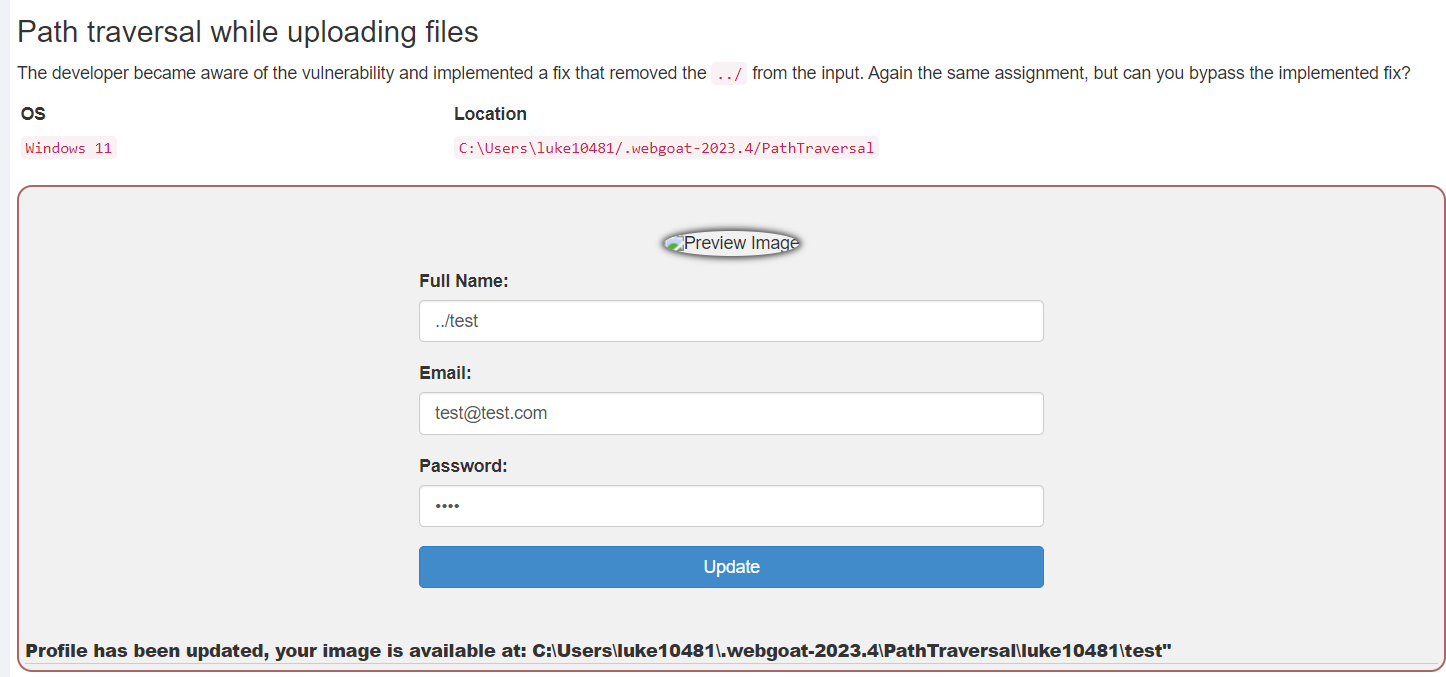
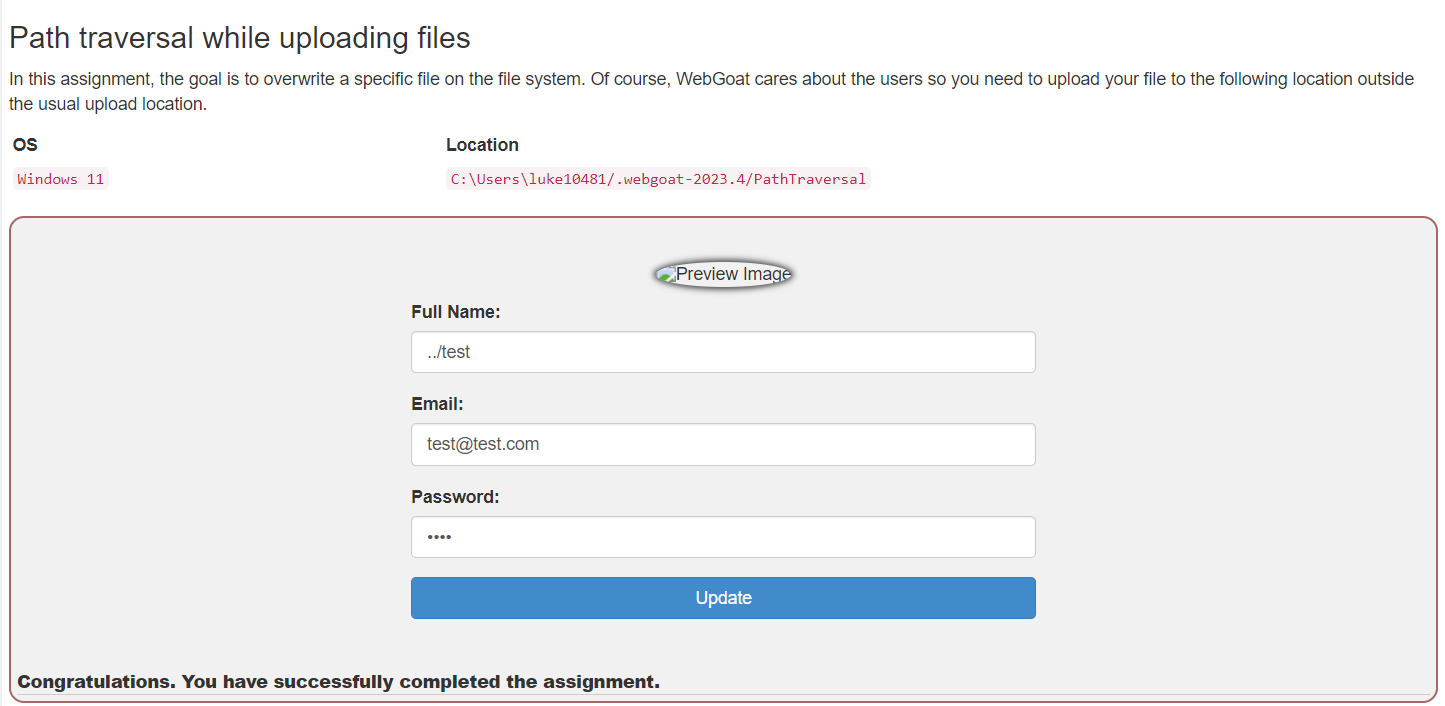
2 Path traversal while uploading files

