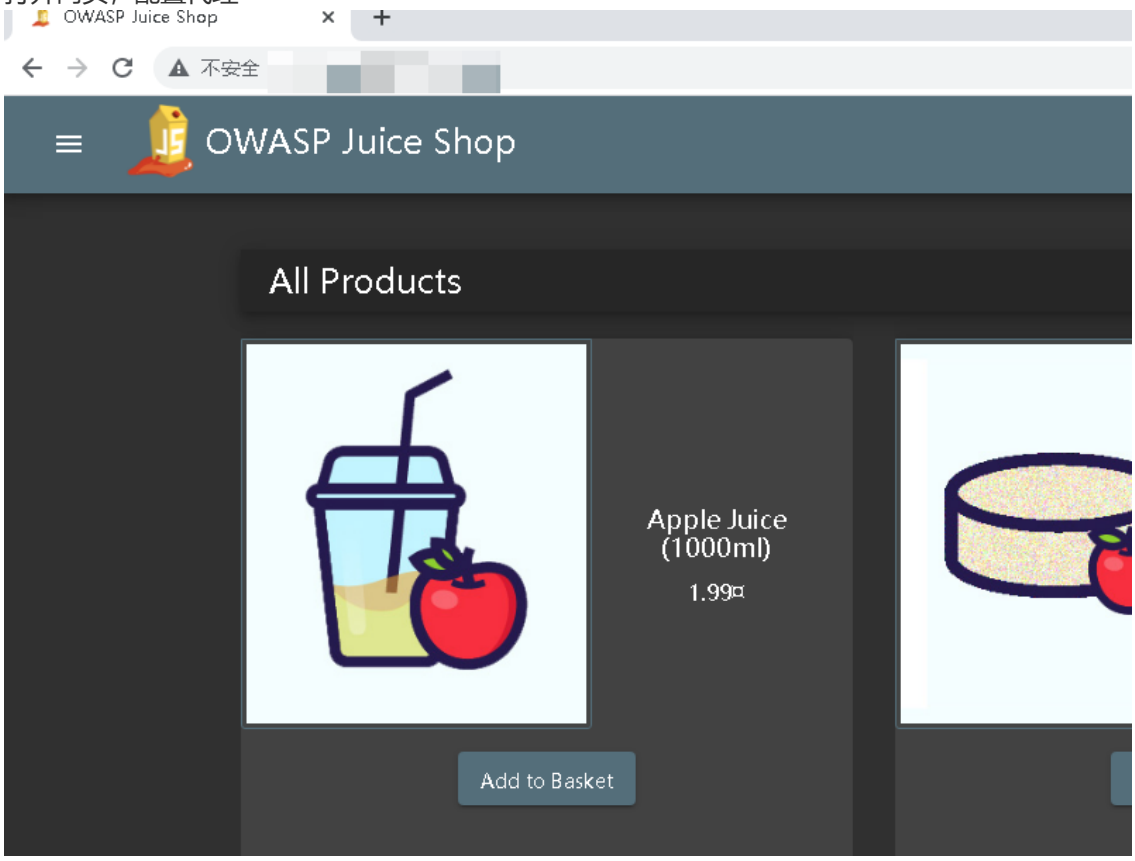
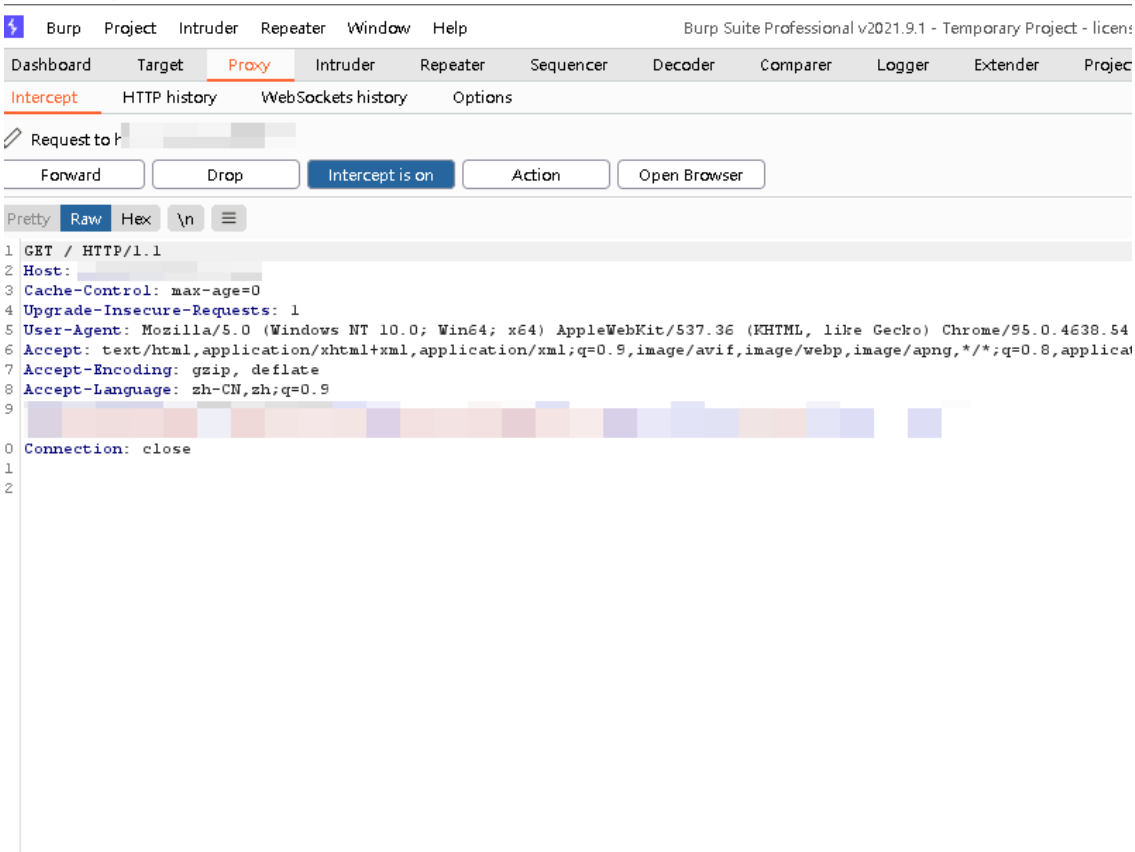
Intruder模块实战

