登录

【reCAPTCHA】一款识别图形验证码的Burp Suite插件

勾陈安全 / 2017-11-01 08:46:06 / 浏览数 7104 安全工具 工具 顶(0) 踩(0)

0x01 简介

一个burp插件，自动识别图形验证码，并用于Intruder中的Payload。

项目主页：https://github.com/bit4woo/reCAPTCHA

0x02 使用

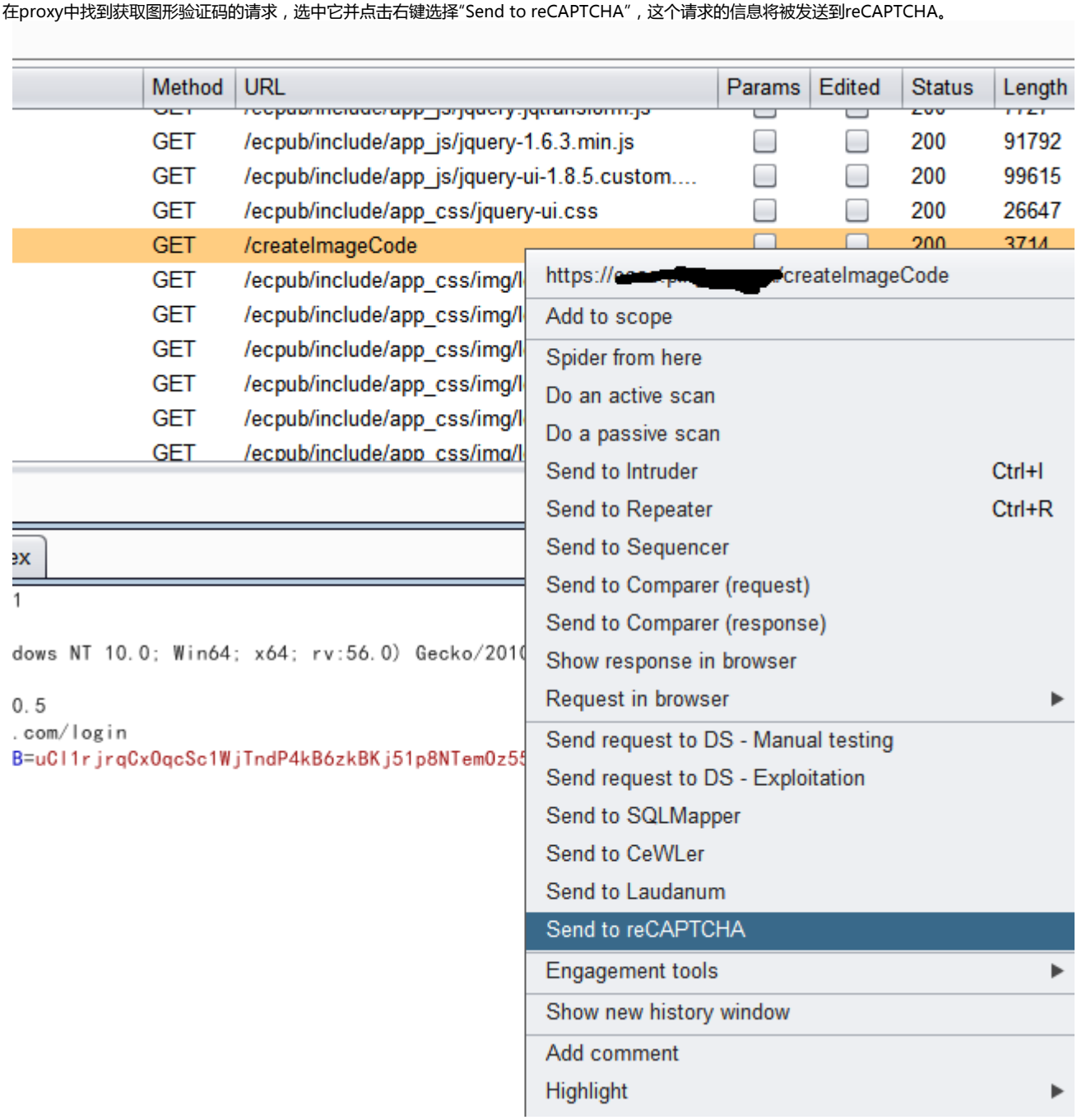
安装：

1. 从这里下载插件。
2. 将它添加到burp。如果没有遇到错误，你将看到一个新的名为“reCAPTCHA”的tab。

准备：

通过burp代理访问目标网站的登录界面。

在proxy中找到获取图形验证码的请求，选中它并点击右键选择“Send to reCAPTCHA”，这个请求的信息将被发送到reCAPTCHA。



切换到reCAPTCHA标签，并配置所需的参数。当参数配置好后，你可以点击"请求"按钮来测试配置。

