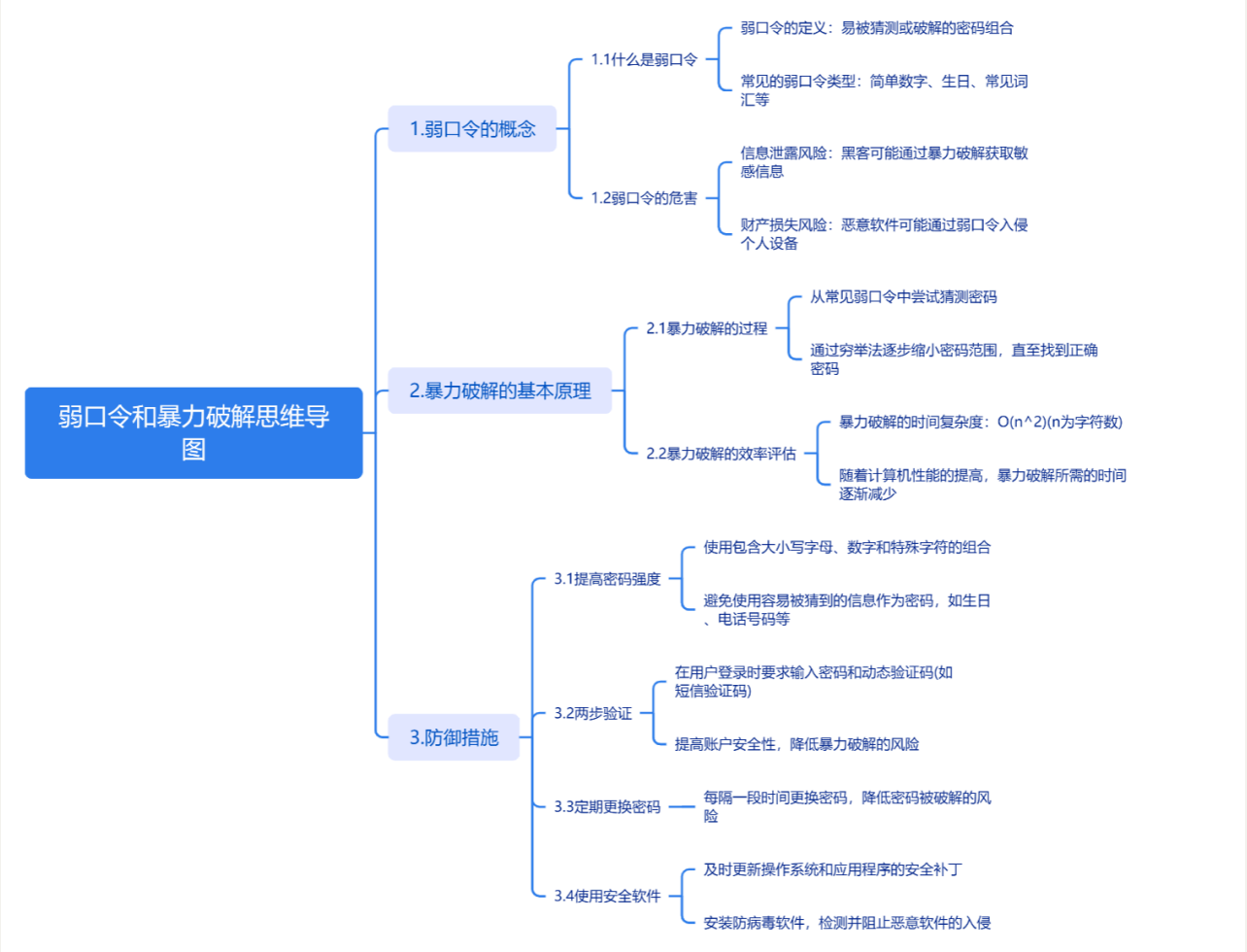
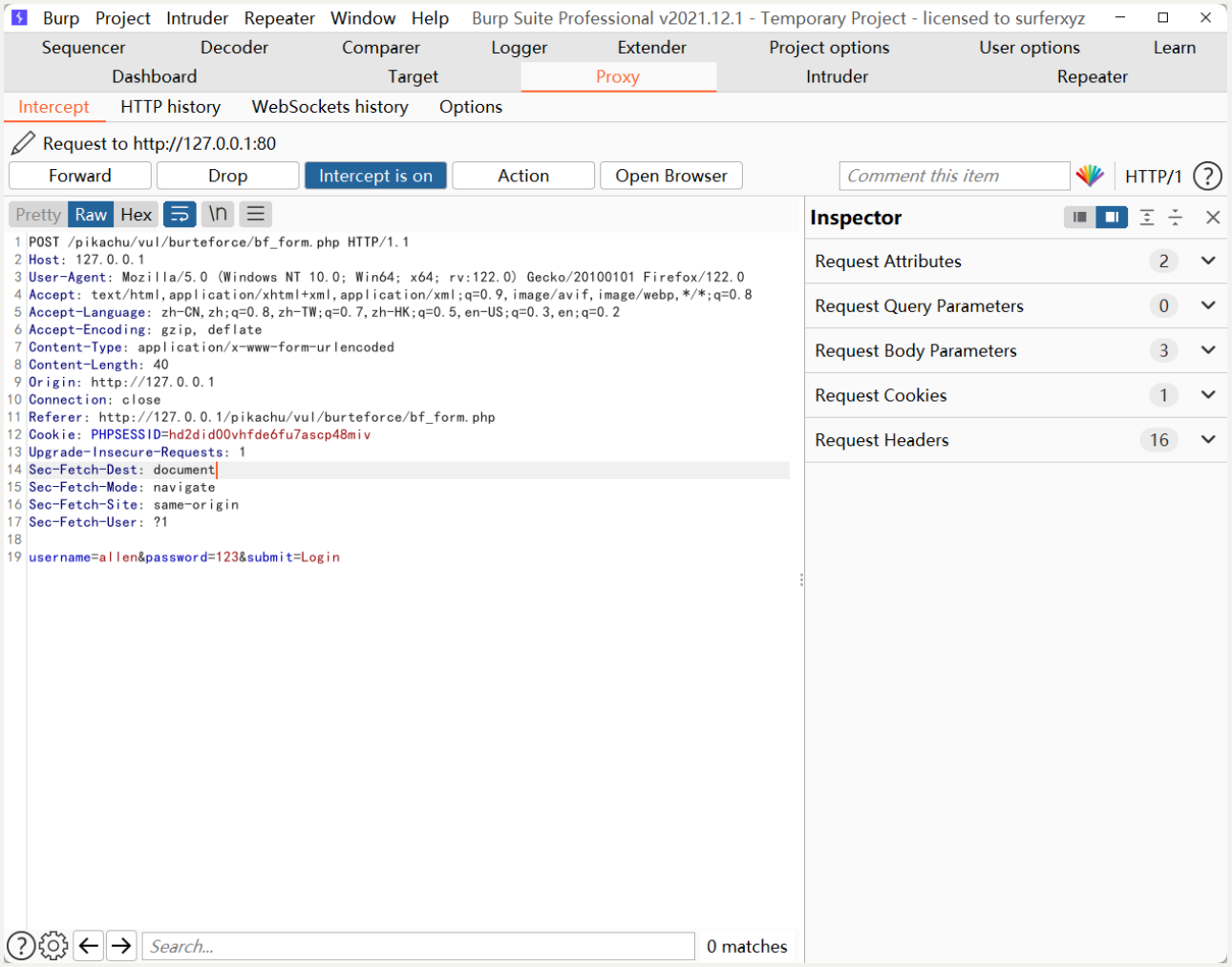
思维导图

