Crack Charles Proxy 4.1.3

0x00 Preface

Found on the Mac `Charles` trial expired (though also how not used, usually are used `Burp Suite`), but it is not quite so willing to delete individual authorized $ 50 and a little expensive, so would like to see if you can break the limit at trial.

Finally found a common crack method, the 4.x version should be no problem, the latest Charles for Mac 4.1.3 version of the crack code see charles.4.1.3.crack.sh .

0x01

Online search for a moment found an existing crack is to replace a `charles.jar` file, which can be seen crucial Charles is written in Java, crack in charles.jar this file.

But as a victim of paralysis patients, the use of the Internet crack patch is a great courage, can not do it yourself out?

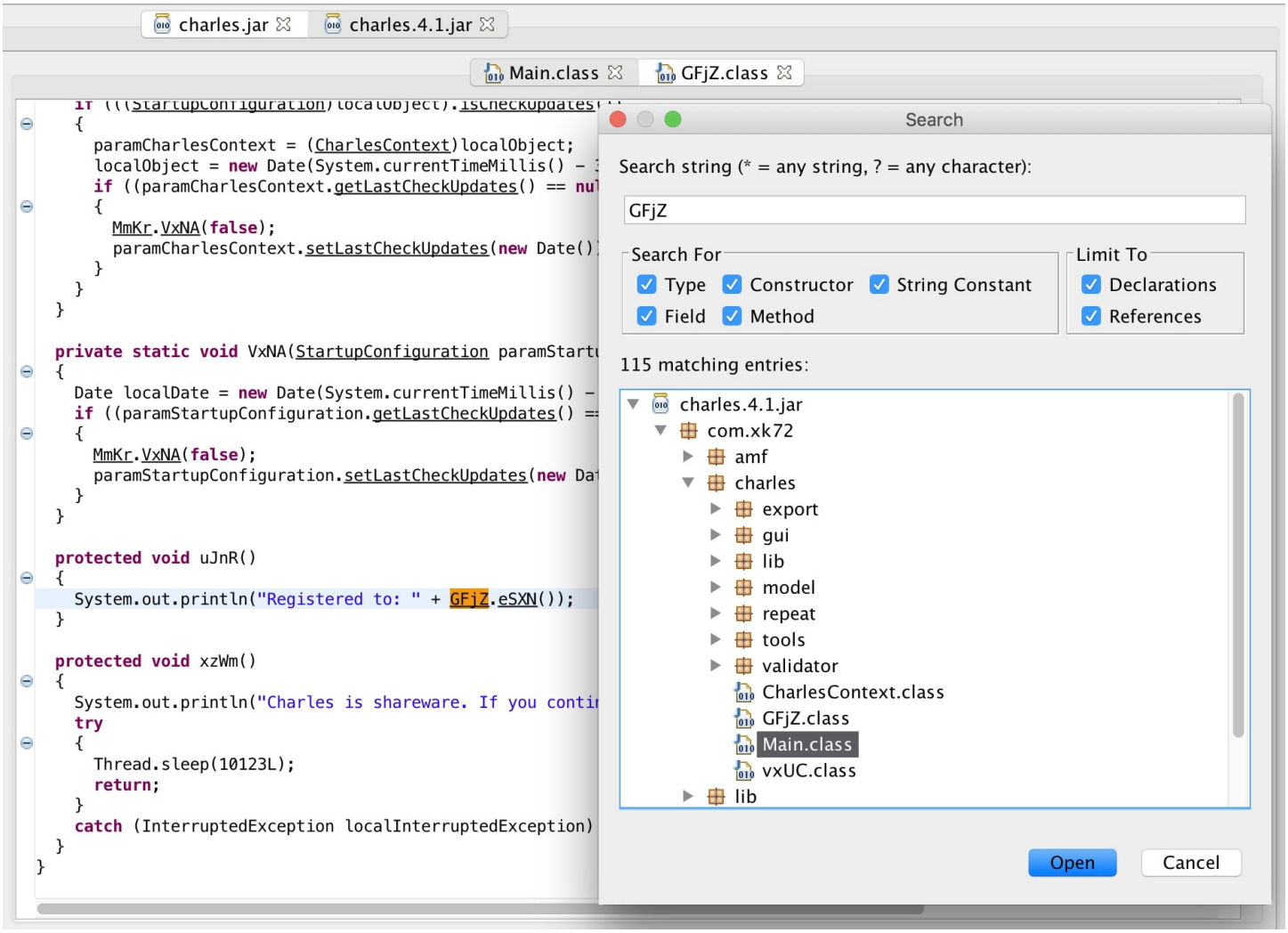
Then on Github found a useful thing: charles-hacking , the author only a few lines of shell code to complete the crack, it looks good :)

