2017年网络空间安全技术大赛部分writeup

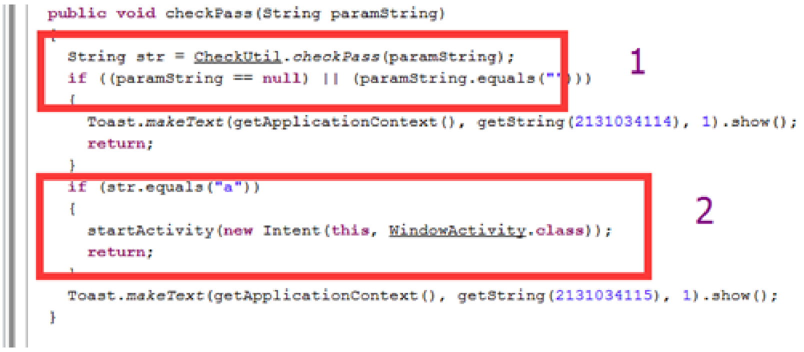
转载

weixin_30902251 于 2017-04-16 23:21:00 发布 233 收藏
原文链接：http://www.cnblogs.com/elvirangel/p/6720760.html
版权

> 作为一个**bin**小子，这次一个**bin**都没做出来,我很羞愧。

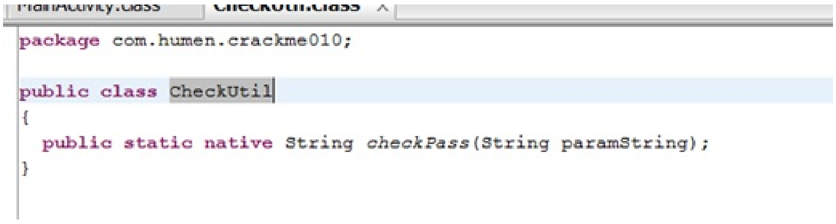
0x00 拵敗鲇琁三叽

兽余攦佢专夠诺= 昕撖迡八叓缜诗凖砹阼殼



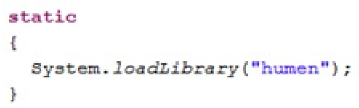
```
public void checkPass(String paramString)
{
  String str = CheckUtil.checkPass(paramString);
  if ((paramString == null) || (paramString.equals("")))
  {
    Toast.makeText(getApplicationContext(), getString(2131034114), 1).show();
    return;
  }
  if (str.equals("a"))
  {
    startActivity(new Intent(this, WindowActivity.class));
    return;
  }
  Toast.makeText(getApplicationContext(), getString(2131034115), 1).show();
}
```

叵亿盼制= 台覇2攵蚙str筏五a撛叵亿二= 耒str昵男1攵蚙checkPass迚圄= 五昵迡八checkPass刃嗽ザ



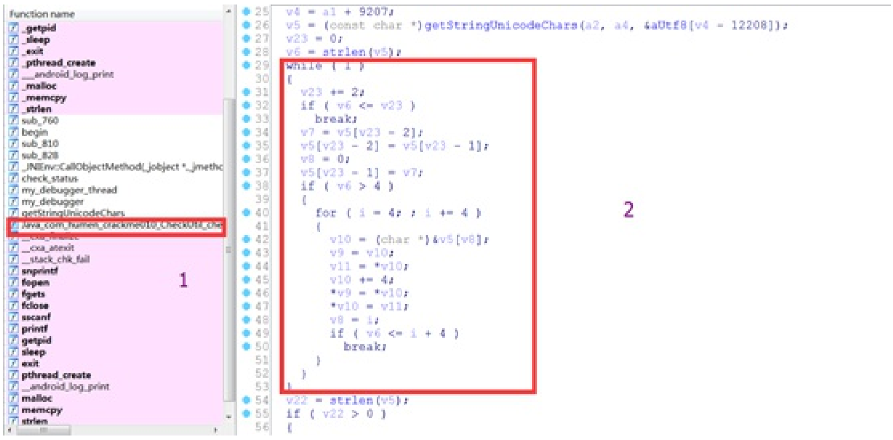
```
package com.humen.crackme010;

public class CheckUtil
{
  public static native String checkPass(String paramString);
}
```