题目要求上传到PathTraversal目录下，PathTraversal为上级目录，因此文件名../跨目录上传到上级目录



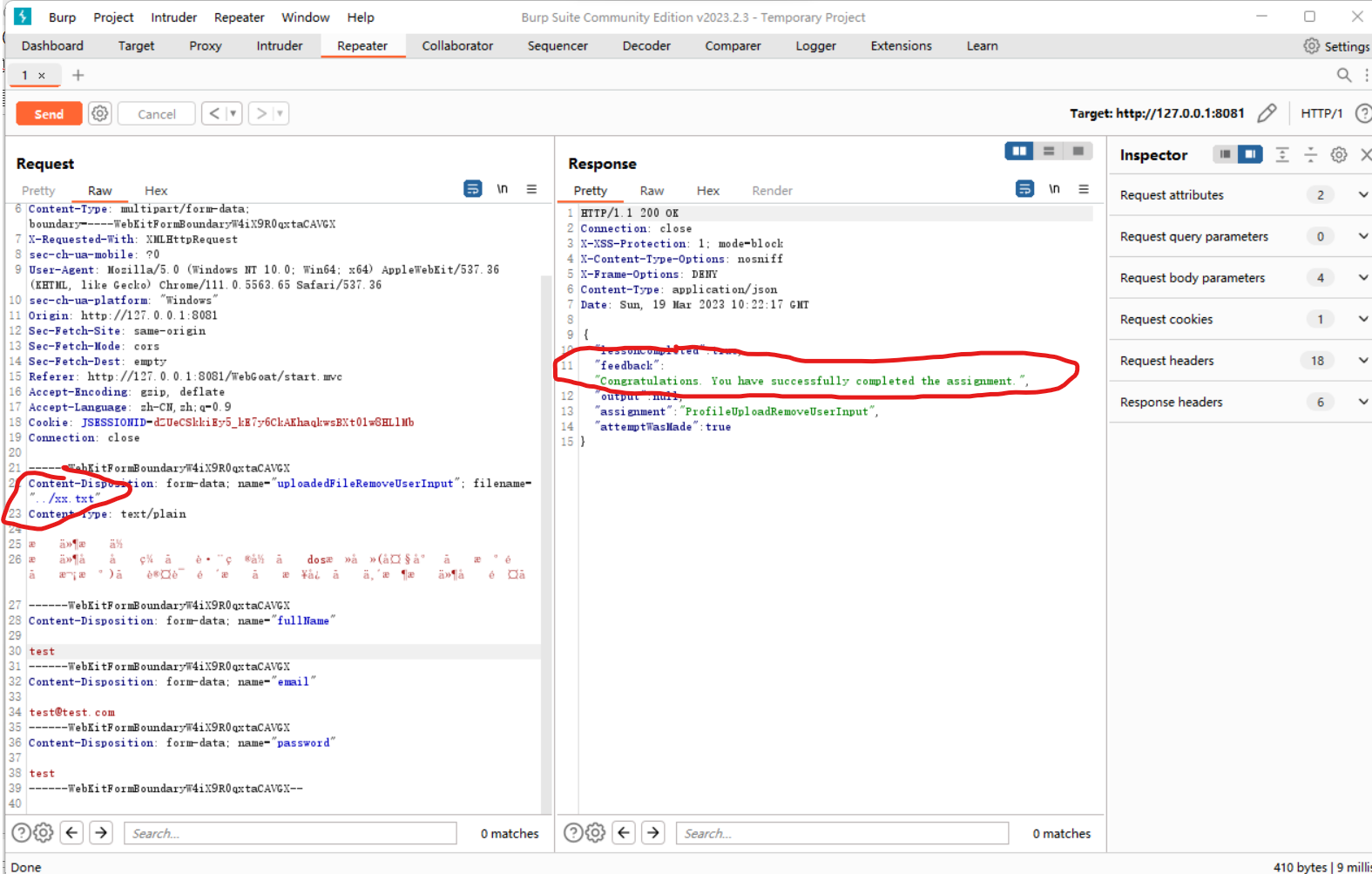
成功

3 Path traversal while uploading files

双写关键字

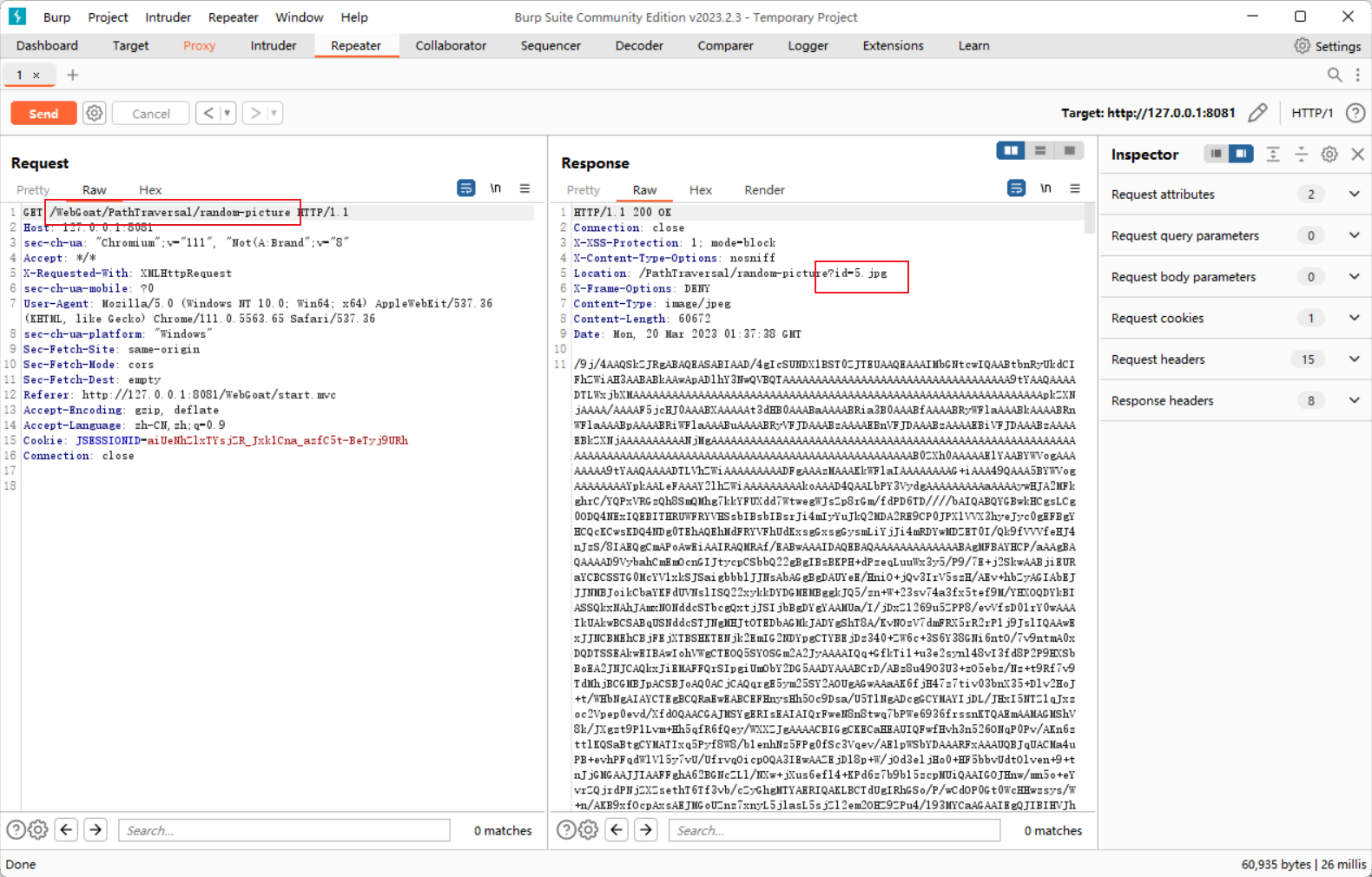
4 Path traversal while uploading files

抓包修改文件名为../发包，成功

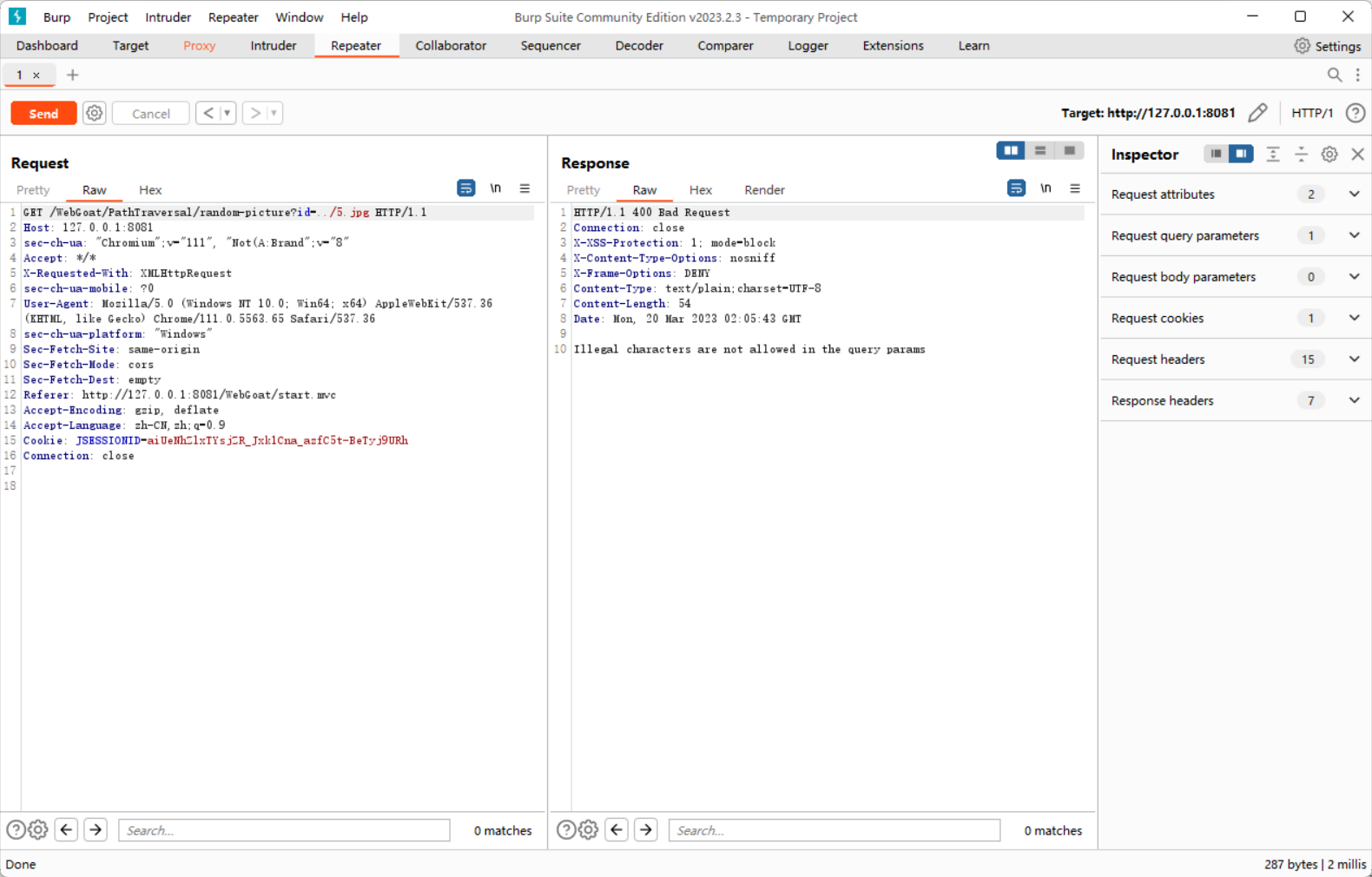


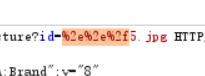
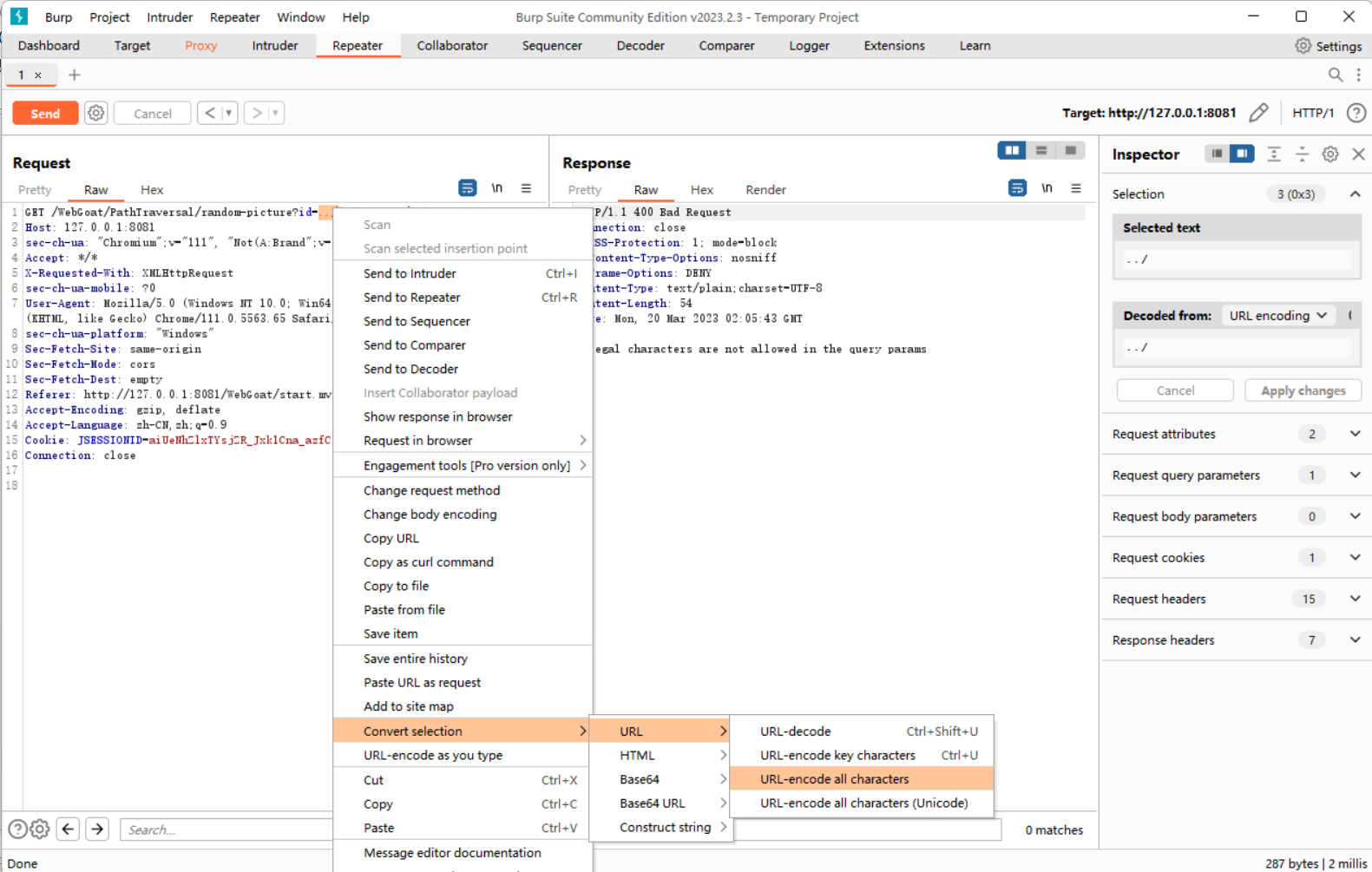
5 Retrieving other files with a path traversal