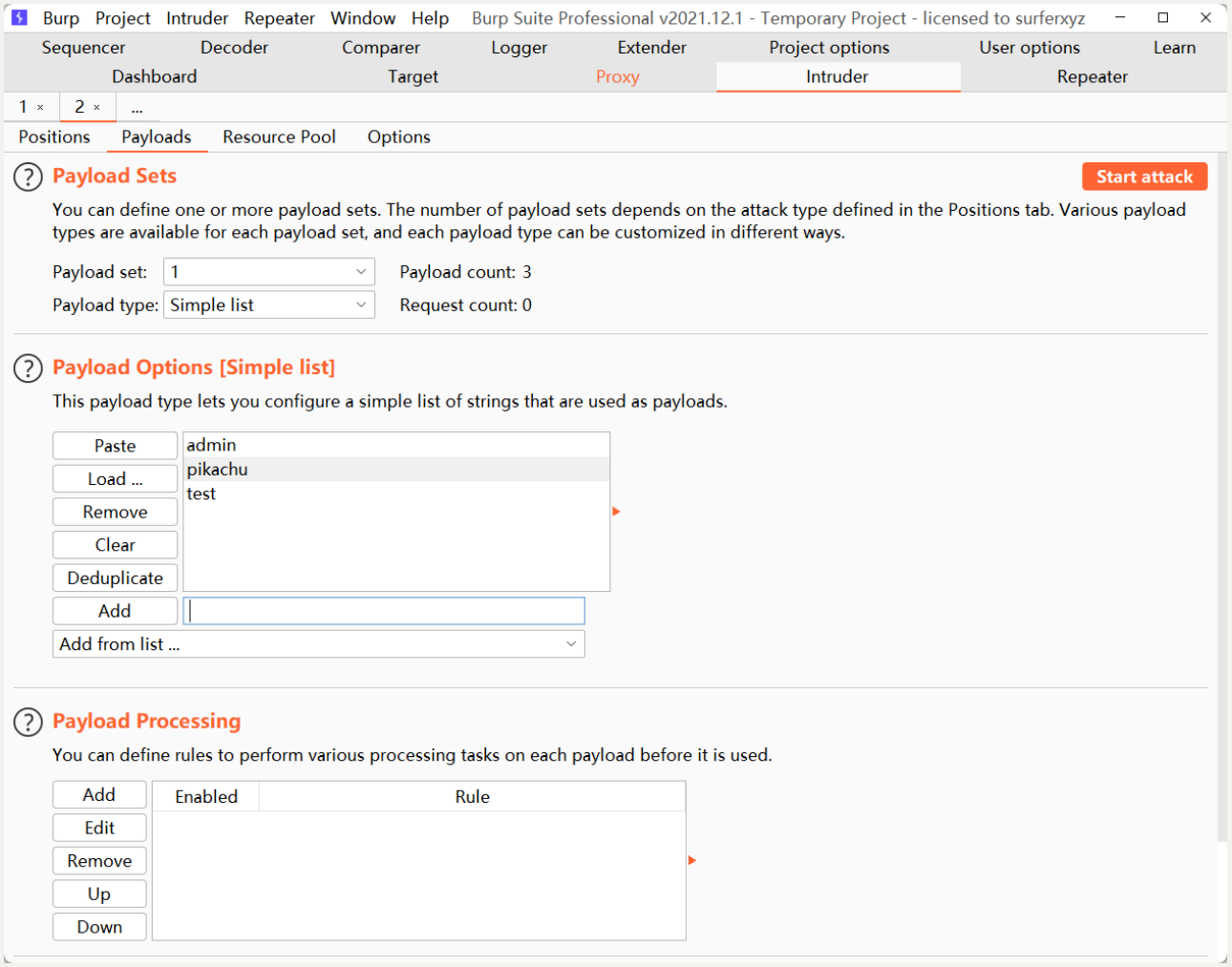


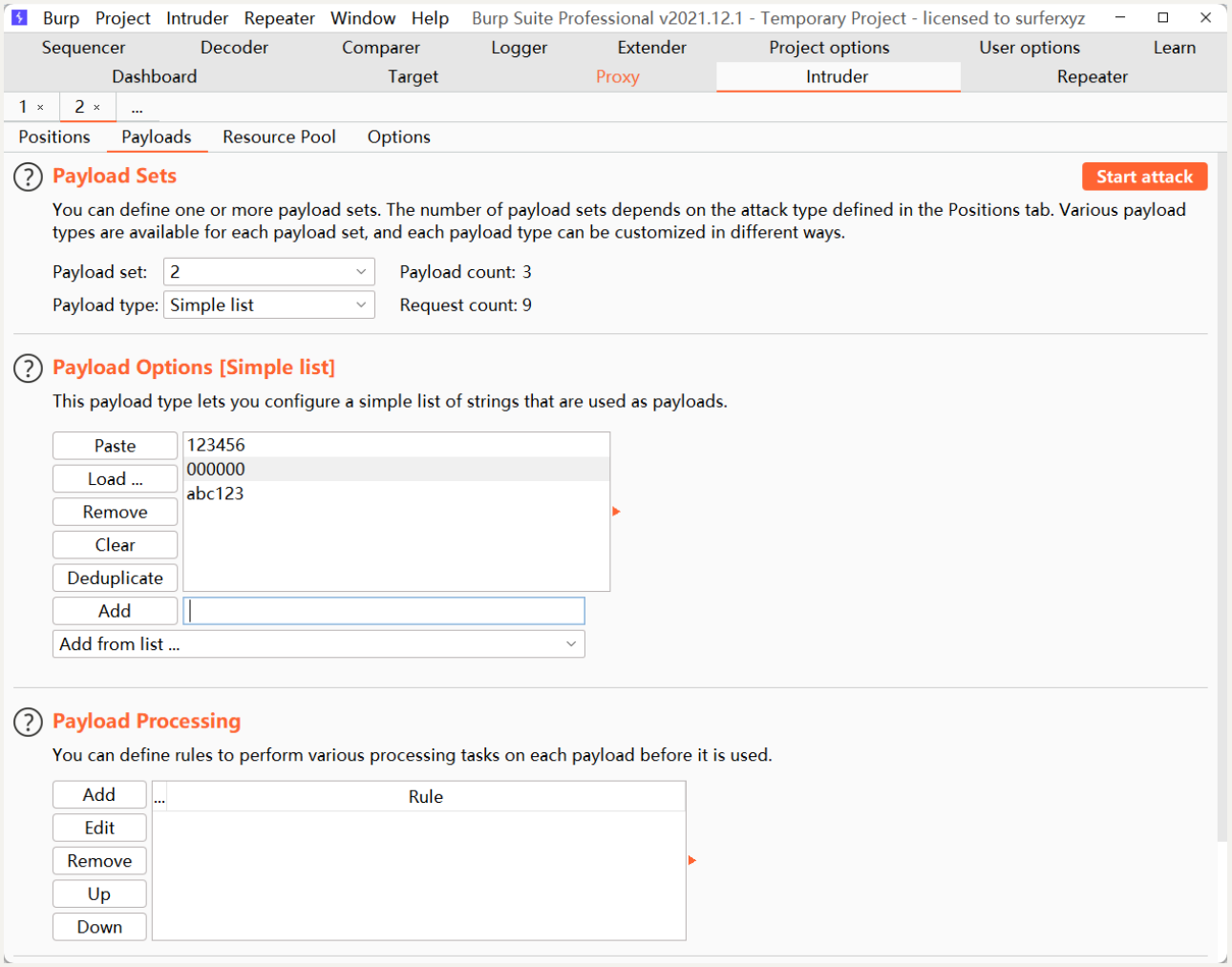
基于表单的暴力破解

1.抓包

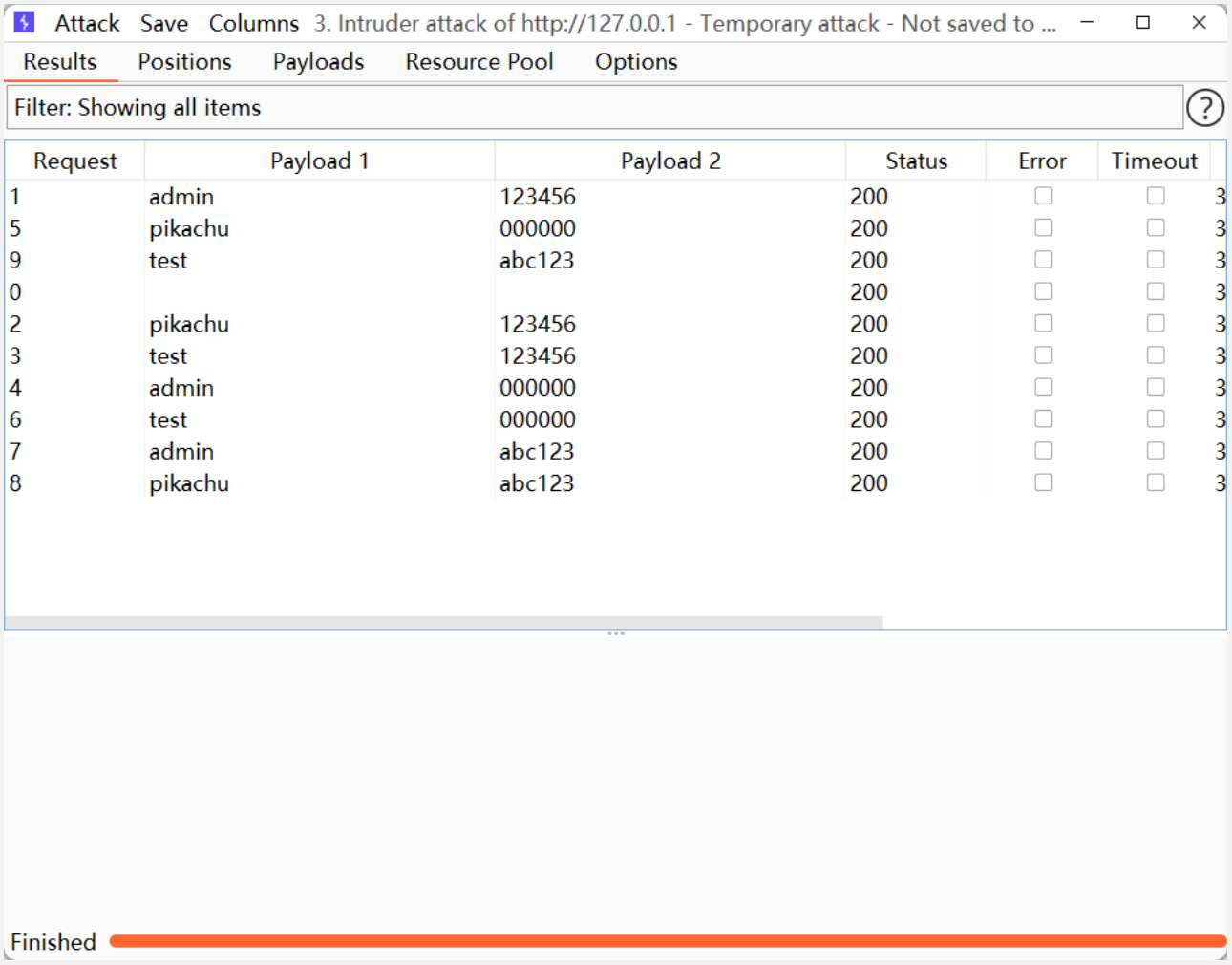


2.发送到intruder后把账户密码这两个地方标记，payloads中写入密码本


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × 2 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start attack