0x02 depth

Paste the original author used to crack Charles 4.1 version of the hack.4.1.sh :

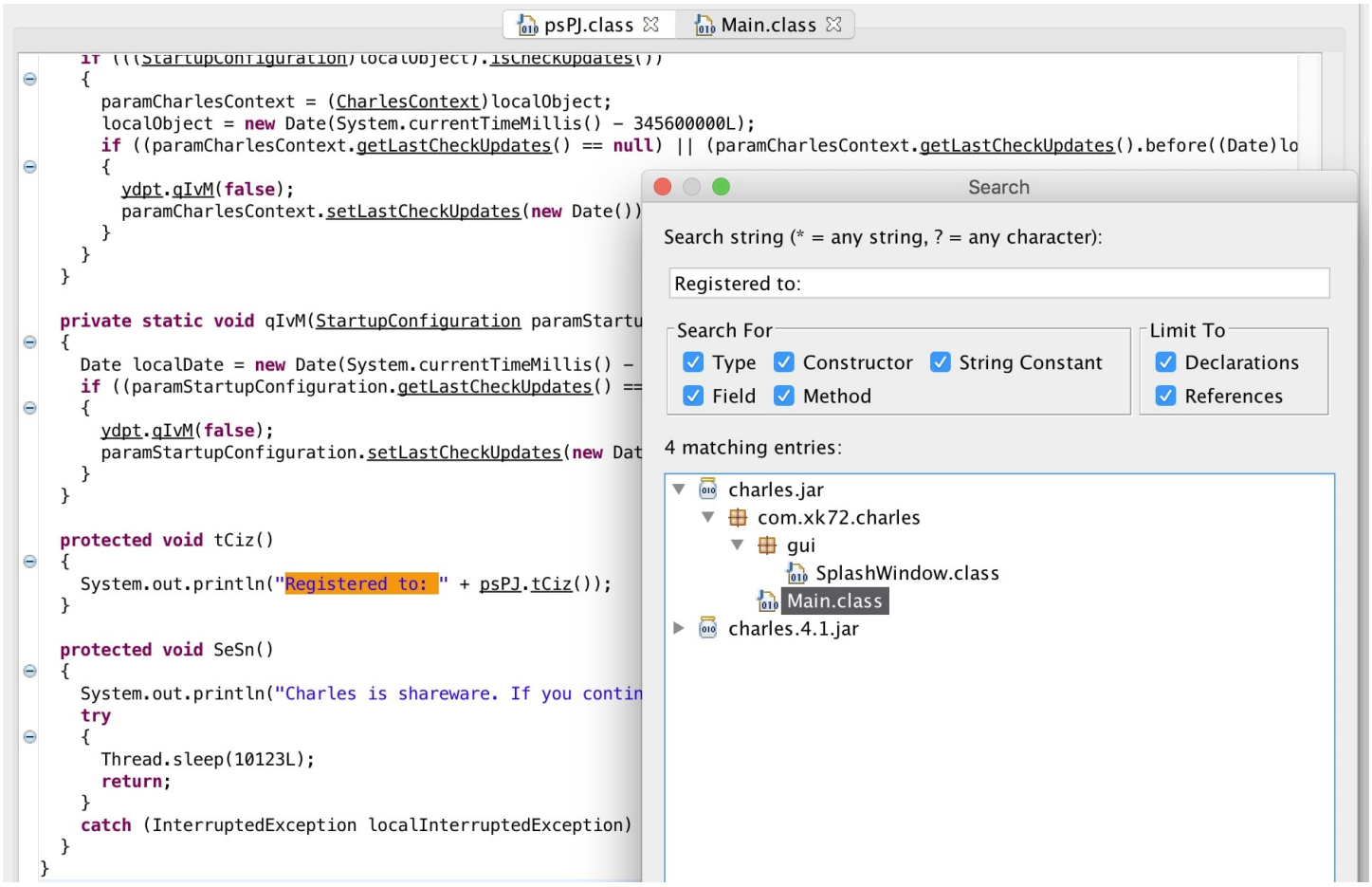
```
charles=/Applications/Charles.app/Contents/Java/charles.jar
dir=charleshack

mkdir $dir
cd $dir
cat >> GFjZ.java <<EOF
package com.xk72.charles;
public final class GFjZ {
    public static boolean VxNA() { return true; }
    public static String eSXN() { return "http://www.gfzj.us"; }
    public static String VxNA(String name, String key) { return null; }
}
EOF
javac -encoding UTF-8 GFjZ.java -d .&& jar -uvf $charles com/xk72/charles/GFjZ.class
cd .. && rm -rf $dir
```