http://www.ysdm.net
的API是目前唯一支持的接口,其中的各项参数需要自行注册帐号并填写，才能成功调用接口完成图片的识别。该API需要的参数如下，请用正确的值替换%s，特别注意typeid值的设定(http://www.ysdm.net/home/PriceType)。

```
username=%s&amp;password=%s&amp;typeid=%s&amp;timeout=%s&amp;softid=%s&amp;softkey=%s
```

在Intruder中使用：

完成了配置并测试成功后，现在可以在Intruder中使用该插件生成的payload了。有2种情况：用户名或密码之一+验证码；用户名+密码+验证码；

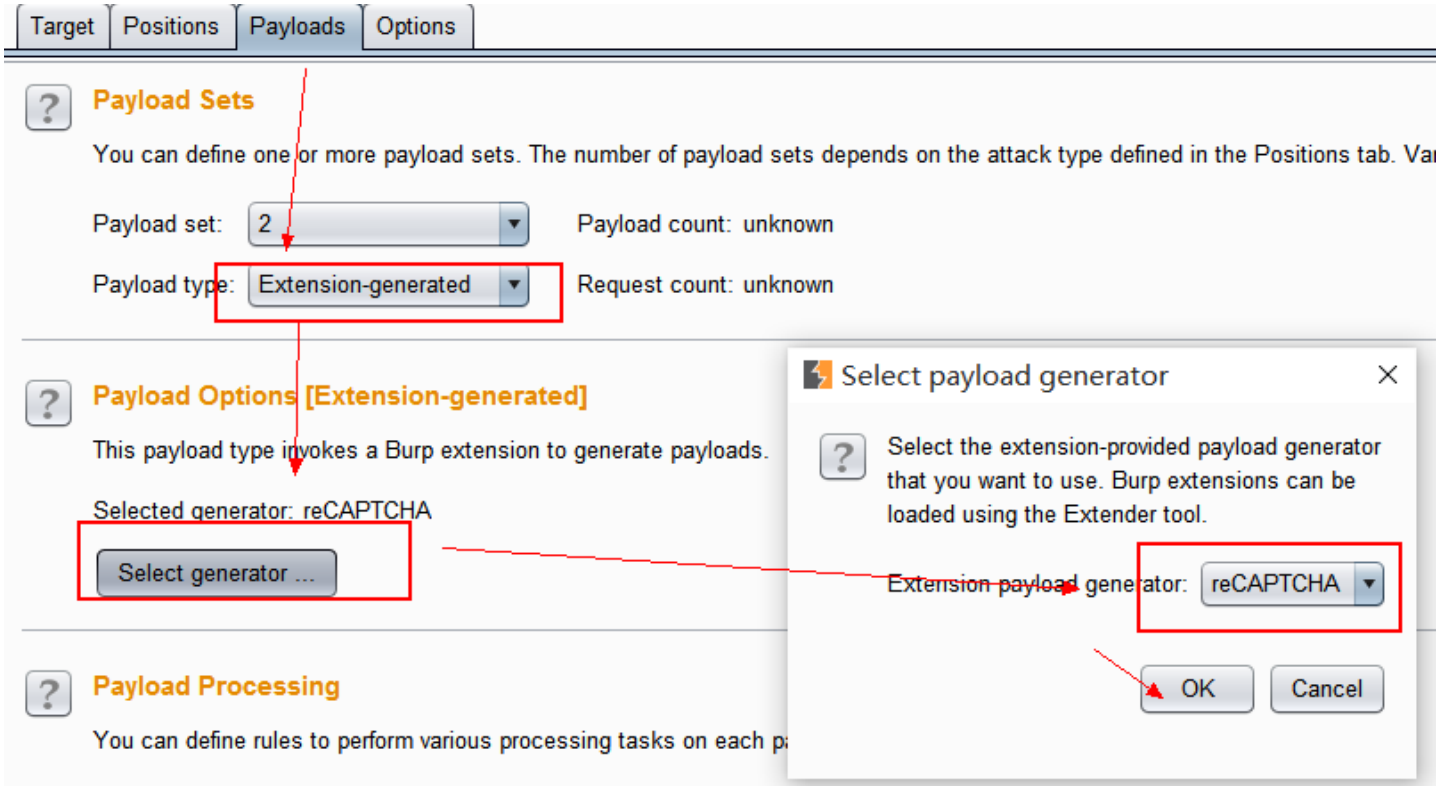
情况一：只有密码或只有用户名需要改变，我们可以用Pitchfork 模式来配置。

