[攻防世界]mobile新手练习区easyjava

原创

byzf 于 2020-05-04 01:00:52 发布 406 收藏

分类专栏： CTF 安全 文章标签： 逆向算法 CTF 攻防世界 APK逆向 反编译

kjcxmx

本文链接：https://blog.csdn.net/kjcxmx/article/details/105902290

版权

CTF 同时被 2 个专栏收录

6 篇文章 1 订阅

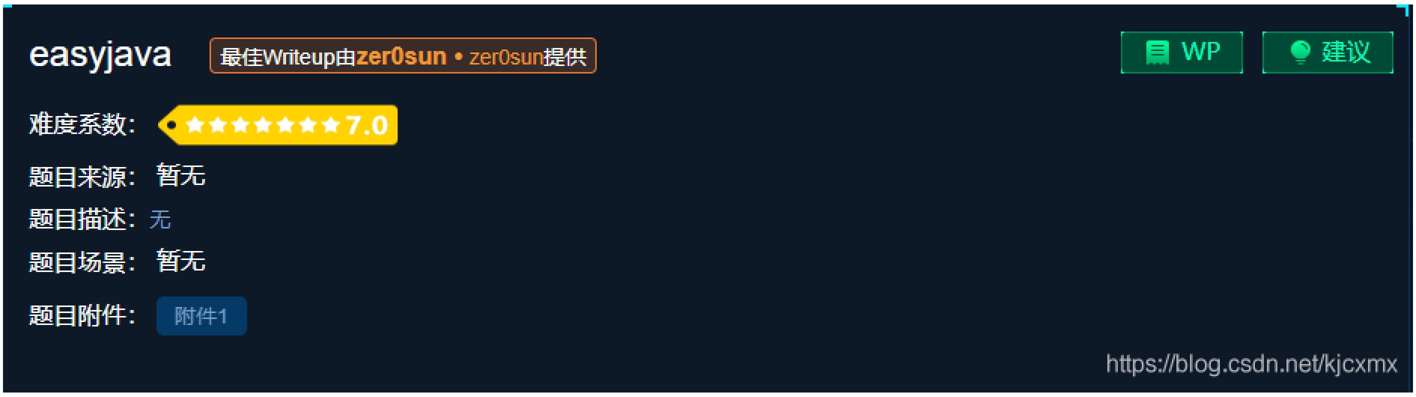
订阅专栏

安全

9 篇文章 0 订阅

订阅专栏

[攻防世界]mobile新手练习区easyjava


easyjava 最佳Writeup由zer0sun • zer0sun提供

难度系数: ★★★★★★★7.0

题目来源: 暂无

题目描述: 无

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/kjcxmx

easyjava最佳Writeup由zer0sun • zer0sun提供

难度系数： 7.0

题目来源： 暂无

题目描述：无

题目场景： 暂无

题目附件： 附件1

反编译后有用的附件内容：

> MainActivity.class
>
> a.class
>
> b.class

```
package com.a.easyjava;

import android.content.Context;
import android.os.Bundle;
import android.support.v7.app.c;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.EditText;
import android.widget.Toast;
import java.util.Timer;
import java.util.TimerTask;

public class MainActivity
  extends c
{
  private static char a(String paramString, b paramb, a parama)
  {
    return parama.a(paramb.a(paramString));
  }

  private static Boolean b(String paramString)
  {
    int i = 0;
    if (!paramString.startsWith("flag{")) {
      paramString = Boolean.valueOf(false);
    }
    for (;;)
    {
      return paramString;
      if (!paramString.endsWith("}"))
      {
        paramString = Boolean.valueOf(false);
      }
      else
      {
        String str = paramString.substring(5, paramString.length() - 1);
        paramString = new b(Integer.valueOf(2));
        a locala = new a(Integer.valueOf(3));
        StringBuilder localStringBuilder = new StringBuilder();
        int k;
        for (int j = 0; i < str.length(); j = k)
        {
          localStringBuilder.append(a(str.charAt(i) + "", paramString, locala));
          Integer localInteger = Integer.valueOf(paramString.b().intValue() / 25);
          k = j;
          if (localInteger.intValue() > j)
          {
            k = j;
            if (localInteger.intValue() >= 1) {
              k = j + 1;
            }
            }
          }
          i++;
        }
        paramString = Boolean.valueOf(localStringBuilder.toString().equals("wigwrkaugala"));
      }
    }
  }

  protected void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130968603);
    findViewById(2131427446).setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        if (MainActivity.a(((EditText)((MainActivity)jdField_this).findViewById(2131427445)).getText().toSt
          Toast.makeText(jdField_this, "You are right!", 1).show();
        }
        for (;;)
        {
          return;
          Toast.makeText(jdField_this, "You are wrong! Bye~", 1).show();
          paramAnonymousView = new TimerTask()
          {
            public void run()
            {
              System.exit(1);
            }
          };
          new Timer().schedule(paramAnonymousView, 2000L);