sniper攻击方式

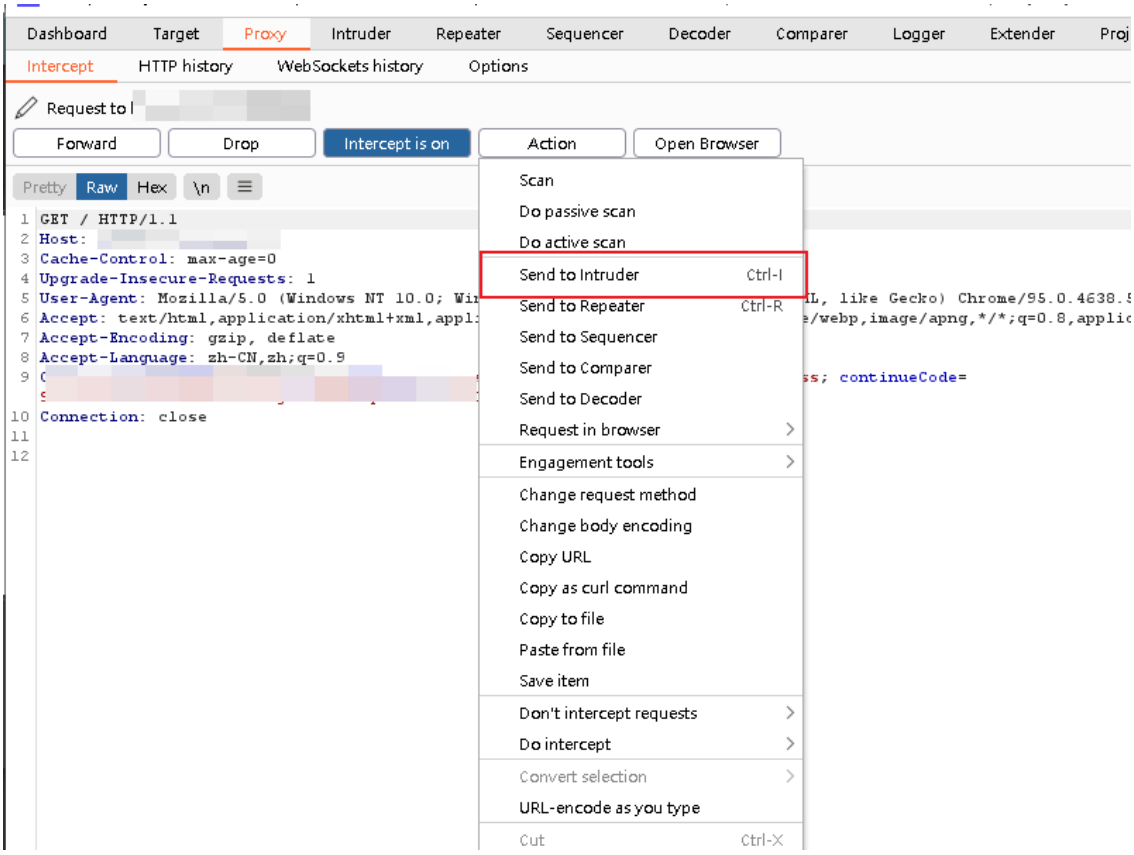
1. 打开网页，配置代理



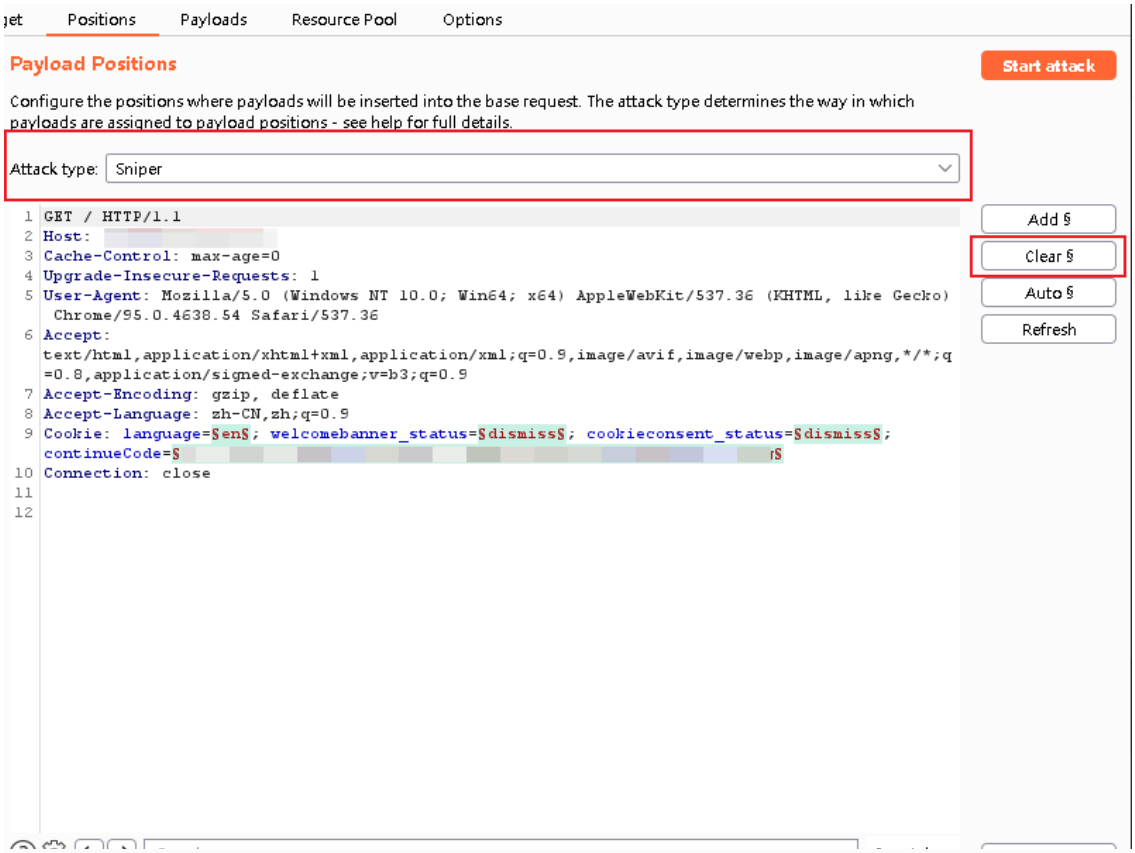
2. 开启Porxy拦截，抓取刷新页面的数据包

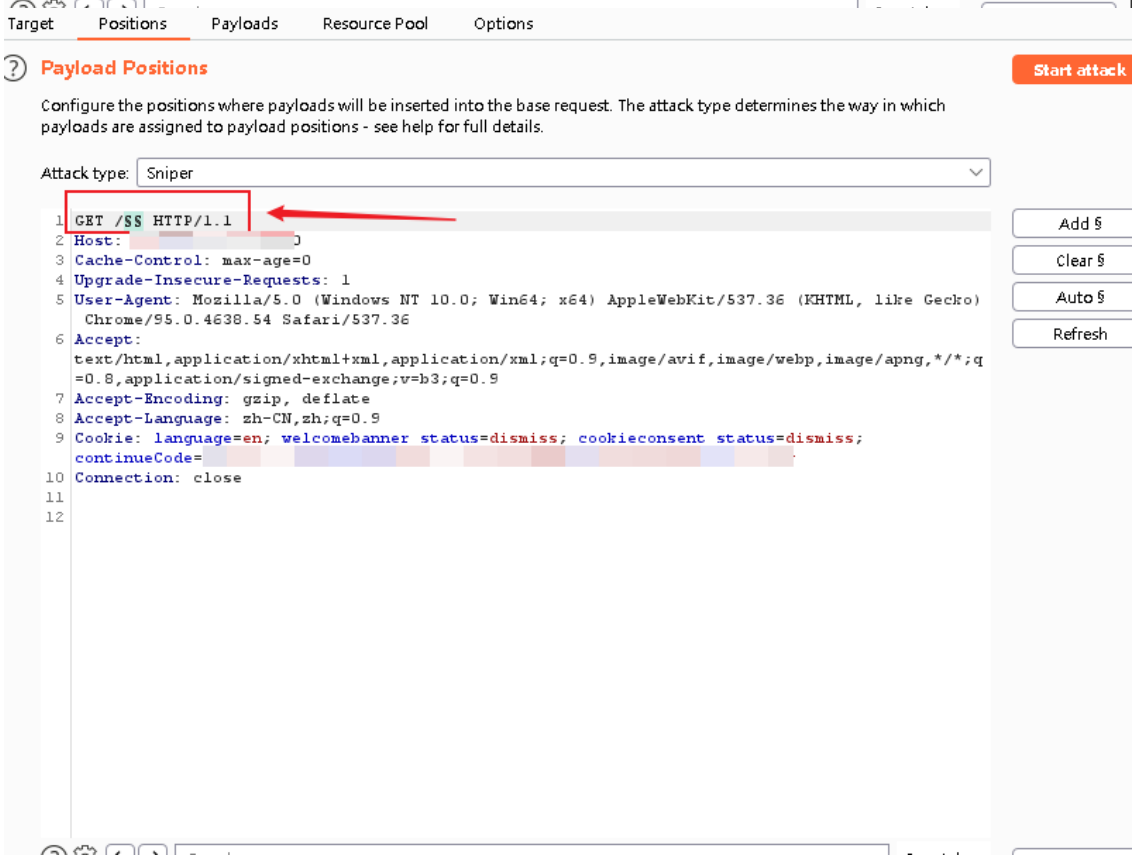


3. 发送拦截数据包到Intruder模块

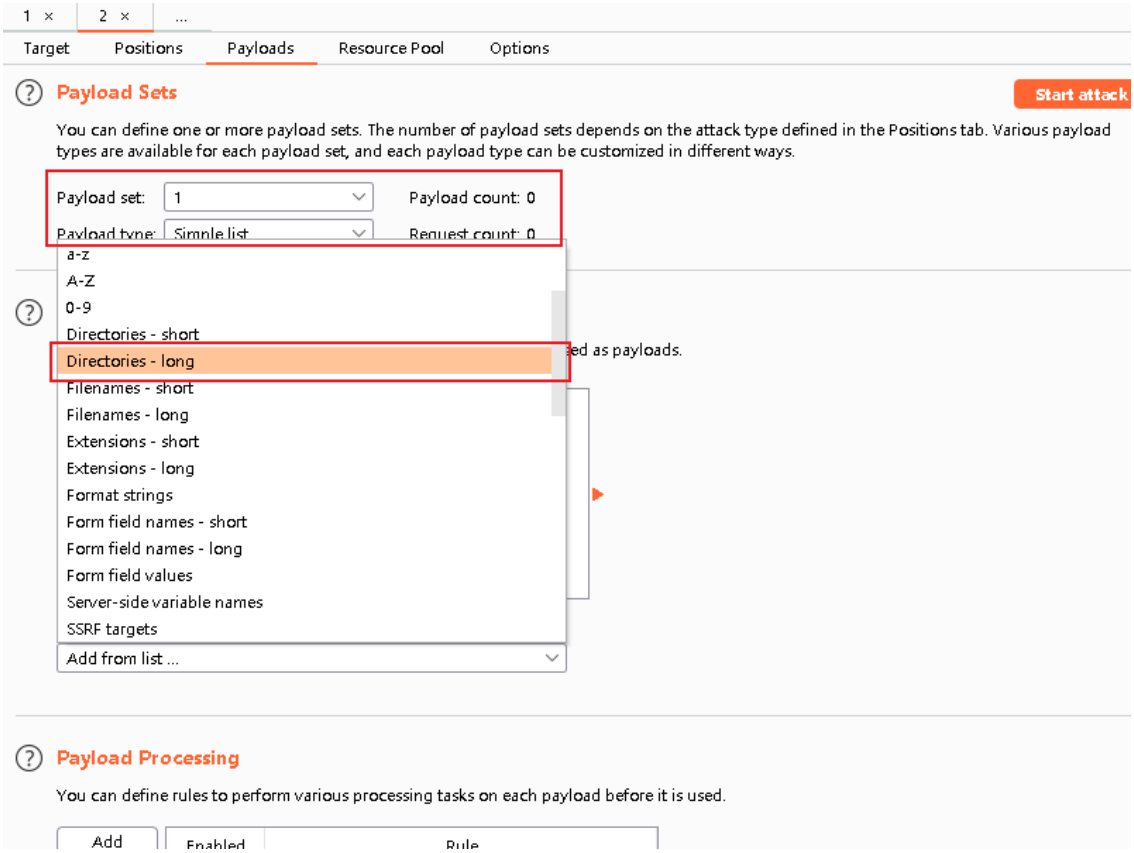


4. 设置Attack type攻击方式为Sniper，清除Burp自动设置的攻击标记位置，在GET请求的/后添加标记位置

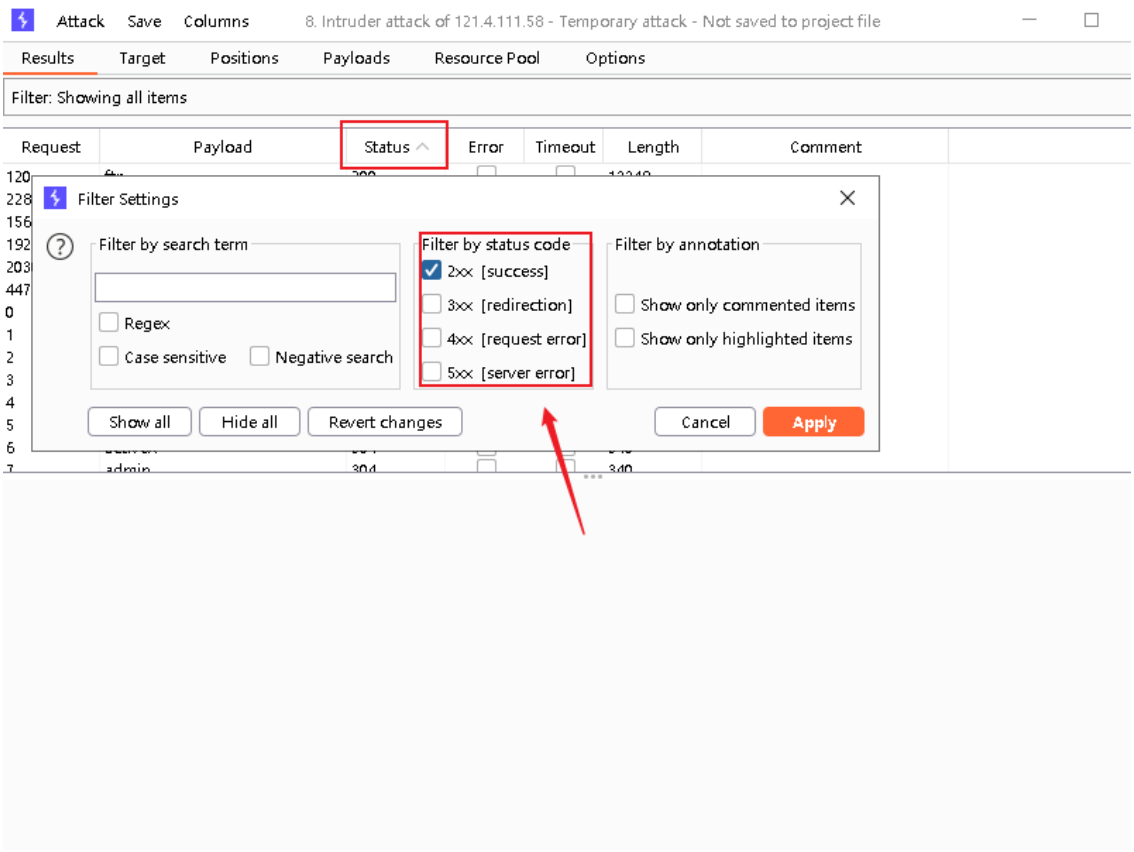

Positions
Payloads
Resource Pool
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET / HTTP/1.1
Host:
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: language=en; welcomebanner_status=$dismiss$; cookieconsent_status=$dismiss$;
continueCode=$
Connection: close
Add §
Clear §
Auto §
Refresh


Target
Positions
Payloads
Resource Pool
Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /§§ HTTP/1.1
Host:
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=
Connection: close
Add §
Clear §
Auto §
Refresh

