




BugkuCTF---管理员系统

原创

&执笔者  于 2019-04-14 13:13:21 发布  2104  收藏 2

分类专栏: [CTF练习](#) 文章标签: [BugkuCTF题库](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43592364/article/details/89295383

版权



[CTF练习](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

题目链接: [链接](#)

Challenge 2785 Solves ×

管理员系统

60

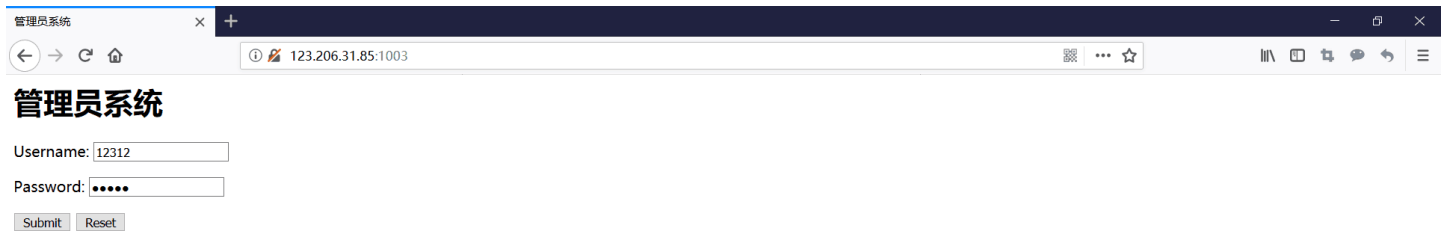