        }
      }
    });
  }
}
```

```
package com.a.easyjava;

import java.util.ArrayList;

public class a
{
  public static ArrayList<Integer> a = new ArrayList();
  static String b = "abcdefghijklmnopqrstuvwxyz";
  static Integer d = Integer.valueOf(0);
  Integer[] c = { Integer.valueOf(7), Integer.valueOf(14), Integer.valueOf(16), Integer.valueOf(21), Intege

  public a(Integer paramInteger)
  {
    for (int i = paramInteger.intValue(); i < this.c.length; i++) {
      a.add(this.c[i]);
    }
    for (i = 0; i < paramInteger.intValue(); i++) {
      a.add(this.c[i]);
    }
  }
  public static void a()
  {
    Integer localInteger = d;
    d = Integer.valueOf(d.intValue() + 1);
    if (d.intValue() == 25)
    {
      int i = ((Integer)a.get(0)).intValue();
      a.remove(0);
      a.add(Integer.valueOf(i));
      d = Integer.valueOf(0);
    }
  }

  public char a(Integer paramInteger)
  {
    int i = 0;
    Integer localInteger = Integer.valueOf(0);
    if (paramInteger.intValue() == -10)
    {
      a();
      i = " ".charAt(0);
    }
    for (int j = i;; j = i)
    {
      return j;
      while (i < a.size() - 1)
      {
        if (a.get(i) == paramInteger) {
          localInteger = Integer.valueOf(i);
        }
        i++;
      }
      a();
      i = b.charAt(localInteger.intValue());
    }
  }
}
```

```
package com.a.easyjava;

import java.util.ArrayList;

public class b
{
  public static ArrayList<Integer> a = new ArrayList();
  static String b = "abcdefghijklmnopqrstuvwxyz";
  static Integer d = Integer.valueOf(0);
  Integer[] c = { Integer.valueOf(8), Integer.valueOf(25), Integer.valueOf(17), Integer.valueOf(23), Intege

  public b(Integer paramInteger)
  {
    for (int i = paramInteger.intValue(); i < this.c.length; i++) {
      a.add(this.c[i]);
    }
    for (i = 0; i < paramInteger.intValue(); i++) {
      a.add(this.c[i]);
    }
  }

  public static void a()
  {
    int i = ((Integer)a.get(0)).intValue();
    a.remove(0);
    a.add(Integer.valueOf(i));
    char c1 = b.charAt(0);
    b = b + "" + c1;
    b = b.substring(1, 27);
    Integer localInteger = d;
    d = Integer.valueOf(d.intValue() + 1);
  }

  public Integer a(String paramString)
  {
    int i = 0;
    Integer localInteger = Integer.valueOf(0);
    if (b.contains(paramString.toLowerCase()))
    {
      int j = b.indexOf(paramString);
      for (;;)
      {
        paramString = localInteger;
        if (i >= a.size() - 1) {
          break;
        }
        if (a.get(i) == Integer.valueOf(j)) {
          localInteger = Integer.valueOf(i);
        }
        i++;
      }
    }
    if (paramString.contains(" ")) {}
    for (paramString = Integer.valueOf(-10);; paramString = Integer.valueOf(-1))
    {
      a();
      return paramString;
    }
  }

  public Integer b()
  {
    return d;
  }
}
```

