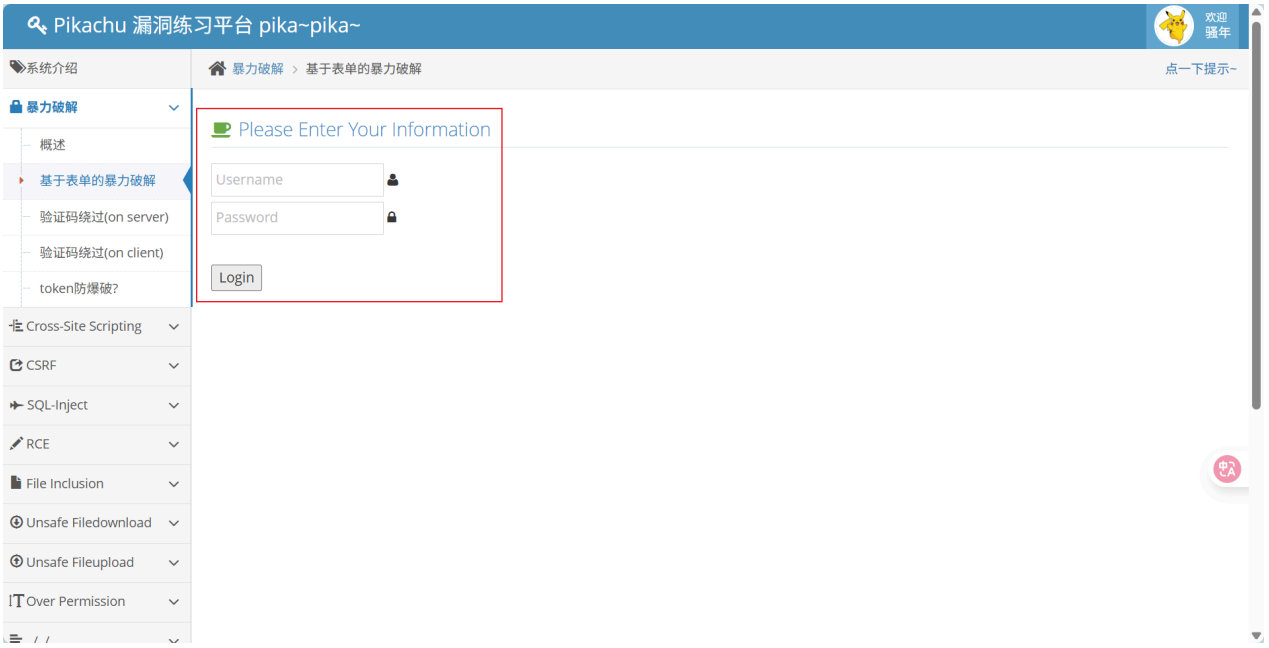
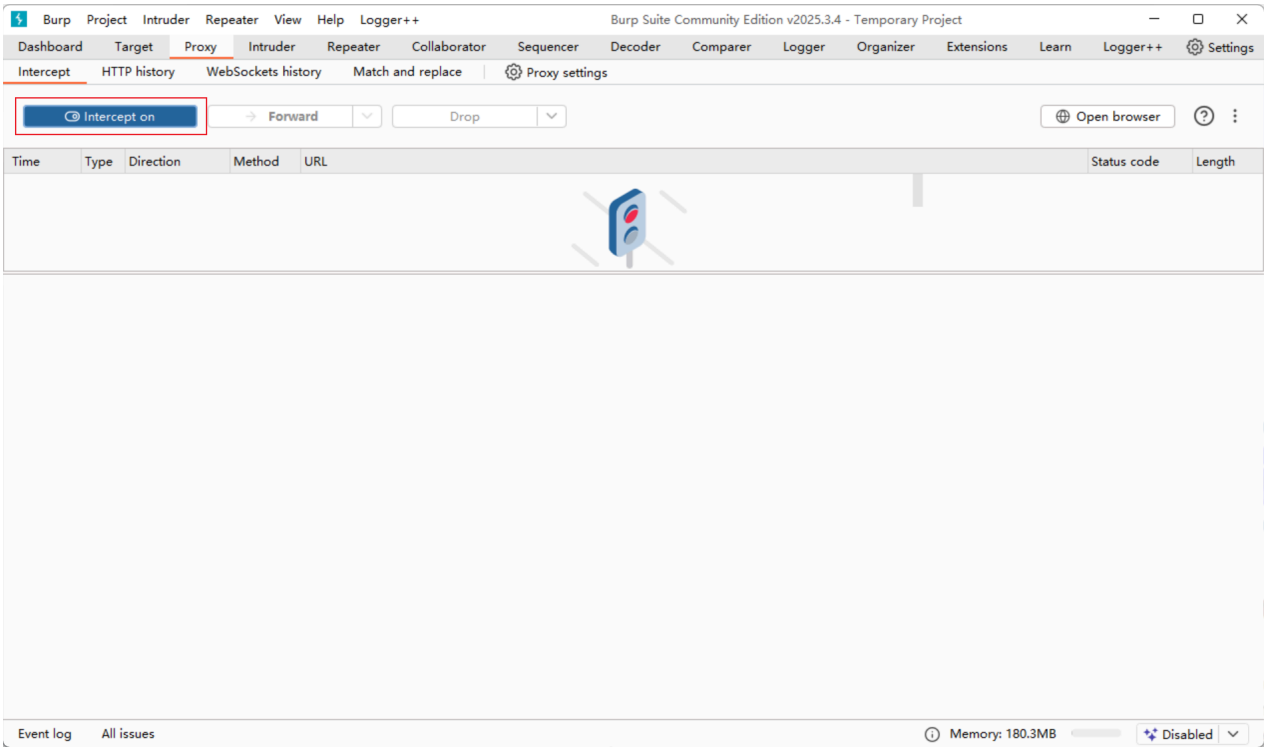
对 Pikachu 靶场弱口令漏洞的暴力破解

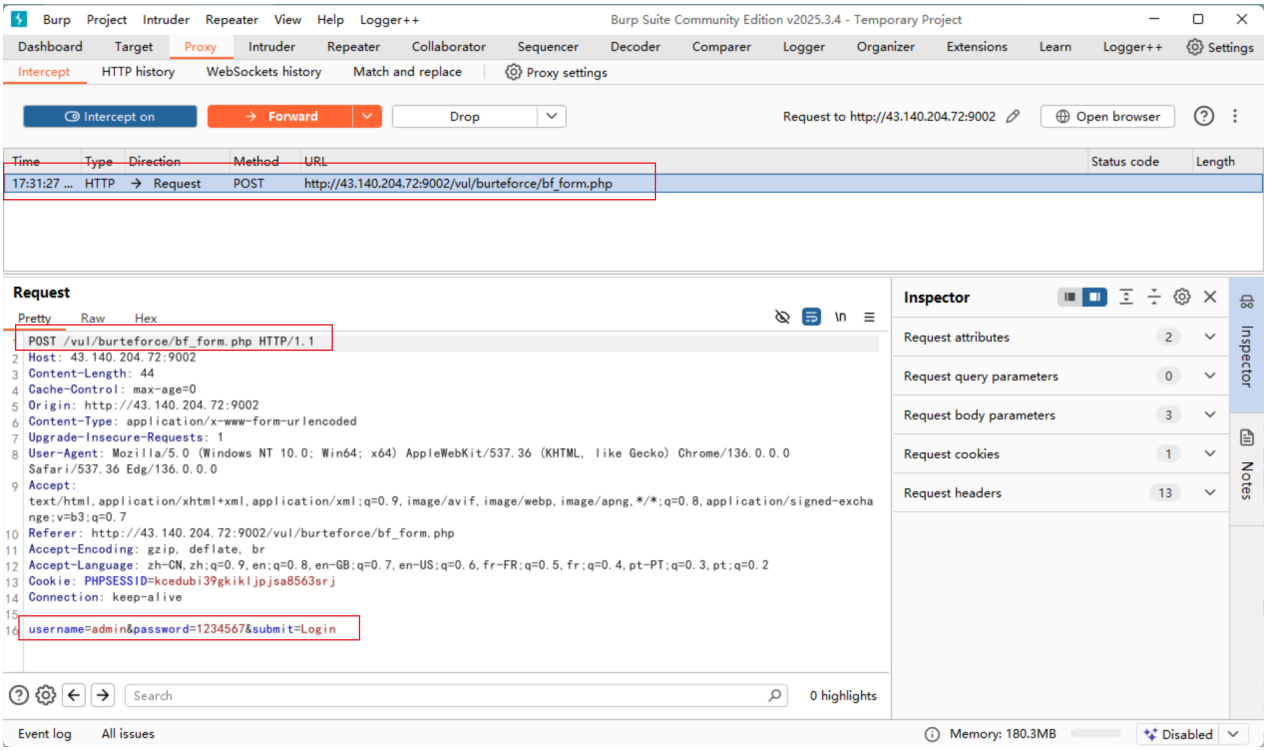
1. 打开靶场页面



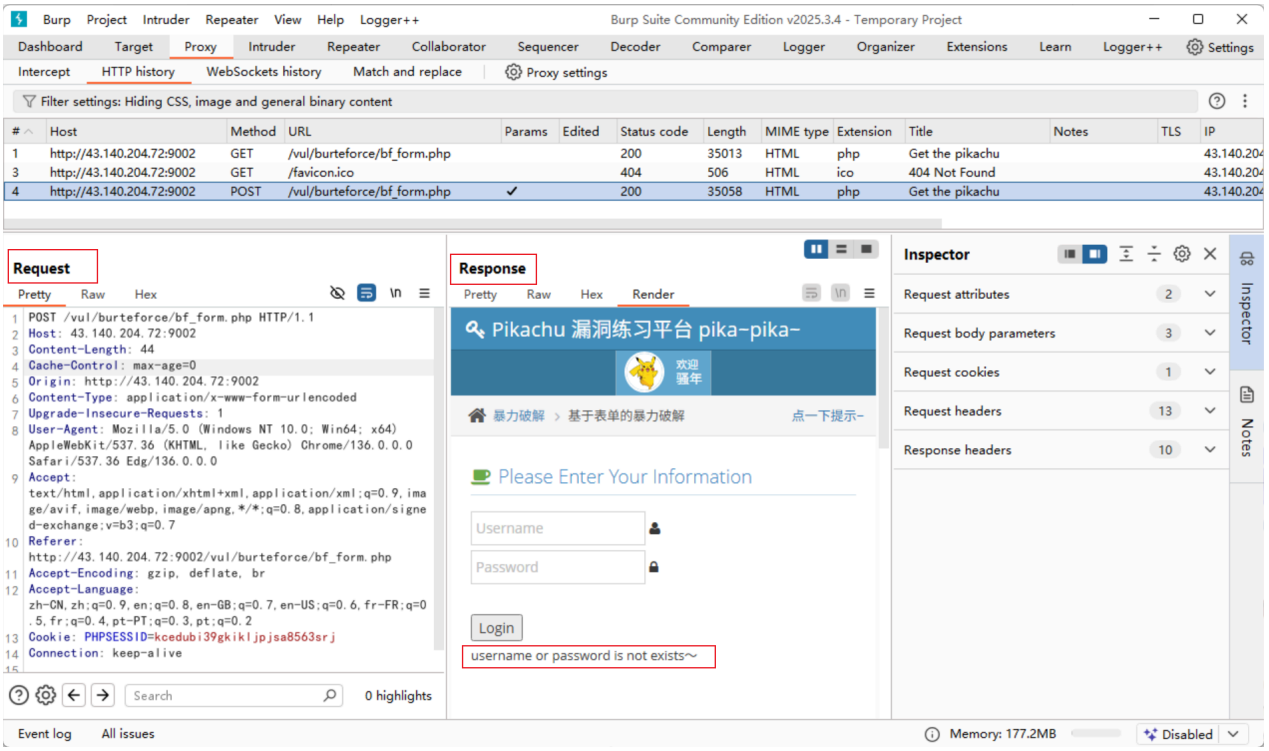
2. 输入账号、密码点击登录，抓取登录数据包。
前提要按照实验报告书要求，配置好浏览器代理和 burpsuite 工具。
开启拦截：



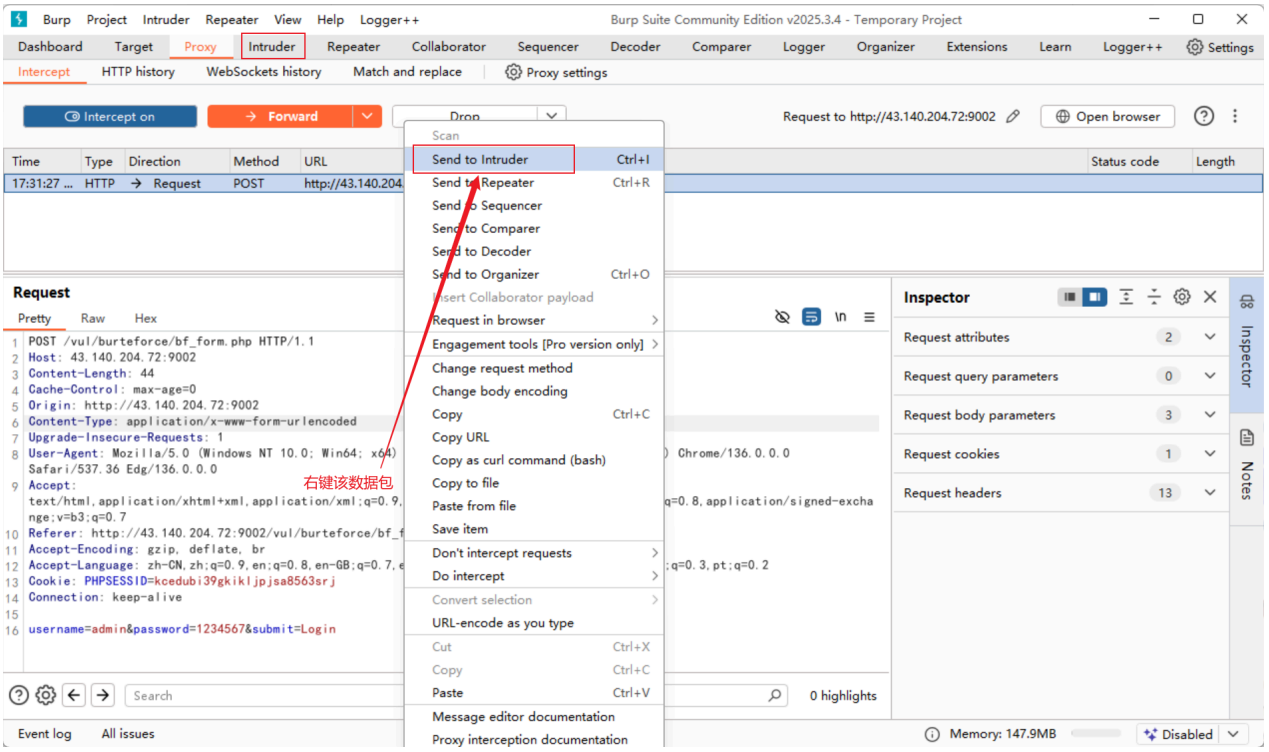
抓取到登录请求的数据包：
其中 username 为用户输入的用户名，password 为用户输入的密码。


