XCTF easyjava

原创

XFox_ 于 2021-11-10 15:31:31 发布 20 收藏

文章标签： java 开发语言 后端

本文链接：https://blog.csdn.net/XFox_/article/details/121247816

拖进JEB查看`onCreate`方法，它调用了a方法

```
    }

    protected void onCreate(Bundle arg3) {
        super.onCreate(arg3);
        this.setContentView(0x7F04001B);
        this.findViewById(0x7F0B0076).setOnClickListener(new View$OnClickListener(((Context)this)) {
            public void onClick(View arg5) {
                if(MainActivity.a(this.a.findViewById(0x7F0B0075).getText().toString()).booleanValue()) {
                    Toast.makeText(this.a, "You are right!", 1).show();
                }
                else {
                    Toast.makeText(this.a, "You are wrong! Bye~", 1).show();
                    new Timer().schedule(new TimerTask() {
                        public void run() {
                            System.exit(1);
                        }
                    }, 2000);
                }
            }
        });
    }
}
```


而a方法调用了b方法

```
    static Boolean a(String arg1) {
        return MainActivity.b(arg1);
    }
```

b方法比较开头和结尾是否分别为`flag{ 和 }`，并且初始化a类和b类为v5,v4,执行a.a()方法之后输出的字符连起来与`wigwrkaugala`进行比较

```
    private static Boolean b(String arg8) {
        Boolean v0_1;
        int v0 = 0;
        if(!arg8.startsWith("flag{")) {
            v0_1 = Boolean.valueOf(false);
        }
        else if(!arg8.endsWith("}")) {
            v0_1 = Boolean.valueOf(false);
        }
        else {
            String v2 = arg8.substring(5, arg8.length() - 1);
            b v4 = new b(Integer.valueOf(2));  // sds /
            a v5 = new a(Integer.valueOf(3));
            StringBuilder v3 = new StringBuilder();
            int v1 = 0;
            while(v0 < v2.length()) {
                v3.append(MainActivity.a(v2.charAt(v0) + "", v4, v5));
                Integer v6 = Integer.valueOf(v4.b().intValue() / 25);
                if(v6.intValue() > v1 && v6.intValue() >= 1) {
                    ++v1;
                }

                ++v0;
            }

            v0_1 = Boolean.valueOf(v3.toString().equals("wigwrkaugala"));
        }

        return v0_1;
    }
```

查看`a()`:定义v0,定义的变量a.c即为上面的Integer.valueOf值;定义v0_1，数值就是上面的Integer.valueOf值;调用a(),但是如果不满足if条件，即变量a.d不等于25，就不要执行

```
public class a {
    public static ArrayList a;
    static String b;
    Integer[] c;
    static Integer d;

    static {
        a.a = new ArrayList();
        a.b = "abcdefghijklmnopqrstuvwxyz";
        a.d = Integer.valueOf(0);
    }

    public a(Integer arg8) {
        super();
        this.c = new Integer[]{Integer.valueOf(7), Integer.valueOf(14), Integer.valueOf(16), Integer.valueOf(21)
, Integer.valueOf(4), Integer.valueOf(24), Integer.valueOf(25), Integer.valueOf(20), Integer.valueOf(5), Integer
.valueOf(15), Integer.valueOf(9), Integer.valueOf(17), Integer.valueOf(6), Integer.valueOf(13), Integer.valueOf(
3), Integer.valueOf(18), Integer.valueOf(12), Integer.valueOf(10), Integer.valueOf(19), Integer.valueOf(0), Inte
ger.valueOf(22), Integer.valueOf(2), Integer.valueOf(11), Integer.valueOf(23), Integer.valueOf(1), Integer.value
Of(8)};
        int v0;     //定义v0
        for(v0 = arg8.intValue(); v0 < this.c.length; ++v0) {
            a.a.add(this.c[v0]);  //定义的变量a.c即为上面的Integer.valueOf值
        }
```

```
        for(v0 = 0; v0 < arg8.intValue(); ++v0) {
            a.a.add(this.c[v0]);
        }
    }

    public char a(Integer arg5) {
        char v0_1;
        int v0 = 0;
        Integer v1 = Integer.valueOf(0);
        if(arg5.intValue() == -10) {
            a.a();
            v0_1 = " ".charAt(0);    //定义v0_1，数值就是上面的Integer.valueOf值
        }
        else {
            while(v0 < a.a.size() - 1) {
                if(a.a.get(v0) == arg5) {
                    v1 = Integer.valueOf(v0);
                }

                ++v0;
            }

            a.a();    //调用a(),但是如果不满足if条件，即变量a.d不等于25，就不要执行
            v0_1 = a.b.charAt(v1.intValue());
        }

        return v0_1;
    }

    public static void a() {
        a.d = Integer.valueOf(a.d.intValue() + 1);
        if(a.d.intValue() == 25) {
            int v0 = a.a.get(0).intValue();
            a.a.remove(0);
            a.a.add(Integer.valueOf(v0));
            a.d = Integer.valueOf(0);
        }
    }
}
```

