配合Burp和Captcha-killer使用

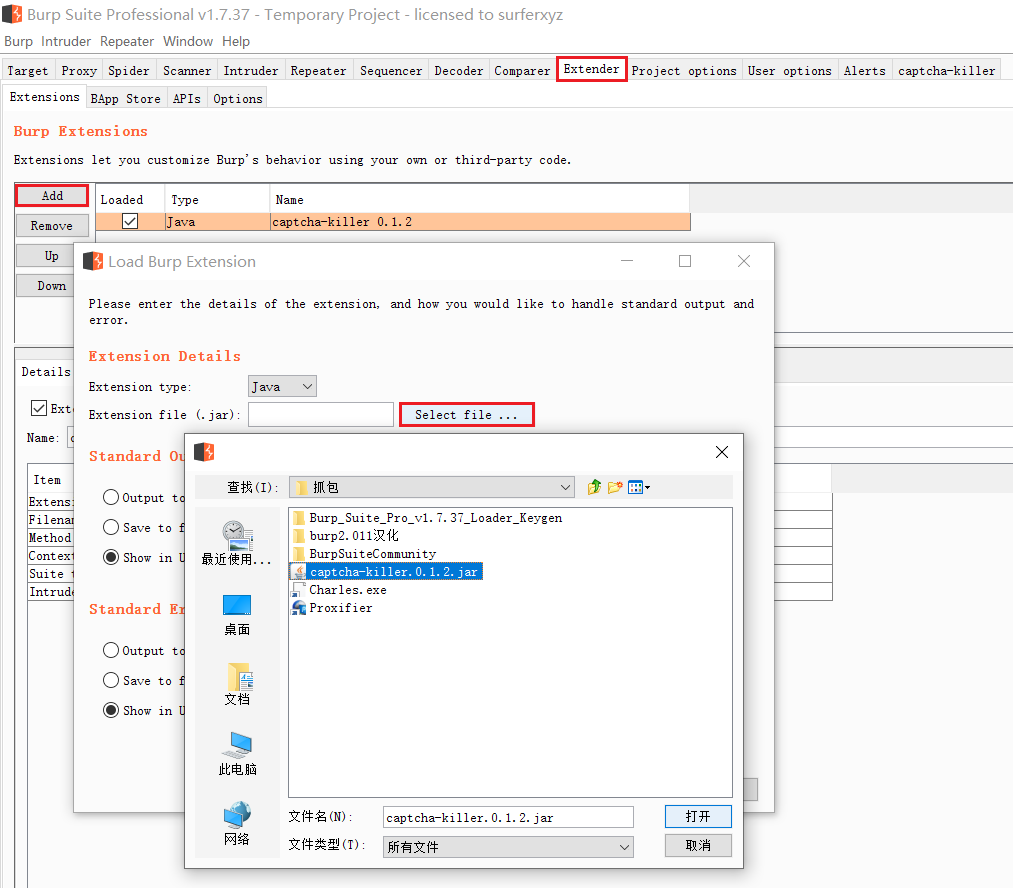
环境：Python>=3.8、PHP

1.安装ddddocr库

cmd：pip install ddddocr -i <https://pypi.tuna.tsinghua.edu.cn/simple/>

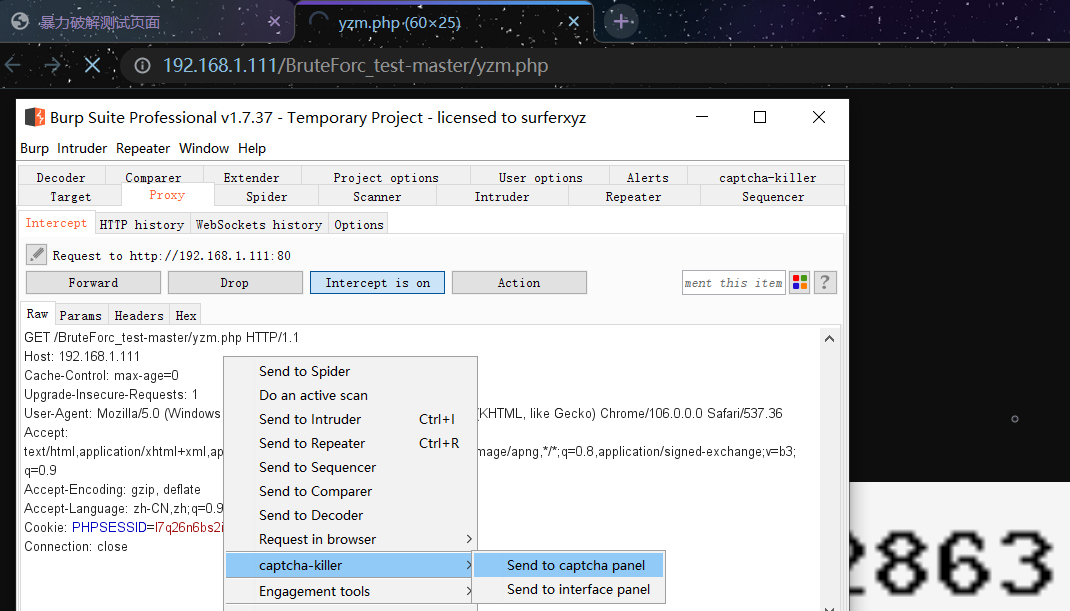
2.Burp安装Captcha-killer插件

下载：<https://github.com/c0ny1/captcha-killer/releases/download/0.1.2/captcha-killer.0.1.2.jar>