比如，已知系统存在一个用户admin，来爆破该用户，插入点标记如下，

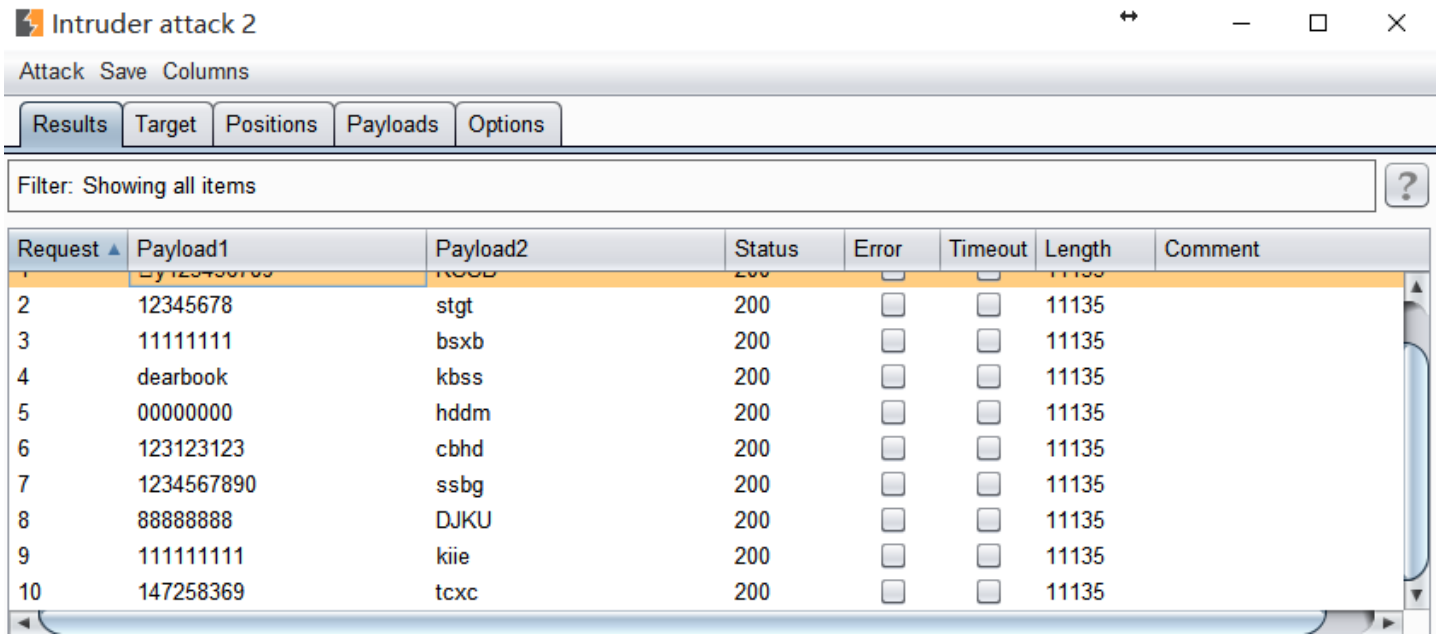
```
j_username=admin&j_password=§admin§&inputRand=§b8cx§&singleFlag=submited&TARGET=
```