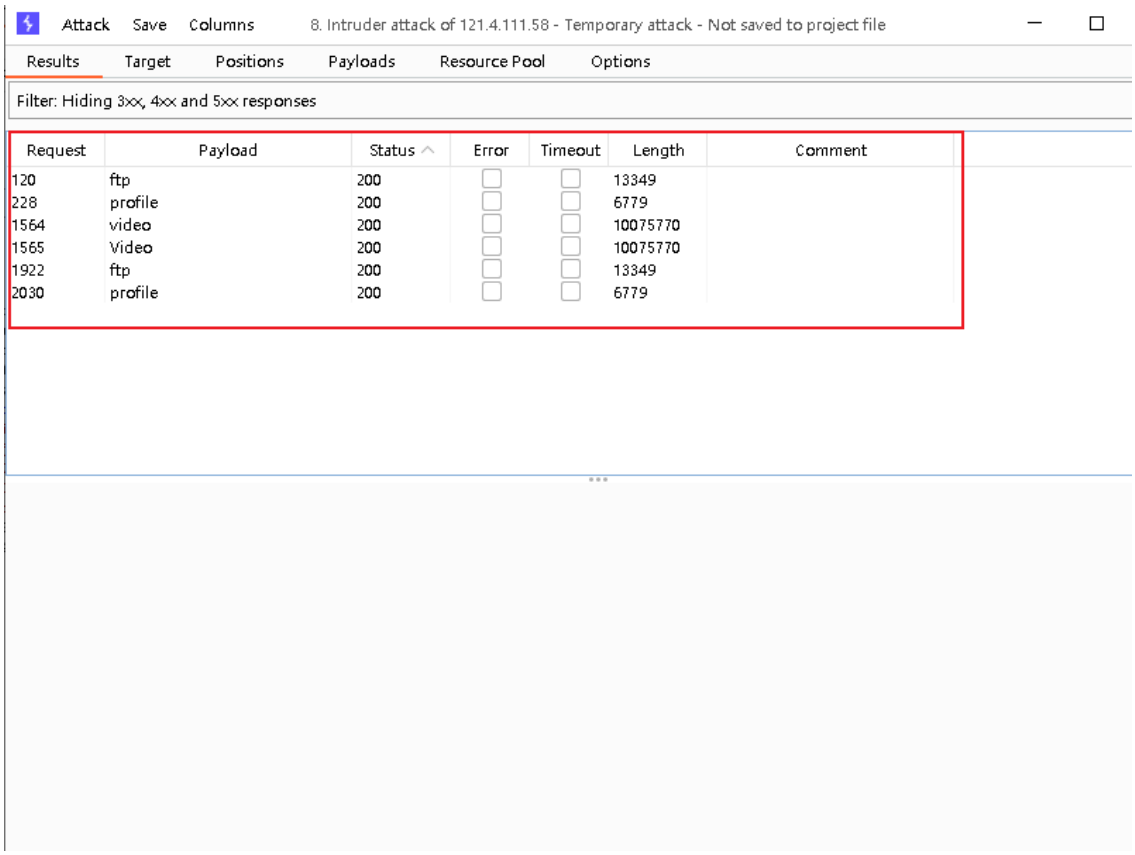
5. 设置Payload type为simple list，添加目录的密码字典



6. 开启攻击，利用HTTP状态码筛选存在的目录名

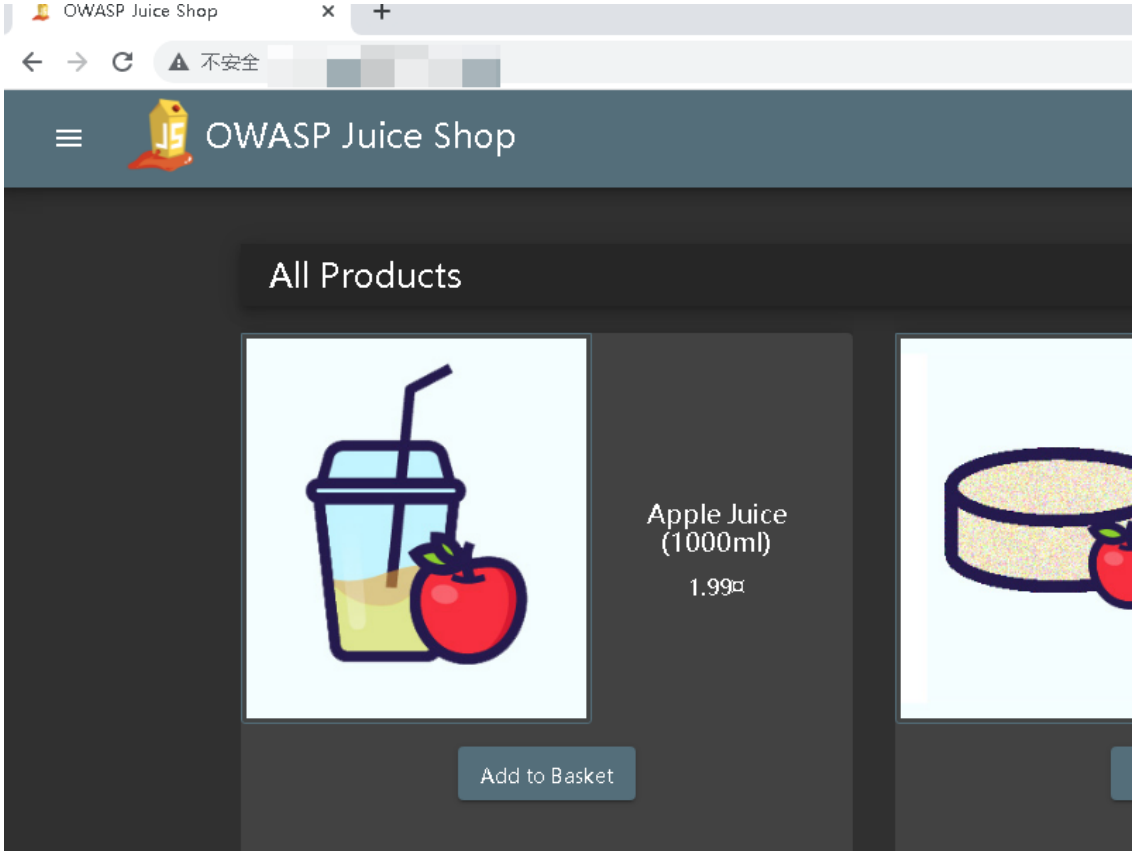


7. 成功爆破出服务器真实存在的目录

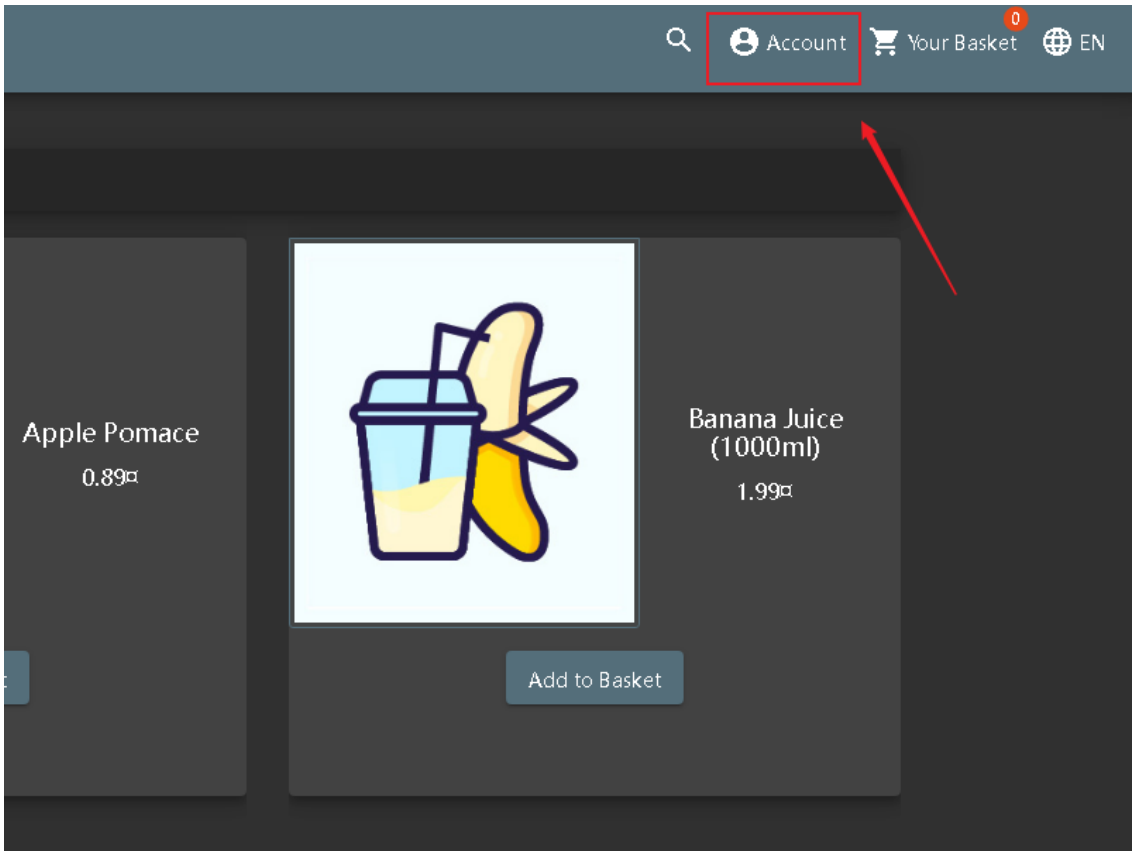


Cluster bomb

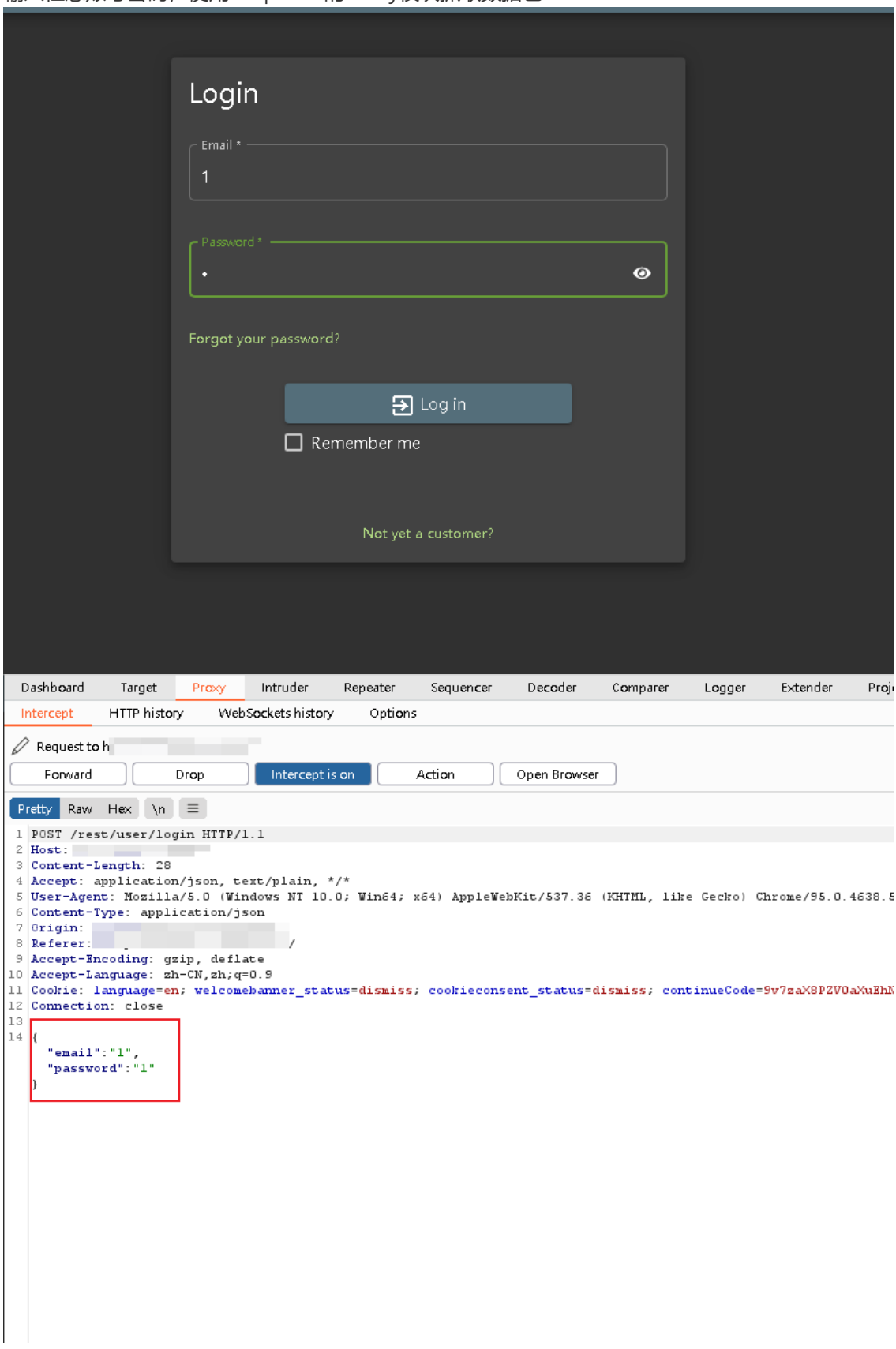
1. 打开网页，配置代理



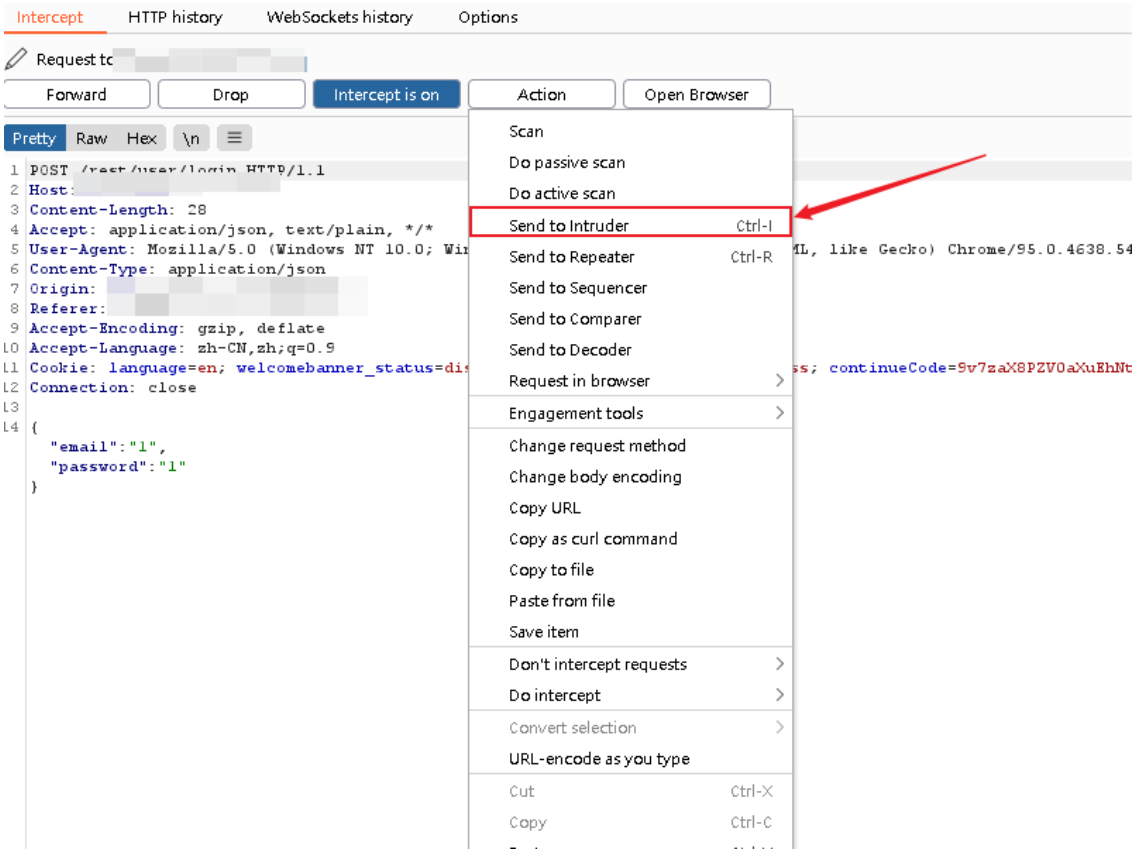
2. 点击Account尝试登陆



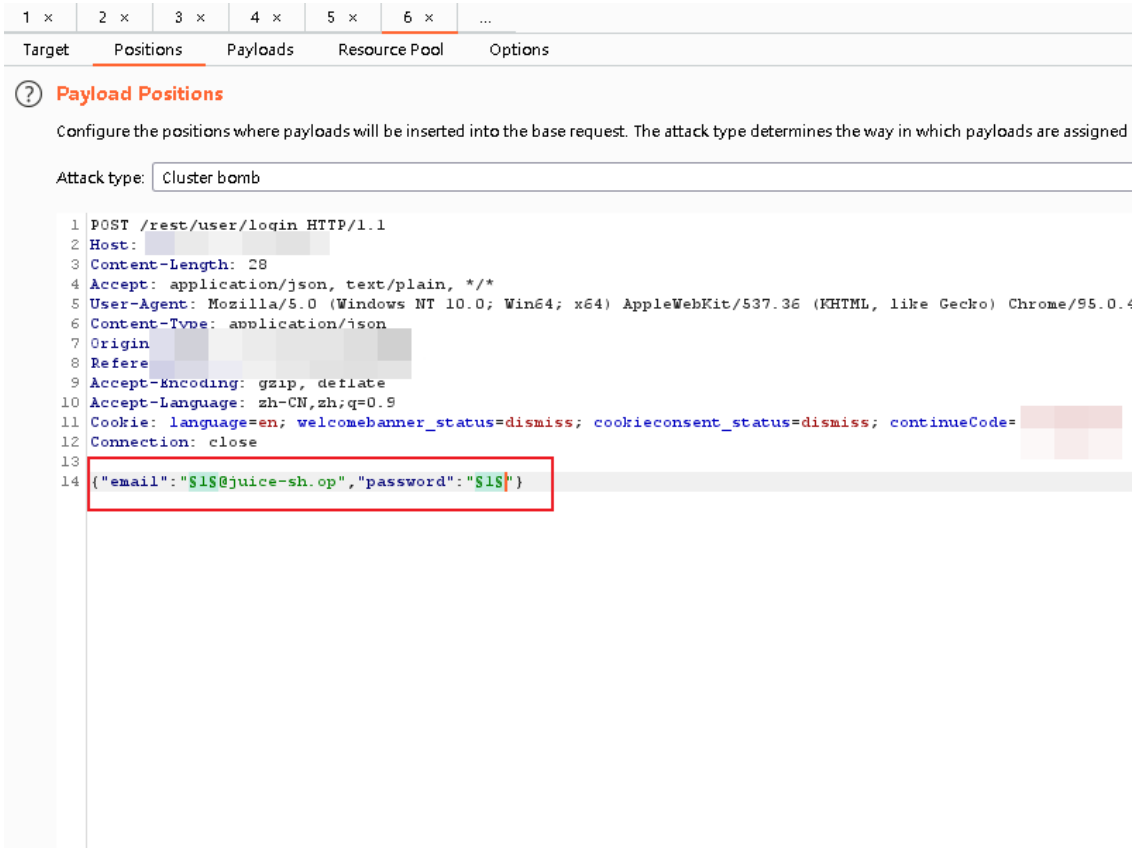
3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包



