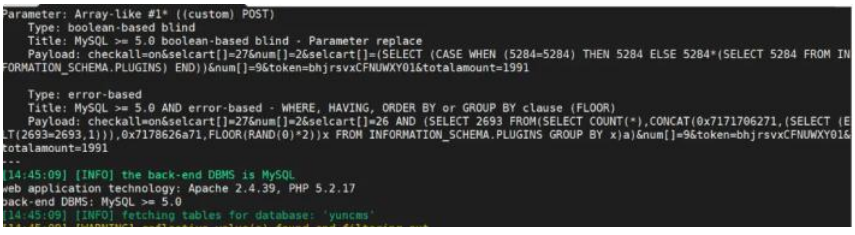
由此可以看到此参数在前台付款时接收到带入并未调用过滤函数直接执行sql语句，此处可直接进行SQL注入。

我对此进行了sql注入测试
有此可以看出已经可以将数据库表显示出来

```
POST /yun/index.php?m=shop&c=cart&a=pay&lang=1 HTTP/1.1
Host: 10.2.7.13
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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: 95
Origin: http://10.2.7.13
Connection: close
Referer: http://10.2.7.13/yun/index.php?m=shop&c=cart&a=index&lang=1
Cookie: PHPSESSID=92f6993af14fb00d2783ee9febdc01a1; YUNYECMS_userid=9; YUNYECMS_username=177777777777; YUNYE
Upgrade-Insecure-Requests: 1

checkall=on&selcart[]=27&num[]=2&selcart[]=26*&num[]=9&token=bhjrsvxCFNUWXY01&totalamount=1991
```





Status
Done

Assignees
Not set

Projects
Unprojected

Pull Requests
None yet
Successfully merging a pull request will close this issue.

Duration (hours)
0

Planed to start - **Planed to end**
Unscheduled - Unscheduled

Top level
Not Top

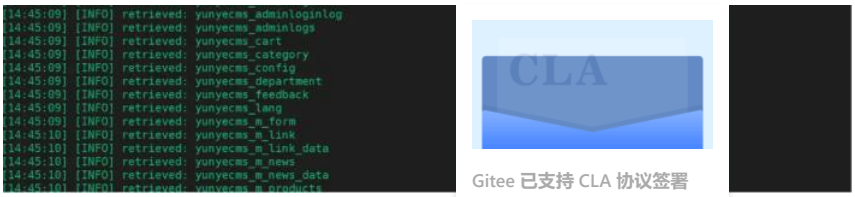
Priority
Not specified

Labels
Not set

Milestones
No related milestones

Branches
No related branch

参与者（1）
晓



修复建议： 对selcart参数进行输入处理转义

晓枫 created **任务** 3 years ago

operation logs

Sign in to comment