payload 1我们从文件中加载，这个不必多说。

payload 2 选择`Extension-Generated`



运行效果如下：



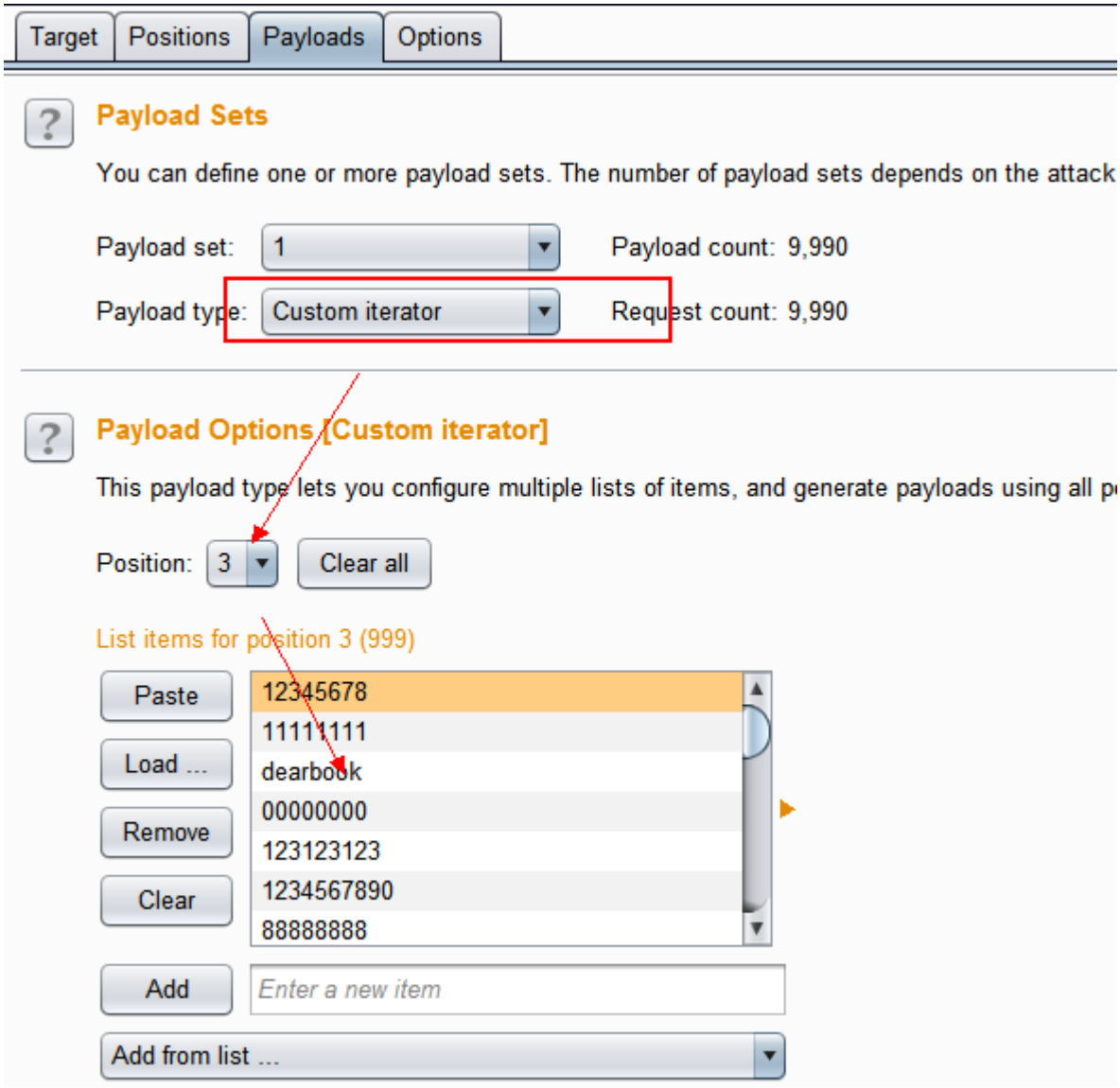
Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
2	12345678	stgt	200			11135	
3	11111111	bsxb	200			11135	
4	dearbook	kbss	200			11135	
5	00000000	hddm	200			11135	
6	123123123	cbhd	200			11135	
7	1234567890	ssbg	200			11135	
8	88888888	DJKU	200			11135	
9	111111111	kiie	200			11135	
10	147258369	tcxc	200			11135	

