### misc-签到

用010打开,在最后找到 ZmxhZ3sxX3dhbnRfam1hbXVzX3Awd2VyfQ== 用base64解码

ZmxhZ3sxX3dhbnRfamlhbXVzX3Awd2VyfQ==

加密

解密

□解密结果以16进制显示

 $\texttt{flag}\{1\_\texttt{want\_jiamus\_p0wer}\}$ 

# baby-web-九曲十八弯

用 view-source查看源码

拉到最下方

发现链接 <script src="./scripts/hello\_world.js"></script>

然后得到 QXN1cm17dm11d19zb3VyY2Unc19wb3d1cn0= 解码

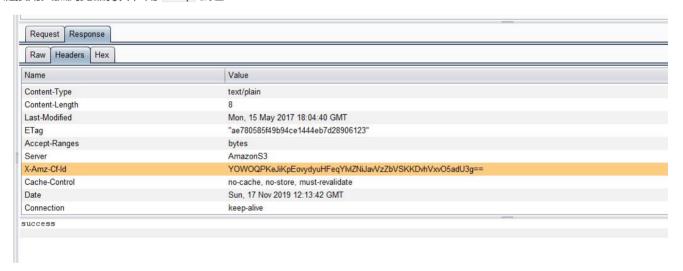
QXN1cm17dm11d19zb3VyY2Unc19wb3d1cn0=

加密 解密 □解密结果以16进制显示

Asuri {view\_source's\_power}

### medium\_web\_justburp

链接用火狐浏览器打开,用 burp 截包



发现 YOWOQPKeJiKpEovydyuHFeqYlvlZNiJavVzZbVSKKDvhVxvO5adU3g==

但是用base64解码不出

#### easy\_pwn

用 IDA打开 分析main 函数

通过输入 passworld size 和 password 来执行

door 函数 从而得到 shell

main 函数地址 0x400777

door函数地址 0x400766

```
var64 地址为 -0x0064
buf地址为 -0x0060
nbytes 地址为 -0x0004
r 返回地址为 +0x0008
```

## medium\_rev

在线反编译python 得到python源码

```
然后新建一个py文件
```

```
89,
117]
key = (lambda .0: continue[ i for i in .0 ])(filter(check_prime, test))
return key
```

但是这里报错 不能执行