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2025.3.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Logger++ Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Request to http://43.140.204.72:9002 Open browser
Time Type Direction Method URL Status code Length
17:31:27 ... HTTP Request POST http://43.140.204.72:9002/vul/burteforce/bf_form.php
Request
Pretty Raw Hex
POST /vul/burteforce/bf_form.php HTTP/1.1
Host: 43.140.204.72:9002
Content-Length: 44
Cache-Control: max-age=0
Origin: http://43.140.204.72:9002
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0
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=0.7
Referer: http://43.140.204.72:9002/vul/burteforce/bf_form.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,fr-FR;q=0.5,fr;q=0.4,pt-PT;q=0.3,pt;q=0.2
Cookie: PHPSESSID=kcedubi39gkikljpjsa8563srj
Connection: keep-alive
username=admin&password=1234567&submit=Login
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 13
Inspector Notes
Event log All issues
Memory: 180.3MB Disabled

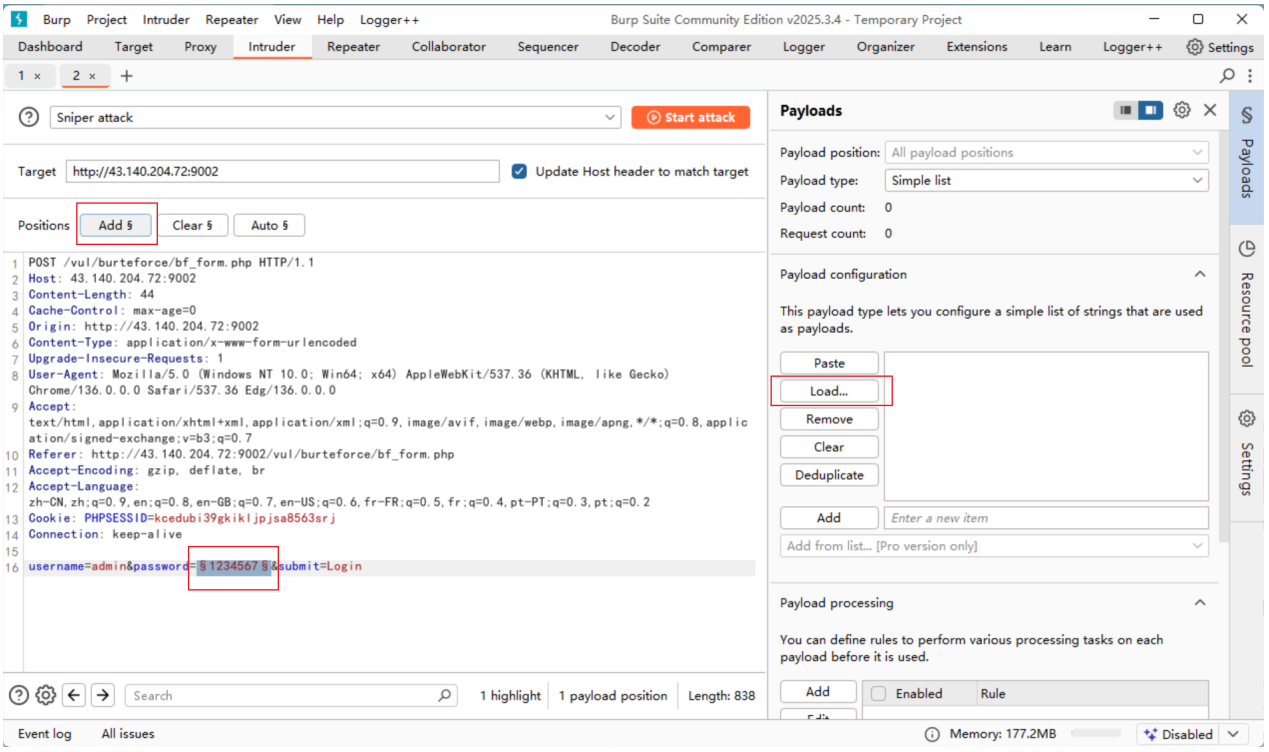
查看该请求的响应：


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2025.3.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Logger++ Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP
