2017年陕西省网络空间安全技术大赛Mobile部分WriteUp

原创

Magic1an 于 2017-08-19 23:50:22 发布 1048 收藏

分类专栏： re 文章标签： re

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/Magic1an/article/details/77418294

版权

re 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

0x0 拯救鲁班七号

载入jeb,在Mainactivity里面可以看到程序将输入放到checkPass函数中验证

```
protected void onCreate(Bundle arg3) {
        super.onCreate(arg3);
        this.setContentView(2130903040);
        this.findViewById(2131165184).setOnClickListener(new View$OnClickListener() {
            public void onClick(View arg4) {
                MainActivity.this.checkPass(MainActivity.this.findViewById(2131165185).getText().toStri
            }
        });
    }
```

在这个checkPass函数里面会调用CheckUtil的checkPass函数验证是否正确，此函数为humen.so文件中的函数，将humen放到ida中进行分析。无用代码比较多，下面只将关键代码发出来。

```
length = strlen(input);
  while ( 1 )
  {
    v23 += 2;
    if ( length <= v23 )
      break;
    v7 = input[v23 - 2];
    input[v23 - 2] = input[v23 - 1];
    v8 = 0;
    input[v23 - 1] = v7;
    if ( length > 4 )
    {
      for ( i = 4; ; i += 4 )
      {
        v10 = (char *)&input[v8];
        v9 = v10;
        v11 = *v10;
        v10 += 4;
        *v9 = *v10;
        *v10 = v11;
        v8 = i;
        if ( length <= i + 4 )
          break;
      }
    }
  }
```

```
 v14 = (&t_ptr)[v4 - 12208];
  v15 = 0;
  if ( *input == *v14 )
  {
    do
      v16 = v14[v15++ + 1];
    while ( input[v15] == v16 );
  }
```

程序将输入的字符串奇数和偶数做交换并且前八位的0,4,8,位分别与4,8,12,做交换，最后与t进行比较，直接附上脚本。

```
stt="S!@#@1FD23154A34"
st=list(stt)
v6=len(st)
for j in range(14,0,-2):
    if v6>4:
        for i in range(12,1,-4):
            st[i-4],st[i]=st[i],st[i-4]
    st[j-1],st[j-2]=st[j-2],st[j-1]

flag=''
for i in range(len(st)):
    flag+=st[i]
print flag
```

0X1 The Marauder’s Map

依照惯例，拖进jeb分析。发现和数据库有关，最近刚好了解了一下安卓连接数据库，只能说好巧。

```java
package com.example.icontest;

public class ReadSe {
    private boolean a;

    static {
        System.loadLibrary("test");
    }

    public ReadSe() {
        super();
        this.a = false;
    }

    public final boolean a(String arg3, String arg4) {
        boolean v0 = false;
        if(arg3 != null && arg3.length() > 0 && arg4 != null && arg4.length() > 0 && (arg4.equals(this.
            v0 = true;
        }

        return v0;
    }

    private native String readbin(String arg1) {
    }
}
```

代码简单明了，将readbin函数的返回值与arg4进行比较，arg4为user数据库中读到的id为2的生日列。

```
    public a() {
        super();
        this.a = "";
        this.b = "dGVzdA==";
        this.c = "WWVhaH4h";
        this.d = "dXNlcnM=";
        this.e = "Mg==";
    }

    public final String a(Context arg10) {
        String v0 = a.a(this.b);
        String v1 = a.a(this.d);
        a.a(this.c);
        String v6 = a.a(this.e);
        SQLiteDatabase v0_1 = new b(arg10, v0, null, 1).getReadableDatabase();
        Cursor v1_1 = v0_1.query(v1, new String[]{"userid", "age", "birthday", "id"}, "id=?", new Strin
        while(v1_1.moveToNext()) {
            v1_1.getString(v1_1.getColumnIndex("userid"));
            v1_1.getString(v1_1.getColumnIndex("age"));
            this.a = v1_1.getString(v1_1.getColumnIndex("birthday"));
        }

        v0_1.close();
        return this.a;
    }

    private static String a(String arg3) {
        return new String(new String(Base64.decode(arg3.getBytes(), 0)).toCharArray());
    }
}
```

数据库可以通过sqlitebrowser软件查看。
然后，我们分析一下readbin函数，
关键代码在sub_1220()中

```
s = (char *)a1;
 v7 = strlen(a1);
 v5 = 0;
 v6 = 0;
 src = (char *)operator new[](2 * v7 + 1);
 do
 {
   v1 = (unsigned __int8)s[v5];
   src[v6] = sub_1078(~(_BYTE)v1 & 0xF);
   v2 = v6 + 1;
   src[v2] = sub_1078((v1 >> 4) ^ 0xE);
   ++v5;
   v6 = v2 + 1;
 }
 while ( v5 < v7 );
 src[2 * v7] = 0;
 strncpy(s, src, 2 * v7 + 1);
 return s;
```

代码如上，只能说算法还是挺简单的
将输入的每一位经过运算化为src的两位，然后返回得到的字符串。
逻辑大概就是这样，flag可以经过爆破得出，直接上脚本。

```
s="9838e888496bfda98afdbb98a9b9a9d9cdfa29"
st=list(s)
def subl(a):
    v1=0
    if(a>9 or a<0):
        if(a<=9 or a>15):
            v1=255
        else:
            v1=a+87
    else:
        v1=a+48
    return v1
print len(s)
key=""
for i in range(0,38,2):
    for j in range(32,128):

        if subl(~j&0xF)==ord(st[i]) and subl((j>>4)^0xE)==ord(st[i+1]):
            key+=chr(j)
            break;
print key
```