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: 3
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
Add
admin
pikachu
test
Add from list ...
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule

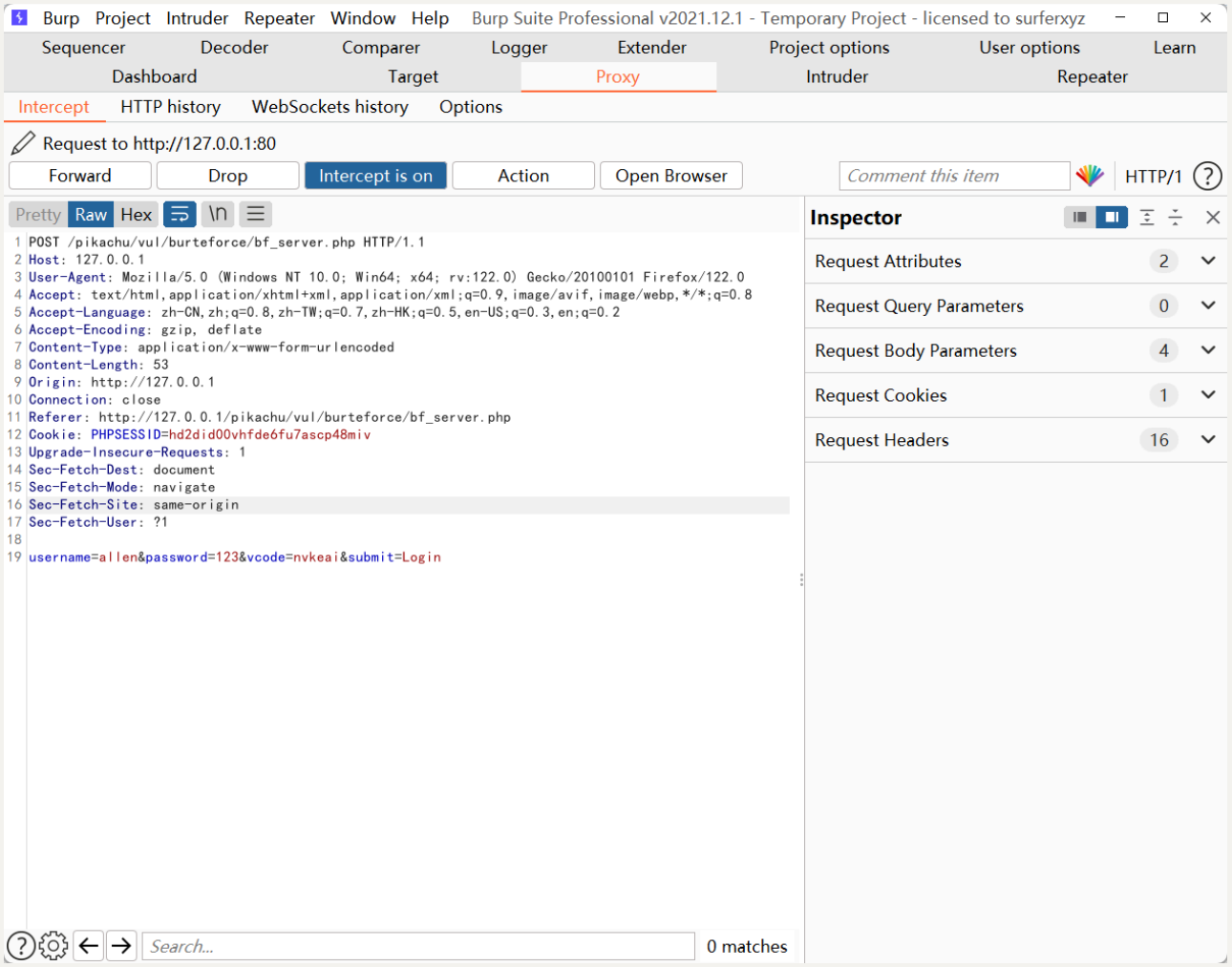

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × 2 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start attack
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: 2
Payload count: 3
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.
Paste
Load ...
Remove
Clear
Deduplicate
Add
123456
000000
abc123
Add from list ...
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
...
Rule