It can be seen that the modified `com.xk72.charles.GFjZ` class, the class name so strange as to why, estimated to be done because of confusion.
The authors provide download version 4.1 patch charles.4.1.jar , with a `JD_GUI` look at `GFjZ` the place which is called:



Obviously this class in Charles GFjZ version 4.1 is responsible for `License` verification of `eSXN()` the function that returns the name of the purchaser.

And then open the 4.1.3 version of the charles.jar, direct search keywords `Registered to:` , positioning to charles 4.1.3 version of the corresponding class name is `psPJ` .



Into the psPJ class, part of the code as follows:

```
1.  private static psPJ mLFE;
2.  private boolean tCiz = false;
3.  private String SeSn = "Unregistered";
4.
5.  public static String tCiz()
6.  {
7.    psPJ localpsPJ = mLFE;
8.    switch (bJif.qIvM[localpsPJ.lvYl.ordinal()])
9.    {
10.   case 1:
11.     return localpsPJ.SeSn;
12.   case 2:
13.     return localpsPJ.SeSn + " - Site License";
14.   case 3:
15.     return localpsPJ.SeSn + " - Multi-Site License";
16.   }
17.   return localpsPJ.SeSn;
18. }
19.
20. public static boolean qIvM()
21. {
```

```
    psPJ localpsPJ;
    return (localpsPJ = mLFE).tCiz;
  }

  public static String qIvM(String paramString1, String paramString2)
  {
    try
    {
      paramString1 = new psPJ(paramString1, paramString2);
    }
    catch (LicenseException localLicenseException)
    {
      return (paramString1 = localLicenseException).getMessage();
    }
    paramString1 = paramString1;
    mLFE = paramString1;
    return null;
  }
```

So replace the original script in the class name and function name on the OK:

```
charles=/Applications/Charles.app/Contents/Java/charles.jar
dir=charleshack

mkdir $dir
cd $dir
cat >> psPJ.java <<EOF
package com.xk72.charles;
public final class psPJ {
    public static boolean qIvM() { return true; }
    public static String tCiz() { return "https://0x0d.im"; }
    public static String qIvM(String name, String key) { return null; }
}
EOF
javac -encoding UTF-8 psPJ.java -d .&& jar -uvf $charles com/xk72/charles/psPJ.class
cd .. && rm -rf $dir
```

Windows crack similar, but the default installation path becomes `C:\Program Files\Charles\lib\charles.jar` .

0x03 reference

- Mac Charles v4.0.2 detailed crack tutorial
- Charles 4.0 latest version of crack

Charles crack

← Previous article

Has 2 comments

kevinchowsec
July 4th, 2017 at 08:47 am

好一个被害妄想症患者，自己动手学一技能丰衣足食。
让我想起此前用Frida来Hook关键函数，绕过检测。
加油~

回复

0x0d
July 4th, 2017 at 04:26 pm

厉害厉害~
—— 来自想玩移动安全但懒死了的 Web 狗

回复

添加新评论 »

称呼 *

电子邮件 *

网站

在这里输入你的评论...

提交评论