攻防世界(easy-apk)

原创

金鳞本鲤 于 2021-04-16 09:11:21 发布 420 收藏
分类专栏： CTF android

本文链接：https://blog.csdn.net/weixin_43906500/article/details/115748008

CTF 同时被 2 个专栏收录
20 篇文章 0 订阅
订阅专栏

android
5 篇文章 0 订阅
订阅专栏

下载链接如下所示：https://adworld.xctf.org.cn/media/task/attachments/989ca07c3f90426fa05406e4369901ff.apk

使用JEB打开apk，如下所示：

```
public class MainActivity extends AppCompatActivity {
    public MainActivity() {
        super();
    }

    protected void onCreate(Bundle arg3) {
        super.onCreate(arg3);
        this.setContentView(2130968603);
        this.findViewById(2131427446).setOnClickListener(new View$OnClickListener() {
            public void onClick(View arg8) {
                if(new Base64New().Base64Encode(MainActivity.this.findViewById(2131427445).getText().toString().getBytes()).equals("5rFf7E2K6rqN7Hpiyush7E
                    Toast.makeText(MainActivity.this, "验证通过!", 1).show();
                }
                else {
                    Toast.makeText(MainActivity.this, "验证失败!", 1).show();
                }
            }
        });
    }
}
```

可知获得输入后进行Base64编码，并进行判断是否与特定字符编码是否一致

打开Bse64New，可知其编码位置进行了改变，需要重新设计代码进行编程

```
static {
    Base64New.Base64ByteToStr = new char[]{'v', 'w', 'x', 'r', 's', 't', 'u', 'o', 'p', 'q', '3', '4', '5', '6', '7', 'A', 'B', 'C', 'D', 'E', 'F', 'G
    Base64New.StrToBase64Byte = new byte[128];
}

public Base64New() {
    super();
}

public String Base64Encode(byte[] arg9) {
    int v7 = 3;
    StringBuilder v3 = new StringBuilder();
    int v1;
    for(v1 = 0; v1 <= arg9.length - 1; v1 += 3) {
        byte[] v0 = new byte[4];
        byte v4 = 0;
        int v2;
        for(v2 = 0; v2 <= 2; ++v2) {
            if(v1 + v2 <= arg9.length - 1) {
                v0[v2] = ((byte)((arg9[v1 + v2] & 255) >>> v2 * 2 + 2 | v4));
                v4 = ((byte)(((arg9[v1 + v2] & 255) << (2 - v2) * 2 + 2 & 255) >>> 2));
            }
            else {
                v0[v2] = v4;
                v4 = 64;
            }
        }

        v0[v7] = v4;
        for(v2 = 0; v2 <= v7; ++v2) {
            if(v0[v2] <= 63) {
                v3.append(Base64New.Base64ByteToStr[v0[v2]]);
            }
            else {
                v3.append('=');
            }
        }
    }
```


python实现代码如下所示：

```
def Base64Decode(str_list):
    list_base = []
    a = str_list[0] << 2
    c = str_list[1] & 15
    b = str_list[1] >> 4
    a = a | b
    list_base.append(a)
    c = c << 4
    a = str_list[2] & 3
    b = str_list[2] >> 2
    c = c | b
    list_base.append(c)
    a = a << 6
    a = a | str_list[3]
    list_base.append(a)
    return list_base

CodingTable = 'vwxrstuopq34567ABCDEFGHIJyz012PQRSTKLMNOZabcdUVWXYefghijklmn89+/'
Ciphertext = '5rFf7E2K6rqN7Hpiyush7E6S5fJg6rsi5NBf6NGT5rs='

i = 0
flag = 'flag{'

while i <= (len(Ciphertext) - 1):
    list1 = []
    n = 0
    for k in range(4):
        if Ciphertext[i + k] == '=':
            list1.append(0)
            n = n + 1
        else:
            # 获取编码在编码表中的位置
            list1.append(CodingTable.index(Ciphertext[i + k]))
    print(list1)
    # 将4个字节转换为3个字节
    ba = Base64Decode(list1)
    print(ba)
    for j in range(3 - n):
        ch = chr(ba[j])
        flag = flag + str(ch)
    i = i + 4

flag = flag + '}'
print(flag)
```

获取最终flag：

flag{05397c42f9b6da593a3644162d36eb01}