发现是get请求，可在url拼接参数，将get请求url按照返回报文Location处拼接id=xx.jpg参数，发送报文

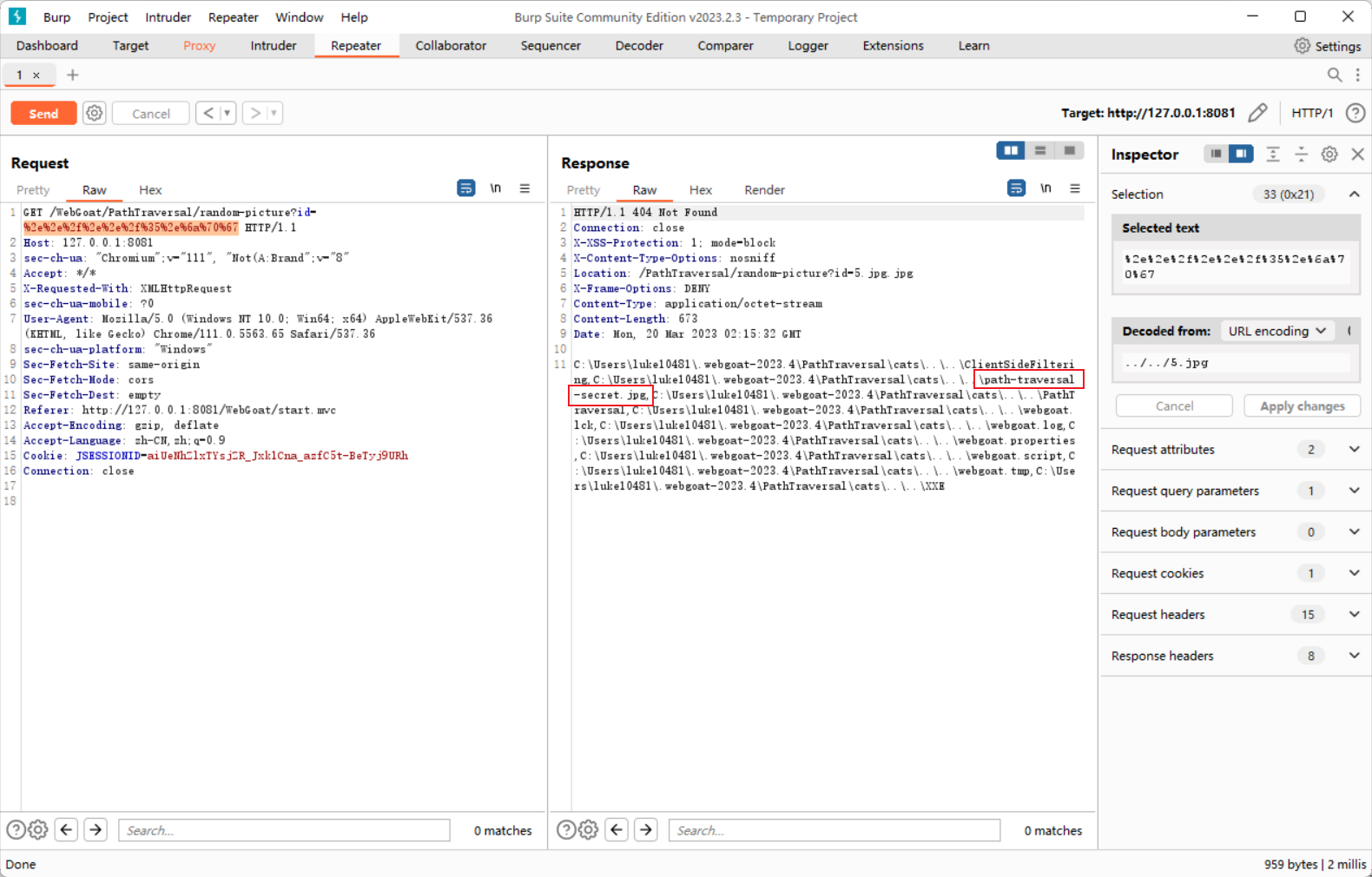
发送报文后发现，出现返回报文都是包含该目录下所有图片目录，目录中没有path-traversal-secret.jpg图片

