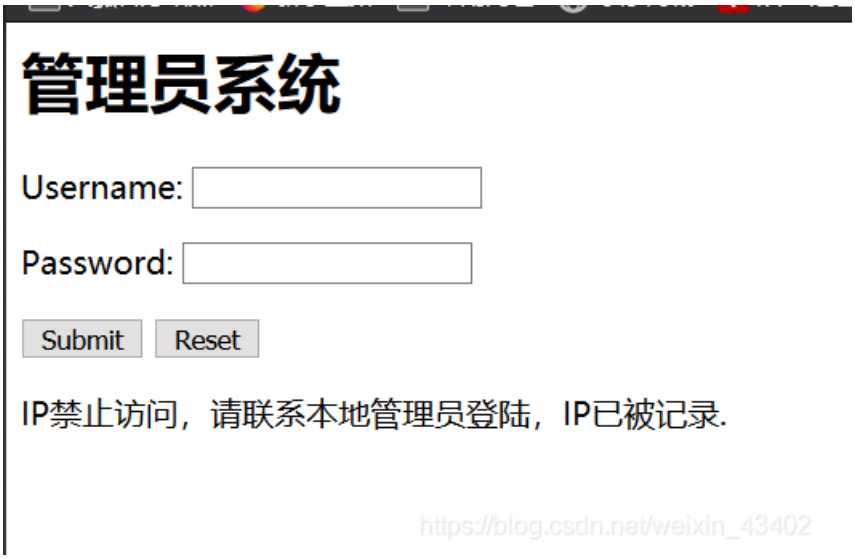
管理员系统 writeup

原创

ctf小菜鸡 于 2020-02-12 21:45:13 发布 144 收藏 1

14.管理员系统 writeup



输入猜测的用户名和密码 发现不正确 ， 而且在下边还提示本地管理员登录
看到这个就想到X-Forwarded-For

```
> **简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP**
```

伪造一个XFF头,伪装成本地登录

```
X-Forwarded_For: 127.0.0.1
```

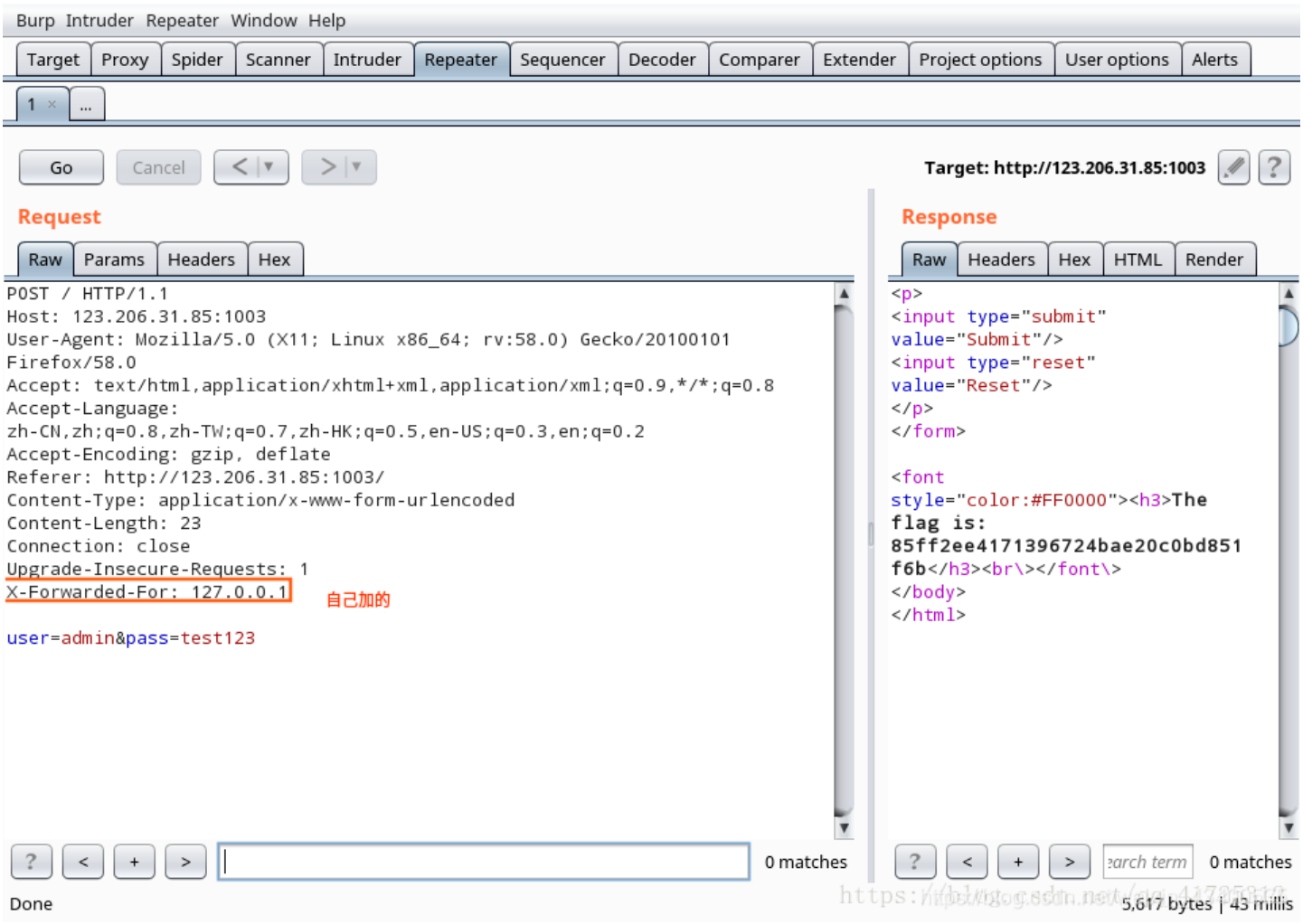
在来看看源码

这个我一直没发现里面的玄机,怪我太s了,后来才看到在源码的最后面有一个base64的编码

```
5020
5021
5022
5023 <!-- dGVzdDEyMw== -->
```

解密为test123,猜测应该是管理员密码

Burp抓包,然后转到Repeater模块中



Go得到了flag,转换为flag格式