情况二：用户名和口令都需要改变，这个稍微复杂点。我们还是使用Pichfork模式，但需要将用户名和密码一起标注为一个插入点。像这样:

```
j_username=§admin&j_password=admin§&inputRand=§b8cx§&singleFlag=submited&TARGET=
```

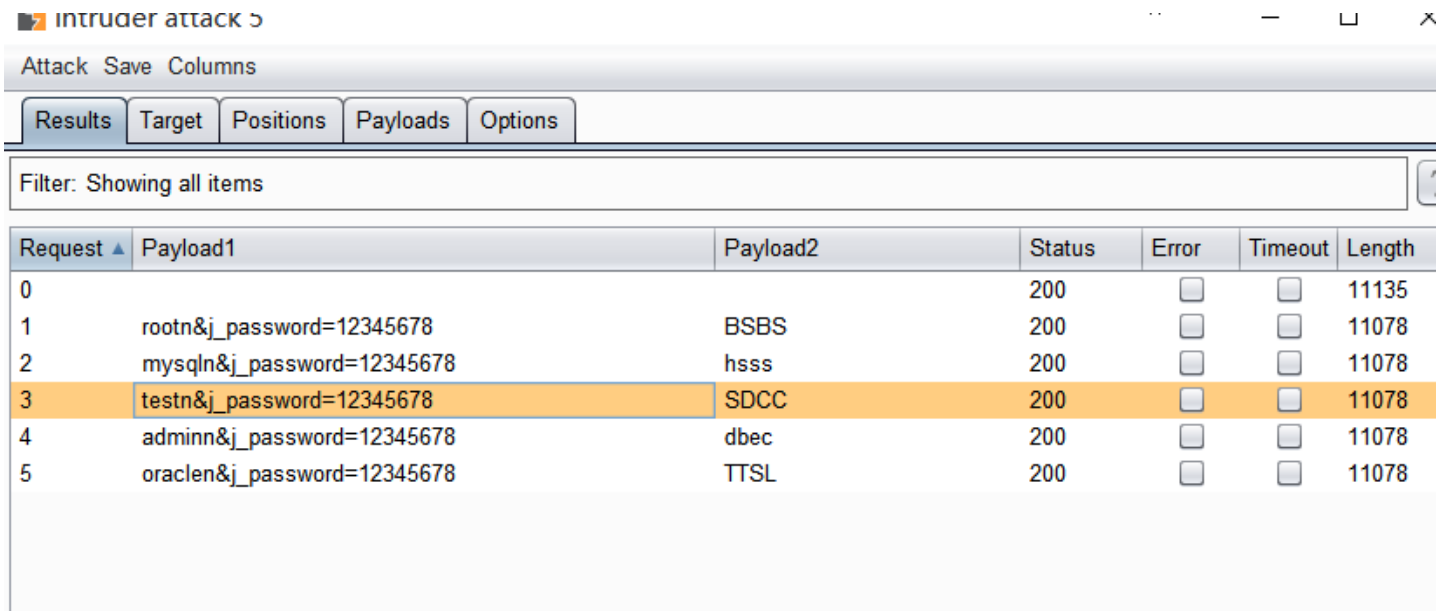
payload 1 使用■■■■■■■Custom interator■。并在迭代器中组合用户名和密码。