1 http://43.140.204.72:9002 GET /vul/burteforce/bf_form.php 200 35013 HTML php Get the pikachu 43.140.204
3 http://43.140.204.72:9002 GET /favicon.ico 404 506 HTML ico 404 Not Found 43.140.204
4 http://43.140.204.72:9002 POST /vul/burteforce/bf_form.php ✓ 200 35058 HTML php Get the pikachu 43.140.204
Request
Pretty Raw Hex
POST /vul/burteforce/bf_form.php HTTP/1.1
Host: 43.140.204.72:9002
Content-Length: 44
Cache-Control: max-age=0
Origin: http://43.140.204.72:9002
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0
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=0.7
Referer: http://43.140.204.72:9002/vul/burteforce/bf_form.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,fr-FR;q=0.5,fr;q=0.4,pt-PT;q=0.3,pt;q=0.2
Cookie: PHPSESSID=kcedubi39gkikljpjsa8563srj
Connection: keep-alive
Search 0 highlights
Response
Pretty Raw Hex Render
Pikachu 漏洞练习平台 pika-pika~
欢迎骚年
暴力破解 › 基于表单的暴力破解 点一下提示~
Please Enter Your Information
Username
Password
Login
username or password is not exists~
Inspector
Request attributes 2
Request body parameters 3
Request cookies 1
Request headers 13
Response headers 10
Inspector Notes
Event log All issues