<http://123.206.31.85:1003/>

flag格式flag{}

Flag Submit

https://blog.csdn.net/qq_43592364

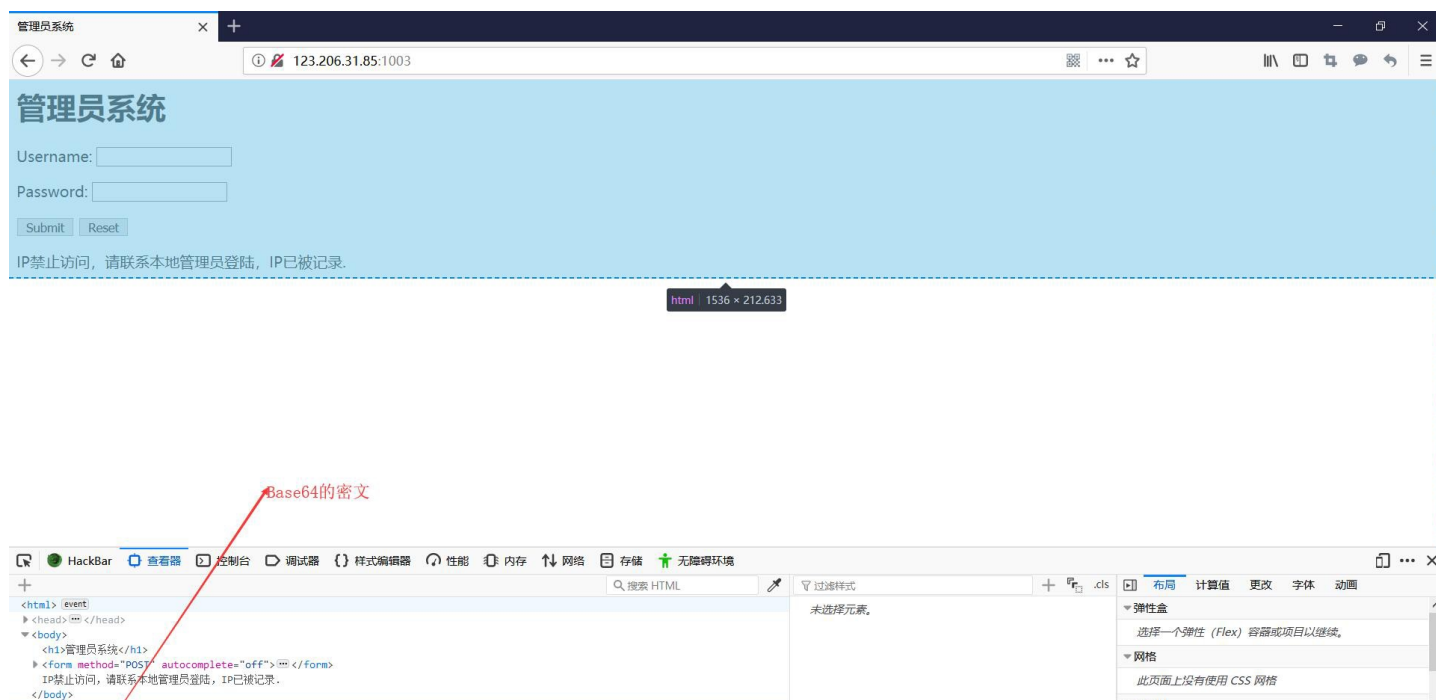
打开题目链接, 看到的是一个登陆界面, 还是先随便试一下用户名和登陆密码吧



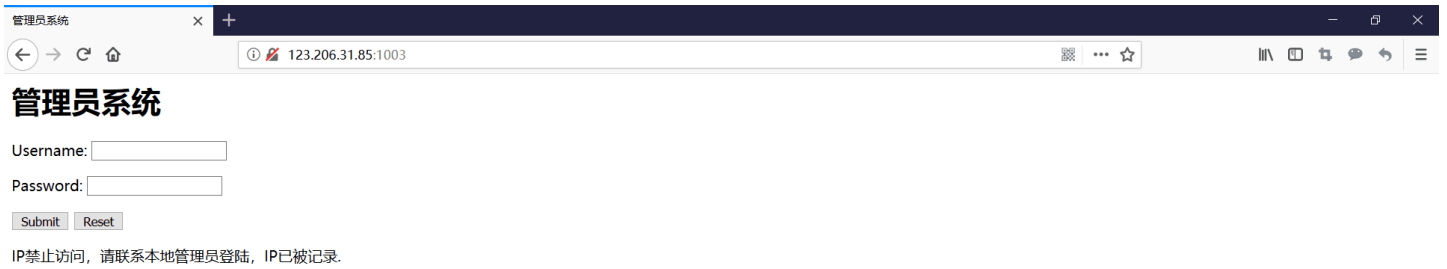
提示是：IP禁止访问，请联系本地管理员登陆，IP已被记录



那就看一下页面元素，发现了一堆Base64的密文，那就用Hackbar来解密一下试试

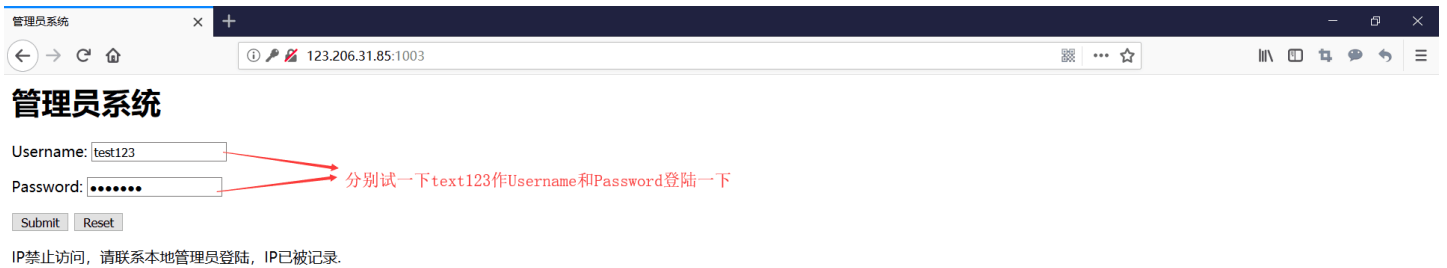


```
</html>
<!--dGVzdDEyMw==-->
html > body
```