开始爆破



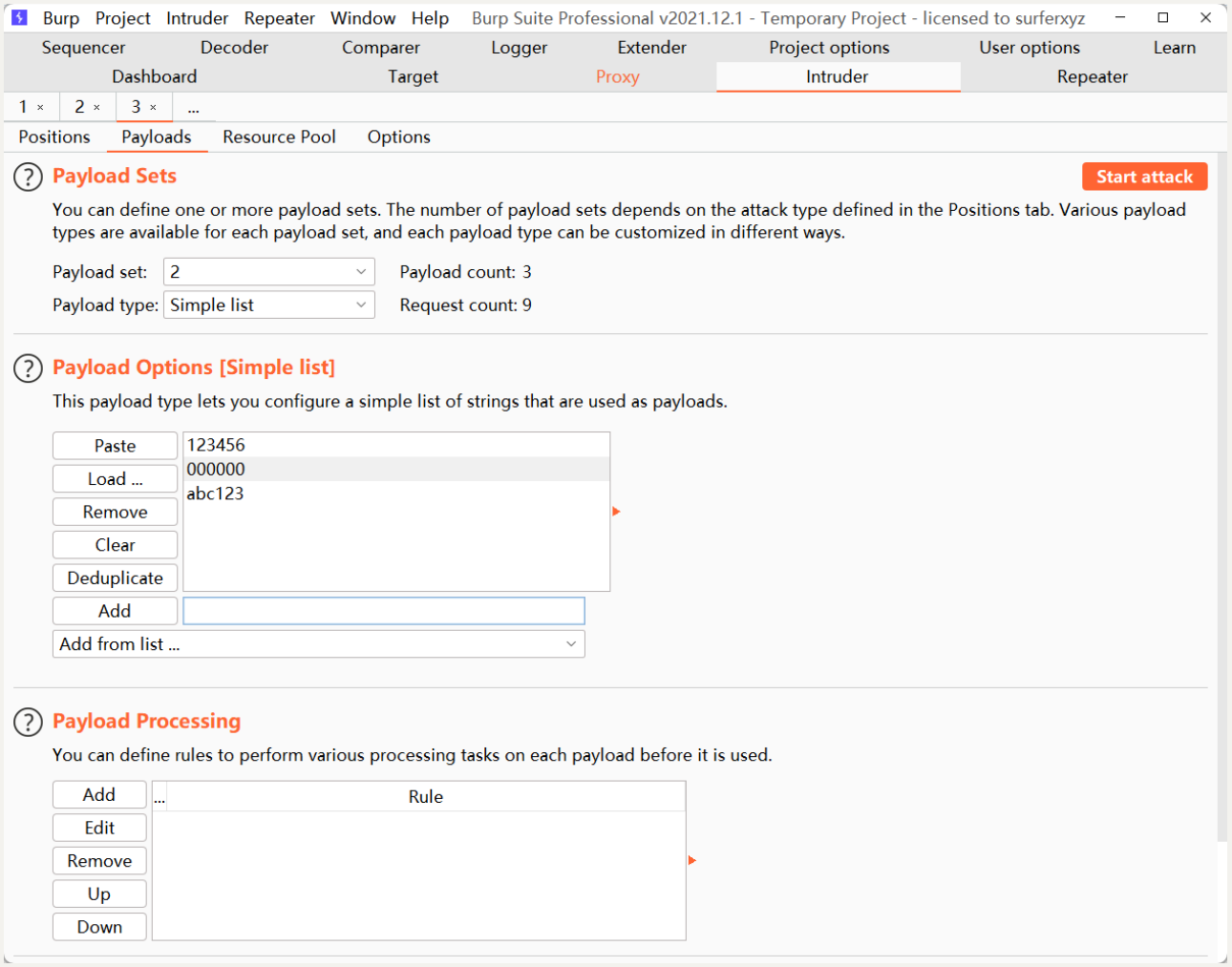
验证码绕过（on server）

1.抓包

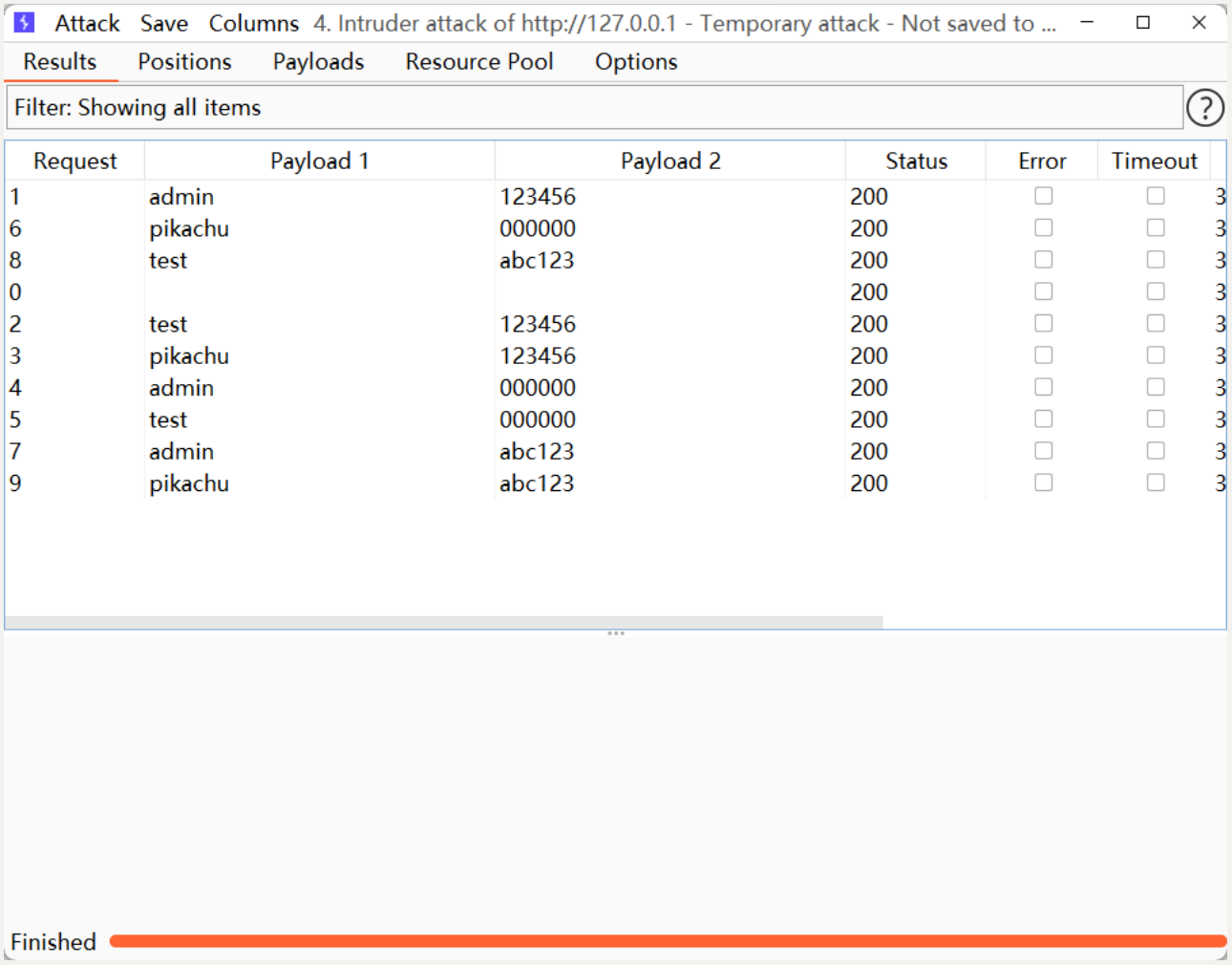


2.发送后标记账户密码验证码改为网站图标的正确验证码

写入密码本

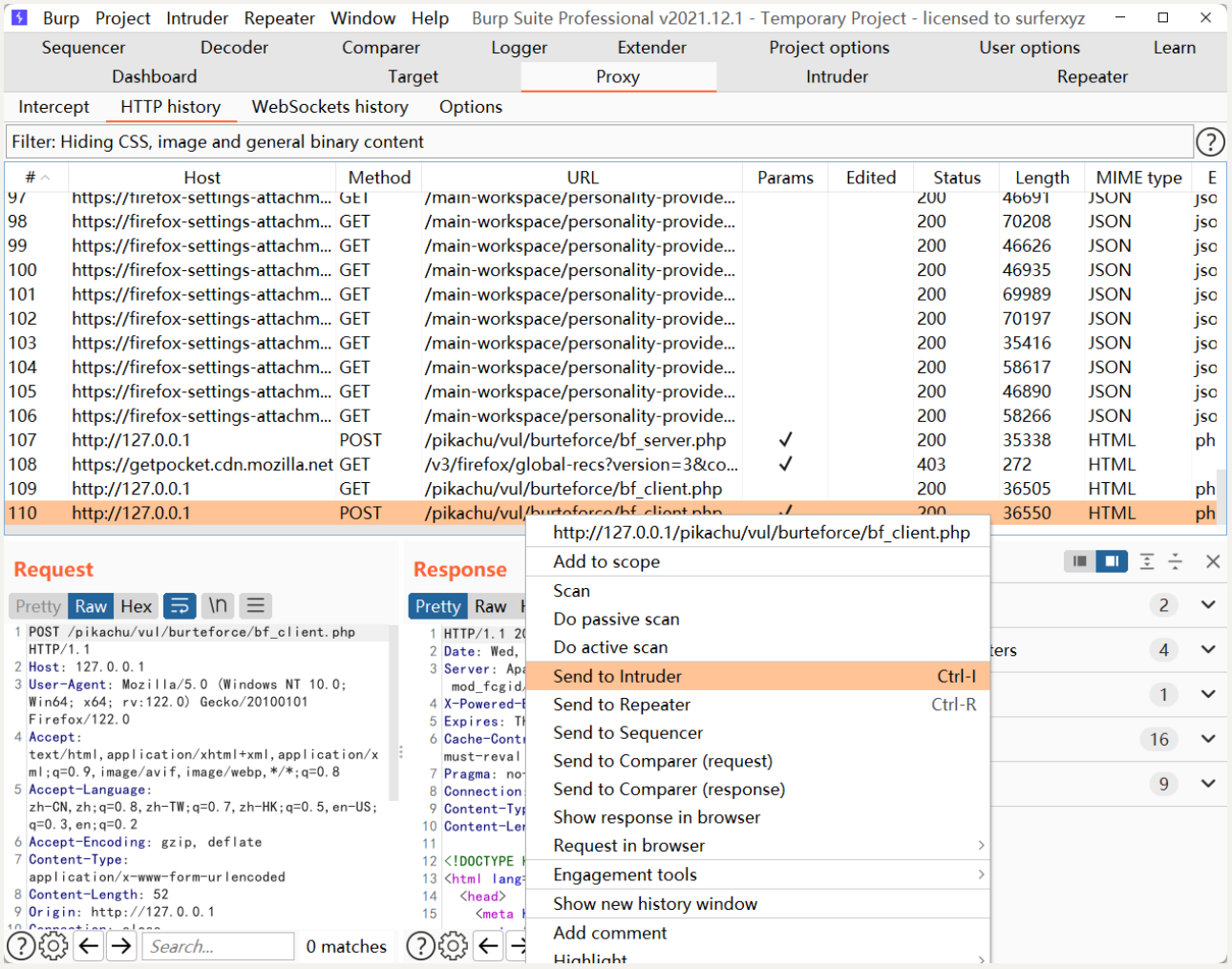

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × 2 × 3 × ...
Positions Payloads Resource Pool Options
Payload Sets
Start attack
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: 2
Payload count: 3
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.
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ...
123456
000000
abc123
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
...
Rule