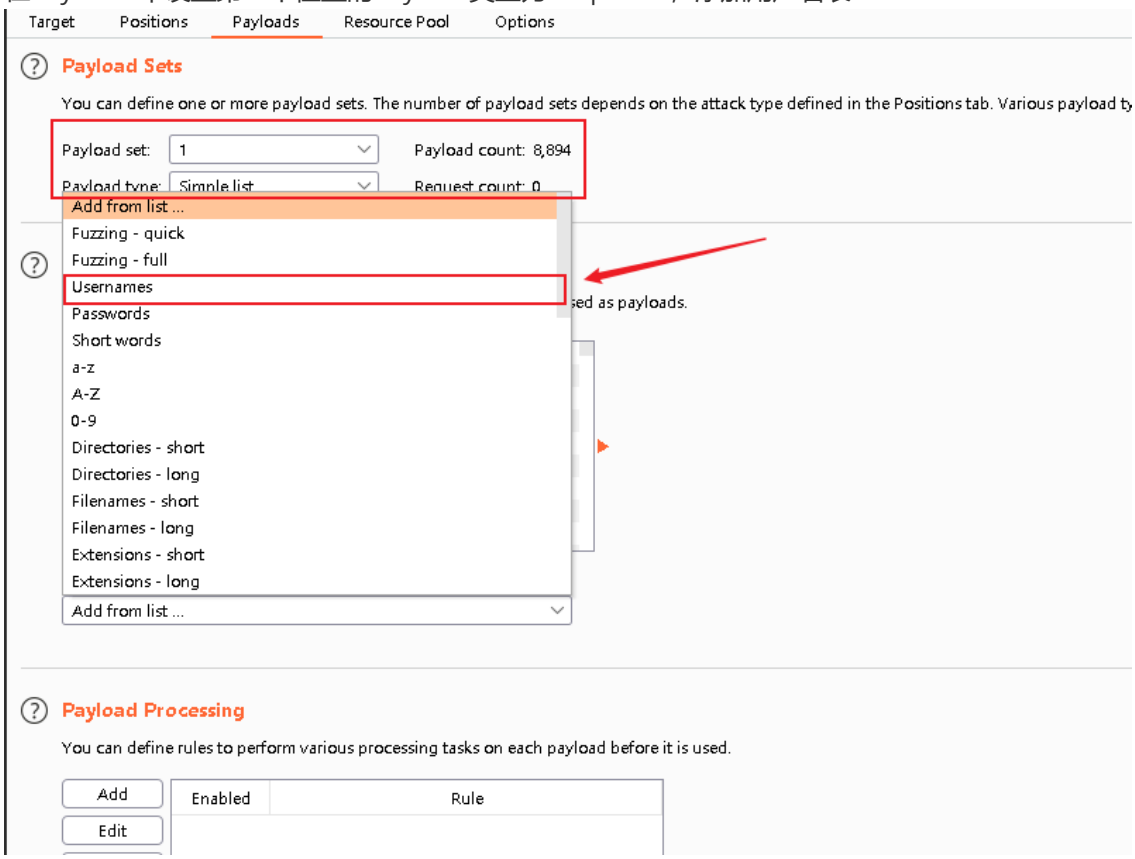
4. 发送到Intruder模块



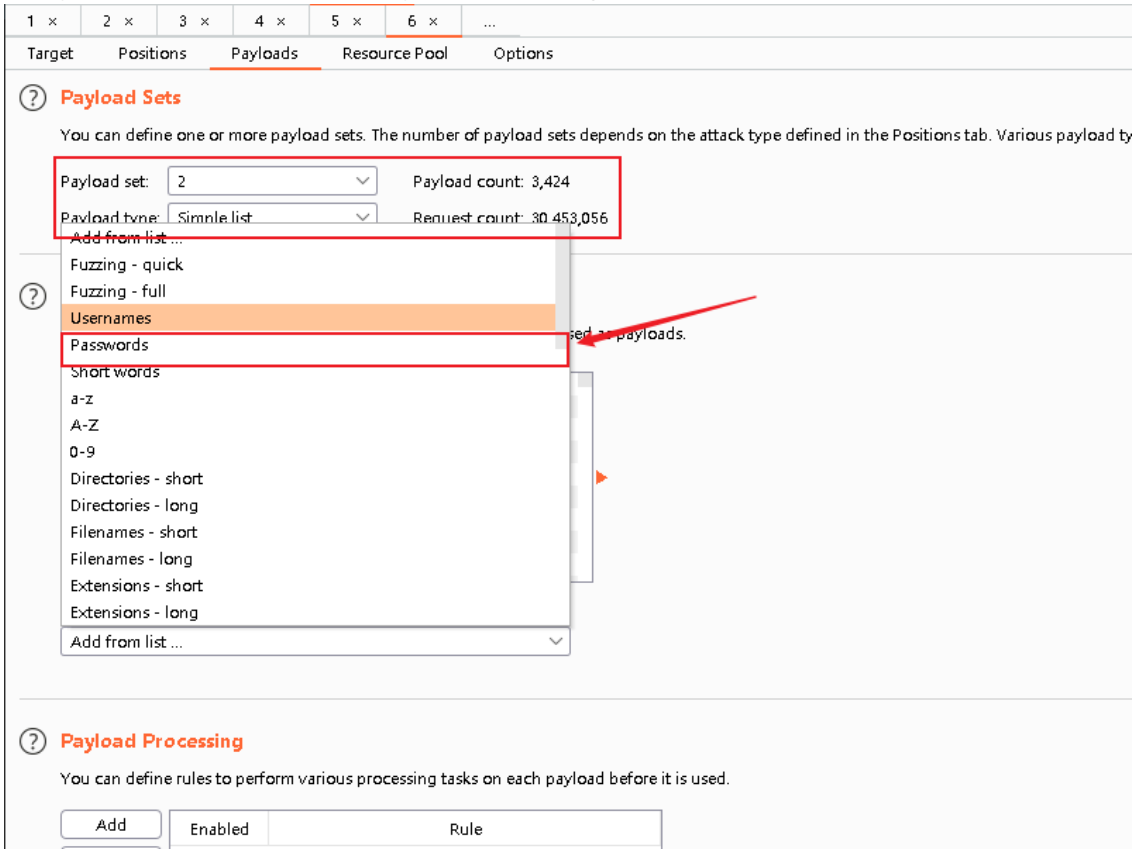
5. 设置Attack type攻击方式为Cluster Bomb，清除Burp自动设置的攻击标记位置，在email和password位置设置标记



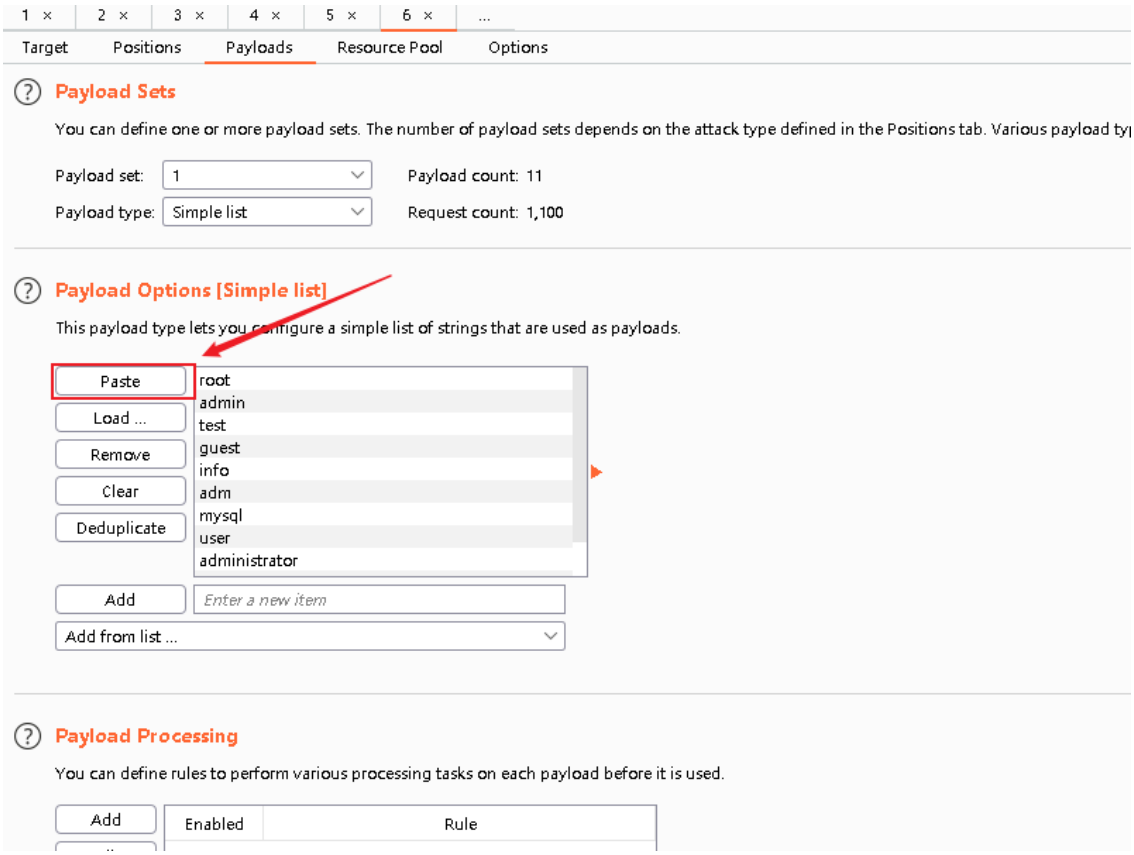
6. 在Payloads中设置第一个位置的Payload类型为simple list，添加用户名表



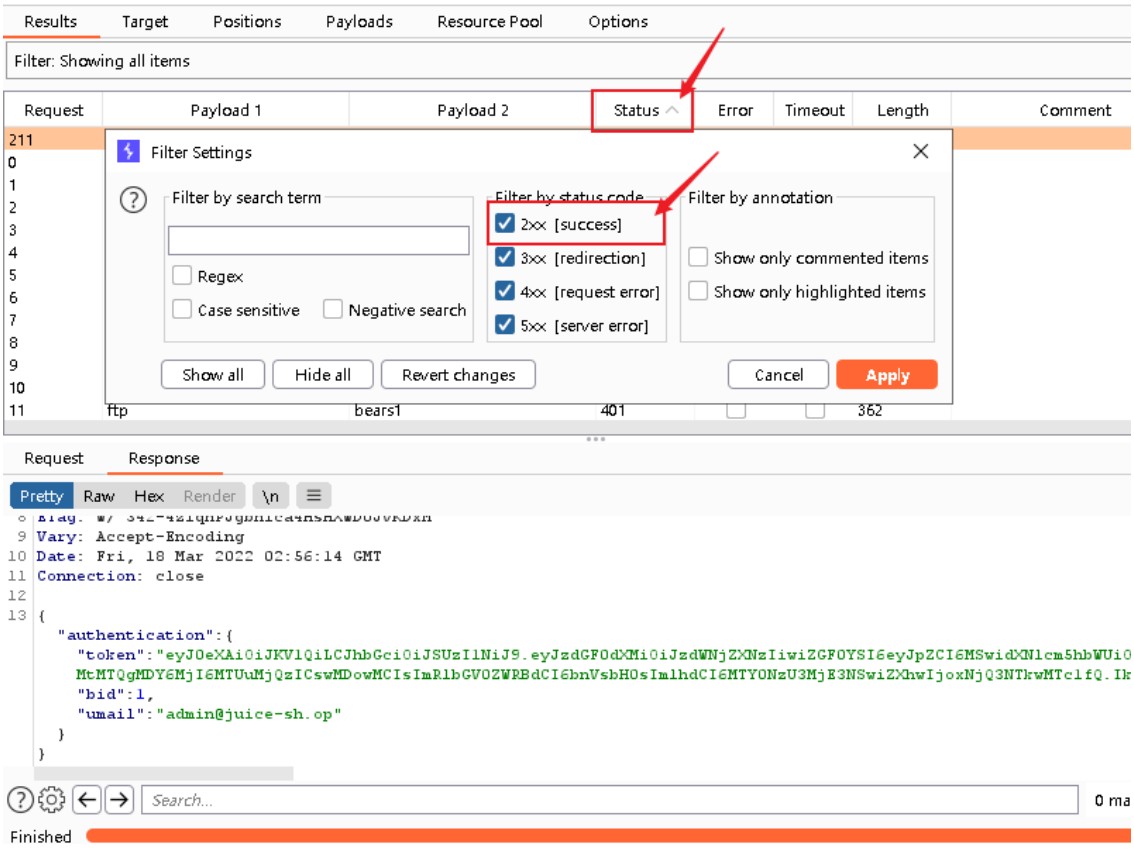
在Payloads中设置第二个位置的Payload类型为simple list，添加密码表



