# 攻防世界WEB进阶之Triangle

原创

harry_c 于 2019-08-06 22:24:40 发布 1205 收藏

分类专栏： 攻防世界 文章标签： 攻防世界web进阶 渗透 攻防 网络安全 Triangle



本文链接：https://blog.csdn.net/harry_c/article/details/98669424





## 攻防世界WEB进阶之Triangle



## 第一步：分析

难度系数：4星

题目来源： Hack.lu-2017

题目描述：暂无

## 第二步：实操

```
get_pw()
XYzaSAAX_PBssisodjsal_sSUVWZYYYb
function getARM1(){
var x = stoh(atob(getBase64Image(“frei”)));
var output = new Array();
for(var i = 0; i < o2.length ; i++){
output[i] = x[o2[i]];
}
return output;
}
function toHexString(byteArray) {
return Array.from(byteArray, function(byte) {
return (‘0’ + (byte & 0xFF).toString(16)).slice(-2)
}).join(’’)
}
oHexString(getARM1())
```

http://armconverter.com/hextoarm/

```
0800a0e10910a0e10a20a0e10030a0e30050a0e30040d0e5010055e30100001a036003e2064084e0064084e2015004e2004
0c1e5010080e2011081e2013083e2020053e1f2ffffba0000a0e30010a0e30020a0e30030a0e30040a0e30050a0e30060a0e30
070a0e30090a0e300a0a0e3
```

```
function getARM2(){
var x = stoh(atob(getBase64Image("eye")));
var output = new Array();
for(var i = 0; i < o1.length ; i++){
output[i] = x[o1[i]];
}
return output;
}
toHexString(getARM2())
```

```
0900a0e10a10a0e10830a0e10040a0e30050a0e300c0a0e30020d0e50060d1e5056086e201c004e200005ce30000000a036
046e2060052e10500001a010080e2011081e2014084e2030054e1f1ffffba0150a0e30000a0e30010a0e30020a0e30030a0e30
040a0e30060a0e30070a0e30080a0e30090a0e300a0a0e300c0a0e3
```

因为对汇编不甚了解，逆向流程也不太清晰。故此参考后面的博文链接流程图等内容。

使用python2编写逆向程序：

```
import string
def enc_pw(s):
# 逆向函数，求解enc_pw内容
res = ''
f = 0
for i, c in enumerate(s):
#遍历 i：序号 c：对应字符
c = ord©
# 返回对应10进制数值
if f == 1:
c += i & 3
c += 6
f = c & 1
res += chr©
print(res)
return res

if name == 'main':
enc = 'XYzaSAAX_PBssisodjsal_sSUVWZYYYb'
enc1 = ''
flag = ''
for i, c in enumerate(enc):
c = ord©
c -= 5 # 源为c += 5
if i & 1:
c += 3 # 源为c -= 3
for d in string.printable:
# 遍历ASCII所有的能够打印的字符
if enc_pw(flag + d)[i] == chr©:
# 判断源和逆向_(:з」∠)_ 字符串是否相等
flag += d # 此处经过每一步的遍历将所有的值都求出
break
# 此时遍历结束，最终的flag求出
print('flag{' + flag + '}')
```

## 第三步：答案

至此最终flag为：flag:{MPmVH94PTH7hhafgYahYaVfKJNLRNQLZ}

## 第四步：参考，本文参考的博客是：

https://blog.csdn.net/gonganDV/article/details/96285636