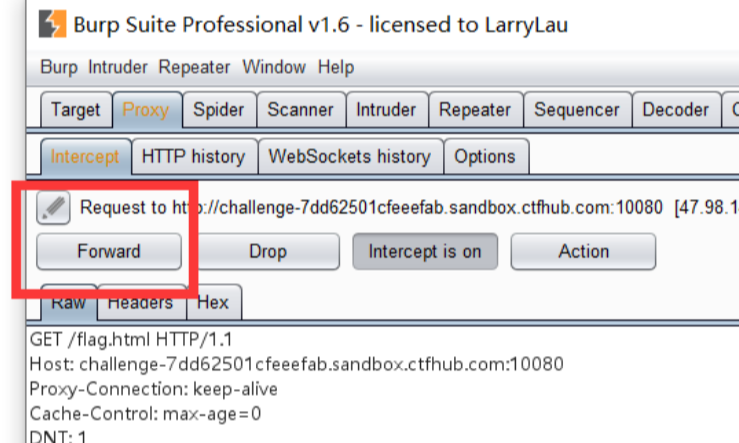
1. **基础认证**

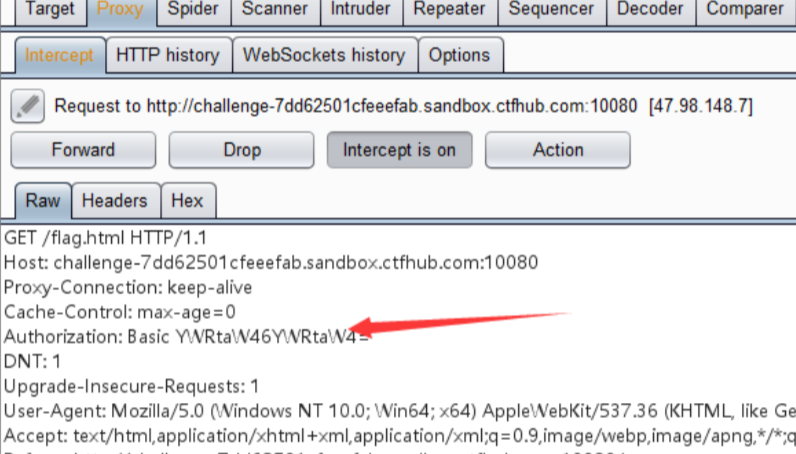
要求进行验证（Basic access authentication），又给了附件密码字典，那么应该就是爆破

