基础工具运用：爆破管理员账户登录后台【配套课时：burp到支付和暴破 实战演练】

原创

E08640104 于 2021-04-14 00:10:03 发布 1034 收藏 4
分类专栏： 渗透测试 文章标签： 渗透测试 安全
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/E08640104/article/details/115682817
版权


渗透测试 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

题目：

第二关拿到密码后，虽然在admin路径中成功登录后台，但那竟然是一个假后台！

不过没关系，尤里也遇到过不少假后台，他决定换个思路入手，通过信息收集…… 它找到了女神的另一个购物网站，尤里决定从这个网站入手……

一、登录爆破

1、http://59.63.200.79:8003/dami_999/dami_666/index.php首页右上角有个登录按钮，厉害了，点击登录

2、居然这么简单，直接就给了登录页面，直接burpsuite进行爆破，一顿操作猛如虎

3、结果用网站提供的词典等了很久，没有登录成功，提示 不存在账号，what！！！

果然没有这么简单，这个登录应该是用户登录页面，小芳是管理员啊，应该还有其他登录地址

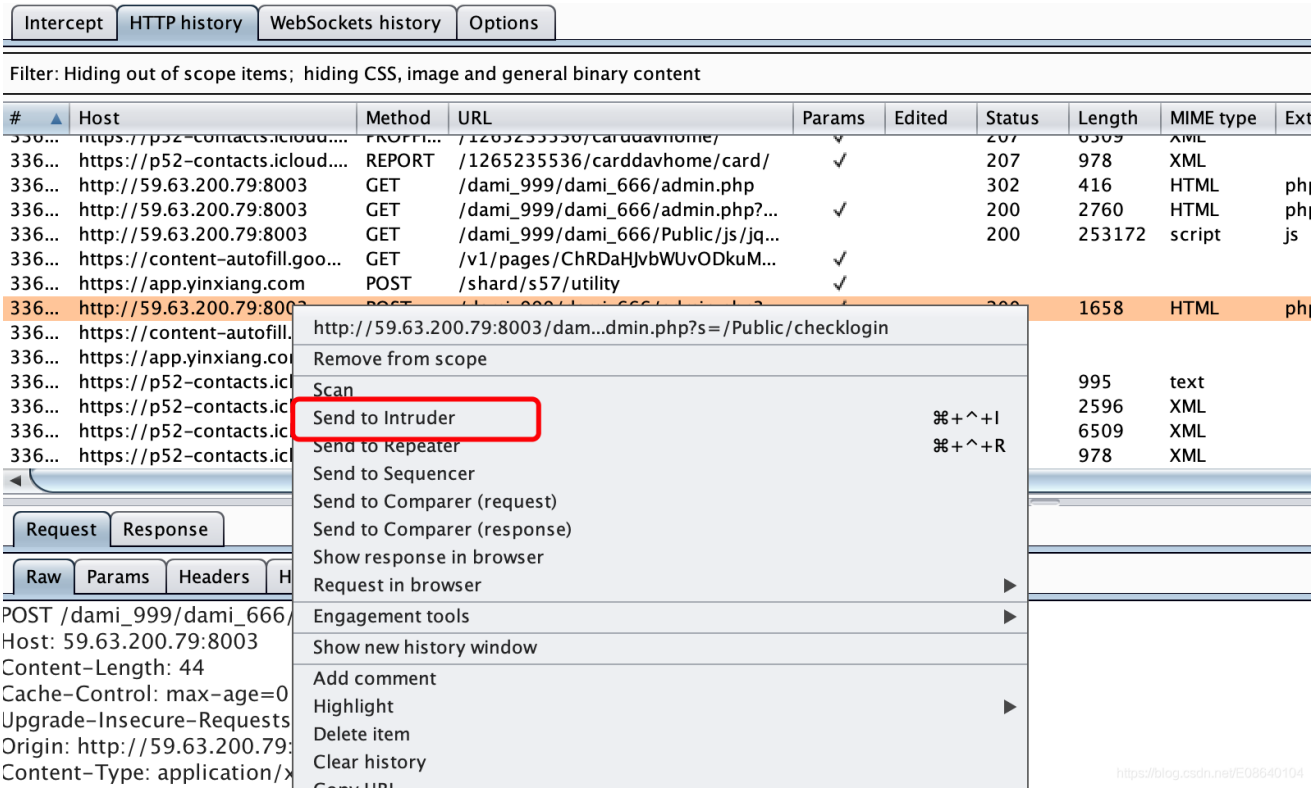
二、扫描后台

找到了后台的登录地址是http://59.63.200.79:8003/dami_999/dami_666/admin.php?