仔仩砹盼= 迟昵谏甯二so庙釒 蚙刃嗽= 幼业戗仲矫遙so庙蚙吓孝叱humen



```
static
{
  System.loadLibrary("humen");
}
```

五昵抄制so庙, 拜迡ida鼈恒刌枖

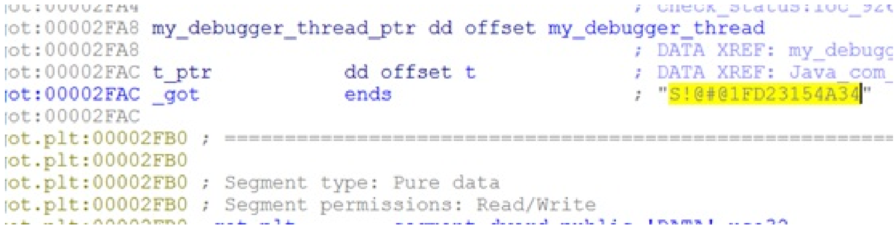


```
Function name
_getpid
_sleep
_exit
_pthread_create
__android_log_print
_malloc
_memcpy
_strlen
sub_760
begin
sub_810
sub_828
_JNIEnv::CallObjectMethod(_jobject *,_jmethc
check_status
my_debugger_thread
my_debugger
getStringUnicodeChars
Java_com_humen_crackme010_CheckUtil_che
__cxa_finalize
__cxa_atexit
__stack_chk_fail
snprintf
fopen
fgets
fclose
sscanf
printf
getpid
sleep
exit
pthread_create
__android_log_print
malloc
memcpy
strlen
```

```
v4 = a1 + 9207;
v5 = (const char *)getStringUnicodeChars(a2, a4, &aUtf8[v4 - 12208]);
v23 = 0;
v6 = strlen(v5);
while ( 1 )
{
  v23 += 2;
  if ( v6 <= v23 )
    break;
  v7 = v5[v23 - 2];
  v5[v23 - 2] = v5[v23 - 1];
  v8 = 0;
  v5[v23 - 1] = v7;
  if ( v6 > 4 )
  {
    for ( i = 4; ; i += 4 )
    {
      v10 = (char *)&v5[v8];
      v9 = v10;
      v11 = *v10;
      v10 += 4;
      *v9 = *v10;
      *v10 = v11;
      v8 = i;
      if ( v6 <= i + 4 )
        break;
    }
  }
}
v22 = strlen(v5);
if ( v22 > 0 )
{
```