用burpsuite intruder 进行爆破

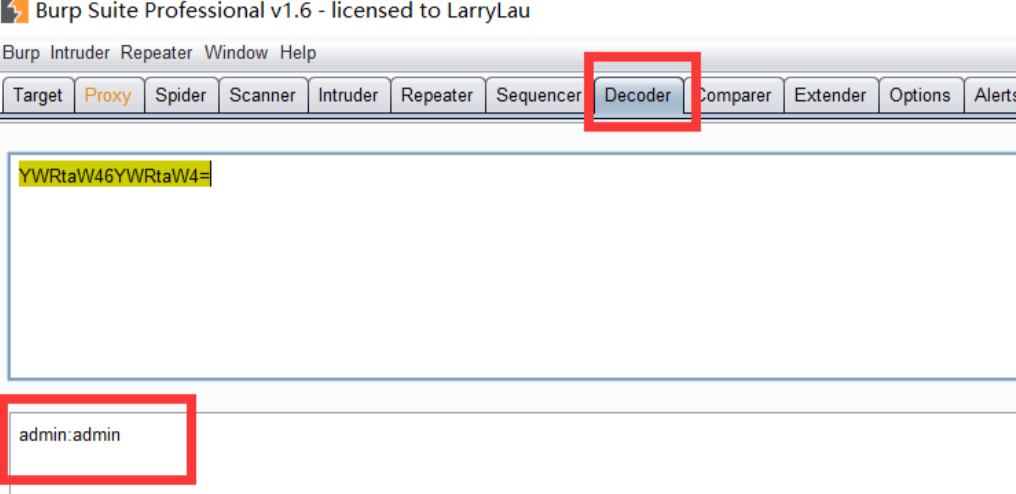
先开启代理，bp抓包，第一个抓到的这样的包要点直接发送



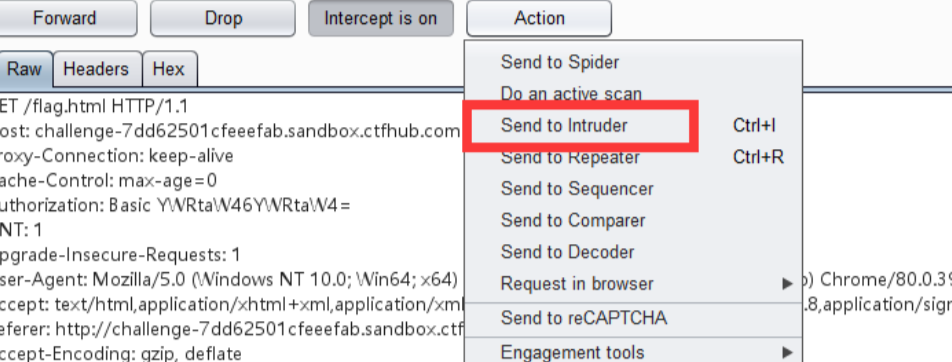
在登陆界面随便填写简单的账号密码，点登录，抓取该数据包时发现



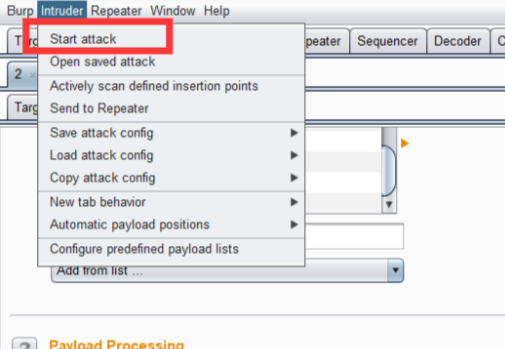
后边的不太规则的字符串是base64编码的字符串，可以拿到bp的decode模块解码，发现解码后就是自己输入的账号密码



那么我可以爆破这个人的账号密码，下面需要用到intruder模块，点击action，然后send to intruder



构造号payload后，选择题目提供的密码字典，一般的网站默认用户名为admin，那么我们就需要爆破密码了，而那段base64的字符串就包含了用户名和密码的信息，那么我们要按照一定的规则，生成base64字符串，之后就可以开始爆破了



找出status或者是length异常的一条结果，即可找到flag

1. **CTFHub-Web-Web前置技能-目录遍历**

打开题目，发现存在文件遍历



一个一个找显然有点费时，简单地写个js脚本即可遍历得到flag

const request = require("request");

url = "http://challenge-cefd47641a6f63ec.sandbox.ctfhub.com:10080/flag\_in\_here/";

for(let i = 1; i <= 4; i++ ){

for(let j = 1; j <= 4; j++){

request(url+i+'/'+j, function(err, res, body){

if(err) console.log(err);

let reg = RegExp(/flag.txt/)

if(body.match(reg)){

console.log(body.match(reg))

console.log(url+i+'/'+j)

}

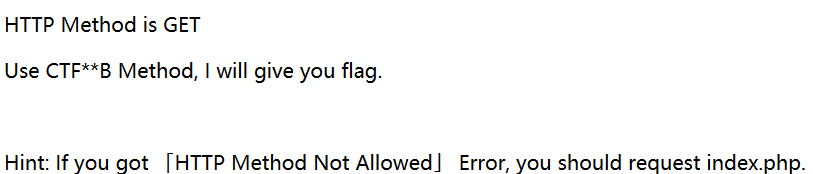
})

}

}

1. **请求方式**

打开时候，是这样的页面。



需要用到CTFHUB 方法请求 index.php来获取flag

HTTP Method 是自定义的，并且区分大小写.采用bp抓包拦截，

然后把请求方式改为CTFHUB即可得到flag

**4. 302跳转**

打开之后是这样的页面，点击链接之后没有什么变化



应该是发生了重定向了

利用curl命令行工具，直接访问index.php，得到flag。  
命令：curl -i CTFHUB <http://challenge-a8d014d13d7651c3.sandbox.ctfhub.com:10080/index>

**5. cookie**

打开之后页面提示只有admin可以得到flag

抓包拦截，发现cookie里有字段admin=0

把admin的值改为1，再发包即可得到flag