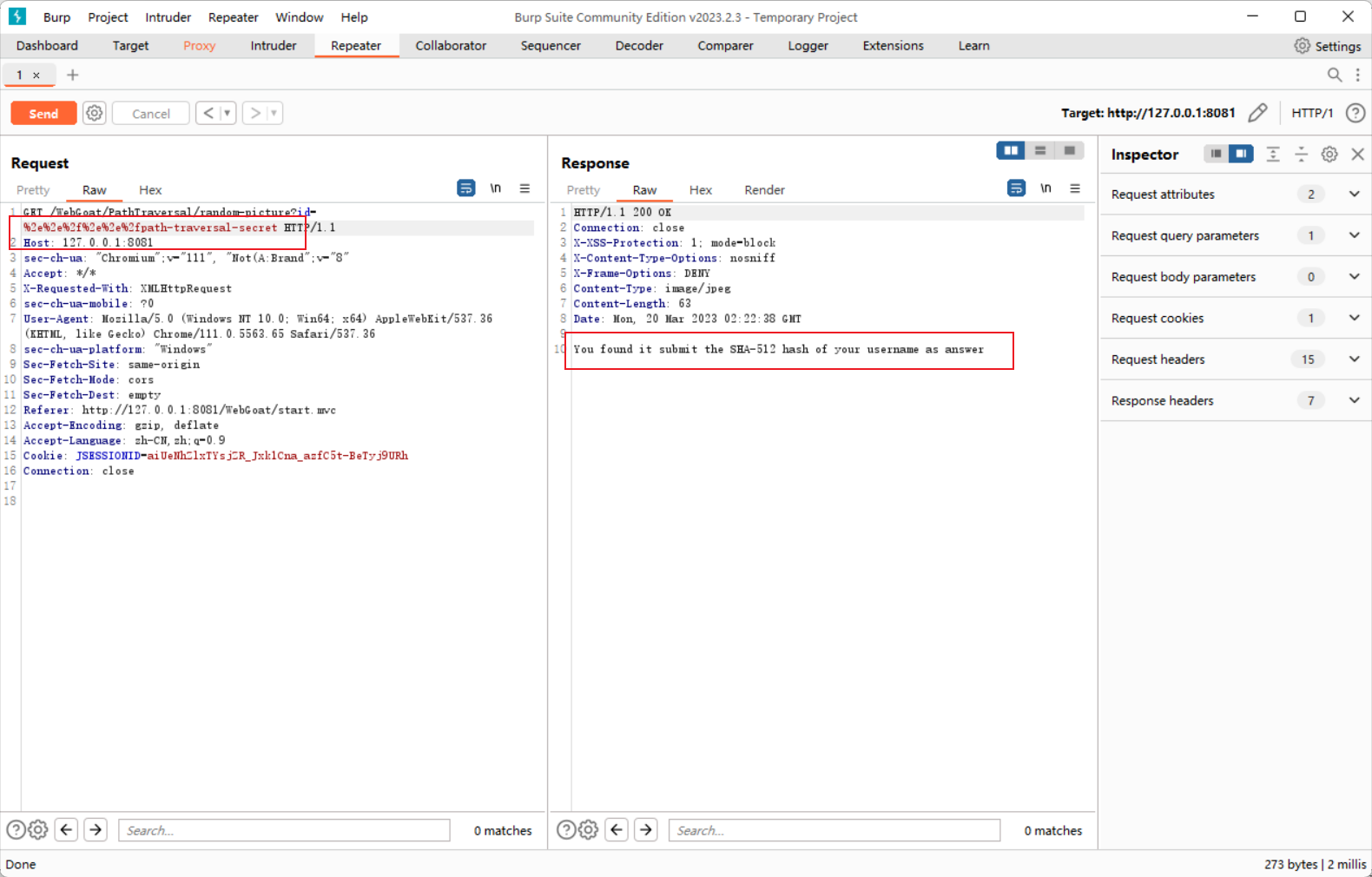
目录加上../遍历上级目录，发现报错，尝试将../进行url编码

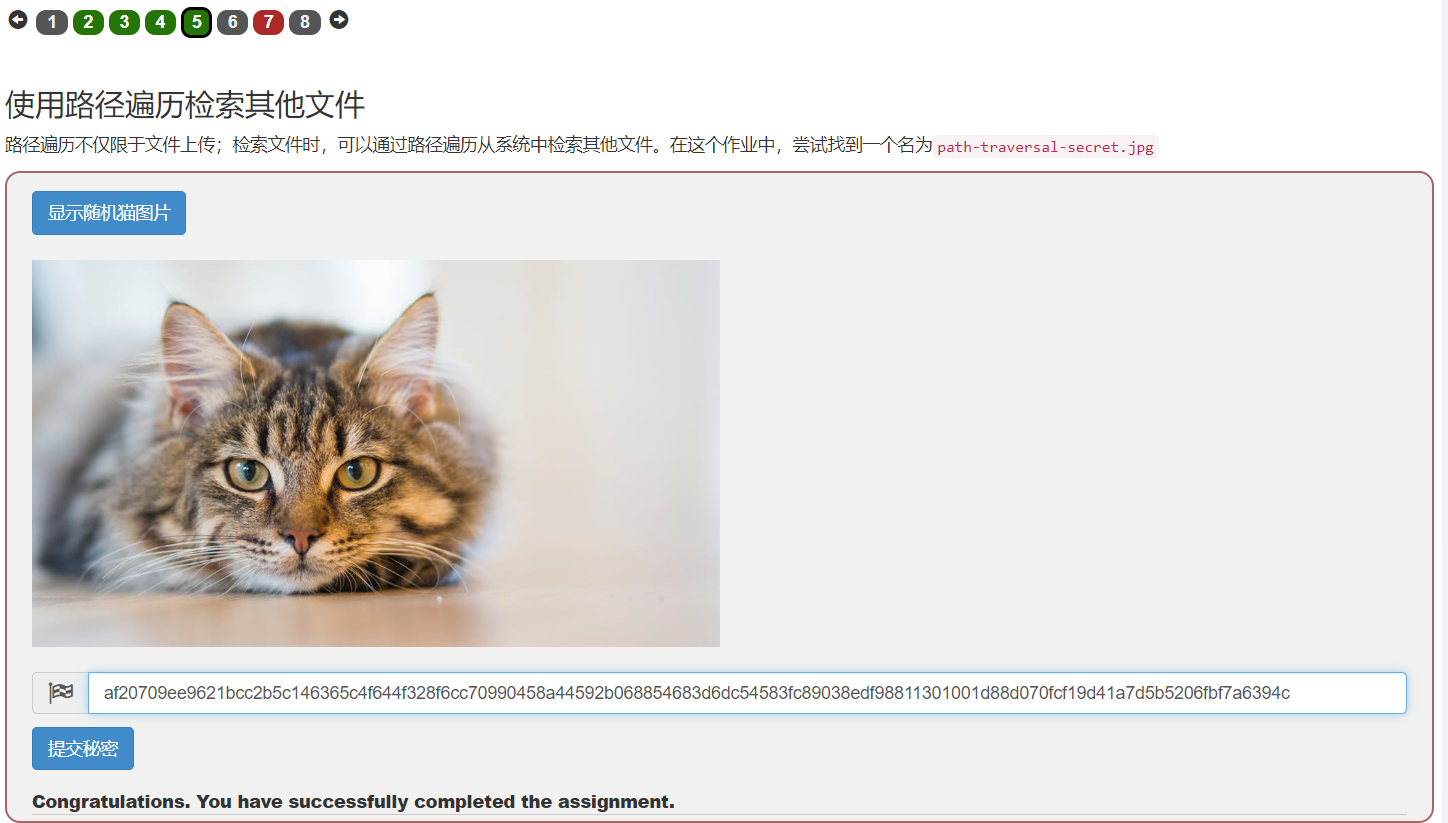
url编码



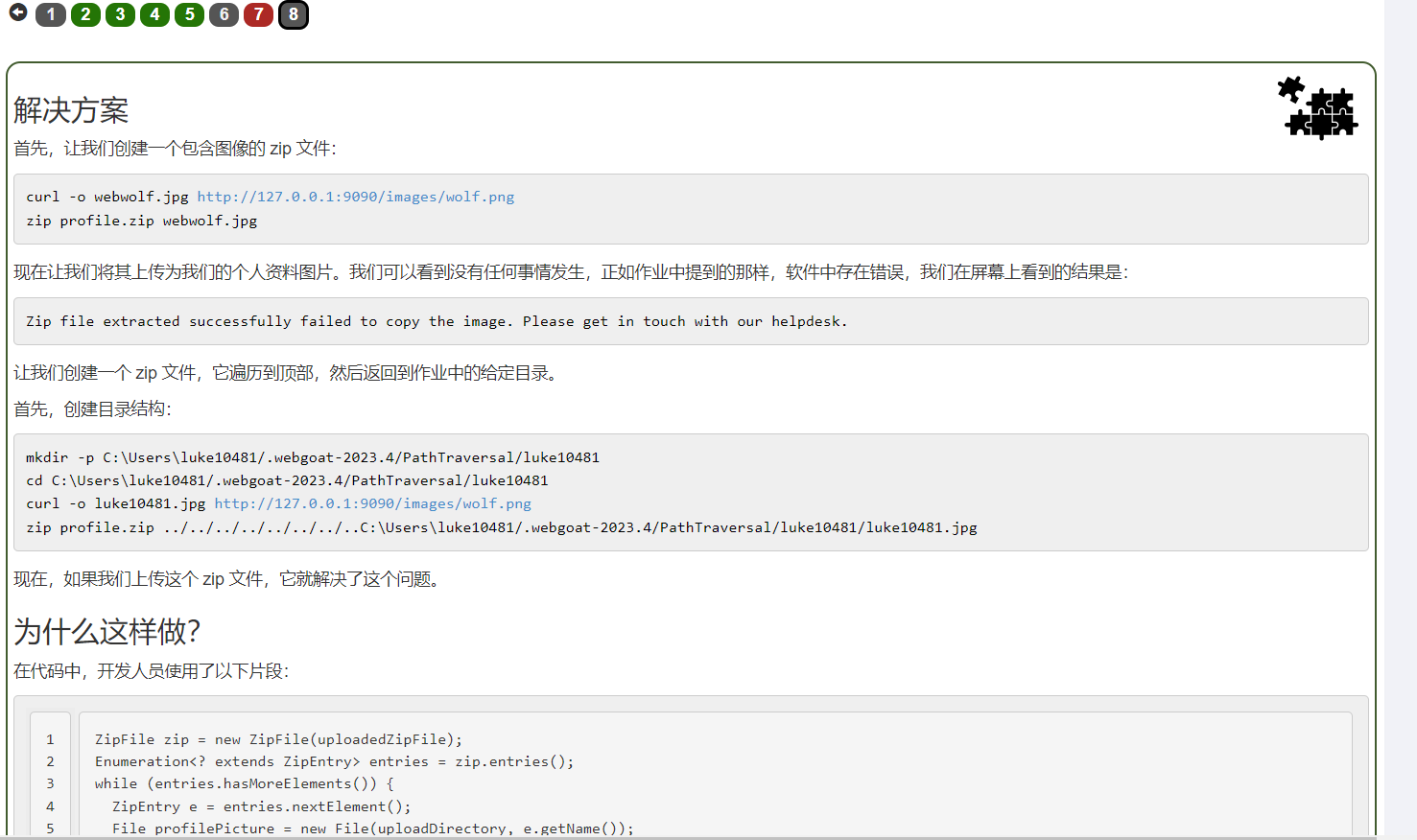
录入上上级目录找到了path-traversal-secret.jpg

修改参数为%2e%2e%2f%2e%2e%2fpath-traversal-secret，成功

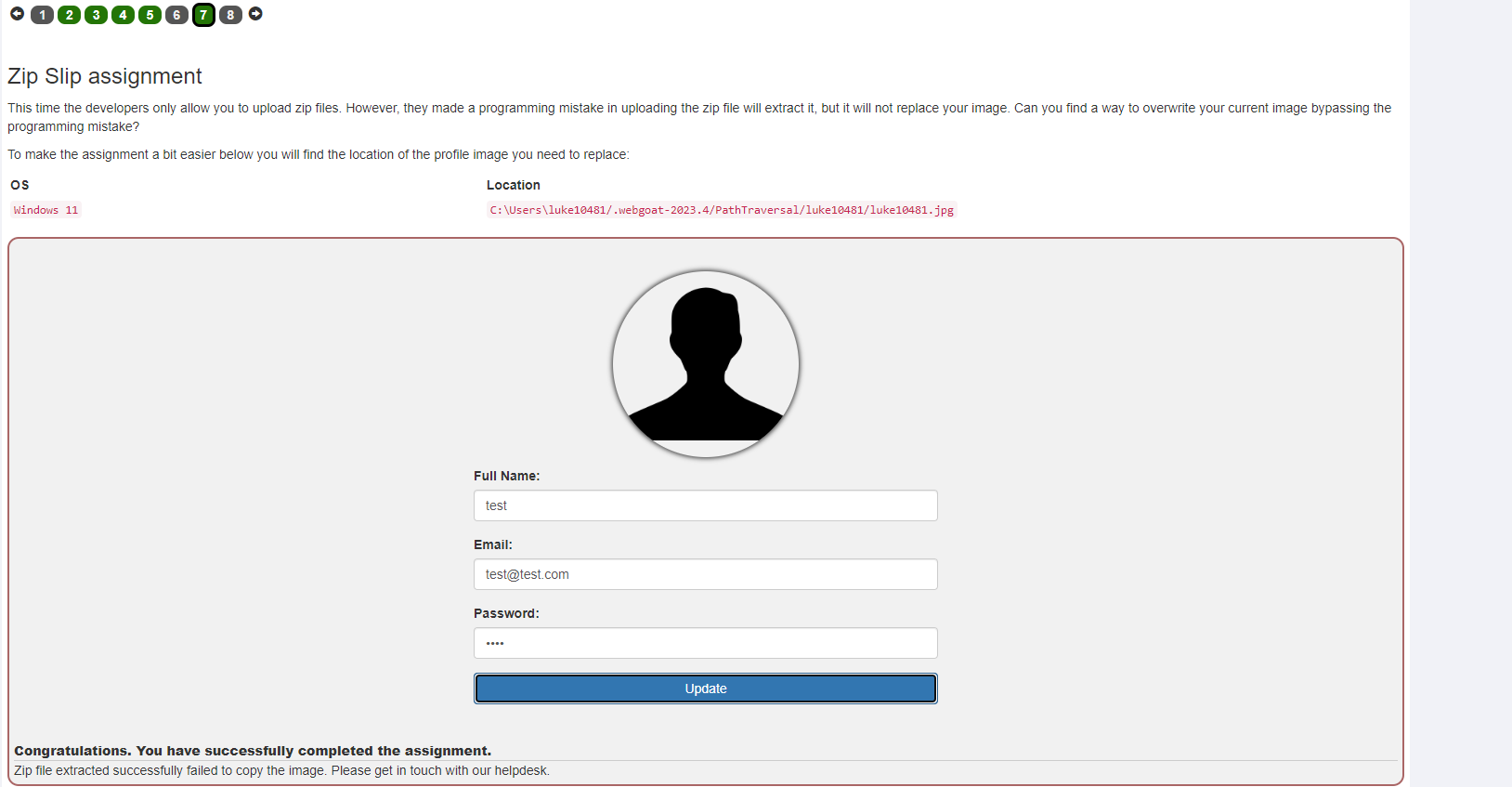
按返回报文提示将账户名按sha-512加密后输入提交后成功

Zip Slip assignment

答案在这，先遍历到根目录，再按题目所给目录拼接的路径作为zip包内目录穿透的图片路径

按此python代码块生成跨目录zip包

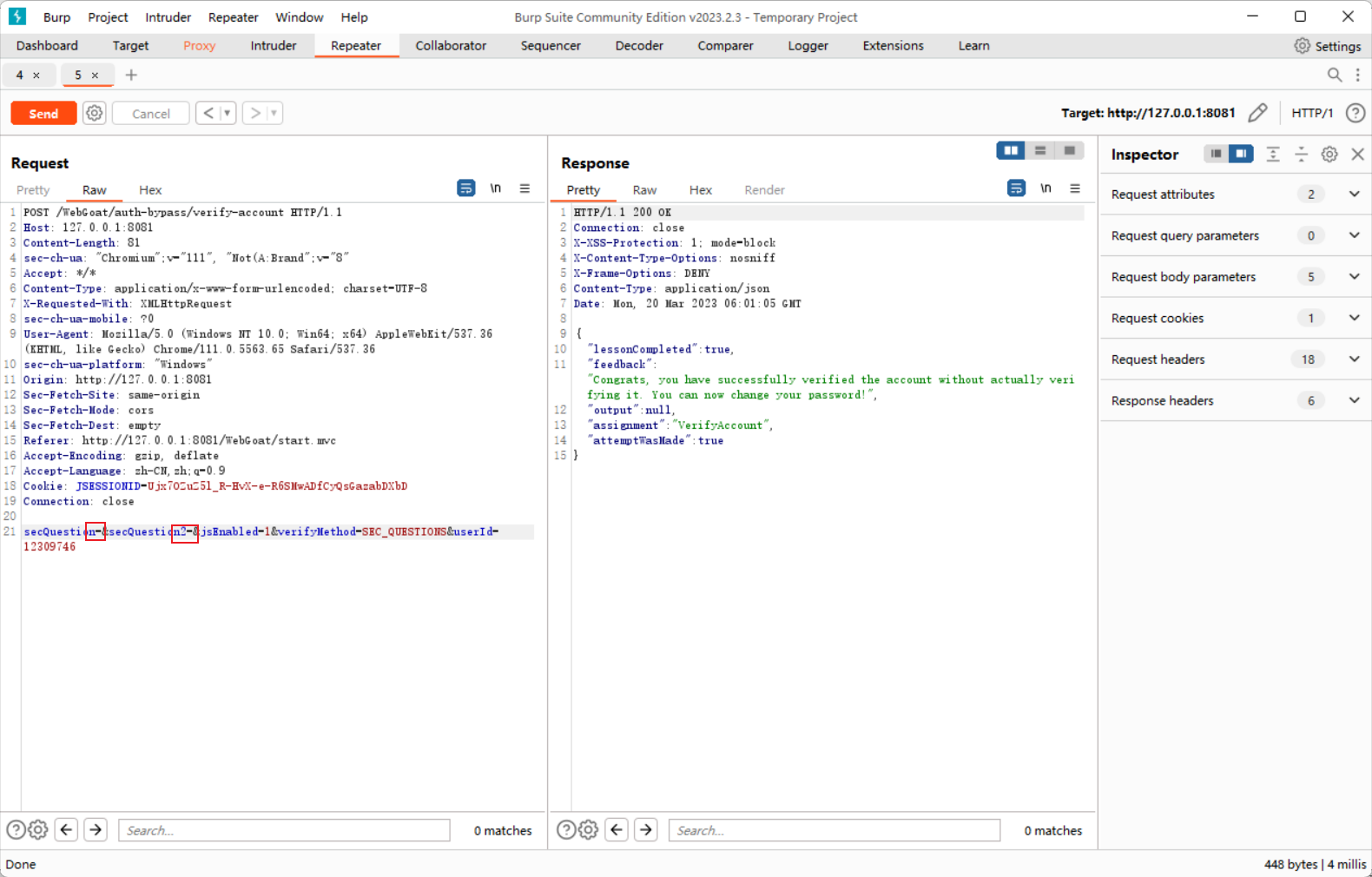




Authentication Bypasses(身份验证绕过)