3.进行匹配

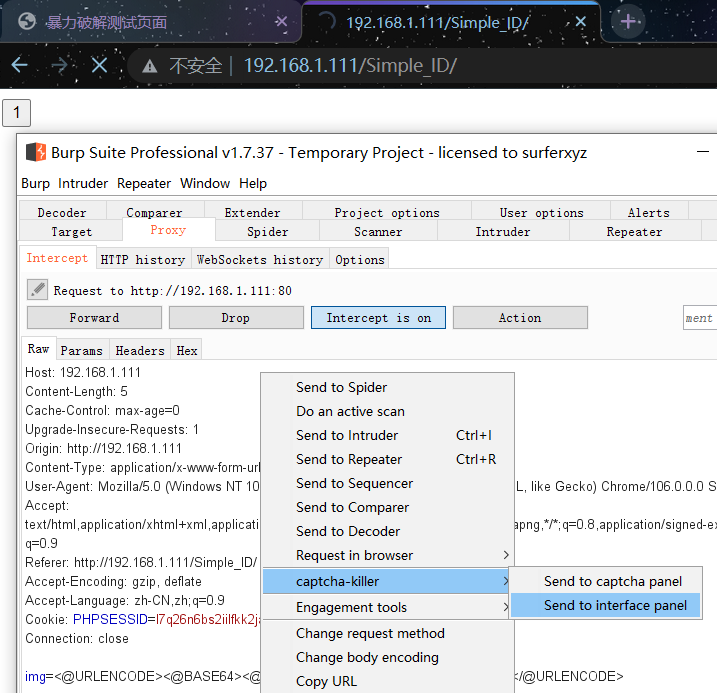
验证码抓包发往模块



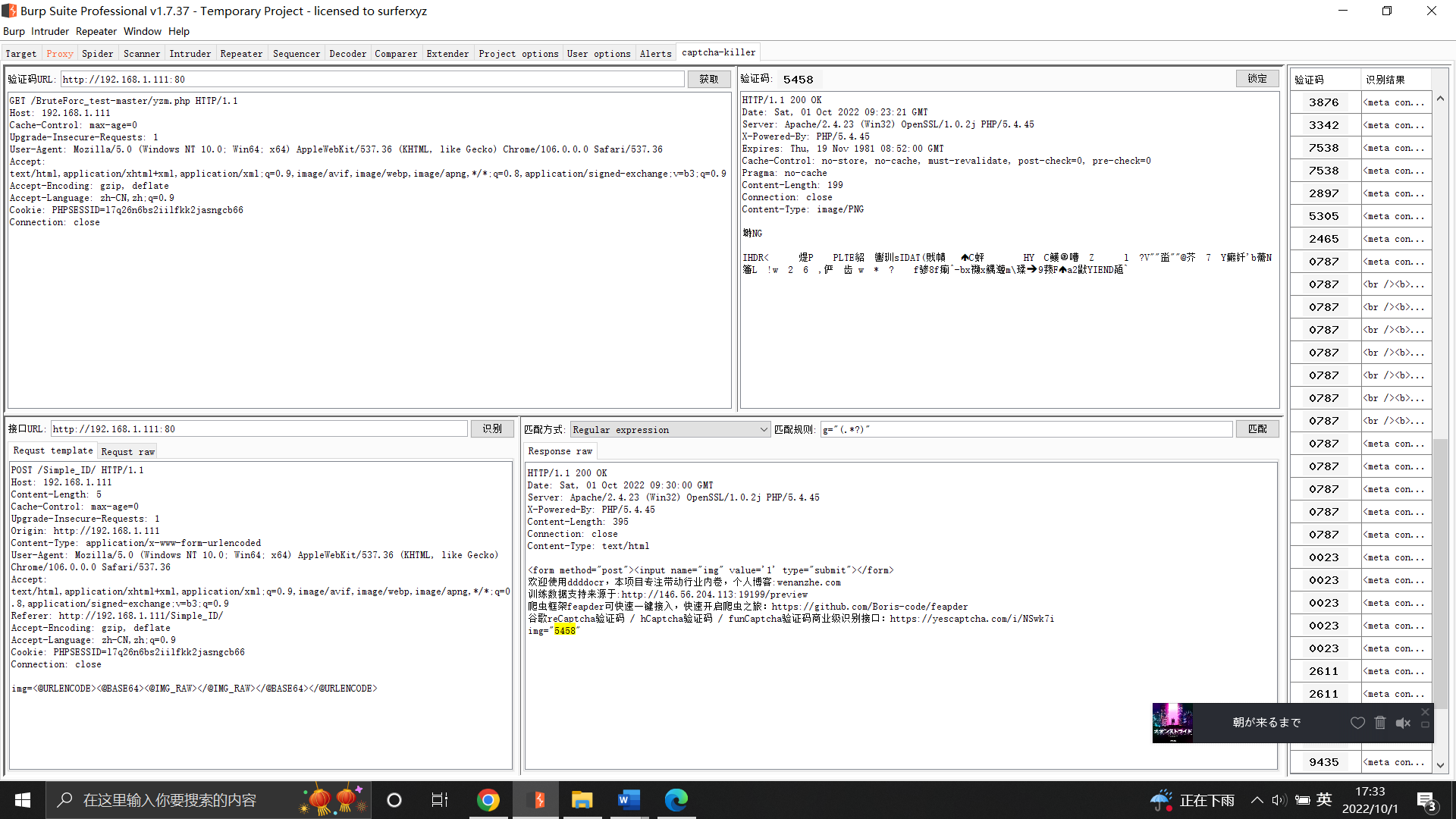
访问"IP/Simple\_ID"点击按钮并抓包

img改为<@URLENCODE><@BASE64><@IMG\_RAW></@IMG\_RAW></@BASE64></@URLENCODE>

发往模块



captcha-killer->获取->识别->匹配方式选Regular expression->匹配规则设为g="(.\*?)"->匹配



4.进行爆破

验证码的Payload这样配置，就可以开始爆破了