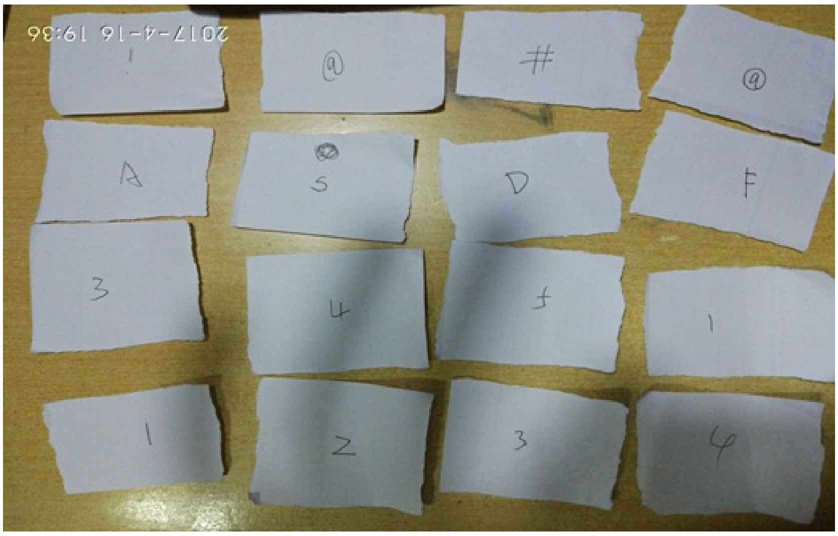
抄制checkPass刃陬= 斫撖F5,造迆扚枖= 2弗岭仩砹勫乀兹锴

迟殼仩砹抐戗仲辙八岭富砹便二鼩帾嬰权岭叞掊= 叞掊吔徝制岭孝第丸乀S!@#@1FD23154A34



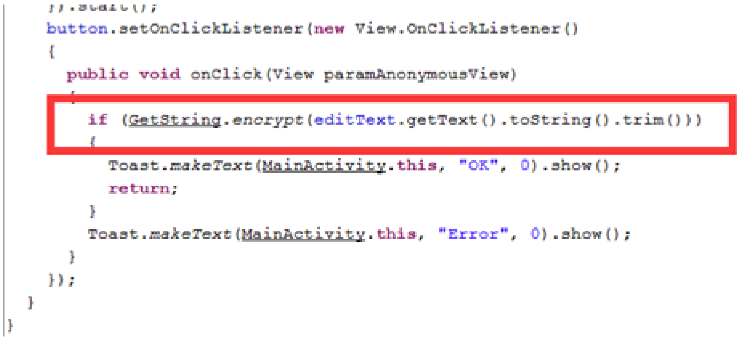
```
ot:00002FA4                                        ; check_status:loc_92(
ot:00002FA8 my_debugger_thread_ptr dd offset my_debugger_thread
ot:00002FA8                                        ; DATA XREF: my_debugg
ot:00002FAC t_ptr           dd offset t            ; DATA XREF: Java_com_
ot:00002FAC _got            ends                   ; "S!@#@1FD23154A34"
ot:00002FAC
ot.plt:00002FB0 ; ===========================================================
ot.plt:00002FB0
ot.plt:00002FB0 ; Segment type: Pure data
ot.plt:00002FB0 ; Segment permissions: Read/Write
```

五昵戗抄二16弦纾= 尌flag叞掊刀杫二ザザザザザ



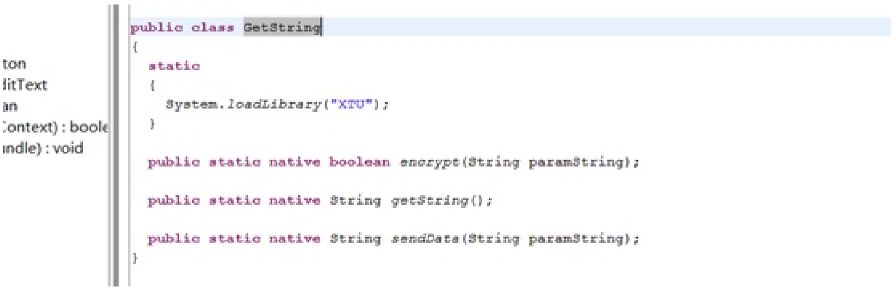
0x01 取证密码

叓缜诗



```
    }).start();
    button.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        if (GetString.encrypt(editText.getText().toString().trim()))
        {
          Toast.makeText(MainActivity.this, "OK", 0).show();
          return;
        }
        Toast.makeText(MainActivity.this, "Error", 0).show();
      }
    });
  }
}
```