Memory: 177.2MB Disabled

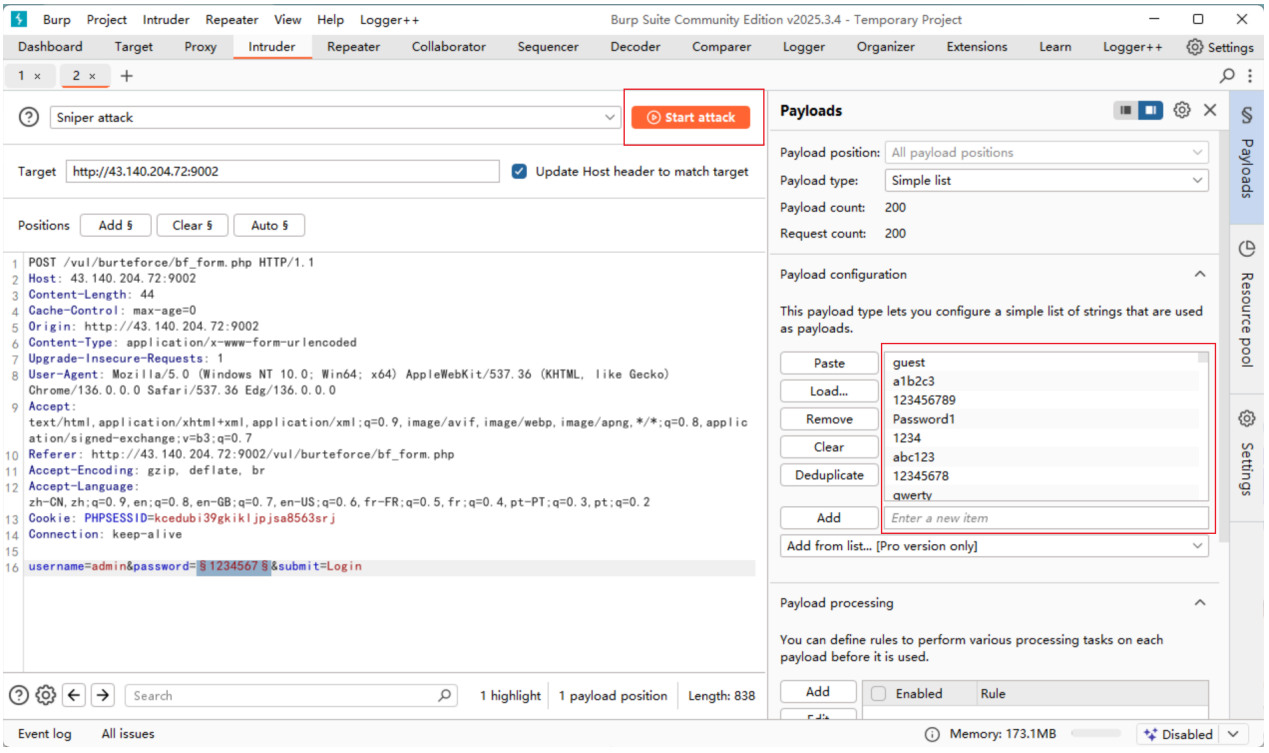
将该数据包发送到 **Intruder** 攻击模块



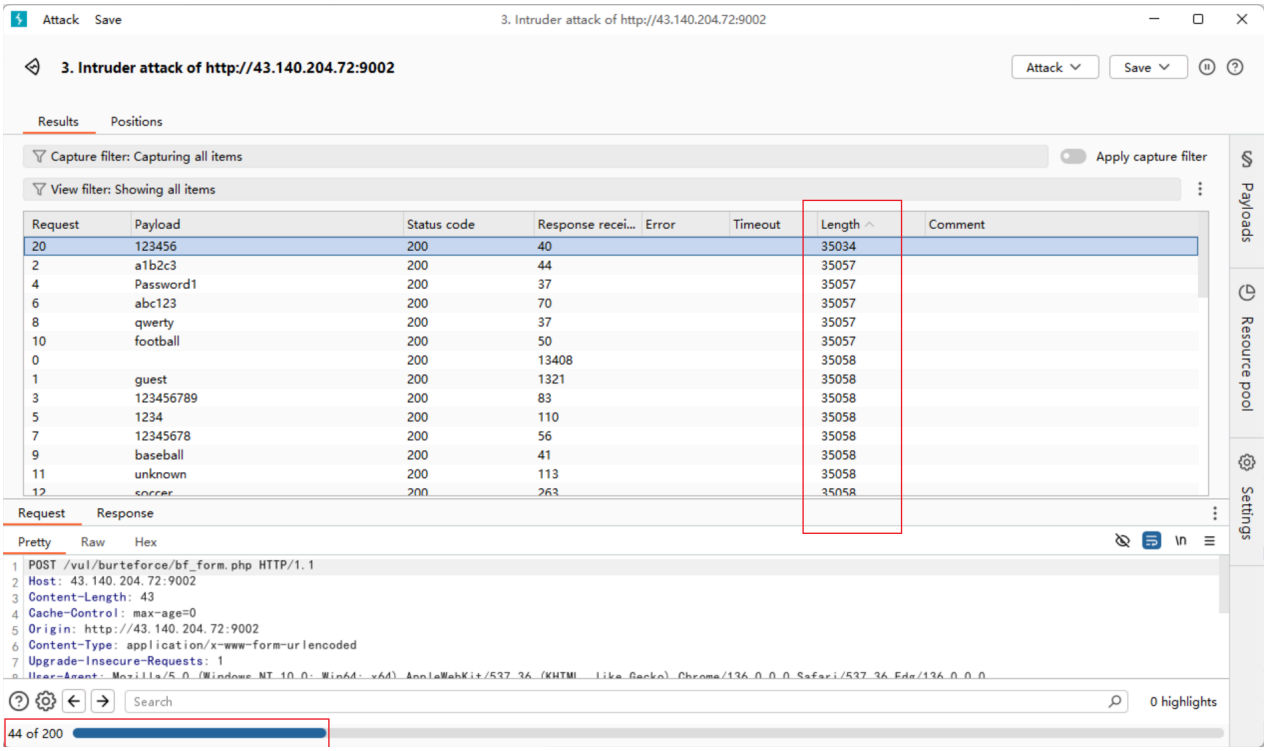
添加payload 的位置，我们将 password 标记为payload的位置，因为是在已知账号的情况下爆破密码



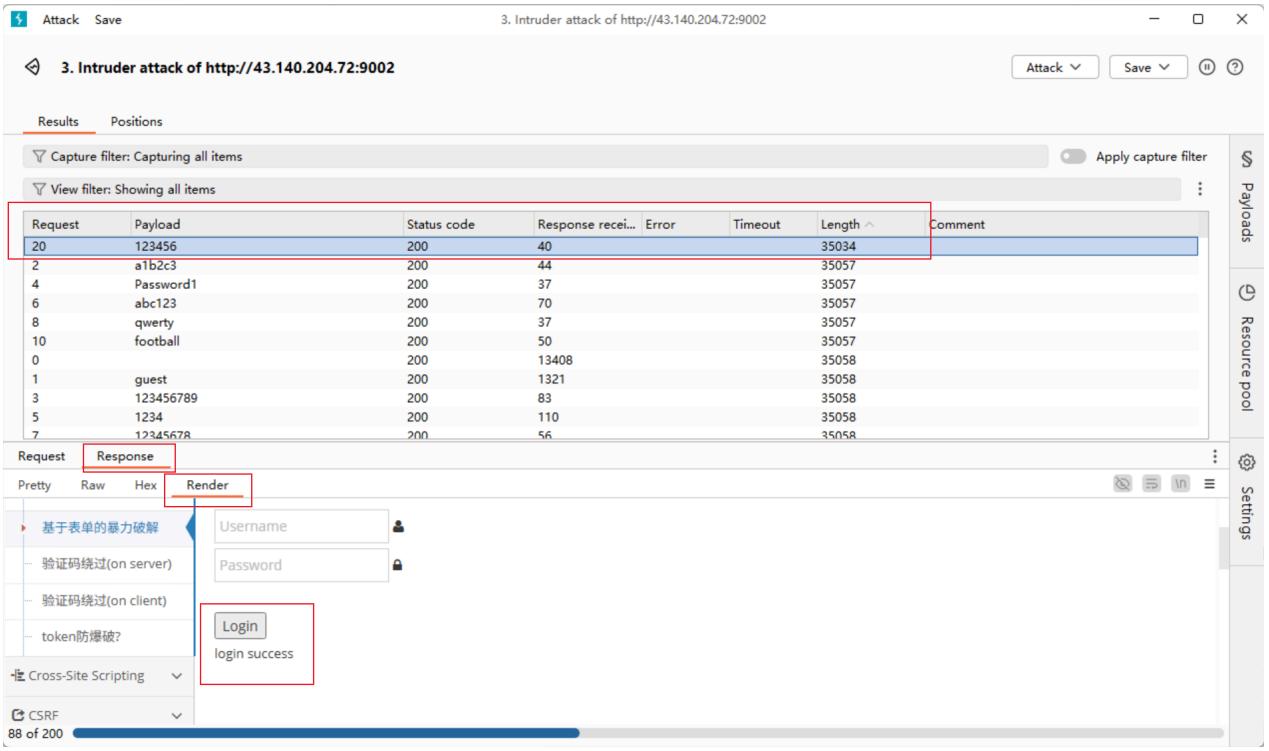
点击 Load 加载弱口令密码字典，点击开始攻击



开始爆破，通过查看响应体的长度可以判断哪个请求是不同于其他请求的，一般登录成功的响应数据包都较短。



我们发现 payload 等于 123456 时，响应数据包的长度最小，我们查看该请求的响应结果。



登录成功，说明 admin 用户的密码为 123456。