开始爆破

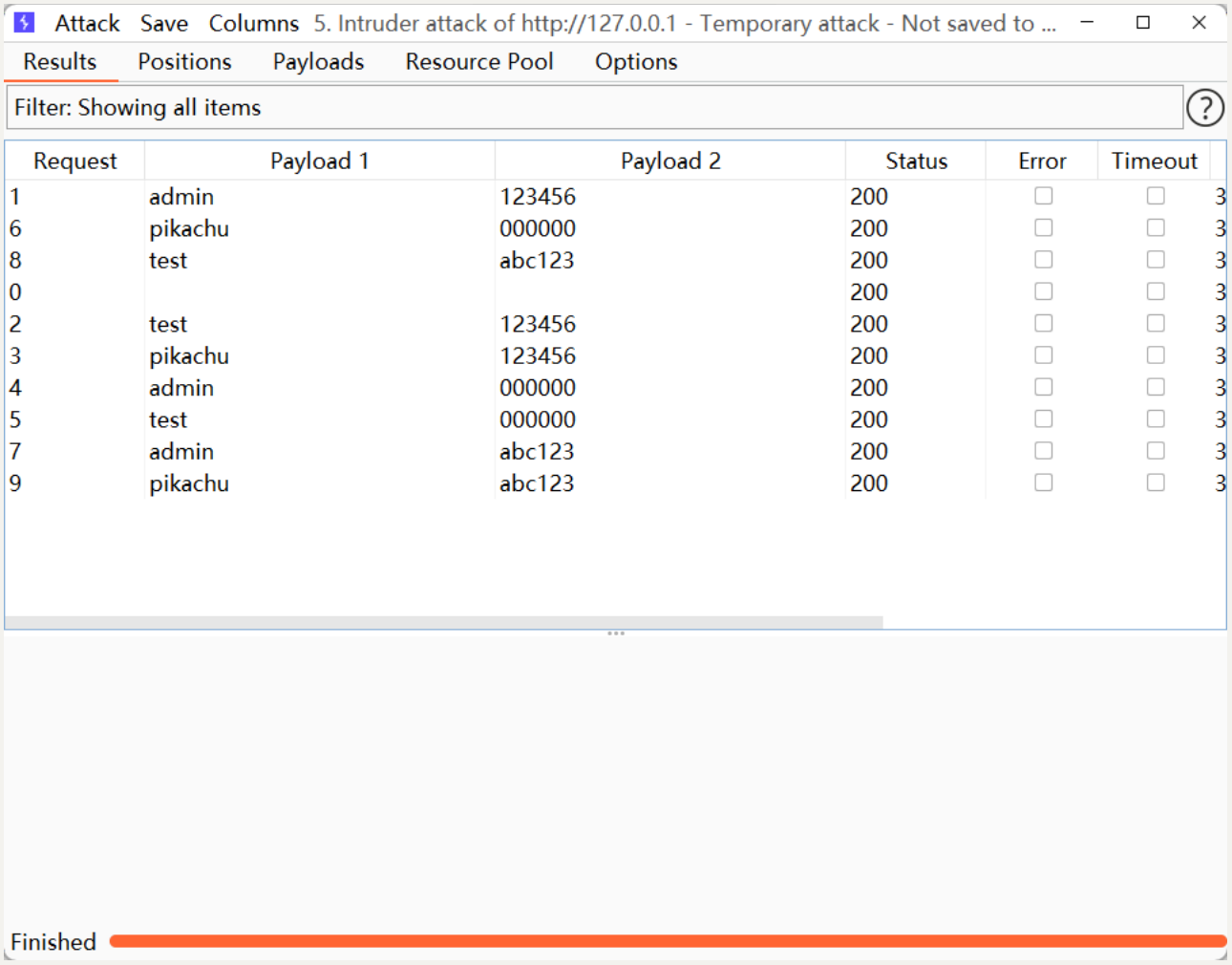


验证码绕过（on client）

1.输入正确验证码才能抓到包后，利用该包发送到模块


Burp Project Intruder Repeater Window Help Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type
98 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 70208 JSON
99 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 46626 JSON
100 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 46935 JSON
101 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 69989 JSON
102 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 70197 JSON
103 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 35416 JSON
104 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 58617 JSON
105 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 46890 JSON
106 https://firefox-settings-attachm... GET /main-workspace/personality-provide... 200 58266 JSON
107 http://127.0.0.1 POST /pikachu/vul/burteforce/bf_server.php ✓ 200 35338 HTML
108 https://getpocket.cdn.mozilla.net GET /v3/firefox/global-recs?version=3&co... ✓ 403 272 HTML
109 http://127.0.0.1 GET /pikachu/vul/burteforce/bf_client.php 200 36505 HTML
110 http://127.0.0.1 POST 36550 HTML
Request
Pretty Raw Hex
1 POST /pikachu/vul/burteforce/bf_client.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 52
9 Origin: http://127.0.0.1
Search... 0 matches
Response
Pretty Raw
http://127.0.0.1/pikachu/vul/burteforce/bf_client.php
Add to scope
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools
Show new history window
Add comment