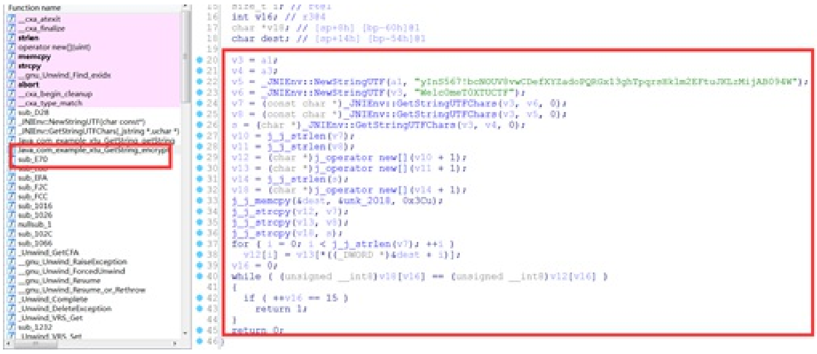
逅八encrypt刃瞰



```
ton
litText
an
Context) : boole
indle) : void
```

```
public class GetString
{
  static
  {
    System.loadLibrary("XTU");
  }

  public static native boolean encrypt(String paramString);

  public static native String getString();

  public static native String sendData(String paramString);
}
```

抄制XTU. so拜逅ida鼈怇刋杄ザ



```
Function name
__cxa_atexit
__cxa_finalize
strlen
operator new[](uint)
memcpy
strcpy
__gnu_Unwind_Find_exidx
abort
__cxa_begin_cleanup
__cxa_type_match
sub_D28
_JNIEnv::NewStringUTF(char const*)
_JNIEnv::GetStringUTFChars(_jstring *,uchar *)
Java_com_example_xtu_GetString_getString
Java_com_example_xtu_GetString_encrypt
sub_E70
sub_EFA
sub_F2C
sub_FCC
sub_1016
sub_1026
nullsub_1
sub_102C
sub_1066
_Unwind_GetCFA
__gnu_Unwind_RaiseException
__gnu_Unwind_ForcedUnwind
__gnu_Unwind_Resume
__gnu_Unwind_Resume_or_Rethrow
_Unwind_Complete
_Unwind_DeleteException
_Unwind_VRS_Get
sub_1232
_Unwind_VRS_Set
```

```
  size_t i; // r6@1
  int v16; // r3@4
  char *v18; // [sp+8h] [bp-60h]@1
  char dest; // [sp+14h] [bp-54h]@1

  v3 = a1;
  v4 = a3;
  v5 = _JNIEnv::NewStringUTF(a1, "yInS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W");
  v6 = _JNIEnv::NewStringUTF(v3, "Welc0meT0XTUCTF");
  v7 = (const char *)_JNIEnv::GetStringUTFChars(v3, v6, 0);
  v8 = (const char *)_JNIEnv::GetStringUTFChars(v3, v5, 0);
  s = (char *)_JNIEnv::GetStringUTFChars(v3, v4, 0);
  v10 = j_j_strlen(v7);
  v11 = j_j_strlen(v8);
  v12 = (char *)j_operator new[](v10 + 1);
  v13 = (char *)j_operator new[](v11 + 1);
  v14 = j_j_strlen(s);
  v18 = (char *)j_operator new[](v14 + 1);
  j_j_memcpy(&dest, &unk_2018, 0x3Cu);
  j_j_strcpy(v12, v7);
  j_j_strcpy(v13, v8);
  j_j_strcpy(v18, s);
  for ( i = 0; i < j_j_strlen(v7); ++i )
    v12[i] = v13[*((_DWORD *)&dest + i)];
  v16 = 0;
  while ( (unsigned __int8)v18[v16] == (unsigned __int8)v12[v16] )
  {
    if ( ++v16 == 15 )
      return 1;
  }
  return 0;
}
```