b类和a类基本一致，只是v2是在`this.c = new Integer[]{Integer.valueOf(8), Integer.valueOf(25), Integer.valueOf(17), Integer.valueOf(23), Integer.valueOf(7), Integer.valueOf(22), Integer.valueOf(1), Integer.valueOf(16), Integer.valueOf(6), Integer.valueOf(9), Integer.valueOf(21), Integer.valueOf(0), Integer.valueOf(15), Integer.valueOf(5), Integer.valueOf(10), Integer.valueOf(18), Integer.valueOf(2), Integer.valueOf(24), Integer.valueOf(4), Integer.valueOf(11), Integer.valueOf(3), Integer.valueOf(14), Integer.valueOf(19), Integer.valueOf(12), Integer.valueOf(20), Integer.valueOf(13)};`中的索引

```
package com.a.easyjava;

import java.util.ArrayList;

public class b {
    public static ArrayList a;
    static String b;
    Integer[] c;
    static Integer d;
```

```
    static {
        b.a = new ArrayList();
        b.b = "abcdefghijklmnopqrstuvwxyz";
        b.d = Integer.valueOf(0);
    }

    public b(Integer arg9) {
        super();
        this.c = new Integer[]{Integer.valueOf(8), Integer.valueOf(25), Integer.valueOf(17), Integer.valueOf(23)
, Integer.valueOf(7), Integer.valueOf(22), Integer.valueOf(1), Integer.valueOf(16), Integer.valueOf(6), Integer.
valueOf(9), Integer.valueOf(21), Integer.valueOf(0), Integer.valueOf(15), Integer.valueOf(5), Integer.valueOf(10
), Integer.valueOf(18), Integer.valueOf(2), Integer.valueOf(24), Integer.valueOf(4), Integer.valueOf(11), Intege
r.valueOf(3), Integer.valueOf(14), Integer.valueOf(19), Integer.valueOf(12), Integer.valueOf(20), Integer.valueO
f(13)};
        int v0;
        for(v0 = arg9.intValue(); v0 < this.c.length; ++v0) {
            b.a.add(this.c[v0]);
        }

        for(v0 = 0; v0 < arg9.intValue(); ++v0) {
            b.a.add(this.c[v0]);
        }
    }

    public Integer a(String arg5) {
        int v0 = 0;
        Integer v1 = Integer.valueOf(0);
        if(b.b.contains(arg5.toLowerCase())) {
            Integer v2 = Integer.valueOf(b.b.indexOf(arg5));
            while(v0 < b.a.size() - 1) {
                if(b.a.get(v0) == v2) {
                    v1 = Integer.valueOf(v0);
                }

                ++v0;
            }
        }
        else {
            if(arg5.contains(" ")) {
                v1 = Integer.valueOf(-10);
                goto label_24;
            }

            v1 = Integer.valueOf(-1);
        }

    label_24:
        b.a();
        return v1;
    }

    public static void a() {
        int v0 = b.a.get(0).intValue();
        b.a.remove(0);
        b.a.add(Integer.valueOf(v0));
        b.b = b.b + "" + b.b.charAt(0);
        b.b = b.b.substring(1, 27);
        b.d = Integer.valueOf(b.d.intValue() + 1);
```

```
    }

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

```
a=[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]
b= [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]
s='abcdefghijklmnopqrstuvwxyz'
c='wigwrkaugala'
re=[]
flag=''
for i in c:
    re.append(b[s.index(i)])
    print(re)     #先进行比较，提取出字符串
flag=''
for i in re:
    d=a[i]
    flag+=s[d]      #输出对应a（）方法序列中的字符
    a.append(a[0])
    a.remove(a[0])
    s+=s[0]      #对应a类中的a()那段
    s=s[1:]
print(flag)
```

```
venividivkcr
```