2FA Password Reset

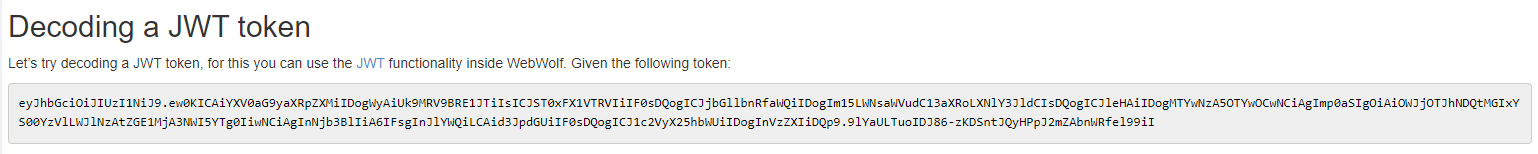
抓包修改参数编号，成功绕过



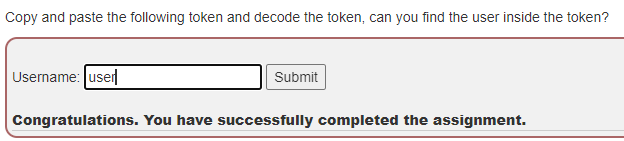
JWT tokens

Decoding a JWT token

将以下jwt token复制到解密网站

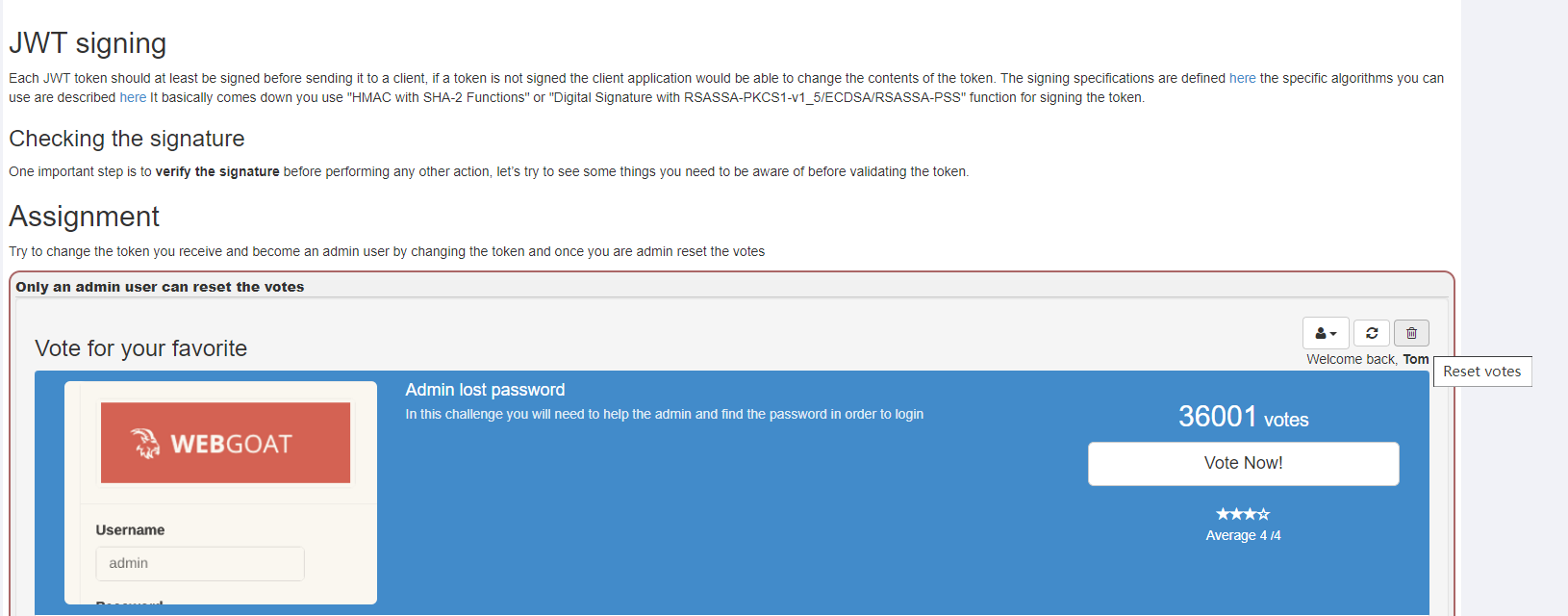
解密成功

成功



JWT signing

以Tom账号登录，发现Tom账号没有reset votes的权限，拦截reset votes请求

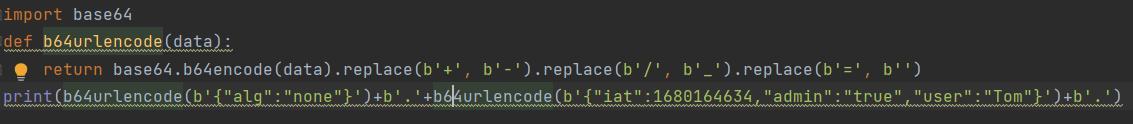


解密令牌后发现存在认证参数admin为false，令牌由HS512加密

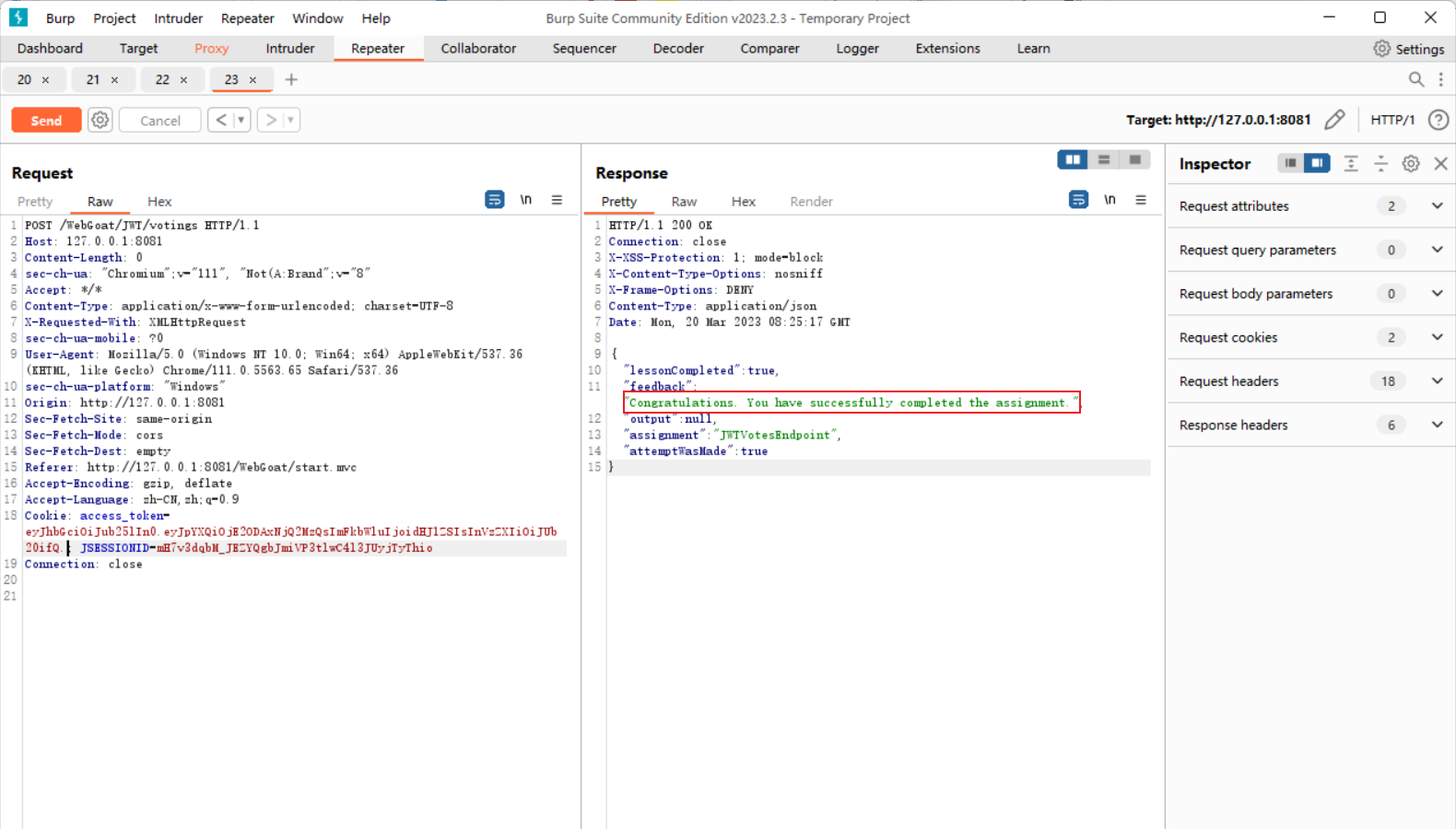


将header的加密参数设为none，payload的admin的false改为true，再按base64url形式编码后，