在该例子中，即position 1为用户名，position 2为&j_password=，postion 3为密码。

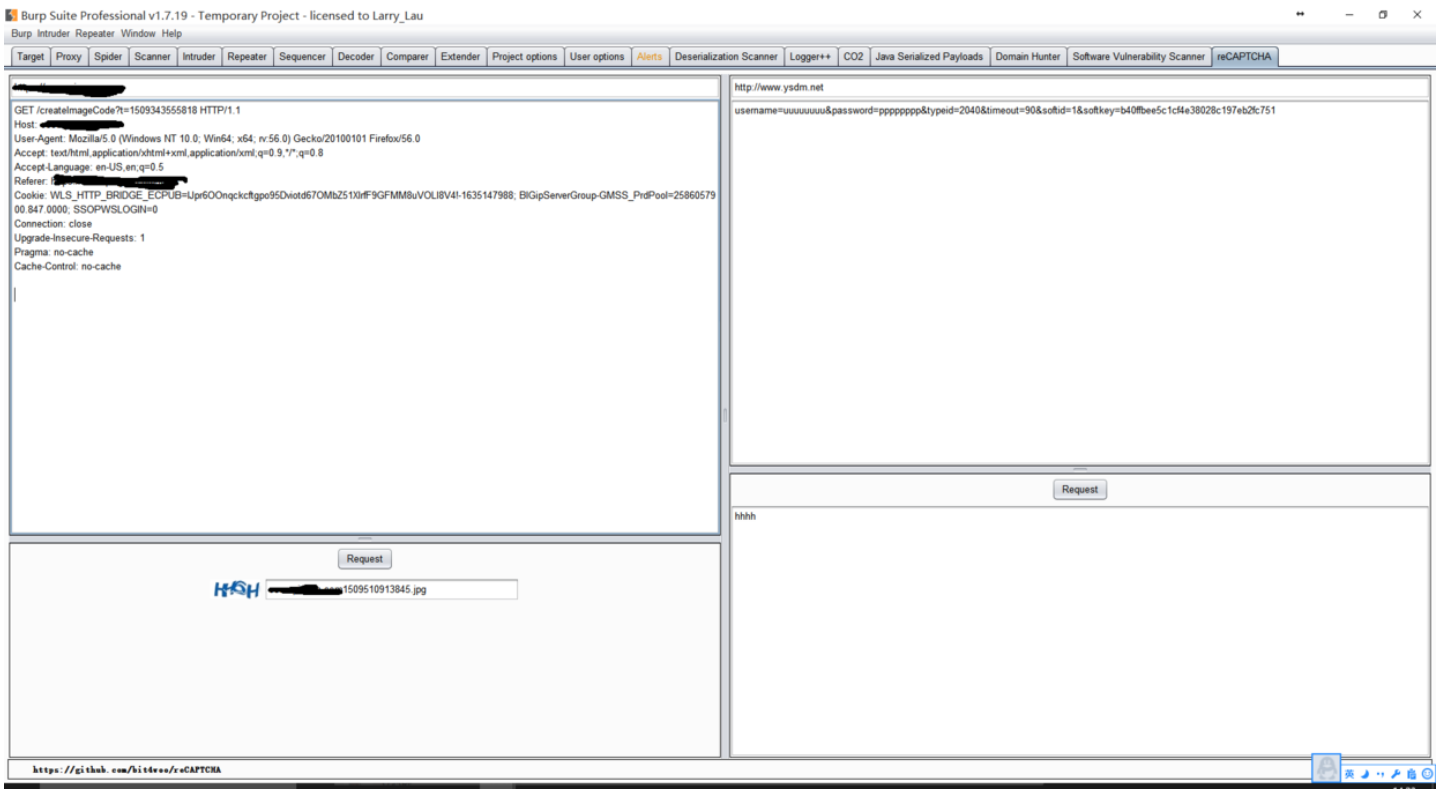


payload 2 的配置和情况一中的配置完全一样。

运行效果如图：



reCAPTCHA界面截图



日志

2017-11-01：第一个demo版本发布。

点击收藏 | 0 关注 | 0

上一篇：应急响应从懵逼到入门 下一篇：ImXSS开源发布附设计文档

1. 16 条回复

静默 2017-11-02 01:40:27

这个东西相当实用啊，就是不知道都支持多复杂的验证码

0 回复Ta

但丁 2017-11-02 01:59:36

这插件怎么28m啊 比burp本身还大..