7. 或粘贴用户名和密码表

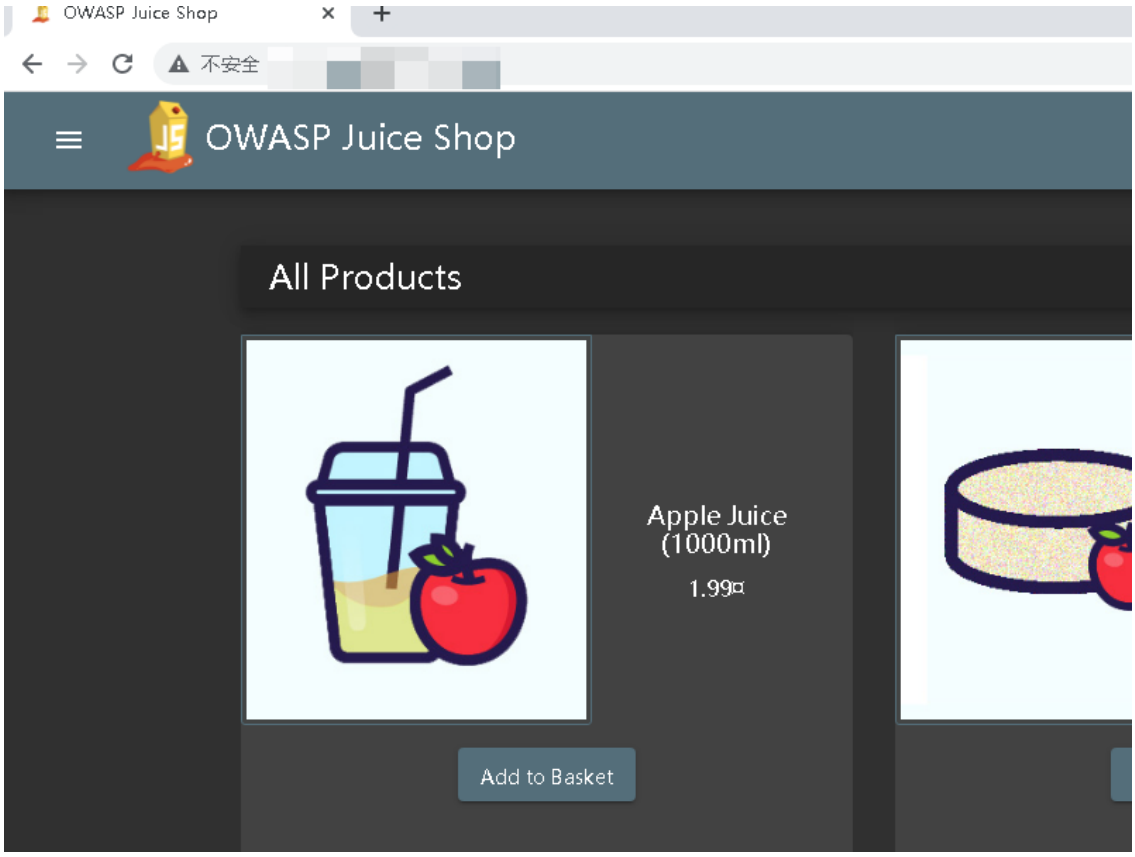


8. 开启攻击后利用HTTP状态码排序或Filter排序筛选账号名和密码

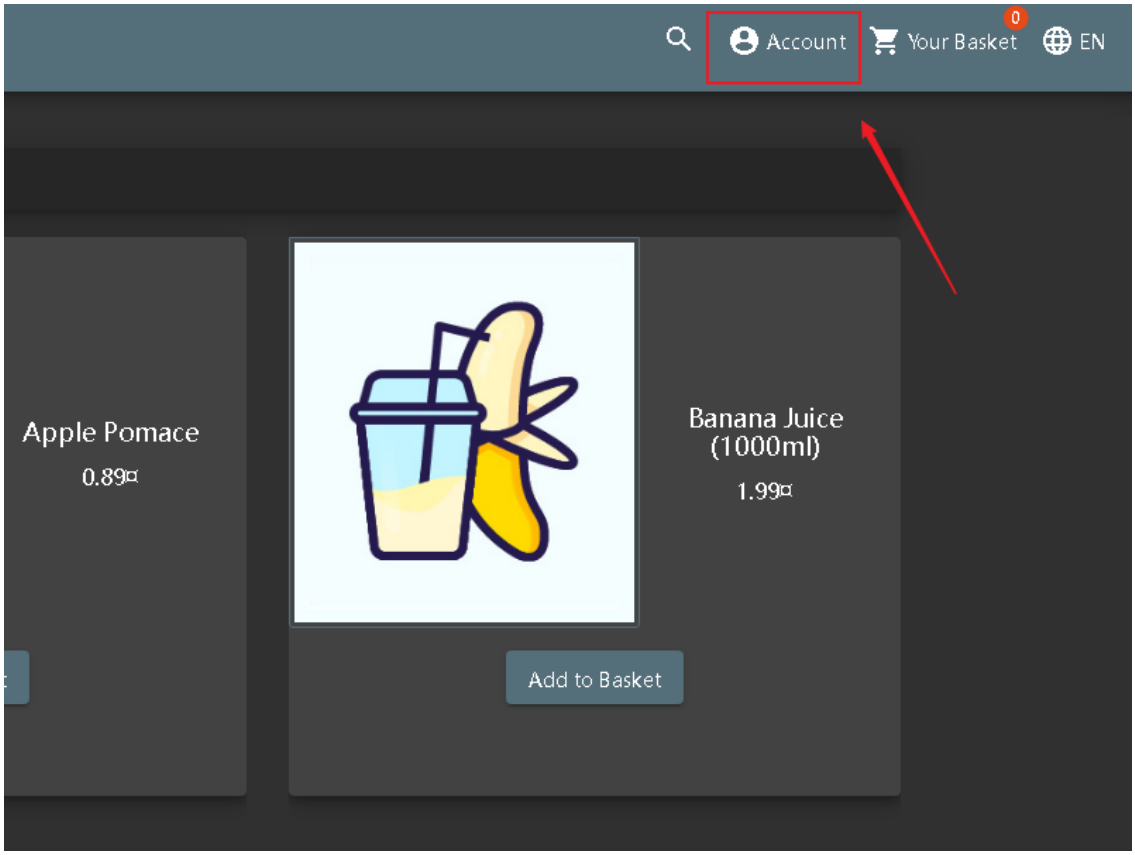


Pitfork

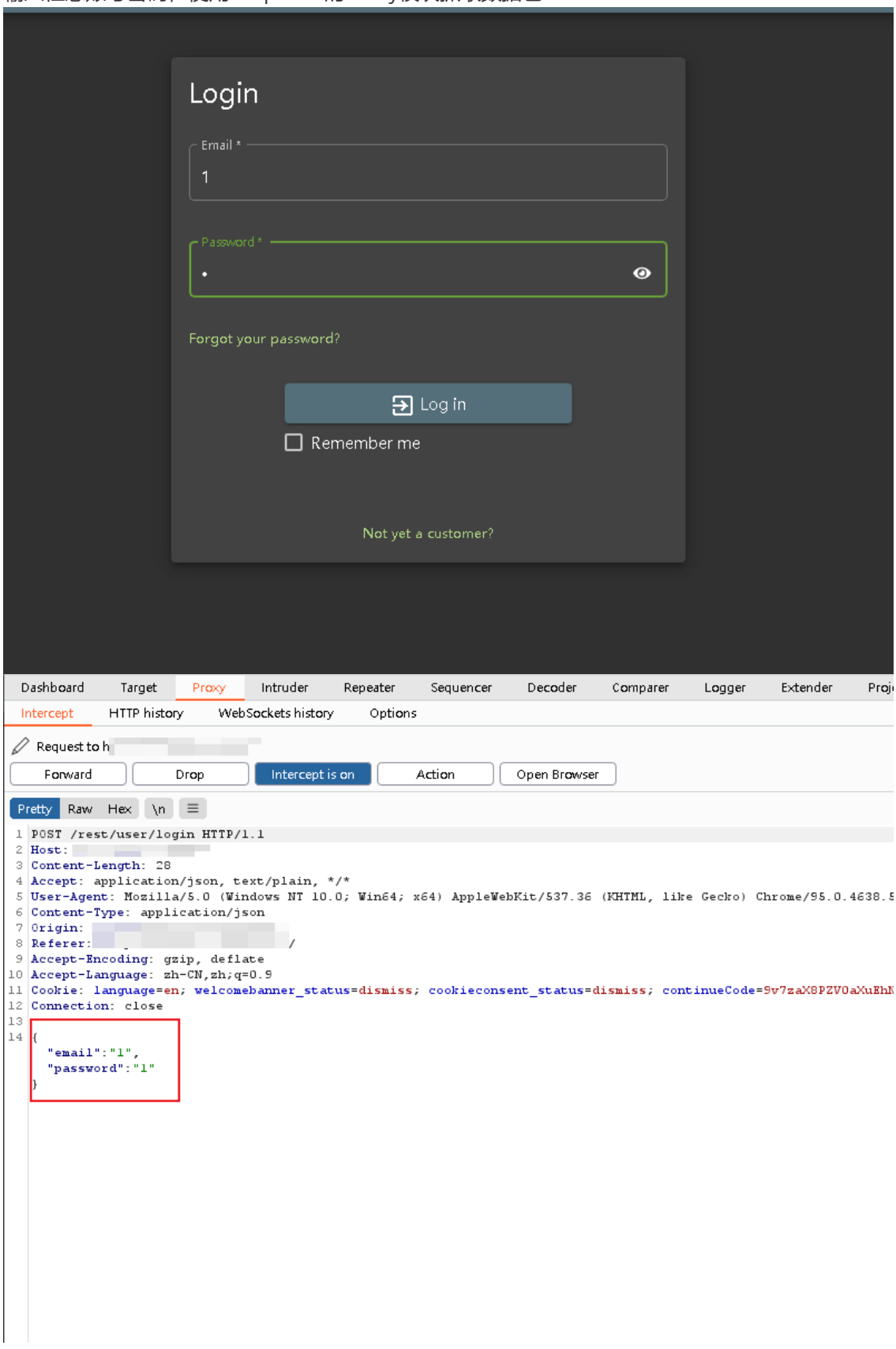
1. 打开网页，配置代理，需先行注册账号保证后缀一致（如1@mail.com和2@mail.com或1@t.com和2@t.com）



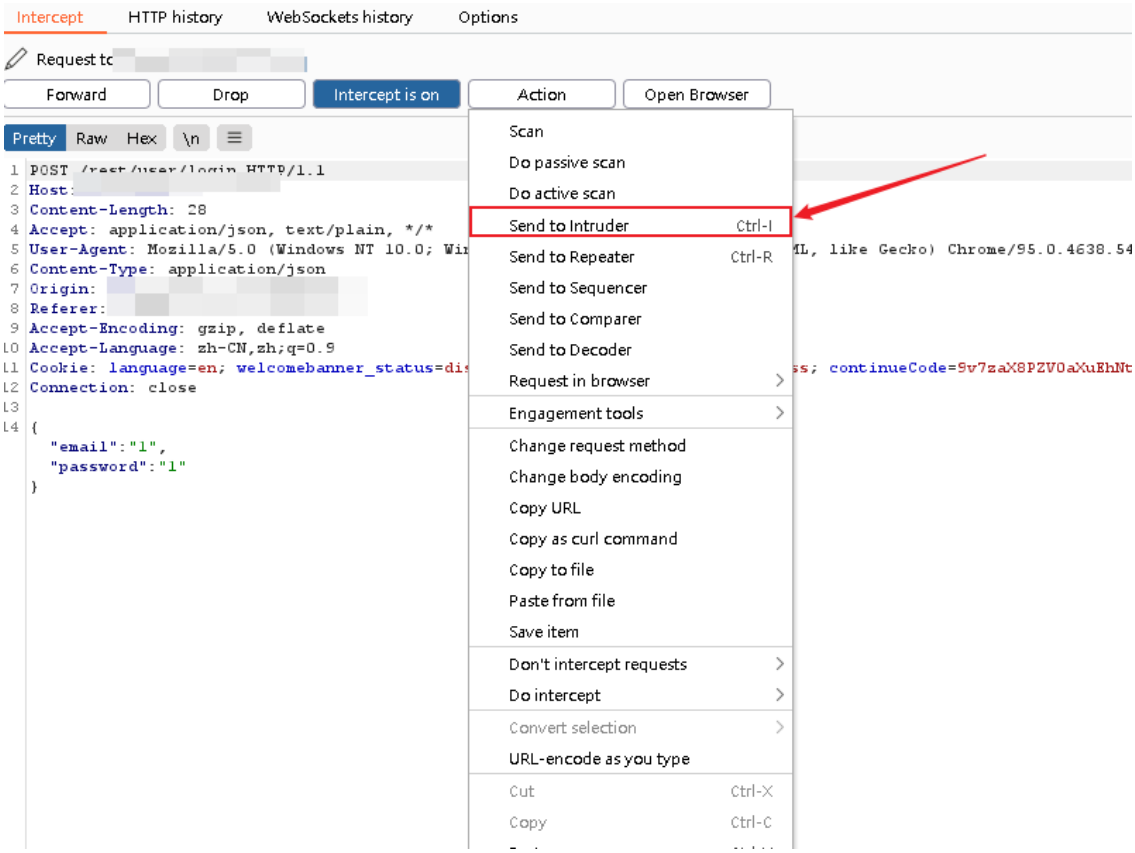
2. 点击Account尝试登陆



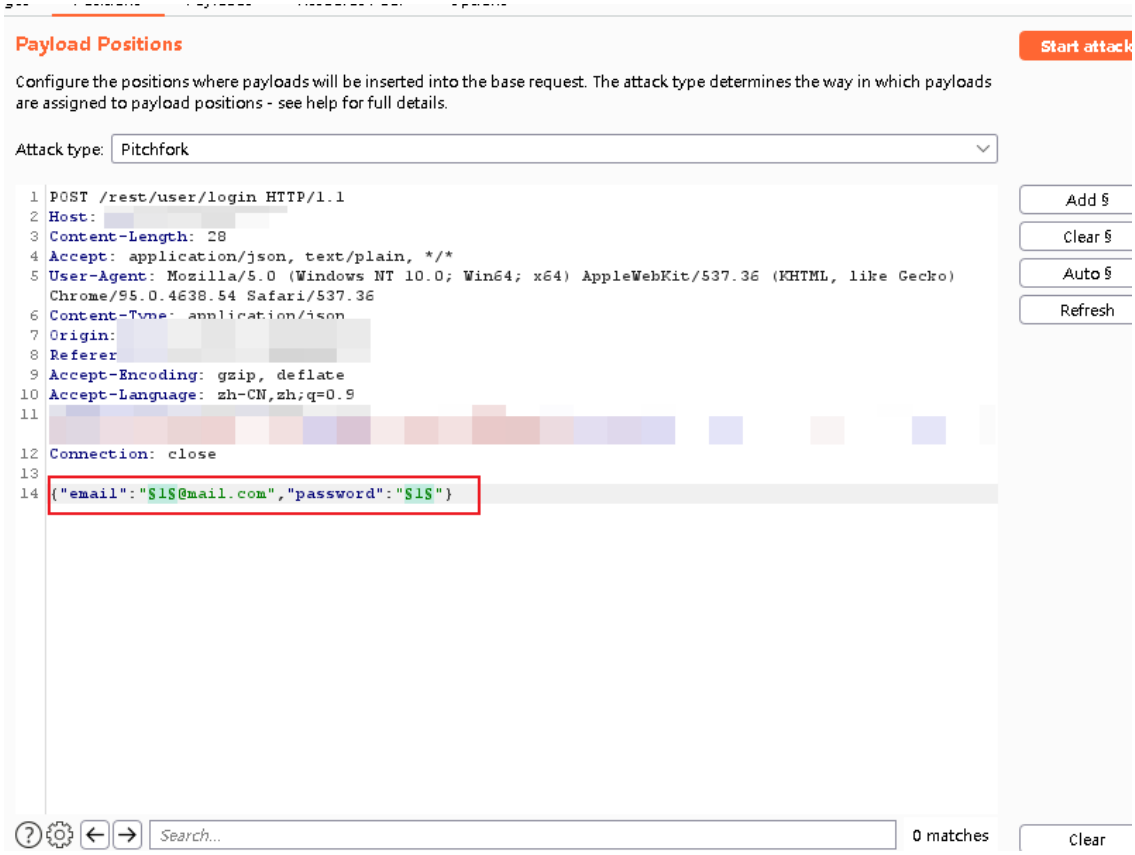
3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包