https://blog.csdn.net/qg_43592364

得到了一个test123的字符串，那就试一试会不会是用户名和密码



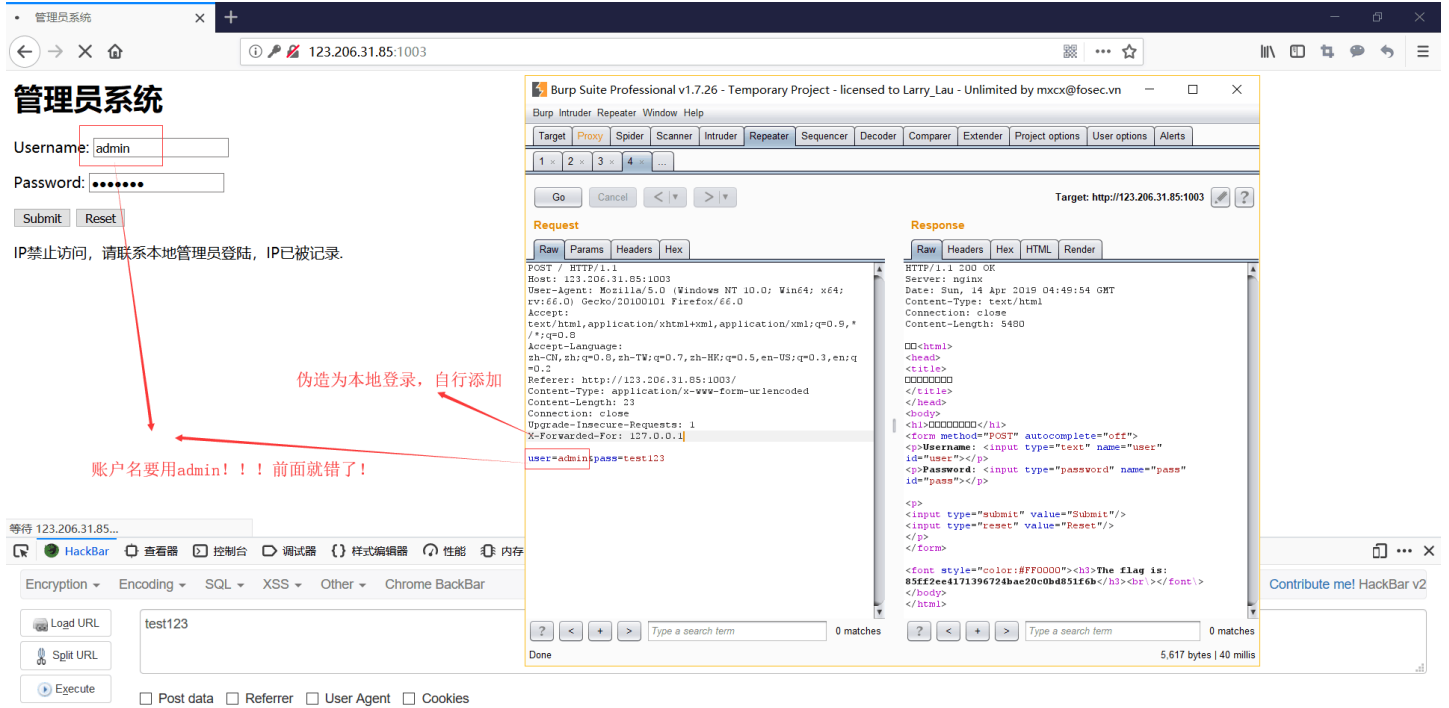
https://blog.csdn.net/qg_43592364

结果还是一样没有任何变化，提示依旧是联系本地管理员，那不如试一下伪造成本地登录用burpsuite抓包，传递给repeater后在row那一栏下方添加X-Forwarded-For: 127.0.0.1

这里的X-Forwarded-For详见链接：[X-Forwarded-For的用法](#)

X-Forwarded-For(XFF)是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。

再点击go进行发包，结果得到flag



https://blog.csdn.net/qq_43592364



https://blog.csdn.net/qq_43592364

//这里想补充的是，在第一次抓包的时候，Username和Password我填的全是test123，再经过上述伪造本地登陆的操作还是没有得到flag。后来是上网查了本地登陆的用户名应当填写admin，再次抓包并伪造才得到flag。