再将header和payload拼接



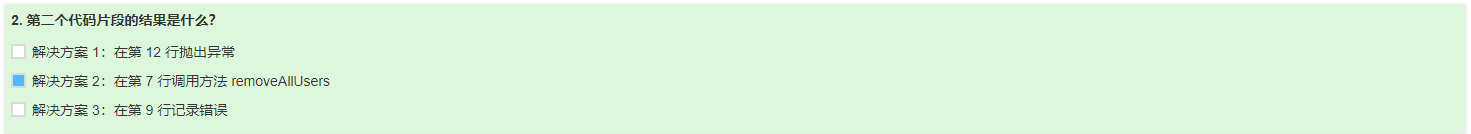
替换令牌重新发包，成功



Code review







JWT cracking

使用字典爆破jwt 密钥

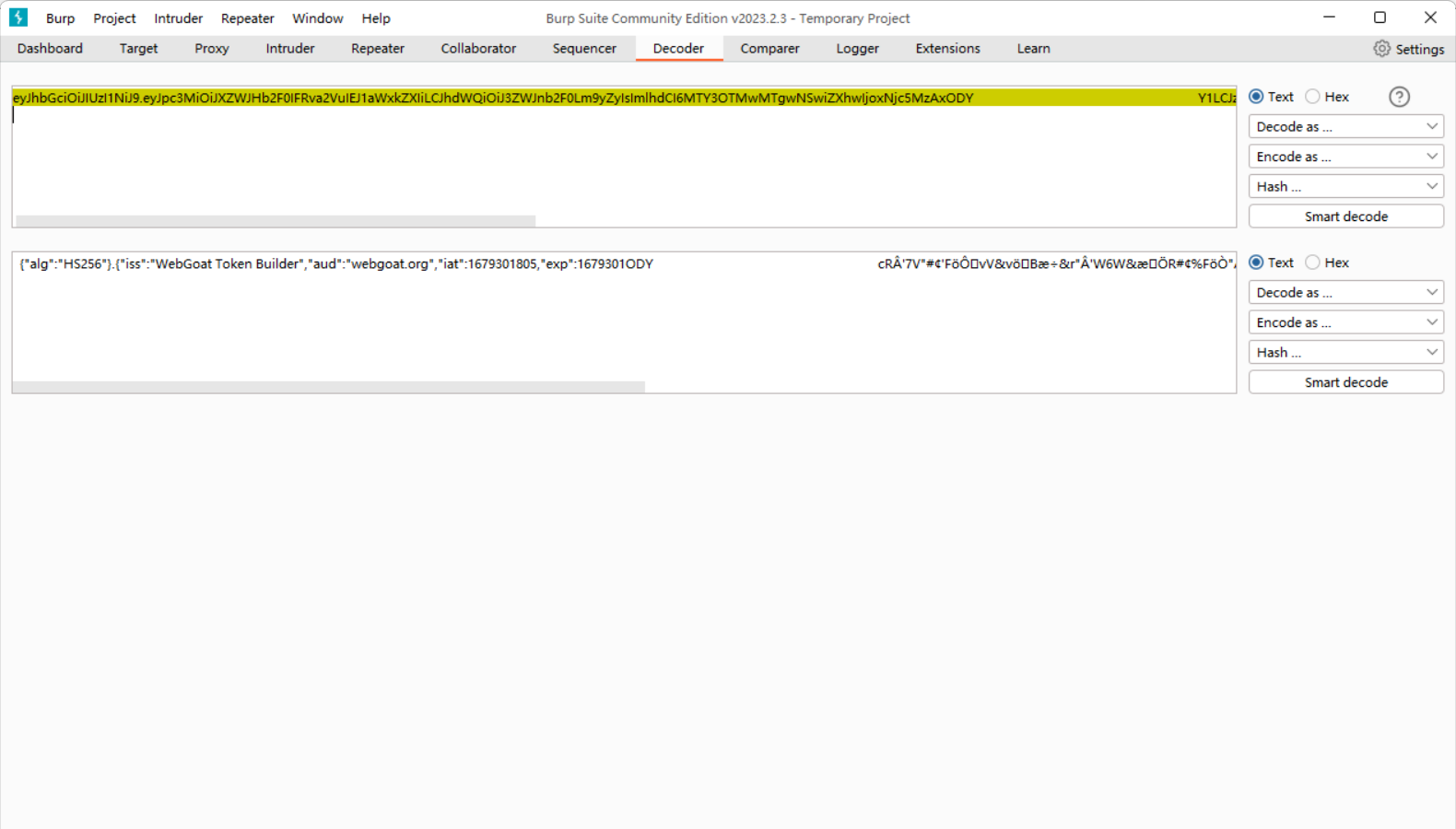
下载字典

https://github.com/first20hours/google-10000-english

使用kali linux虚拟机爆破jwt

hashcat -m 16500 jwt.txt -a 3 -w 3 20k.txt –force

将爆破获得的jwt解码，部分解码失败



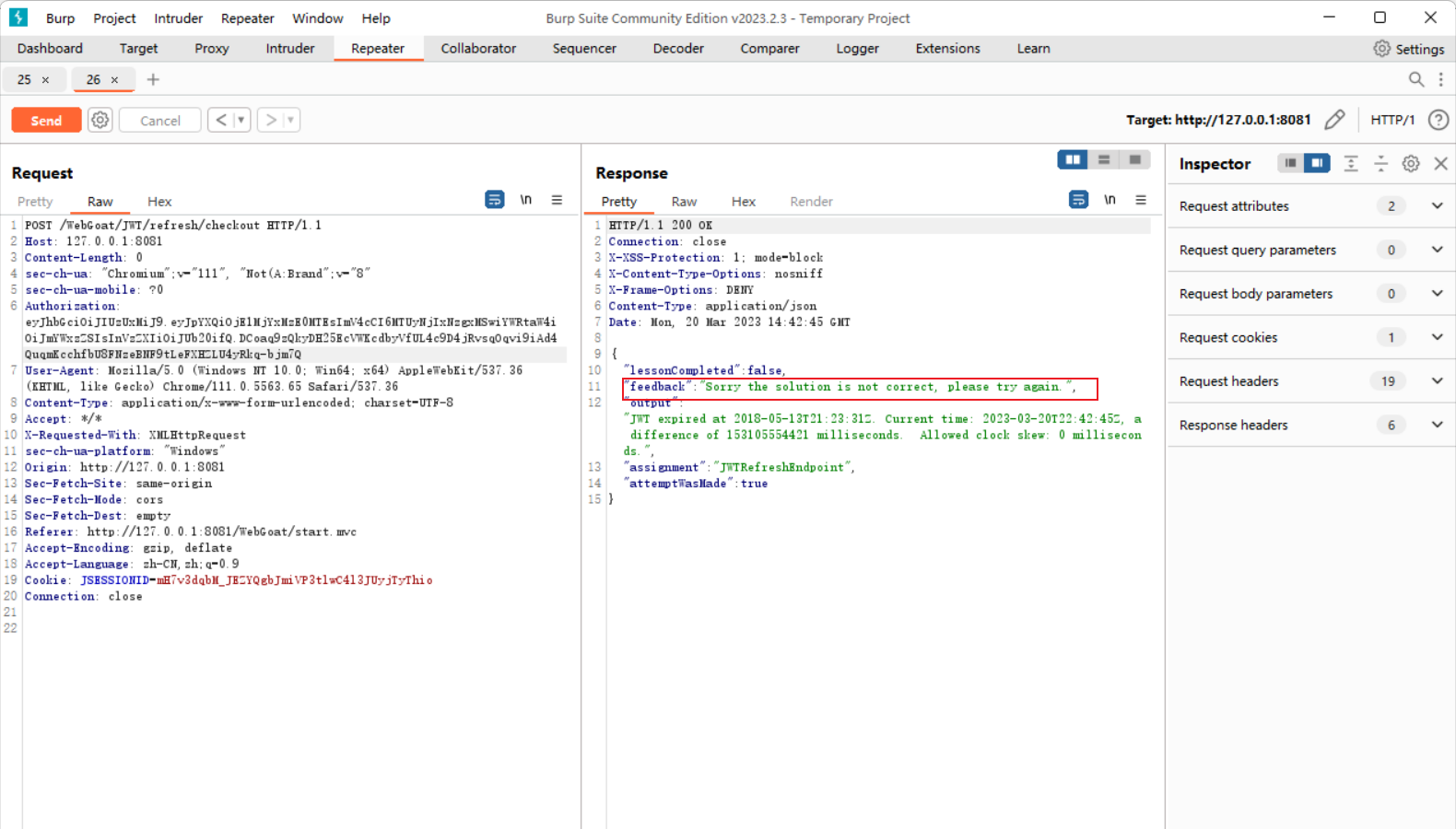
Refreshing a token

题目意思，攻击者利用Tom过期的token攻击

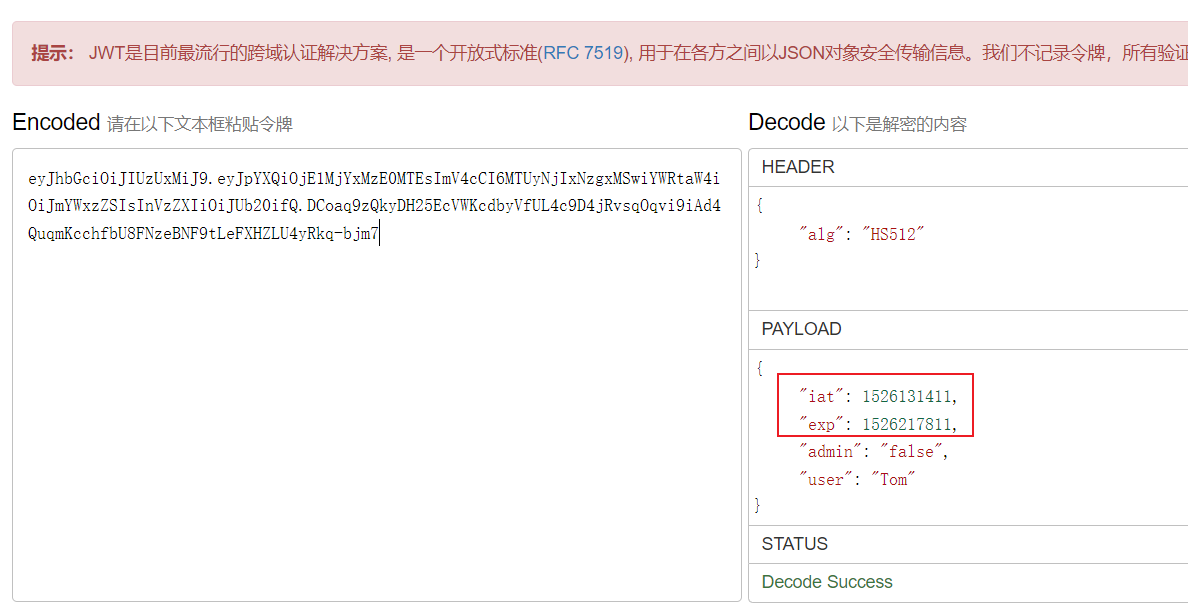
点击这里获得刷新token



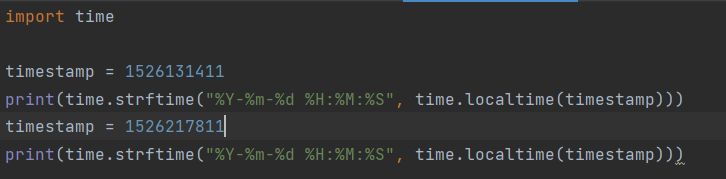