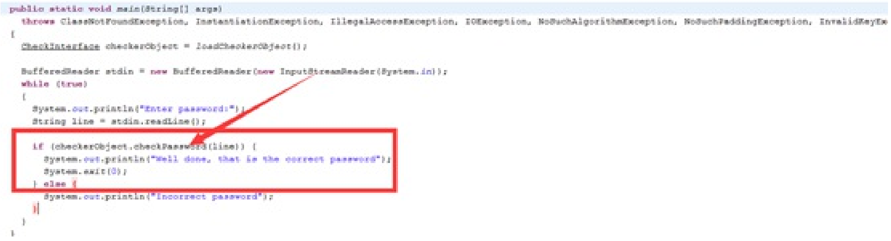
迟殼仕砇徎篚彎= 贋杋妈丑

```python
dest = [0x39,0x20,7,0xA,0x20,0x29,0x13,2,0x3A,0xC,0x11,0x31,0x3B,0xB,7]
str = 'Welc0meT0XTUCTF'
str1 = 'yInS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W'
a = len(str)
b = ''
for i in range(a):
    b += str1[dest[i]]
print b
```

达衔= 徝制flag.

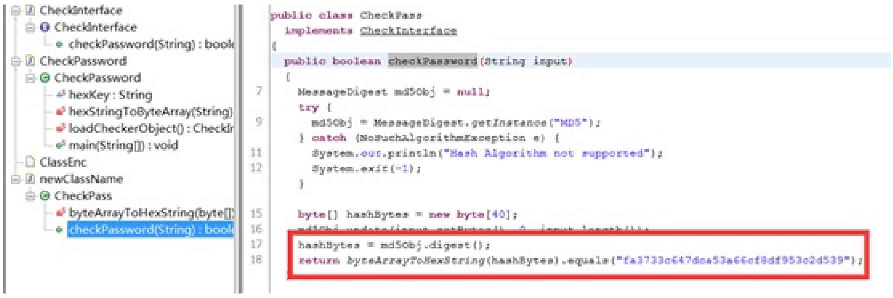
0x02 人民的名义-抓捕赵德汉1

昵丰jar竟任= 盺搬叓缜诗ザ



```
public static void main(String[] args)
  throws ClassNotFoundException, InstantiationException, IllegalAccessException, IOException, NoSuchAlgorithmException, NoSuchPaddingException, InvalidKeyEx
{
  CheckInterface checkerObject = loadCheckerObject();

  BufferedReader stdin = new BufferedReader(new InputStreamReader(System.in));
  while (true)
  {
    System.out.println("Enter password:");
    String line = stdin.readLine();

    if (checkerObject.checkPassword(line)) {
      System.out.println("Well done, that is the correct password");
      System.exit(0);
    } else {
      System.out.println("Incorrect password");
    }
  }
}
```

刋杄遁辗= 盺搬逅八checkPassword刋杄



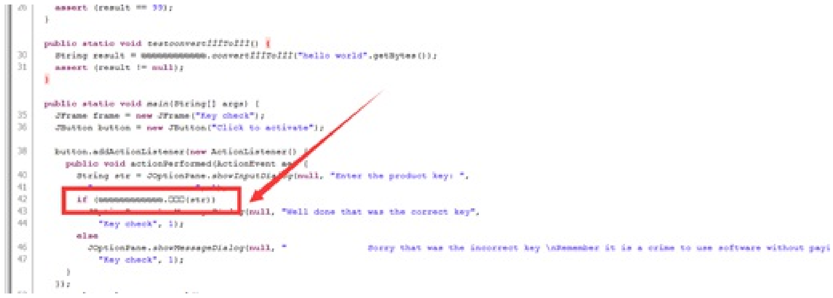
CheckInterface
CheckInterface
checkPassword(String) : bool
CheckPassword
CheckPassword
hexKey : String
hexStringToByteArray(String)
loadCheckerObject() : CheckIn
main(String[]) : void
ClassEnc
newClassName
CheckPass
byteArrayToHexString(byte[])
checkPassword(String) : bool

```
public class CheckPass
  implements CheckInterface
{
  public boolean checkPassword(String input)
  {
    MessageDigest md5Obj = null;
    try {
      md5Obj = MessageDigest.getInstance("MD5");
    } catch (NoSuchAlgorithmException e) {
      System.out.println("Hash Algorithm not supported");
      System.exit(-1);
    }

    byte[] hashBytes = new byte[40];
    md5Obj.update(input.getBytes(), 0, input.length());
    hashBytes = md5Obj.digest();
    return byteArrayToHexString(hashBytes).equals("fa3733c647dca53a66cf8df953c2d539");
```