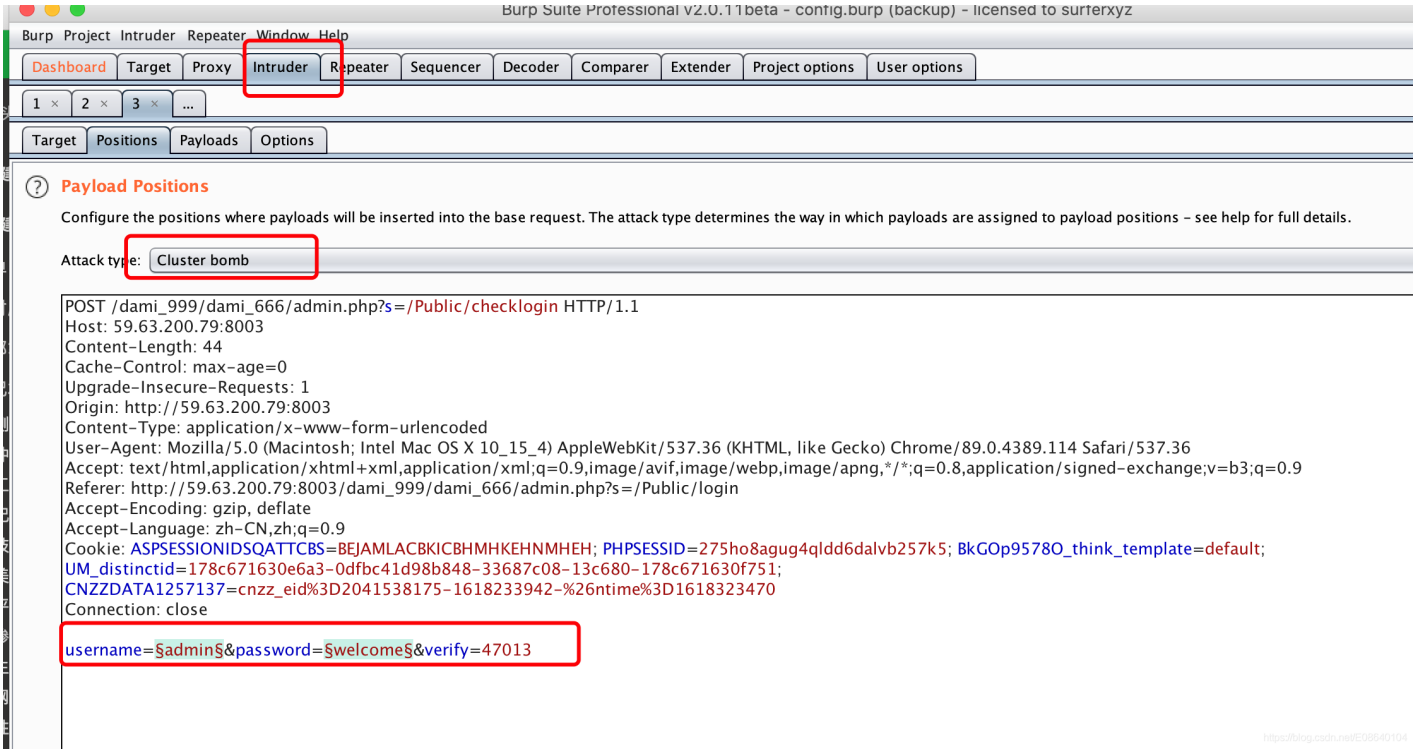
三、登录爆破

既然找到了，继续爆破