直接使用token，失败

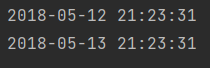


更换token时间戳

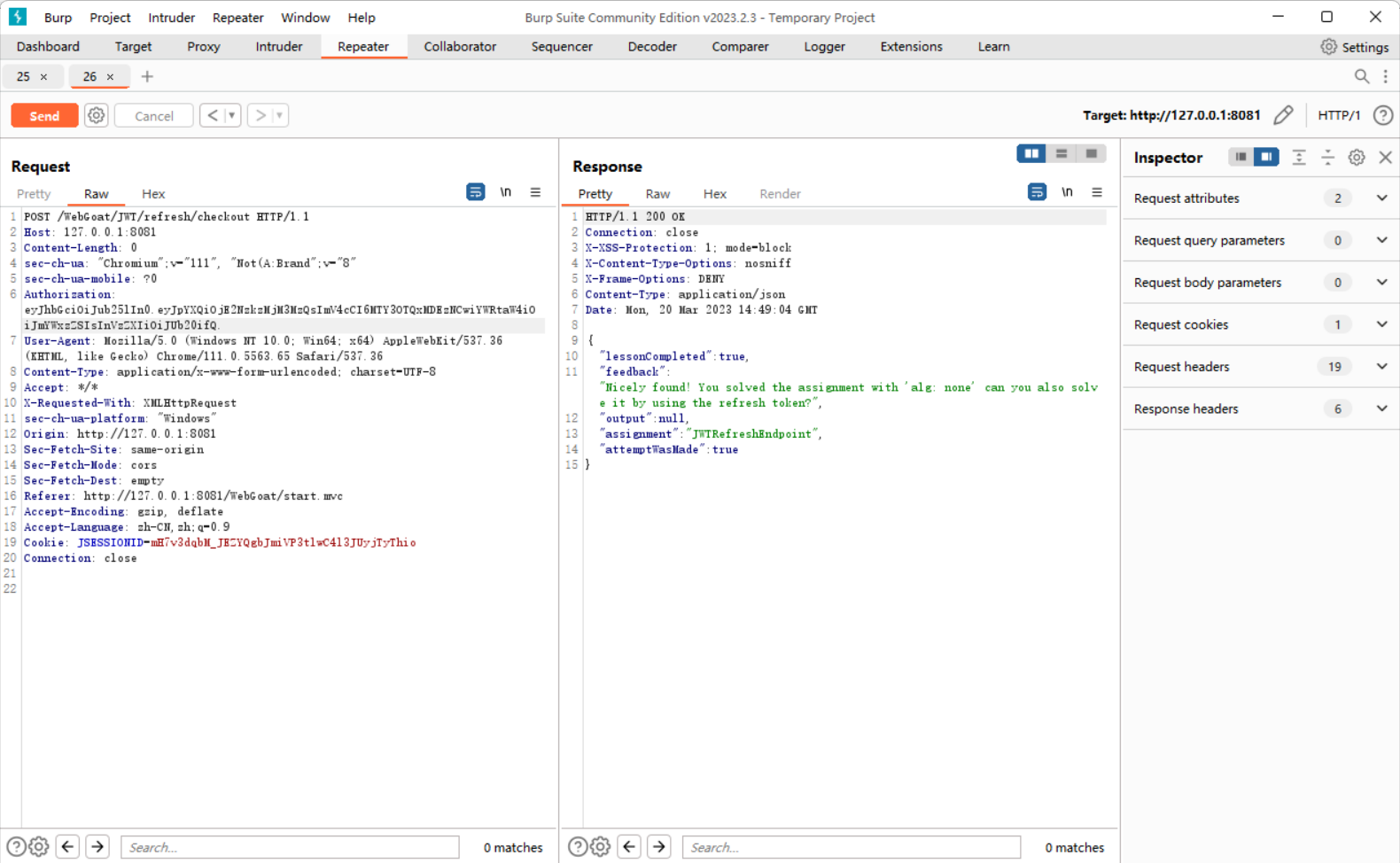


时间戳转换，发现是过期事件，时间差是一天





将时间戳iat改成现在的时间戳，exp改成与iat有一天时间差的，随后再进行b64url编码，再将header和payload拼接，替换jwt



Final challenge

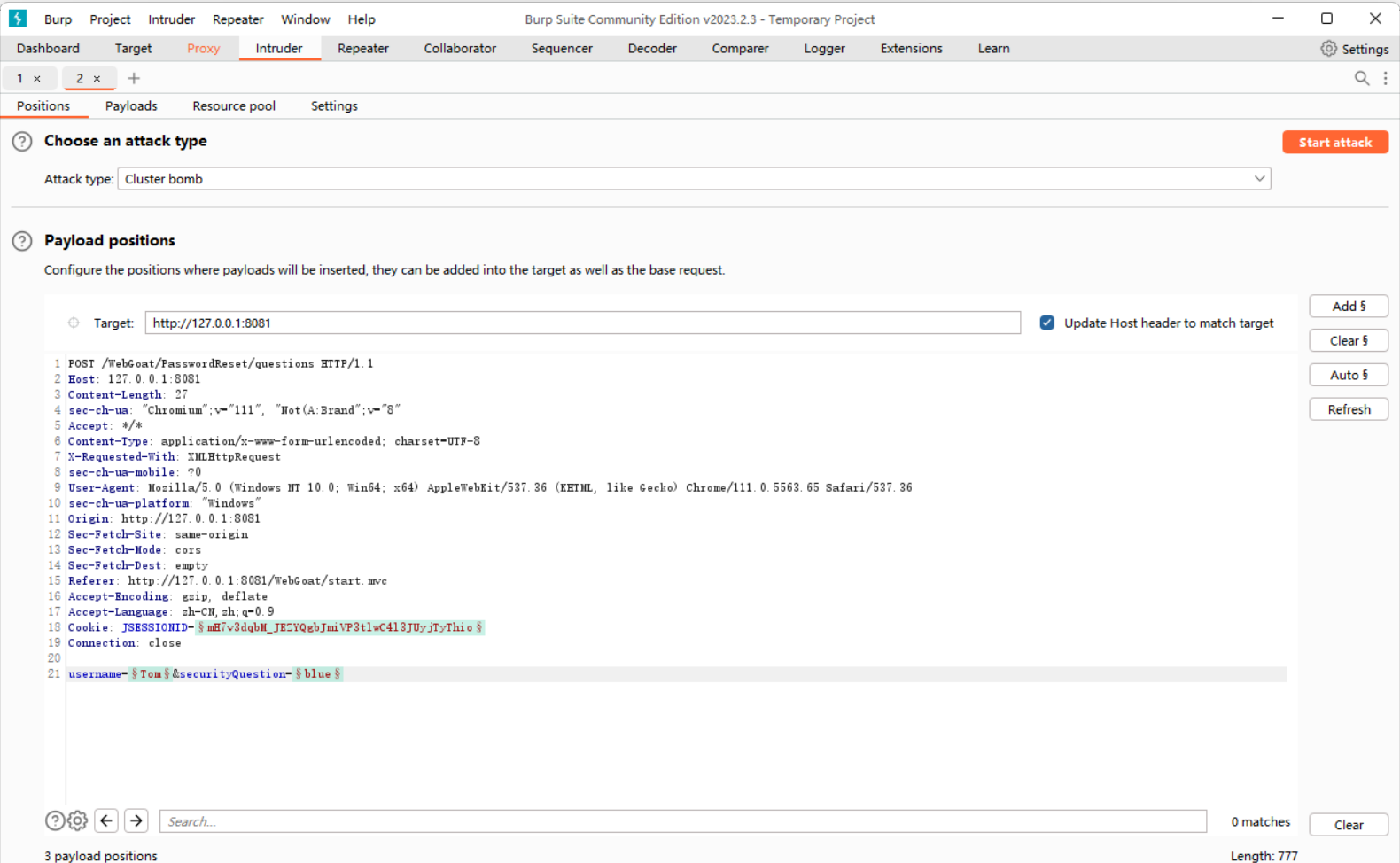
略

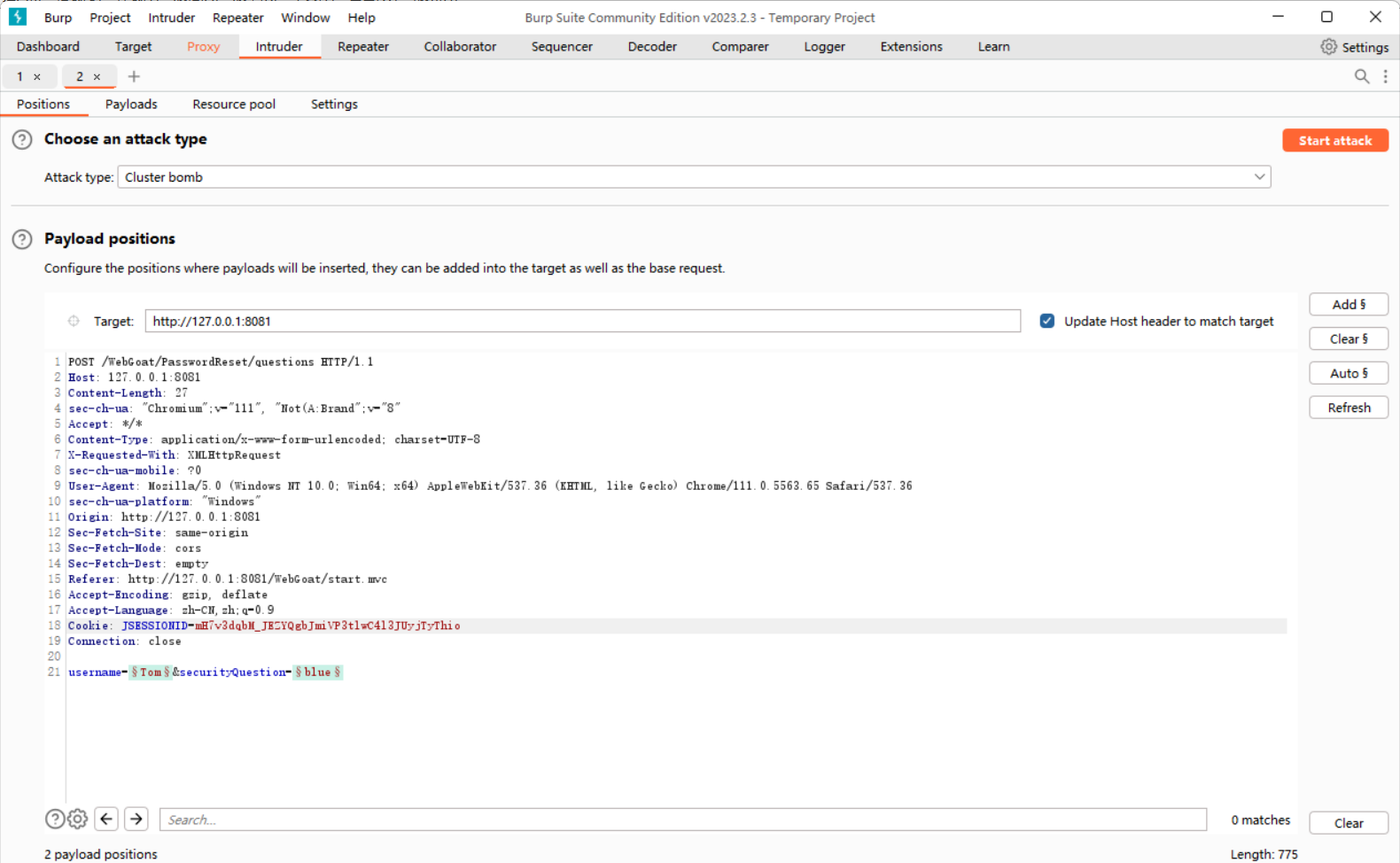
Password reset

Security questions

题意是更改tom、admin或larry的账户密码，还要输入最喜欢的颜色，可以尝试暴力破解

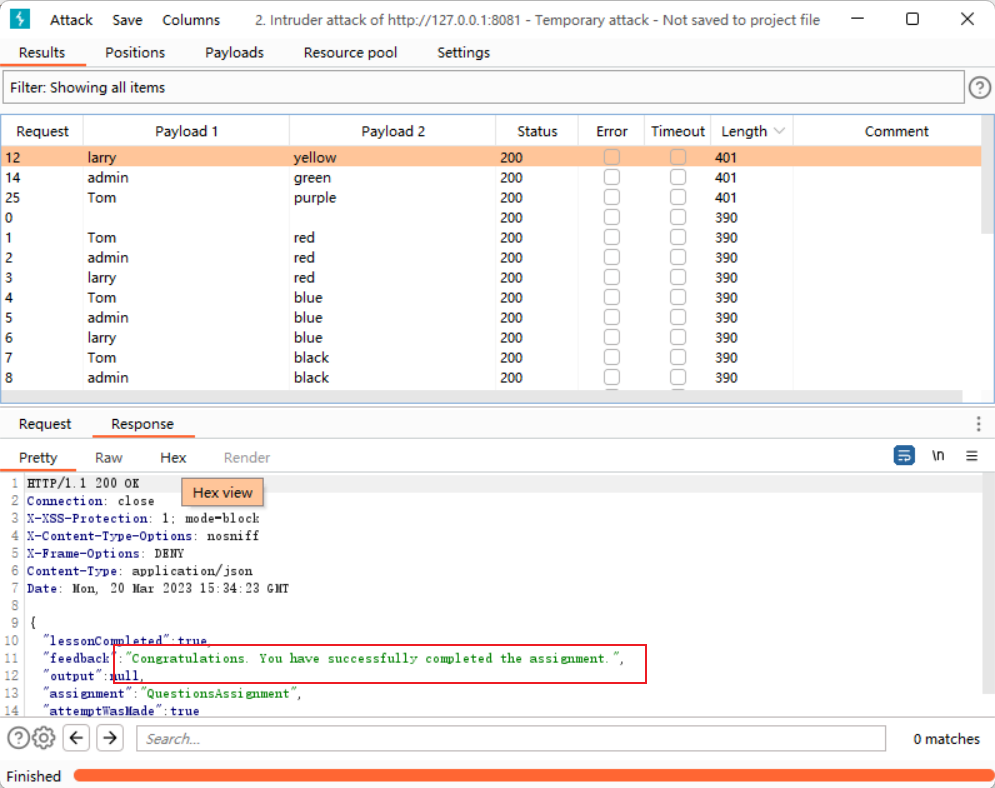
选择集束炸弹

负载1



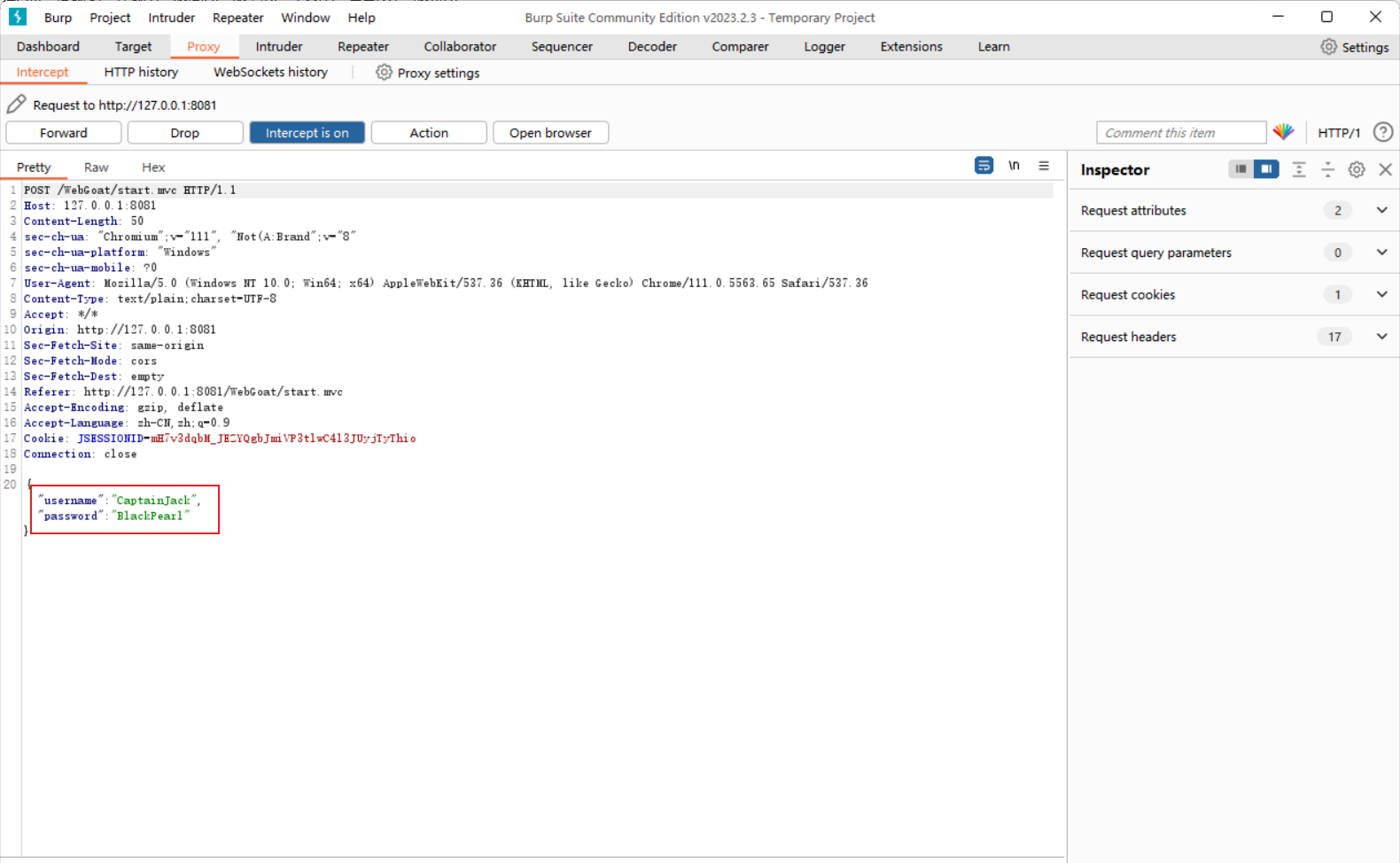