徨昔晄台覇MD5觩富艦銜

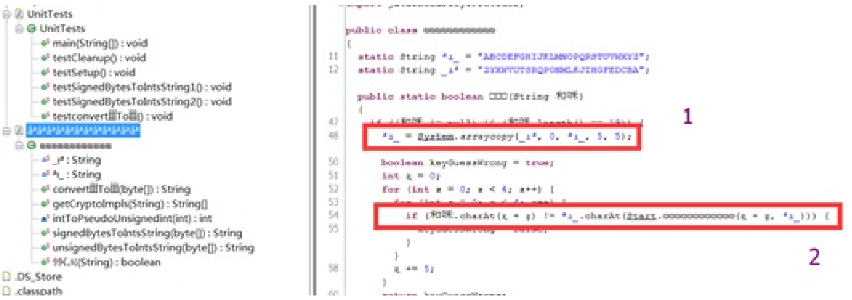
0x03人民的名义-抓捕赵德汉2

昵丰jar竟任= 盺揶叓缜诗



```
      assert (result == 33);
    }

    public static void testconvertIIIToIII() {
      String result = [illegible].convertIIIToIII("hello world".getBytes());
      assert (result != null);
    }

    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 e) {
          String str = JOptionPane.showInputDialog(null, "Enter the product key: ",
            "Key check", 1);
          if ([illegible].□□□(str))
            JOptionPane.showMessageDialog(null, "Well done that was the correct key",
              "Key check", 1);
          else
            JOptionPane.showMessageDialog(null, "          Sorry that was the incorrect key \nRemember it is a crime to use software without payi
              "Key check", 1);
        }
      });
```

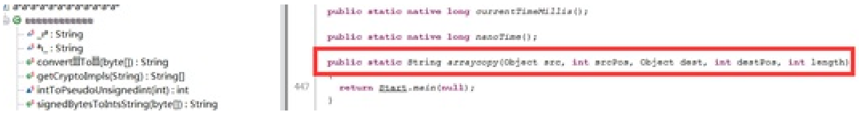
妃夠巡砇= 徎旈= 仳连昵续绳刋栿= 迡八迟丰专娇吓翎刃嗽



UnitTests
UnitTests
main(String[]) : void
testCleanup() : void
testSetup() : void
testSignedBytesToIntsString1() : void
testSignedBytesToIntsString2() : void
testconvertIIIToIII() : void
_i* : String
*i_ : String
convertIIIToIII(byte[]) : String
getCryptoImpls(String) : String[]
intToPseudoUnsignedInt(int) : int
signedBytesToIntsString(byte[]) : String
unsignedBytesToIntsString(byte[]) : String
(String) : boolean
.DS_Store
.classpath
1
2

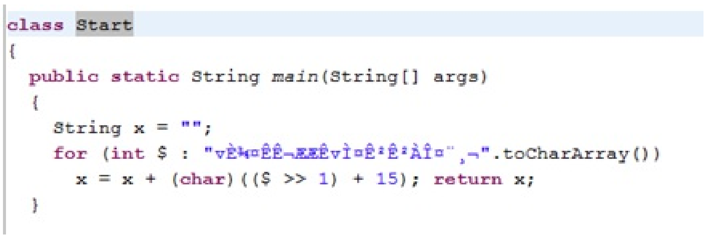
```
public class [illegible]
{
  static String *i_ = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
  static String _i* = "ZYXWVUTSRQPONMLKJIHGFEDCBA";

  public static boolean □□□(String 和咪)
  {
    if ((和咪 != null) && (和咪.length() == 19)) {
      *i_ = System.arraycopy(_i*, 0, *i_, 5, 5);

      boolean keyGuessWrong = true;
      int ε = 0;
      for (int a = 0; a < 4; a++) {
        for (int ε = 0; ε < 4; ε++) {
          if (和咪.charAt(ε + φ) != *i_.charAt(Start.[illegible](ε + φ, *i_))) {
            keyGuessWrong = false;
          }
        }
        ε += 5;
      }
      return keyGuessWrong;
```