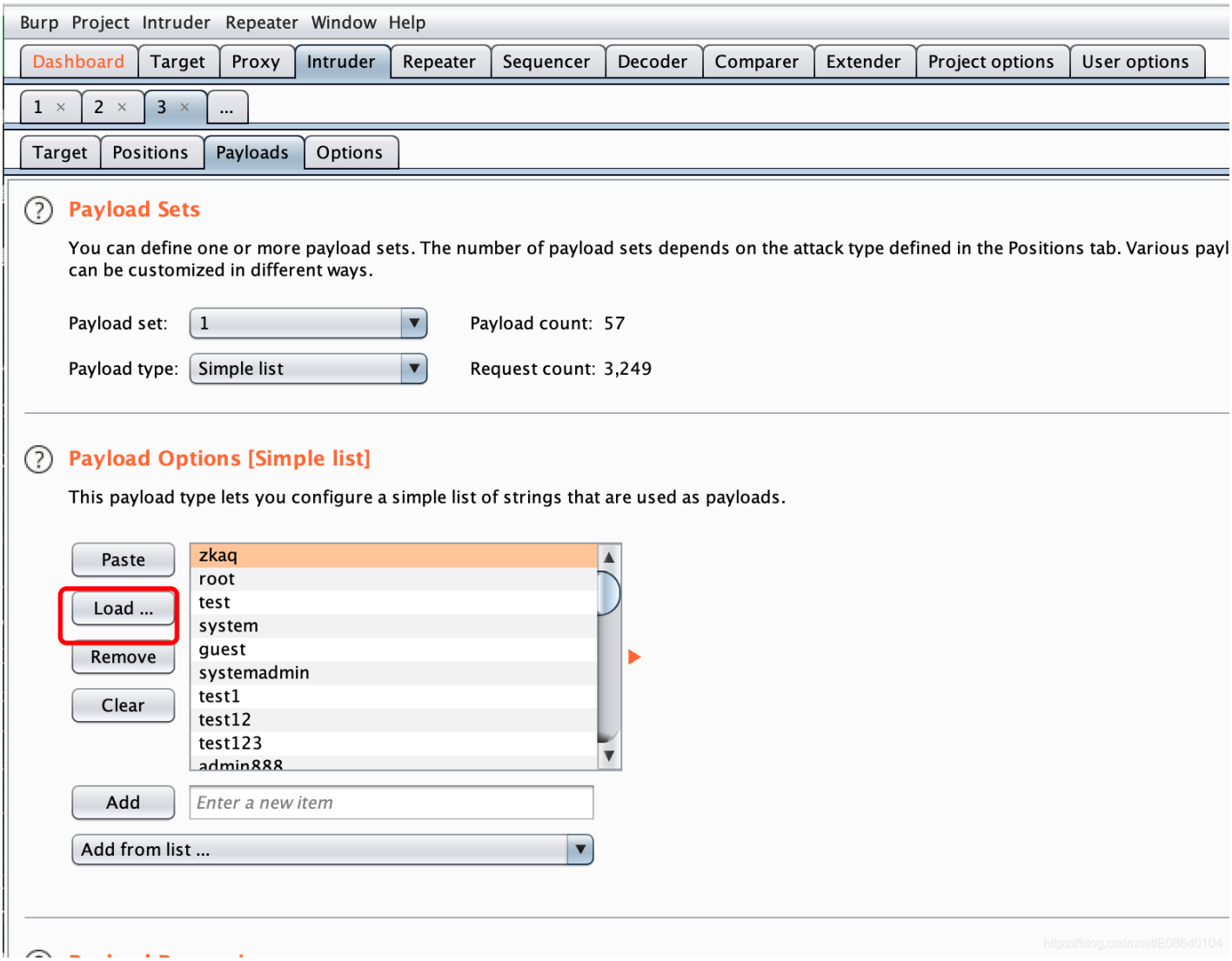
1）首先burpsuite找到登录请求（需要先填一个错误的密码提交），右击选择send to intruder