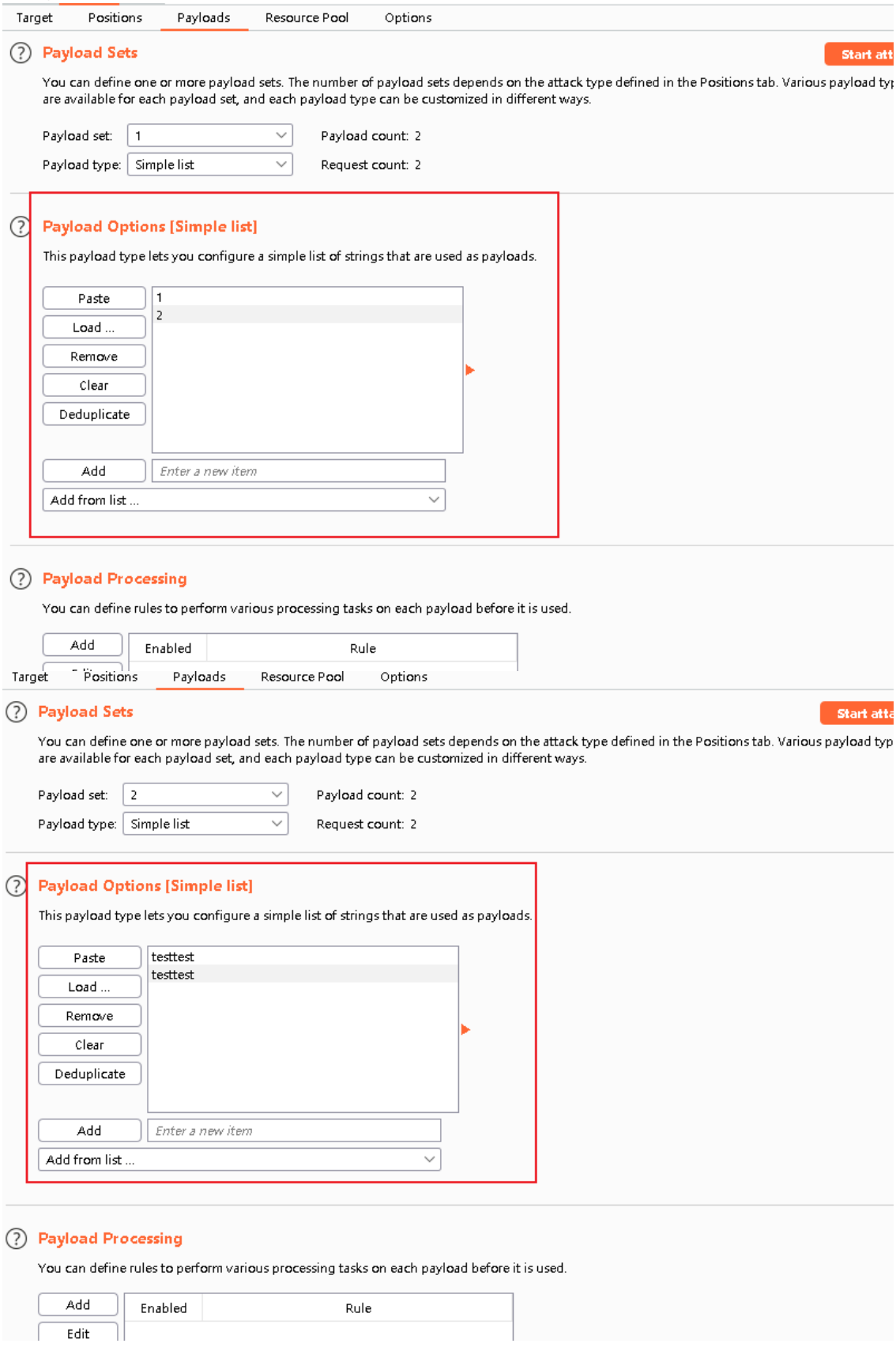
4. 发送到Intruder模块



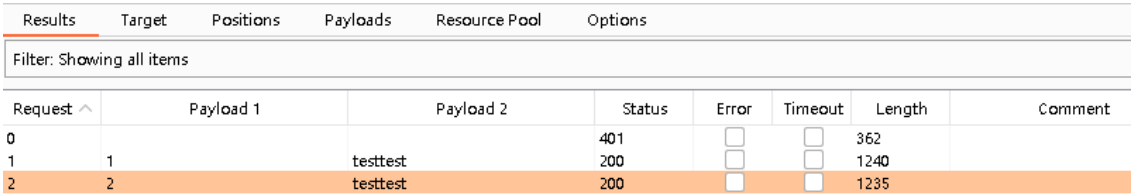
5. 设置Attack type攻击方式为Pitfork，清除Burp自动设置的攻击标记位置，在email和password位置设置标记