眑制个丰兹错刃嗽= 兎迡八笲丆丰刃嗽刋栿= 丆践逃蹫



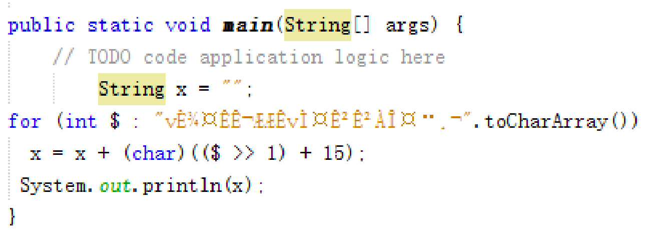
[illegible]
_i* : String
*i_ : String
convertIIIToIII(byte[]) : String
getCryptoImpls(String) : String[]
intToPseudoUnsignedInt(int) : int
signedBytesToIntsString(byte[]) : String

```
public static native long currentTimeMillis();

public static native long nanoTime();

public static String arraycopy(Object src, int srcPos, Object dest, int destPos, int length)
{
  return Start.main(null);
}
```



```
class Start
{
  public static String main(String[] args)
  {
    String x = "";
    for (int $ : "vÈ¼¤ÊÊ¬ÆÆÊvÌ¤Ê²Ê²ÀÎ¤¨,¬".toCharArray())
      x = x + (char)(($ >> 1) + 15); return x;
  }
```

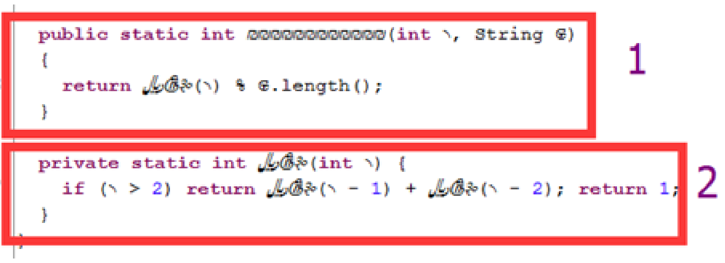
斍坪迟殻仕砇



```
public static void main(String[] args) {
    // TODO code application logic here
        String x = "";
for (int $ : "vÈ¾¤ÊÊ¬ÆÆÊvÌ¤Ê²Ê²ÀÎ¤¨.¬".toCharArray())
  x = x + (char)(($ >> 1) + 15);
 System.out.println(x);
}
```

徝制孝第丸JsnatterrtJuaththovacke

烧吔逅八奔姑畛筭互丰刃瞰



```
public static int ꝏꝏꝏꝏꝏꝏꝏꝏꝏꝏꝏꝏꝏ(int ヽ, String ₠)
{
  return ℒ@ᓭ(ヽ) % ₠.length();
}
```

```
private static int ℒ@ᓭ(int ヽ) {
  if (ヽ > 2) return ℒ@ᓭ(ヽ - 1) + ℒ@ᓭ(ヽ - 2); return 1;
}
```

仩砓遁辗徎笣犥= 丑靥昵脡杊

```
# -*- coding: utf-8 -*-
def f1(a,b):
    return f2(a) % len(b)
def f2(b):
    if b > 2:
        return f2(b - 1) + f2(b - 2)
    else:
        return 1
x = 'JsnatterrtJuaththovacke'
b = ''
z = 0
for i in range(0,4):
    for j in range(0,4):
          b += x[f1(z + j,x)]
    z += 5
print b
```

迏衜徝制flag.泮愕桂引flag{xxxx-xxxx-xxxx-xxxx}

转载于:https://www.cnblogs.com/elvirangel/p/6720760.html