照旧写入密码本，爆破



这里也可以直接禁用JS

就和第一个一样简单了

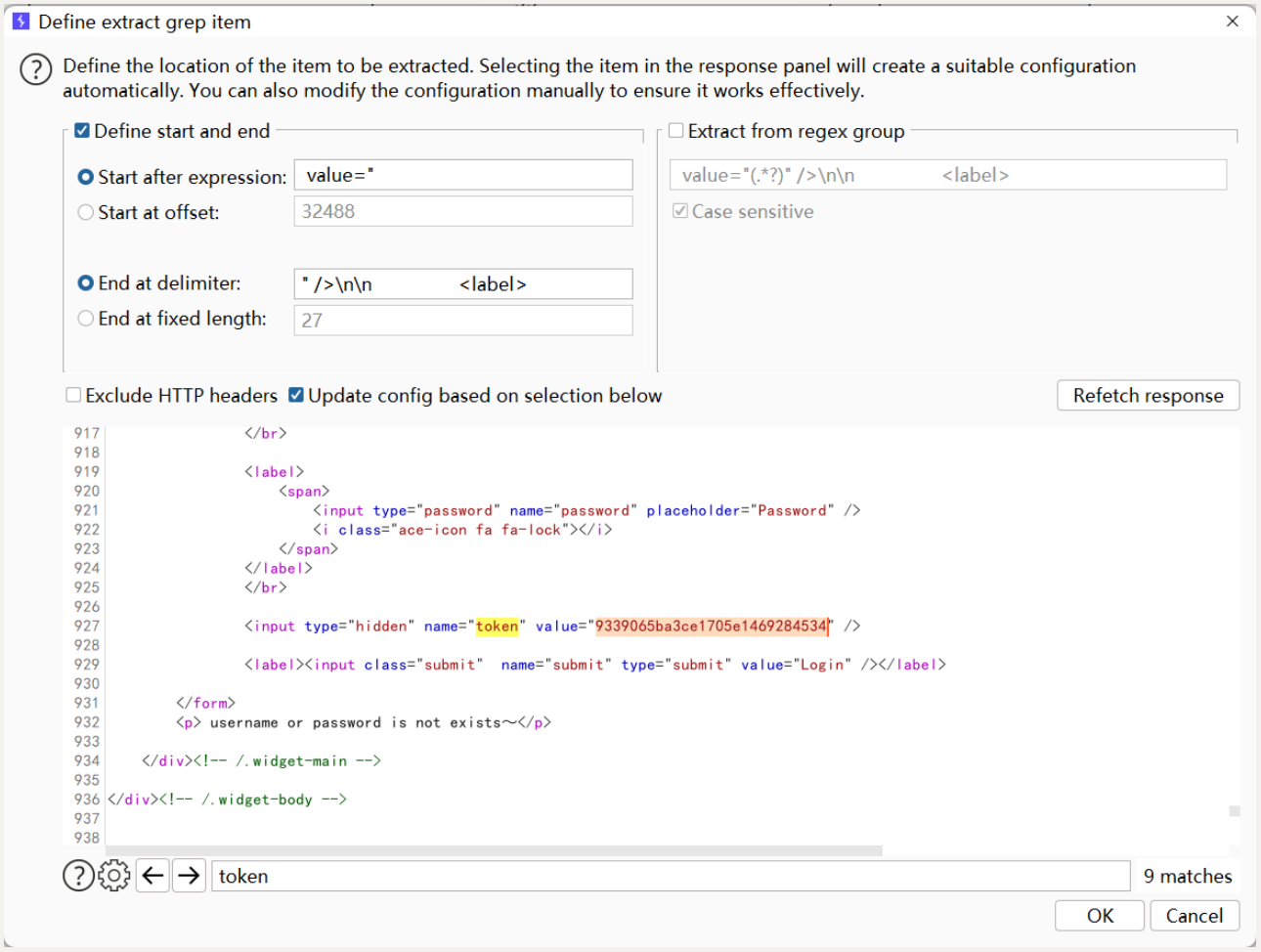
token防爆破

经过几次抓包发现本次token值就是上次服务器发送回来的token值，所以用递归来重定向token（题目默认知道账户名，所以还是两个变量，使用鱼叉是因为第二个变量token是每次都重定向）

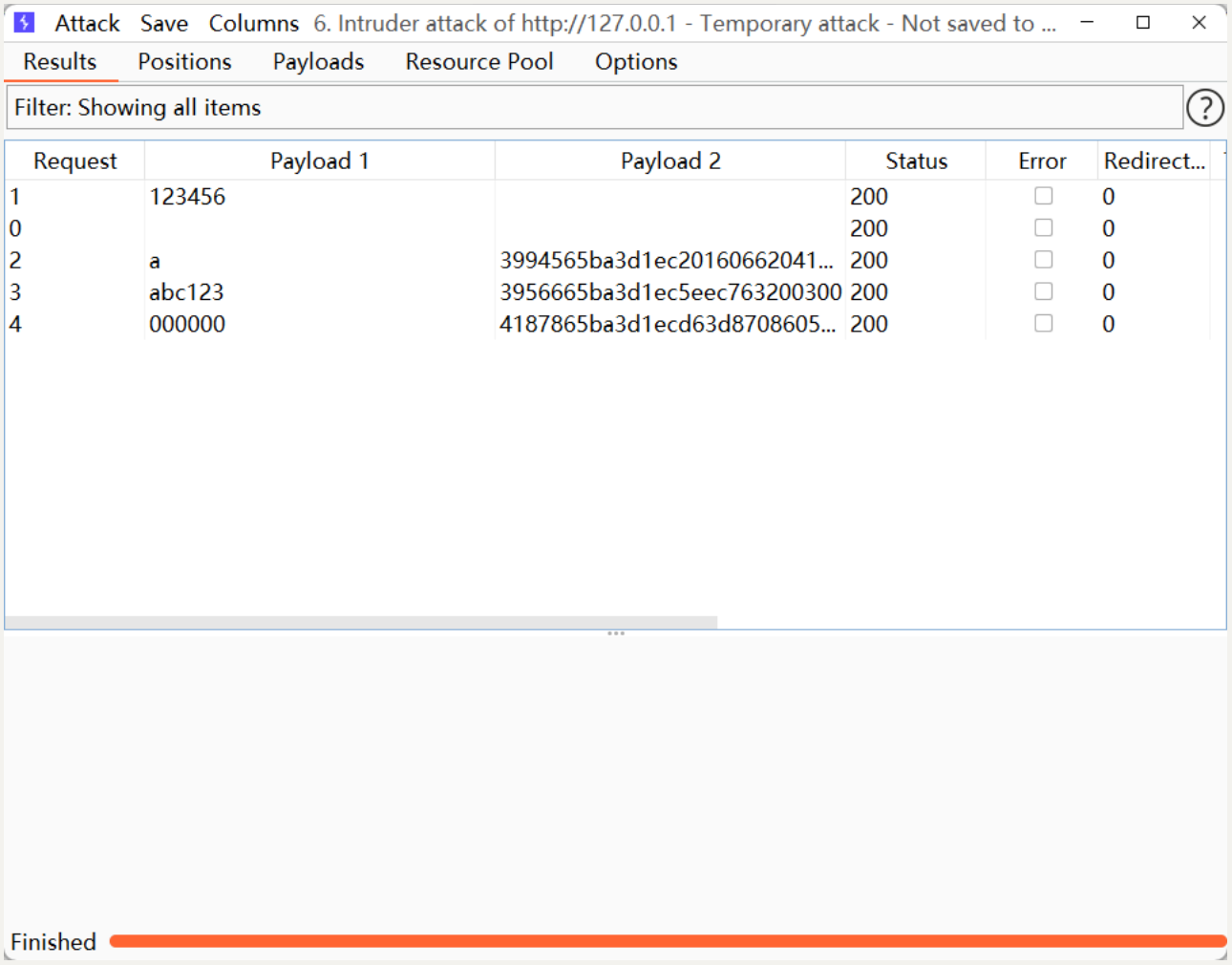
1.先抓包

2.写入密码，并定义线程为1，因为每一次循环后重定向，不是单线程token引用就乱了

3.设置重定向



爆破


Attack Save Columns 6. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to ...
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Redirect...
1 123456 200 0
0 200 0
2 a 3994565ba3d1ec20160662041... 200 0
3 abc123 3956665ba3d1ec5eec763200300 200 0
4 000000 4187865ba3d1ecd63d8708605... 200 0
Finished