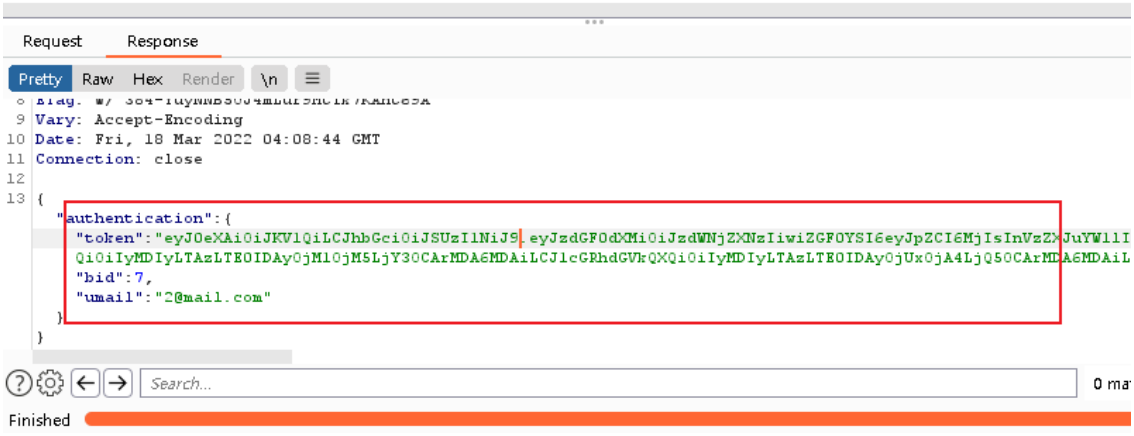


6. 在Payload中粘贴用户名和密码



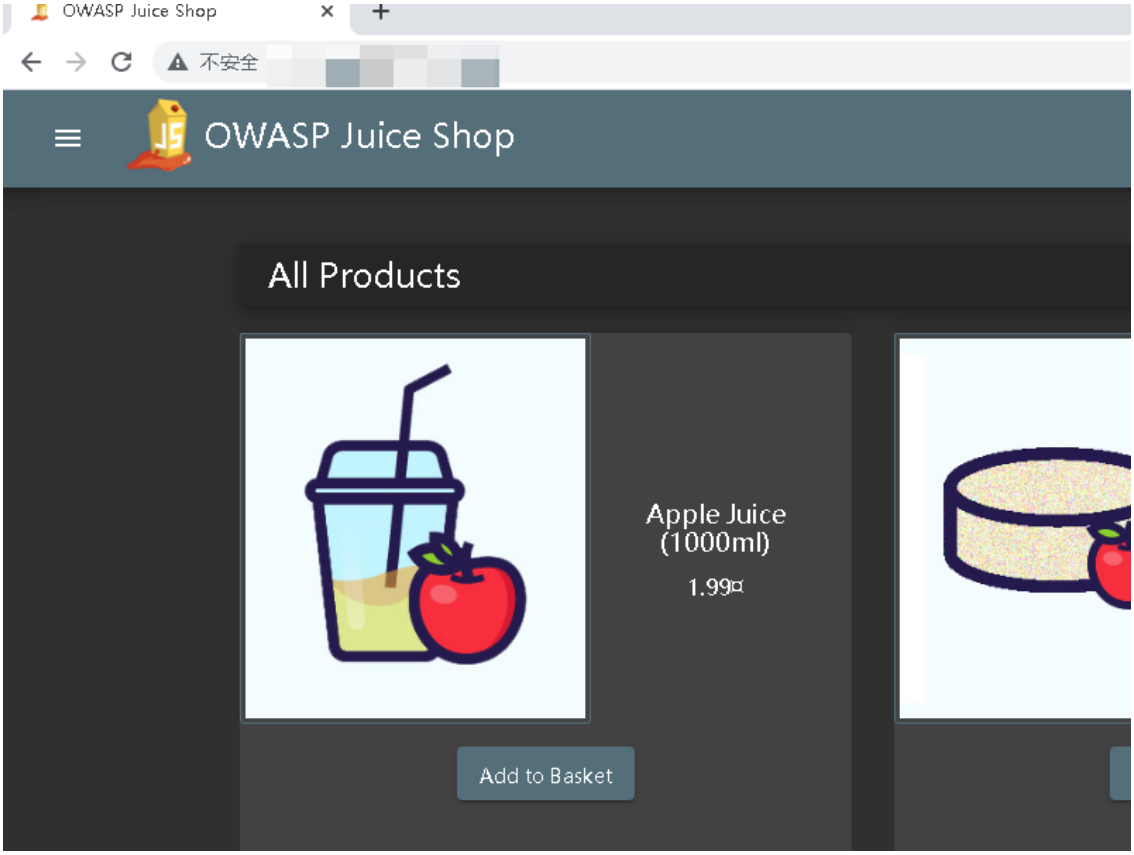
7. 开启攻击，成功返回



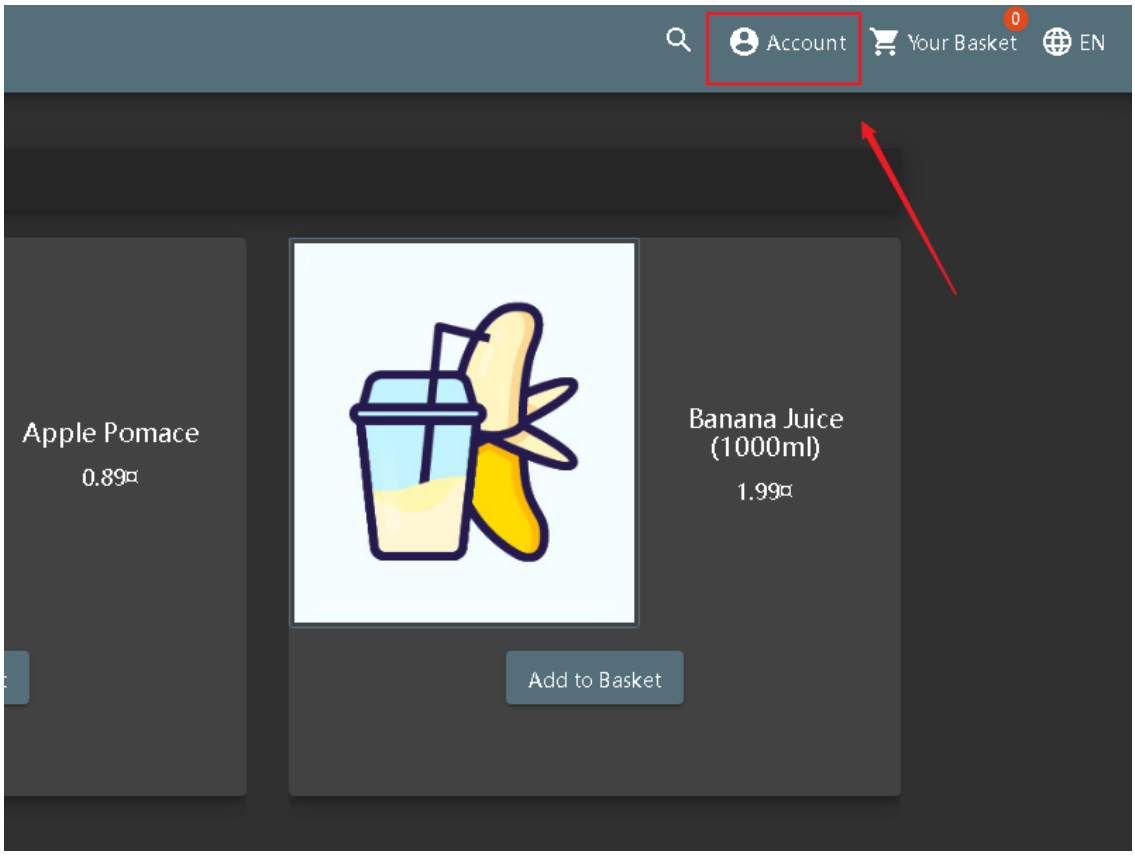


Battering ram

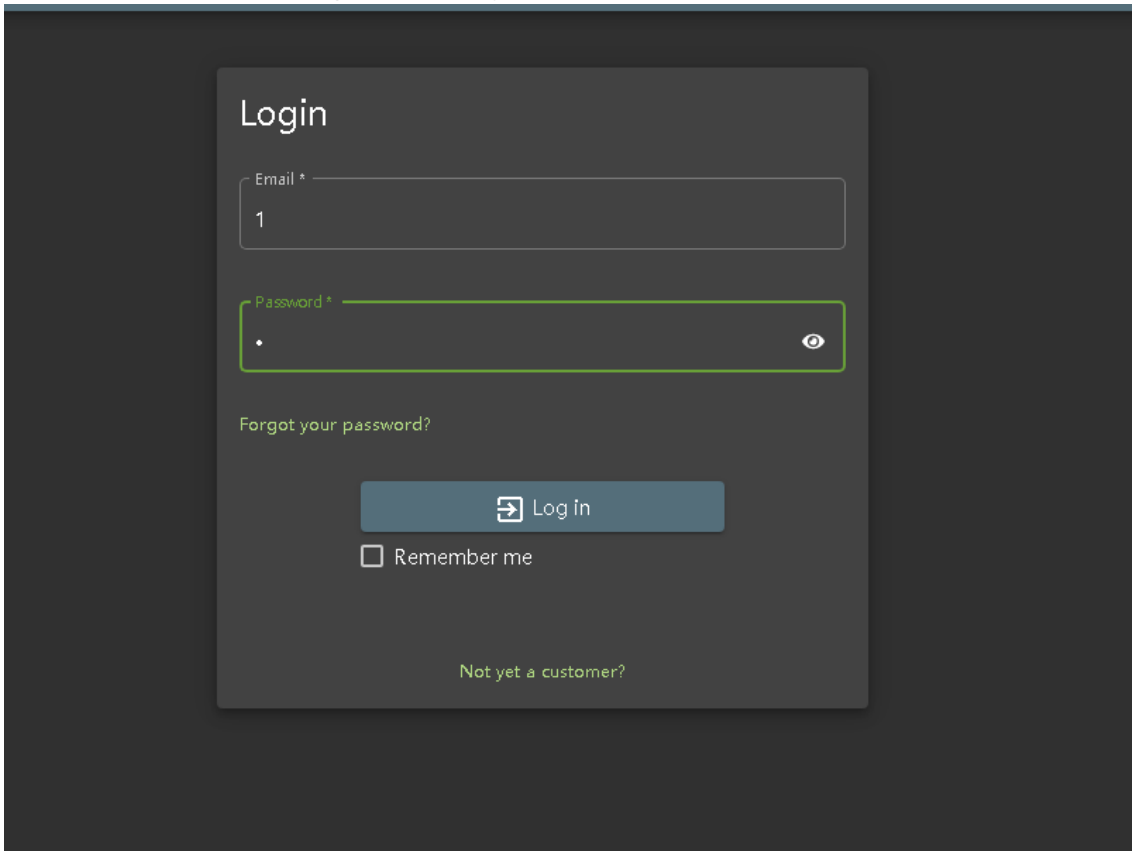
1. 打开网页，配置代理

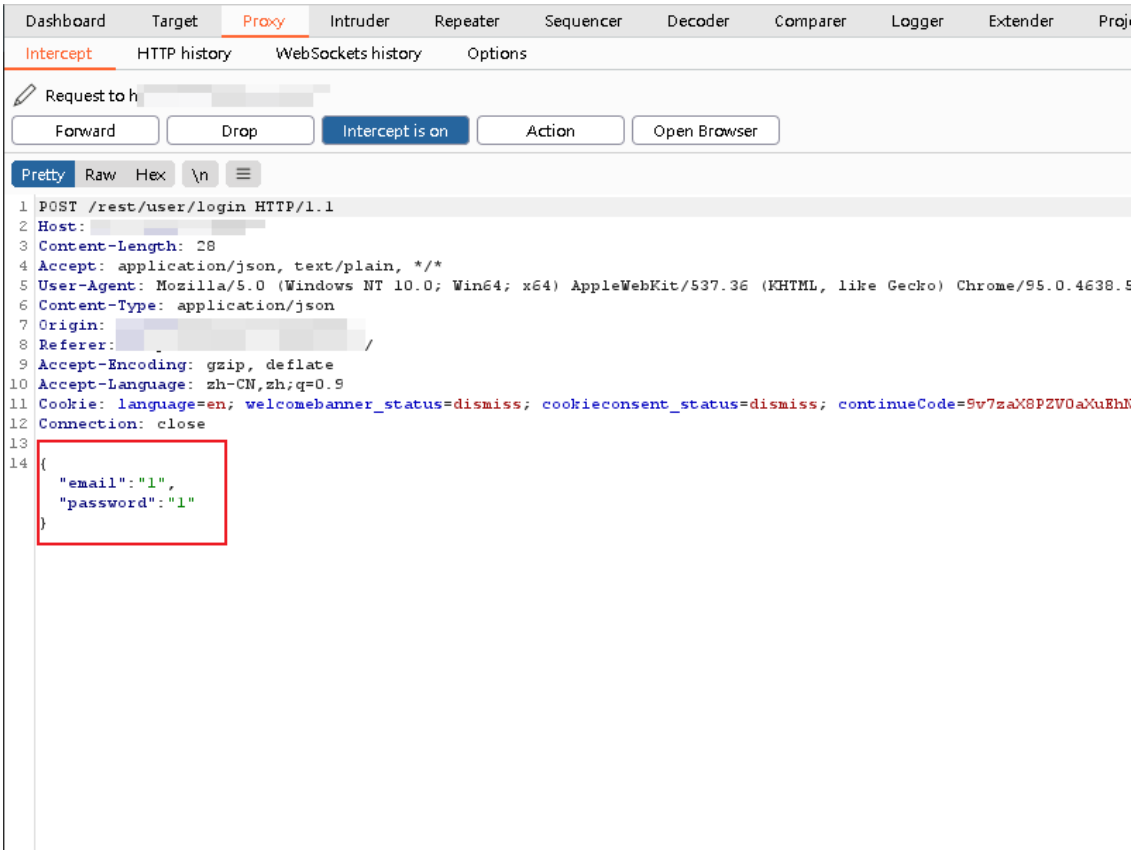


2. 点击Account尝试登陆

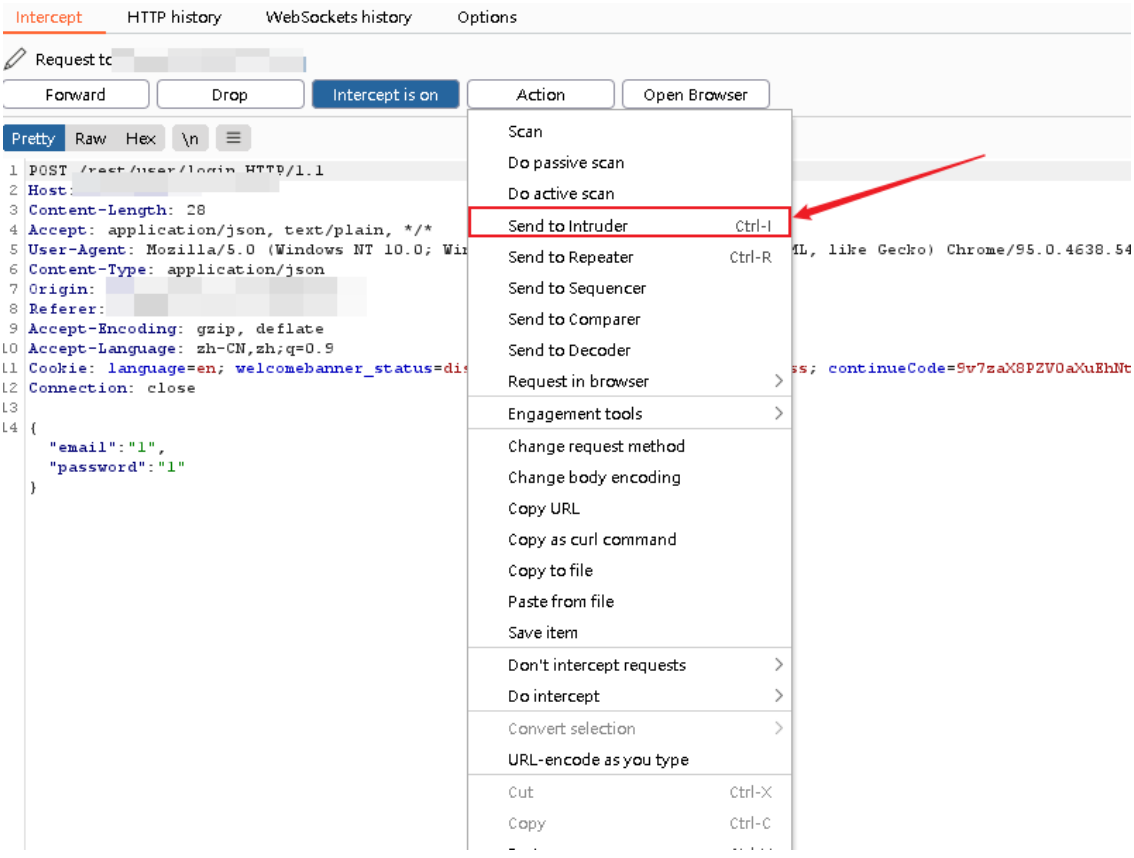


3. 输入任意账号密码，使用BurpSuite的Proxy模块抓取数据包



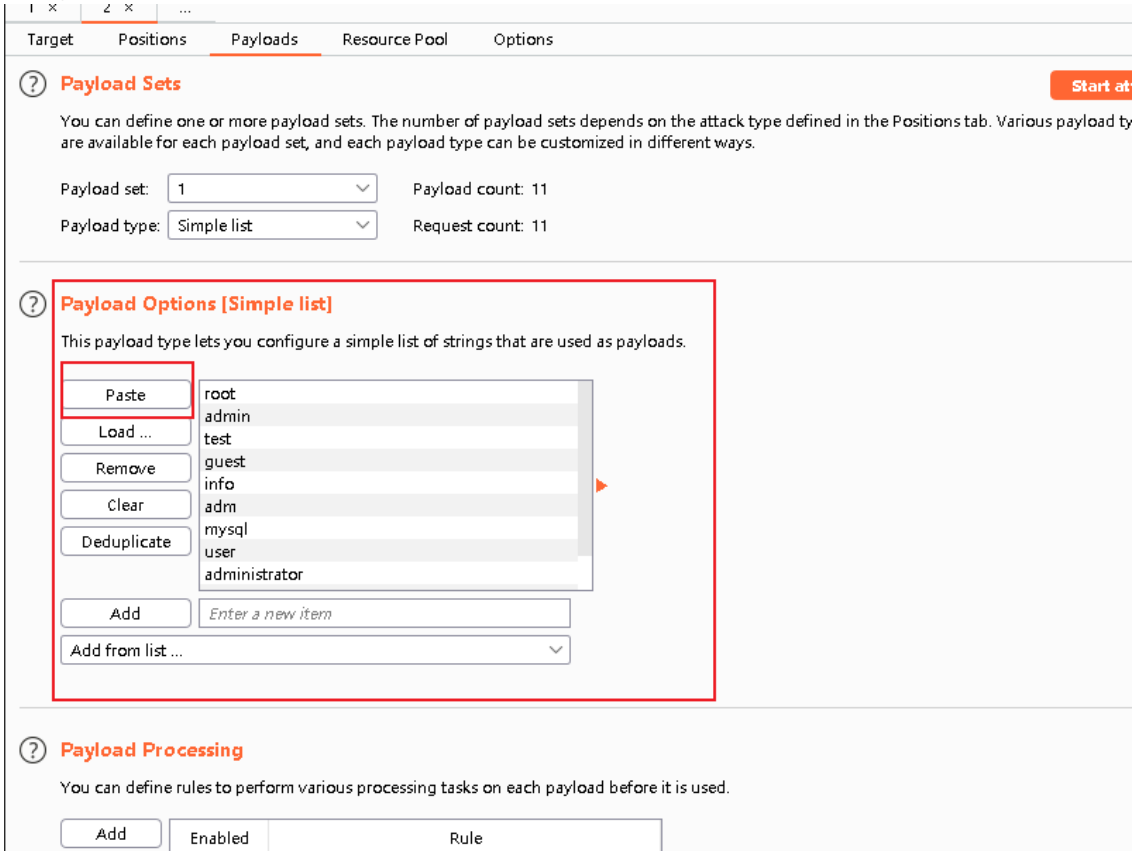


4. 发送到Intruder模块

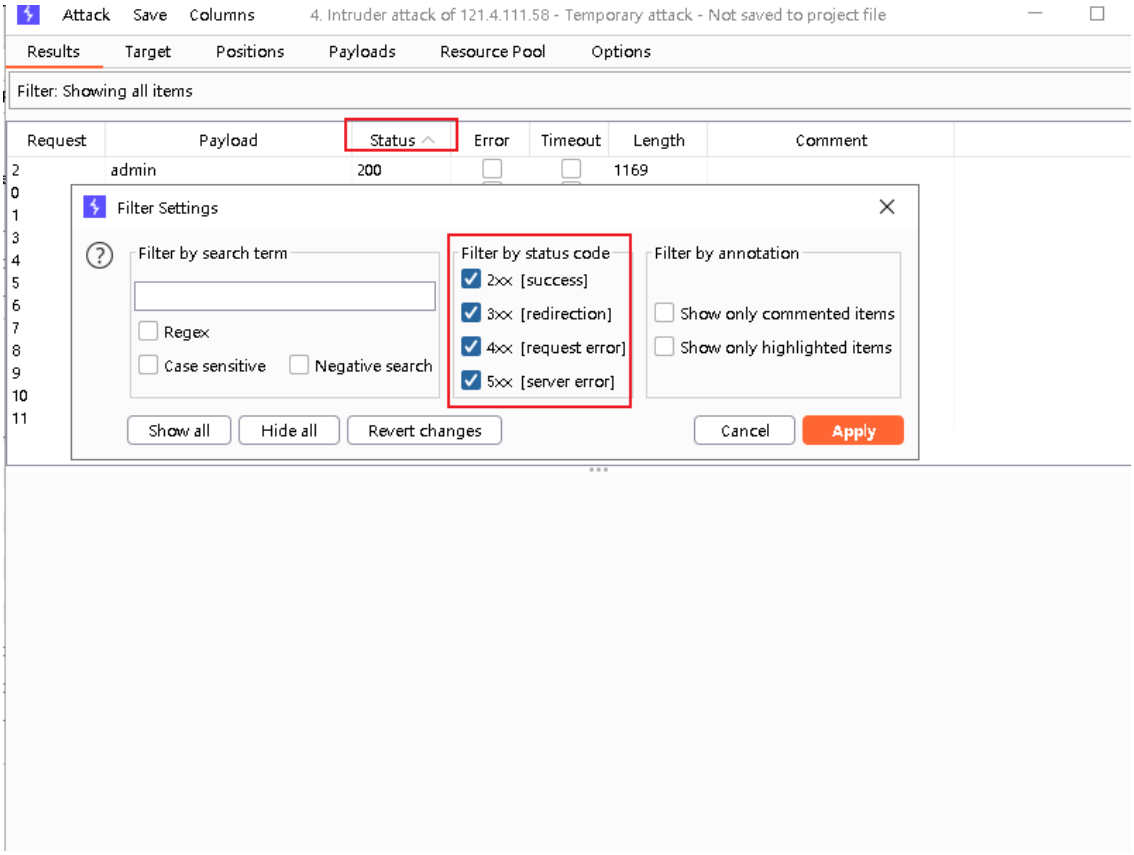


5. 设置Attack type攻击方式为Battering ram，清除Burp自动设置的攻击标记位置，在email和password位置设置标记

6. 在Payload中粘贴用户名

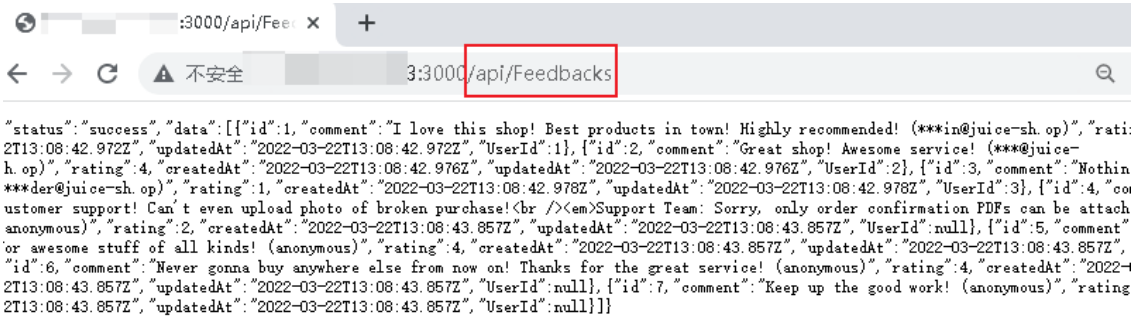


7. 开启攻击，对HTTP状态码直接或Filter排序



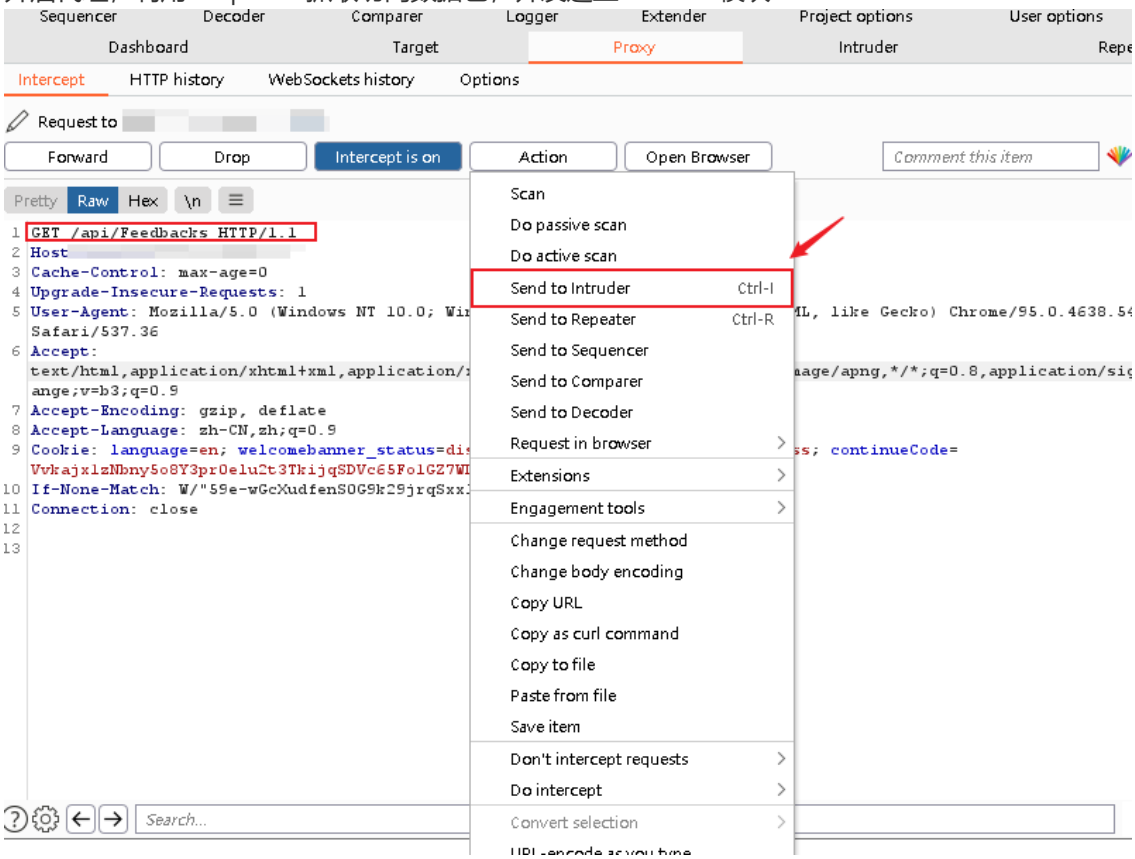
CAPTCHA Bypass

1. 打开ip:3000/api/Feedbacks/

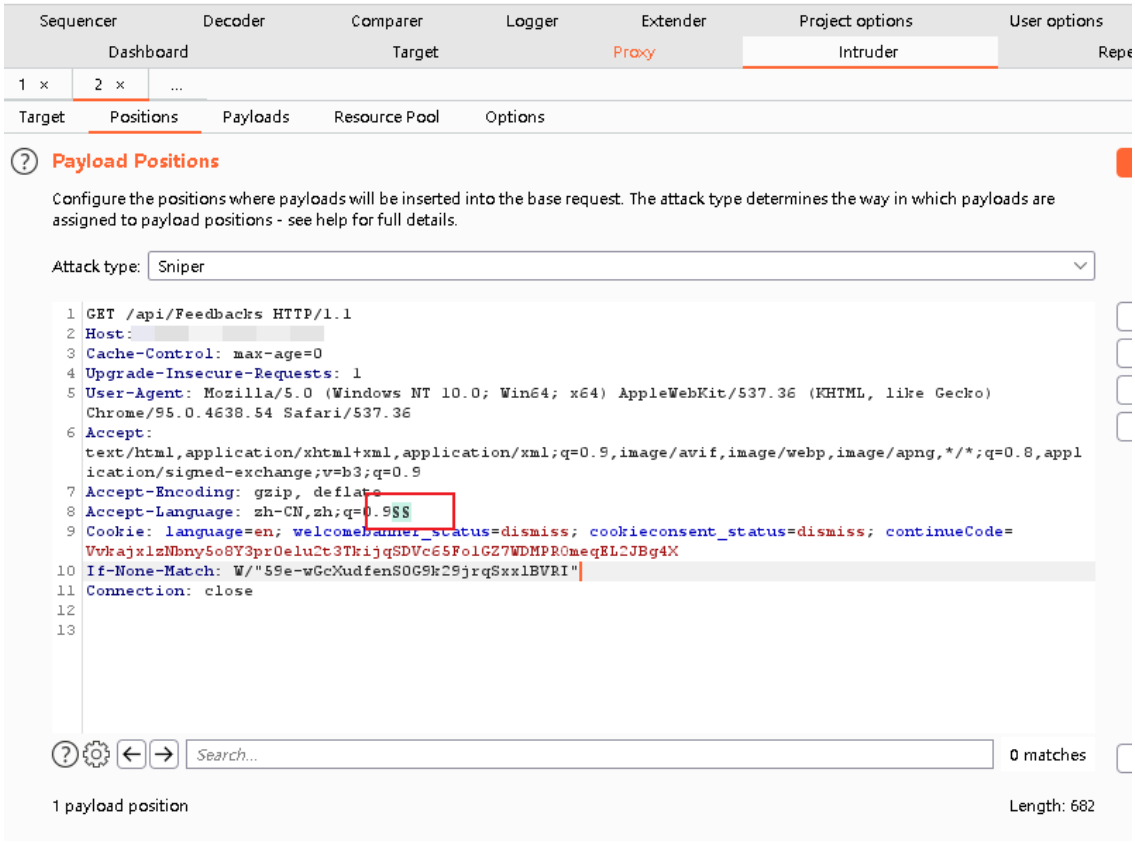


"status":"success","data":[{"id":1,"comment":"I love this shop! Best products in town! Highly recommended! (***in@juice-sh.op)","rati
2T13:08:42.972Z","updatedAt":"2022-03-22T13:08:42.972Z","UserId":1},{"id":2,"comment":"Great shop! Awesome service! (***@juice-
h.op)","rating":4,"createdAt":"2022-03-22T13:08:42.976Z","updatedAt":"2022-03-22T13:08:42.976Z","UserId":2},{"id":3,"comment":"Nothin