解题

拿到附件989ca07c3f90426fa05406e4369901ff.apk，flag一定要反编译。博主用的ApkIDE进行反编译。先找到入口主类MainActivity，发现super调用了自身onCreate方法，点击事件MainActivity.a(((EditText)((MainActivity)jdField_this).findViewById(2131427445)).getText().toString()).booleanValue()为真时成功。MainActivity调用了方法a，根据每一个函数调用关系，分析得出flag。具体可参见这位博主的文章https://blog.csdn.net/shuaicenglou3032/article/details/104309962/

解题思路：apk逆向->分析源码->逆向算法->得出flag

代码的实现

博主也找了相关的代码实现，思路是对给定的字符串和数组进行索引和取值。在析构函数中对数组做了一定的变换。如下。

> b = "abcdefghijklmnopqrstuvwxyz"
> localStringBuilder = "wigwrkaugala"

```
#逆向后的代码实现

s_b2 = [17, 23, 7, 22, 1, 16, 6, 9, 21, 0, 15, 5, 10, 18, 2, 24, 4, 11, 3, 14, 19, 12, 20, 13, 8, 25]
s_a3 = [21, 4, 24, 25, 20, 5, 15, 9, 17, 6, 13, 3, 18, 12, 10, 19, 0, 22, 2, 11, 23, 1, 8, 7, 14, 16]
b = "abcdefghijklmnopqrstuvwxyz"
s3 = "wigwrkaugala"
re1 = []
for i in s3:
    re1.append(s_a3[b.index(i)])
print(re1)
flag = ''
for i in re1:
    s4 = s_b2[i]
    flag += b[s4]
    s_b2.append(s_b2[0])
    s_b2.remove(s_b2[0])
    b += b[0]
    b = b[1:]
flag = 'flag{'+flag+'}'
print(flag)
```

如此就可以得到flag

> venividivkcr
>
> flag{venividivkcr}

话说这个题目有点坑，就是没有提示flag的形式，必须裹上flag{}才可以。

也看到了Java的同学给出的答案

```
import java.util.ArrayList;
import java.util.List;
import java.util.Arrays;
public class Main
{
    public static void main(String[] args)
    {
        List < Integer > tableListA = new ArrayList < > (Arrays.asList(21, 4, 24, 25, 20, 5, 15, 9, 17, 6,
        List < Integer > tableListB = new ArrayList < > (Arrays.asList(17, 23, 7, 22, 1, 16, 6, 9, 21, 0, 1
        String tableB = "abcdefghijklmnopqrstuvwxyz";
        String tableA = "abcdefghijklmnopqrstuvwxyz";
        String pwd = "wigwrkaugala";
        char[] pwdChars = pwd.toCharArray();
        String key = "";
        for(int i = 0; i < pwdChars.length; i++)
        {
            int pwdIndex = tableA.indexOf(pwdChars[i]);
            int tabBIndex = tableListA.get(pwdIndex); //获取tabB的index
            key += tableB.charAt(tableListB.get(tabBIndex)); //修改tableB
            int intValue = tableListB.get(0);
            tableListB.remove(0);
            tableListB.add(intValue);
            tableB += tableB.charAt(0);
            tableB = tableB.substring(1, 27);
        }
        System.out.println("flag{" + key + "}");
    }
}
```

如此也可以得到flag

> venividivkcr
>
> flag{venividivkcr}

附录：
https://baike.baidu.com/item/base64

https://blog.csdn.net/qq_42967398/article/details/101778364