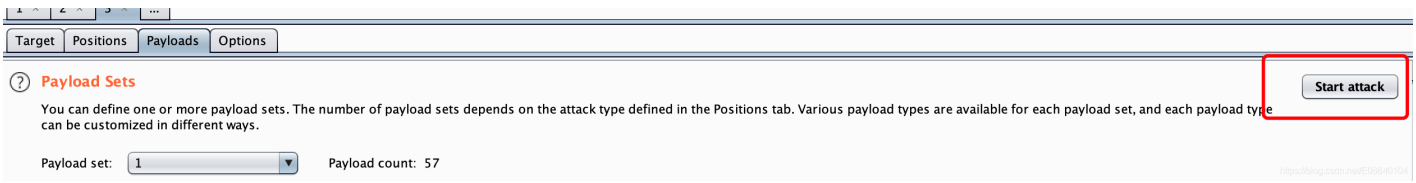
2）选择交叉爆破，2个变量



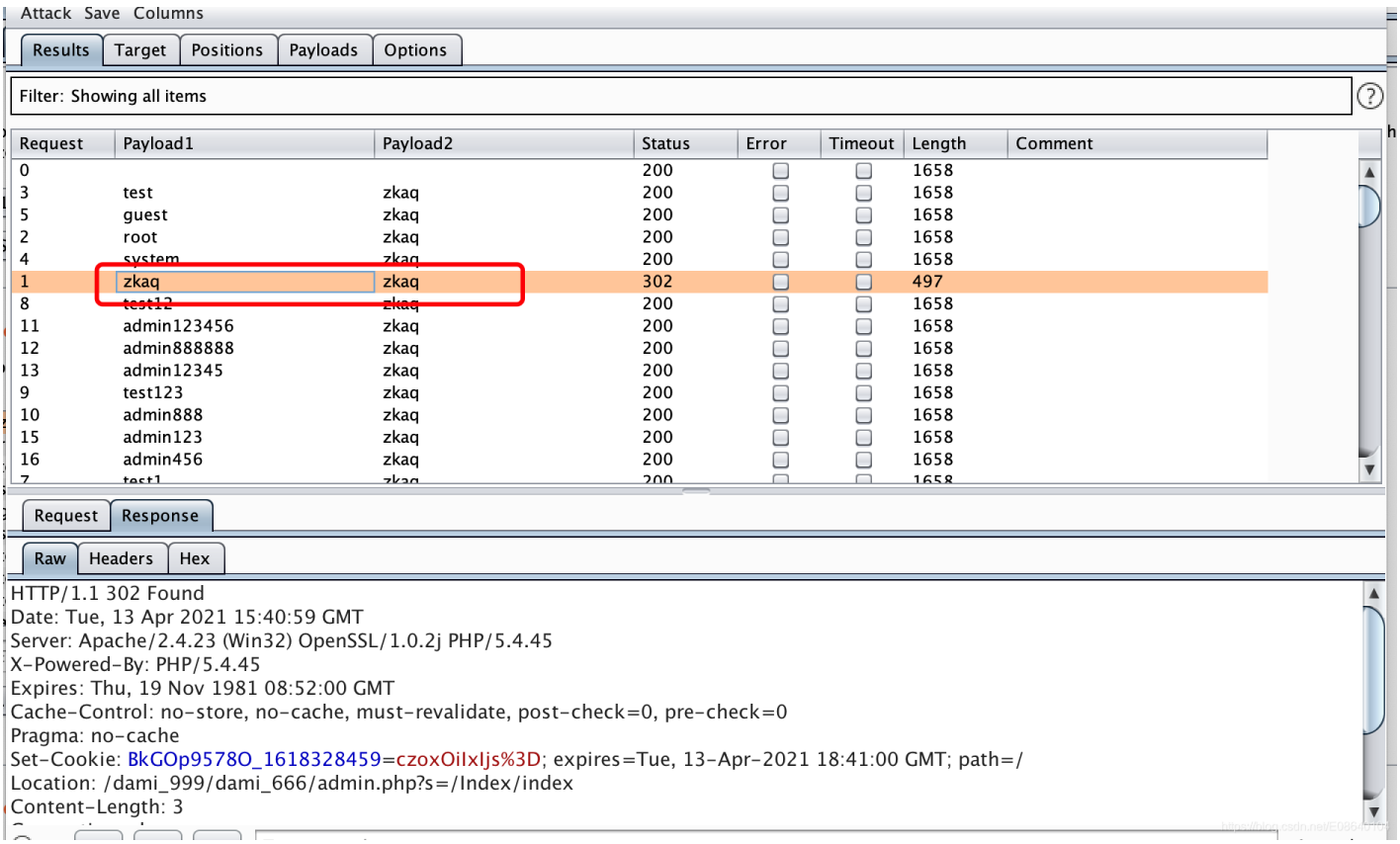
3）加载词典



4）点击start attack 开始爆破！



5）查看爆破情况，只有账号zkaq密码zkaq的 返回状态码是302，其余200的都显示账号错误，就是他了！



四、拿到flag

用账号zkaq密码zkag登录http://59.63.200.79:8003/dami_999/dami_666/admin.php?，哈哈哈，看到flag了，成功