负载2

找到正确颜色

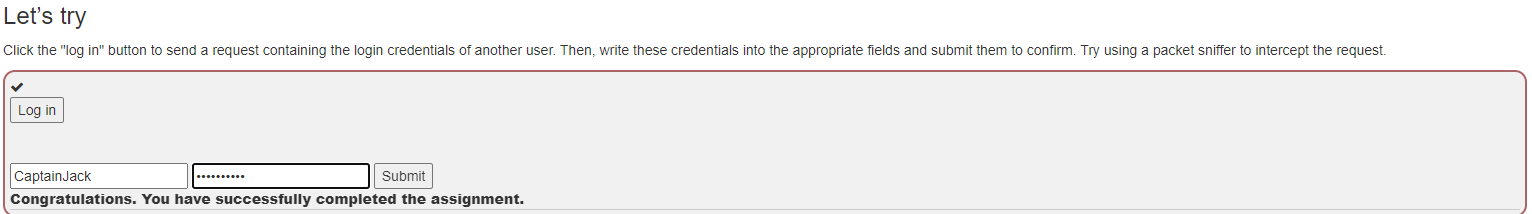


Insecure Login

按题意拦截log in请求，发现账号密码



登录成功

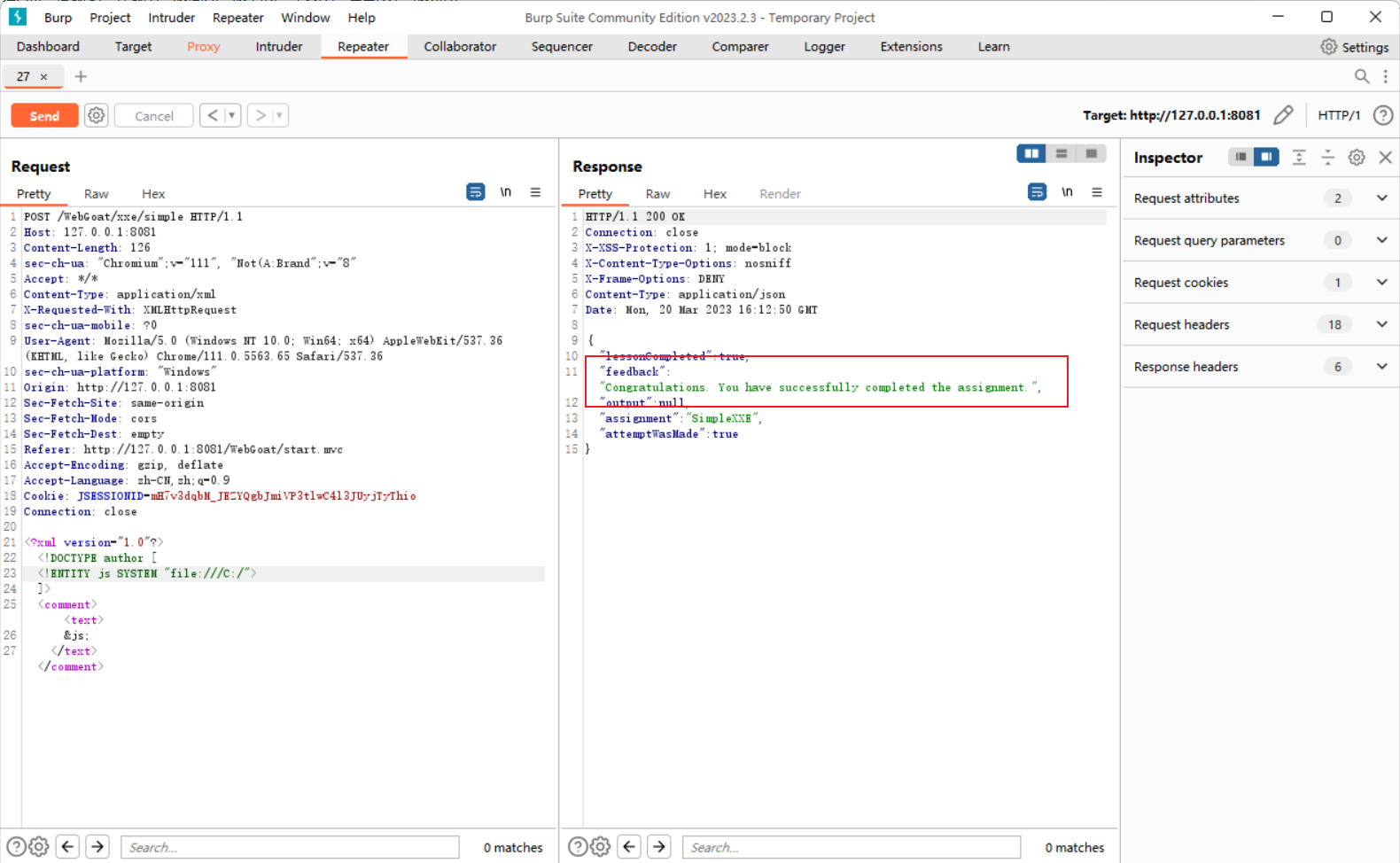


XXE

Let’s try

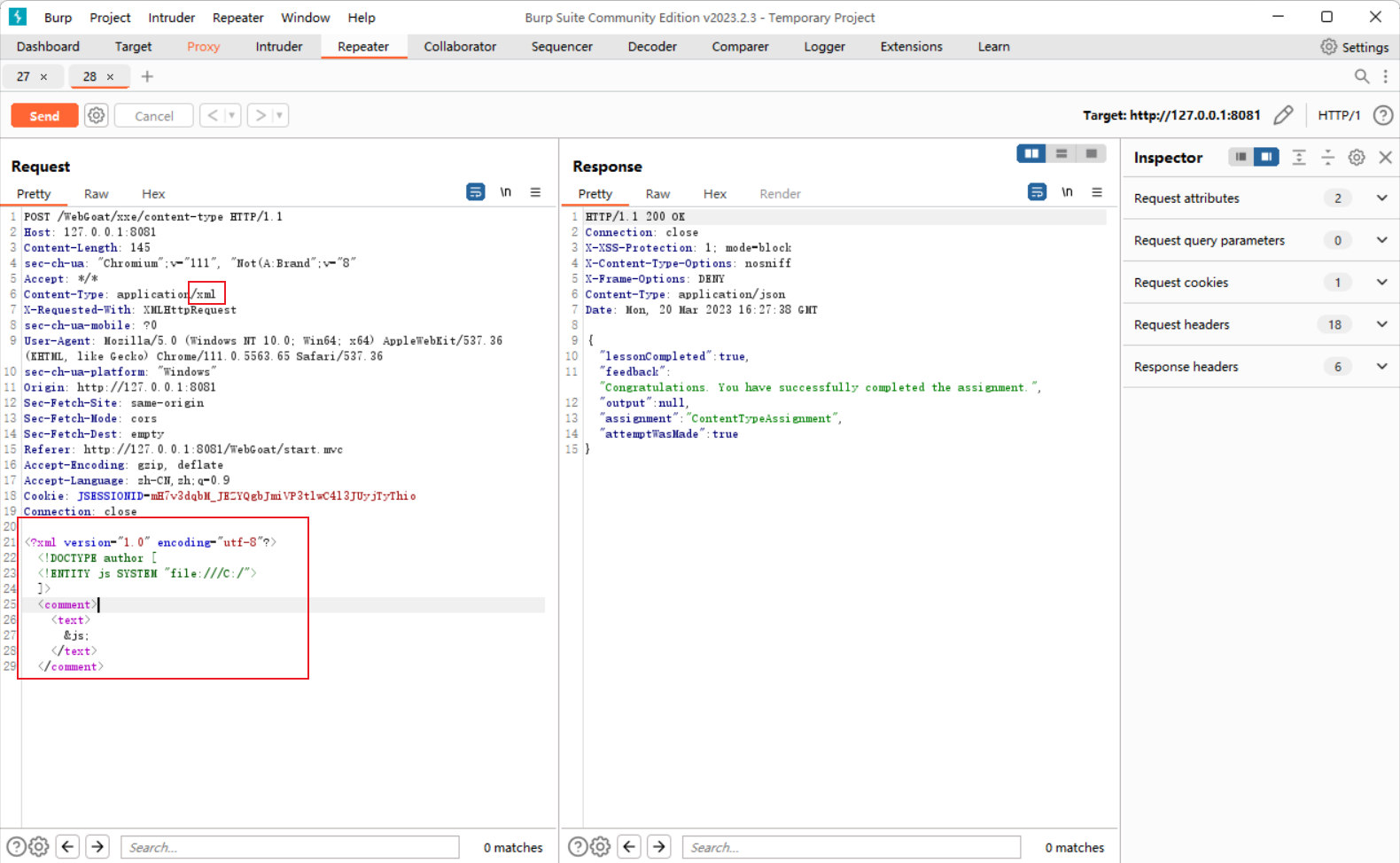
根据题意列出服务器系统目录C盘信息

按照1.3示例外部注入



Modern REST framework

根据题意，攻击者可能修改数据类型入侵，获取目标服务器系统根目录



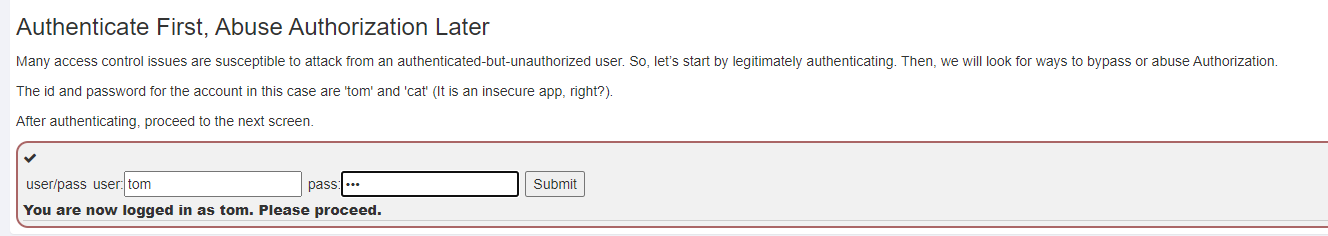
Blind XXE assignment

略

Broken Access Control

Insecure Direct Object References

题意说，输入用户名和密码



Observing Differences & Behaviors