0 回复Ta

luanwu 2017-11-02 02:23:40

楼主，使用出现这样的bug是怎么回事，，单个验证的时候是正确的

0 回复Ta

bit4 2017-11-02 12:21:10

刚更新了一个版本，需要配置的参数更少了
https://github.com/bit4woo/reCAPTCHA/releases

0 回复Ta


bit4 2017-11-02 12:22:21

@luanwu
师傅这个问题，我还没见到过，我将尝试修复代码显示问题，以便后续定位

0 回复Ta


bit4 2017-11-02 12:27:52

@但丁 应该和打包方式有关，我是把所有依赖包都加在jar包里的。

0 回复Ta


bit4 2017-11-02 12:28:49

@静默 对接的第三方打码平台，识别能力主要看第三方，如果有好的平台可以推荐给我，加到插件里面。

0 回复Ta


wooyun 2017-11-02 13:35:26

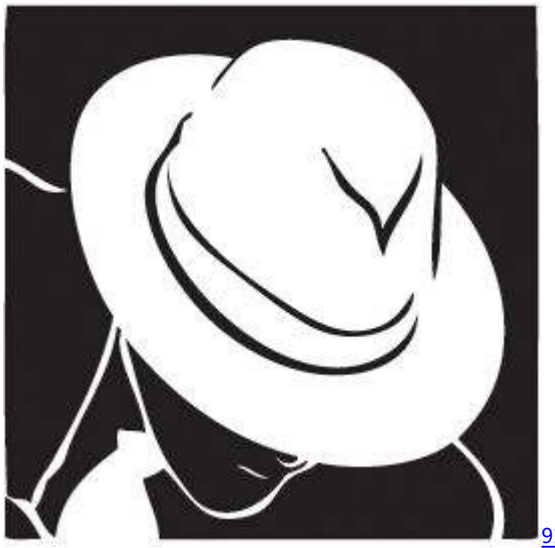
我这里为什么没 都没有验证码回显，账户有充值，纯4位数字验证码

0 回复Ta


vinc 2017-11-02 13:59:04

试试

0 回复Ta


91shell 2017-11-02 15:48:44

下来试试看效果咋样

0 回复Ta


静默 2017-11-02 16:03:32

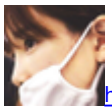
@bit4 原来如此，我还没遇到过什么平台呢，有好的一定推荐

0 回复Ta


bit4 2017-11-02 16:05:02

@wooyun 图片都获取不到吗？我又更新了，试试新版的

0 回复Ta


hades 2017-11-02 22:22:04

@静默 https://xianzhi.aliyun.com/forum/topic/1470/ 这个由时间可以本地测试测试 有朋友说是效果还不错

0 回复Ta


静默 2017-11-06 10:27:19

@hades 好的，谢谢，我等的试试

0 回复Ta


风之传说 2017-11-08 15:51:06

```
java.lang.UnsupportedClassVersionError: burp/BurpExtender : Unsupported major.minor version 52.0 at
java.lang.ClassLoader.defineClass1(Native Method) at java.lang.ClassLoader.defineClass(Unknown Source) at
java.security.SecureClassLoader.defineClass(Unknown Source) at java.net.URLClassLoader.defineClass(Unknown Source)
at java.net.URLClassLoader.access$100(Unknown Source) at java.net.URLClassLoader$1.run(Unknown Source) at
java.net.URLClassLoader$1.run(Unknown Source) at java.security.AccessController.doPrivileged(Native Method) at
java.net.URLClassLoader.findClass(Unknown Source) at java.lang.ClassLoader.loadClass(Unknown Source) at
java.lang.ClassLoader.loadClass(Unknown Source) at java.lang.Class.forName0(Native Method) at
java.lang.Class.forName(Unknown Source) at burp.hie.a(Unknown Source) at burp.hie.<init>(Unknown Source) at
burp.sxf.a(Unknown Source) at burp.r5h.run(Unknown Source) at java.lang.Thread.run(Unknown Source) The extension
could not be loaded because it requires a later version of Java. To use this extension you will need to start Burp
with the required or later Java version.
```

将它添加到burp。如果没有遇到错误，你将看到一个新的名为“reCAPTCHA”的tab。 我偏偏就是遇到错误的那个。。怎么解决呢

0 回复Ta


hk****@qq.com 2017-12-15 22:10:37

google图形验证码
https://www.thehackr.com/bypass-recaptcha-using-speech-recog-api/

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板