***der@juice-sh.op)","rating":1,"createdAt":"2022-03-22T13:08:42.978Z","updatedAt":"2022-03-22T13:08:42.978Z","UserId":3},{"id":4,"co
ustomer support! Can't even upload photo of broken purchase!
Support Team: Sorry, only order confirmation PDFs can be attach
anonymous)","rating":2,"createdAt":"2022-03-22T13:08:43.857Z","updatedAt":"2022-03-22T13:08:43.857Z","UserId":null},{"id":5,"comment"
or awesome stuff of all kinds! (anonymous)","rating":4,"createdAt":"2022-03-22T13:08:43.857Z","updatedAt":"2022-03-22T13:08:43.857Z",
"id":6,"comment":"Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)","rating":4,"createdAt":"2022-
2T13:08:43.857Z","updatedAt":"2022-03-22T13:08:43.857Z","UserId":null},{"id":7,"comment":"Keep up the good work! (anonymous)","rating
2T13:08:43.857Z","updatedAt":"2022-03-22T13:08:43.857Z","UserId":null}]}

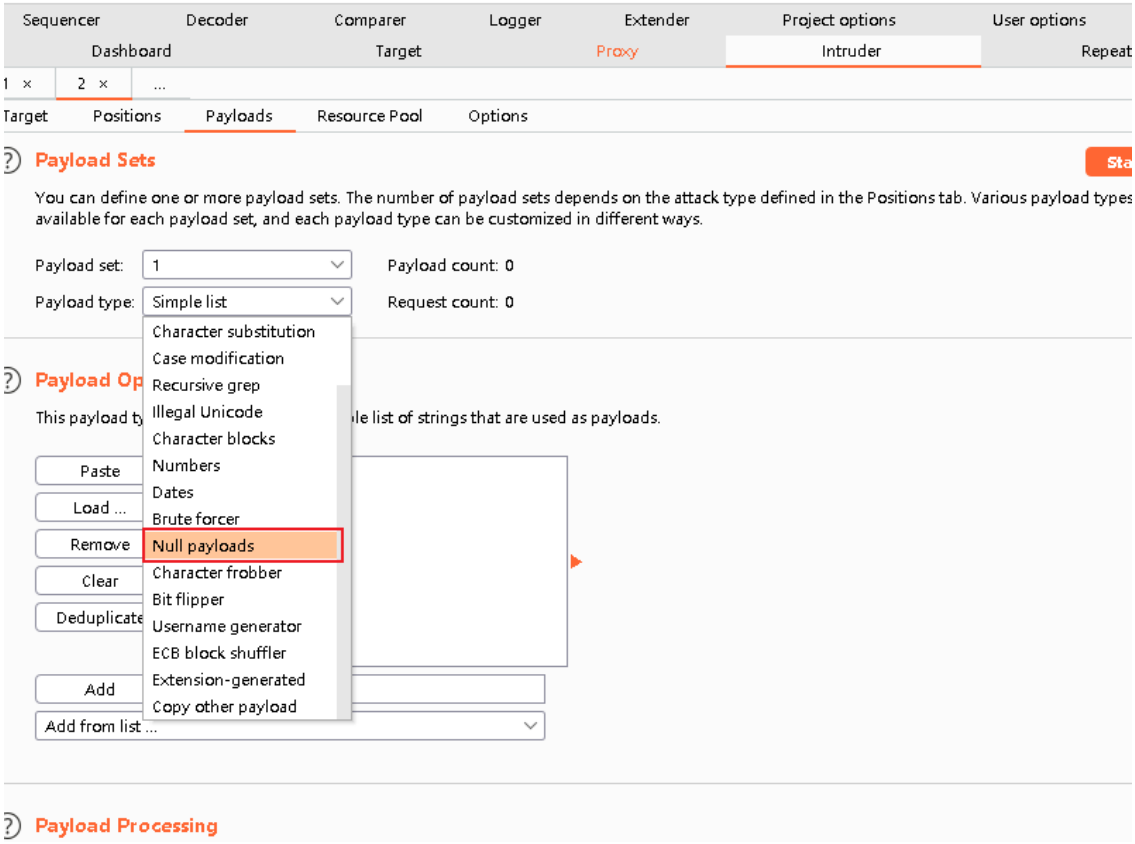
2. 开启代理，利用BurpSuite抓取访问数据包，并发送至Intruder模块



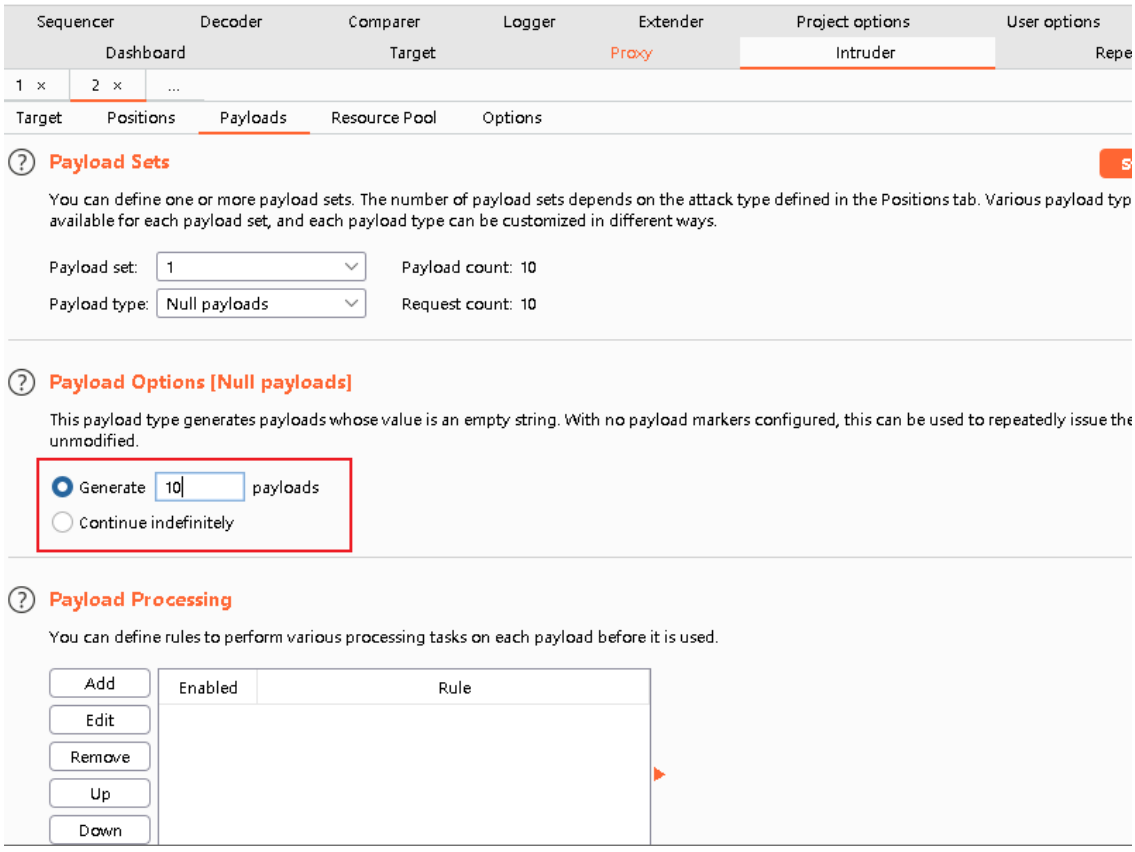
3. 清除现有Positions，任意设置位置处为空Payload，攻击类型为Sniper



4. Payload type设置为Null payloads



5. 设置发出10次请求



6. 开启攻击，完成CAPTCHA Bypass挑战