0x2取证密码

输入在GetString.encrypt函数里面进行验证，encrypt为XTU.so文件的函数，代码如下

```
v3 = a1;
  _JNIEnv::NewStringUTF(a1, "yInS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W");
  _JNIEnv::NewStringUTF(v3, "Welc0meT0XTUCTF");
  v4 = (const char *)_JNIEnv::GetStringUTFChars((int)v3);
  str = (const char *)_JNIEnv::GetStringUTFChars((int)v3);
  input = (char *)_JNIEnv::GetStringUTFChars((int)v3);
  v7 = j_j_strlen(v4);
  v8 = j_j_strlen(str);
  temp = (char *)j_operator new[](v7 + 1);
  v10 = (char *)j_operator new[](v8 + 1);
  v11 = j_j_strlen(input);
  v15 = (char *)j_operator new[](v11 + 1);
  j_j_memcpy(&dest, &unk_2018, 0x3Cu);
  j_j_strcpy(temp, v4);
  j_j_strcpy(v10, str);
  j_j_strcpy(v15, input);
  for ( i = 0; i < j_j_strlen(v4); ++i )
    temp[i] = v10[*((_DWORD *)&dest + i)];
  v13 = 0;
  while ( (unsigned __int8)v15[v13] == (unsigned __int8)temp[v13] )
  {
    if ( ++v13 == 15 )
      return 1;
  }
  return 0;
```

看见这个代码开始我是蒙逼的，，找不到代表输入的临时变量是哪个，，
只能大胆的猜测，v15既input为输入，str为ylnS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W，
取dest的值作为str的下标赋值给temp，然后与input进行比较，脚本如下。

```
s="yInS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W"
dest=[0x39,0x20,7,0xA,0x20,0x29,0x13,2,0x3A,0xC,0x11,0x31,0x3B,0xB,7]
s=list(s)
flag=""
for i in range(len(dest)):
    flag+=s[dest[i]]
print flag
```

没想到真的是这样，，getflag。

0x3 人民的名义-抓捕赵德汉1

由于是jar文件，所以直接用jd-gui软件打开。
将输入的字符串载入checkPassword函数验证。
无用代码比较多，差点就被迷惑了~~

将输入的字符串进行md5加密，然后与fa3733c647dca53a66cf8df953c2d539进行比较。
由于以前做的md5加密的题比较多，这个题还挺简单的。
将fa3733c647dca53a66cf8df953c2d539解密md5即可。

0x4 人民的名义-抓捕赵德汉2

程序载入jd-hui后乱码比较多，这个题难度比上一个题提升了不少。

```
 public static void main(String[] args)
  {
    JFrame frame = new JFrame("Key check");
    JButton button = new JButton("Click to activate");

    button.addActionListener(new ActionListener()
    {
      public void actionPerformed(ActionEvent ae)
      {
        String str = JOptionPane.showInputDialog(null, "Enter the product key: ",
          "xxxx-xxxx-xxxx-xxxx", 1);
        if (????????????.???(str)) {
          JOptionPane.showMessageDialog(null, "Well done that was the correct key",
            "Key check", 1);
        } else {
          JOptionPane.showMessageDialog(null, "              Sorry that was the incorrect key \nRememb
            "Key check", 1);
        }
      }
    });
    JPanel panel = new JPanel();
    panel.add(button);
    frame.add(panel);
    frame.setSize(300, 100);
    frame.setDefaultCloseOperation(3);
    frame.setVisible(true);
  }
}
```

这里需要注意的一点就是，输入是以xxxx-xxxx-xxxx-xxxx格式进行输入的！
将验证函数修改一下如下，

```
public class iiiiiiiiiii
{
  static String key1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
  static String _ii = "ZYXWVUTSRQPONMLKJIHGFEDCBA";

  public static boolean iii(String str)
  {
    if ((str != null) && (str.length() == 19))
    {
      key1 = System.arraycopy(_ii, 0, key1, 5, 5);

      boolean keyGuessWrong = true;
      int i = 0;
      for (int i = 0; i < 4; i++)
      {
        for (int j = 0; j < 4; j++) {
          if (str.charAt(i + j) != key1.charAt(Start.operate(i + j, key1))) {
            keyGuessWrong = false;
          }
        }
        i += 5;
      }
      return keyGuessWrong;
    }
    return false;
  }
```

将i+j,和key1放到operate函数进行变换，然后与输入进行比较。
其中key1为start.main（）得到的字符串。

```
public static String main(String... args)
  {
    String x = "";
    char[] arrayOfChar;
    int j = (arrayOfChar = "v??��??????v?��??????????��??".toCharArray()).length;
    for (int i = 0; i < j; i++)
    {
      int $ = arrayOfChar[i];
      x = x + (char)(($ >> 1) + 15);
    }
    return x;
  }
```

但是这有个乱码，，，很是难为了一番。最后经Simp1er表哥提示换种别工具可以得到这一个字符串，如下图。

最后，按照惯例附上脚本

```
key1="JsnatterrtJuaththovacke"
li=[0x76,0xC3,0x88,0xC2,0xBE,0xC2,0xA4,0xC3,0x8A,0xC3,0x8A,0xC2,0xAC,0xC3,0x86,
    0xC3,0x86,0xC3,0x8A,0x76,0xC3,0x8C,0xC2]
key=""
for i in li:
    key+=chr((i>>1)+15)
s=list(key1)
def digui(a):
    if a>2:
        return digui(a-1)+digui(a-2)
    else:
        return 1
flag=""
for i in range(4):
    a=i*5
    for j in range(4):
        flag+=s[digui(a+j)%len(s)]
    if i!=3:
        flag+="-"
print flag
```

附上题目及工具：http://pan.baidu.com/s/1eRl2HSA
密码：xpxn