BugkuCTF---管理员系统

原创

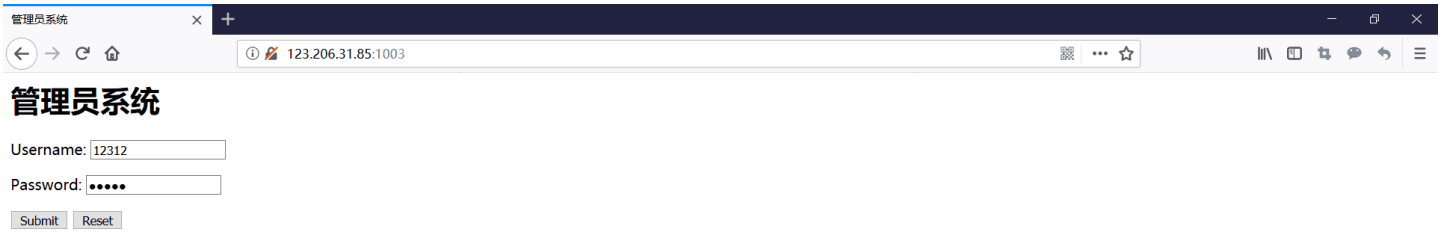
&执笔者 于 2019-04-14 13:13:21 发布 2104 收藏 2

分类专栏： CTF练习 文章标签： BugkuCTF题库

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

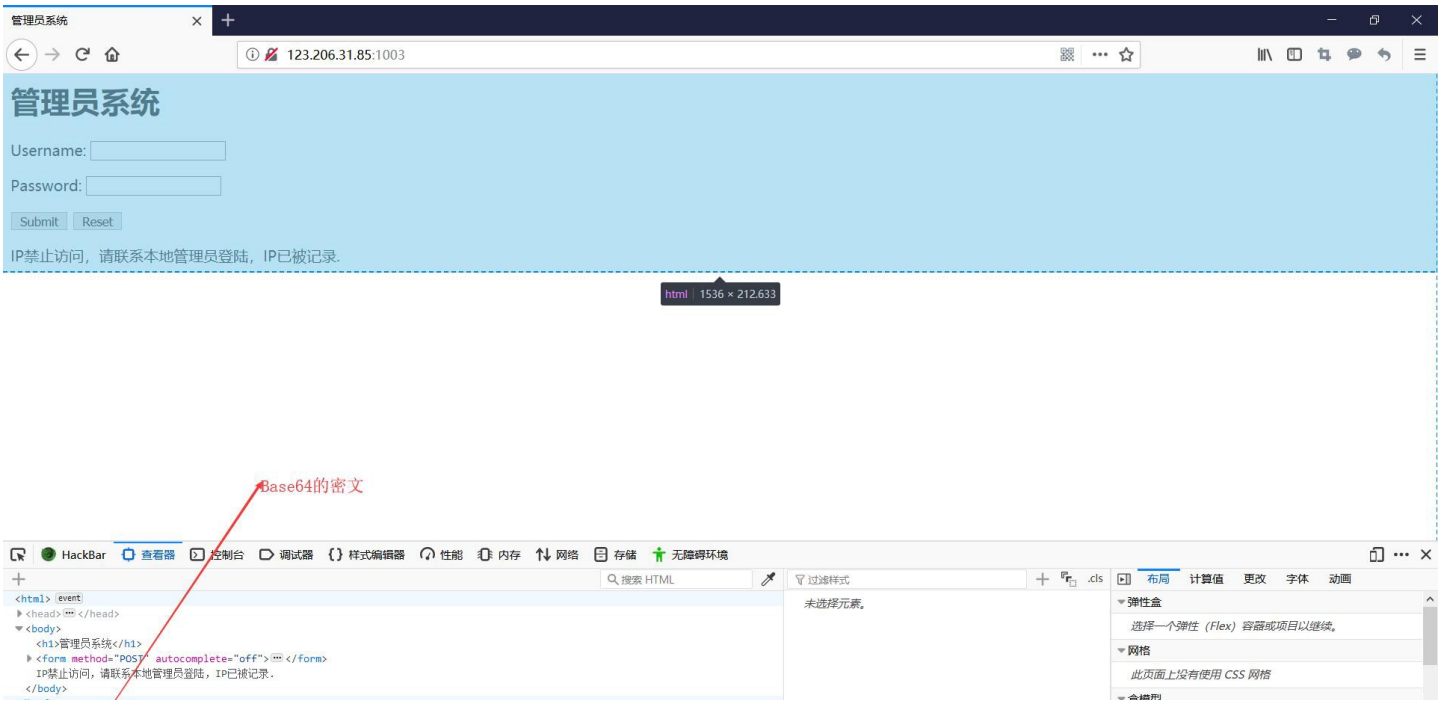
题目链接：链接

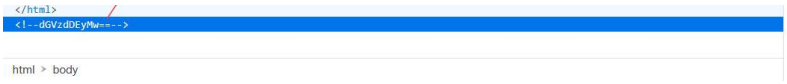
打开题目链接，看到的是一个登陆界面，还是先随便试一下用户名和登陆密码吧

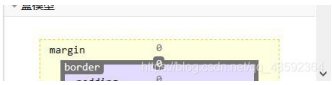


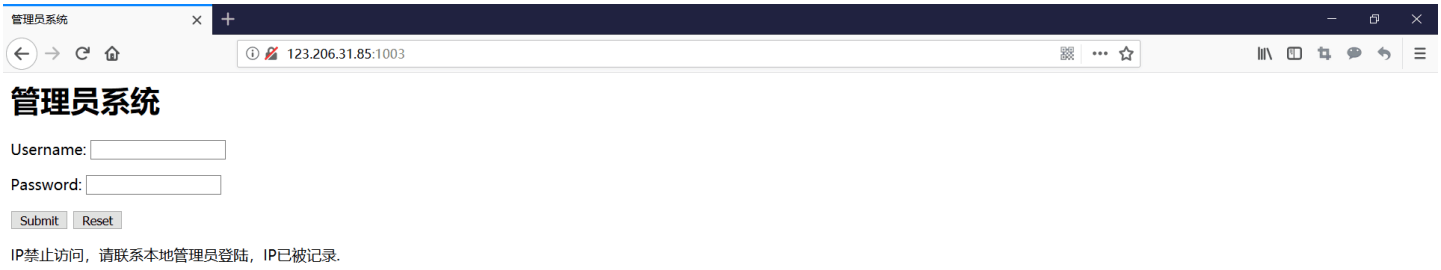
提示是：**IP禁止访问，请联系本地管理员登陆，IP已被记录**

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

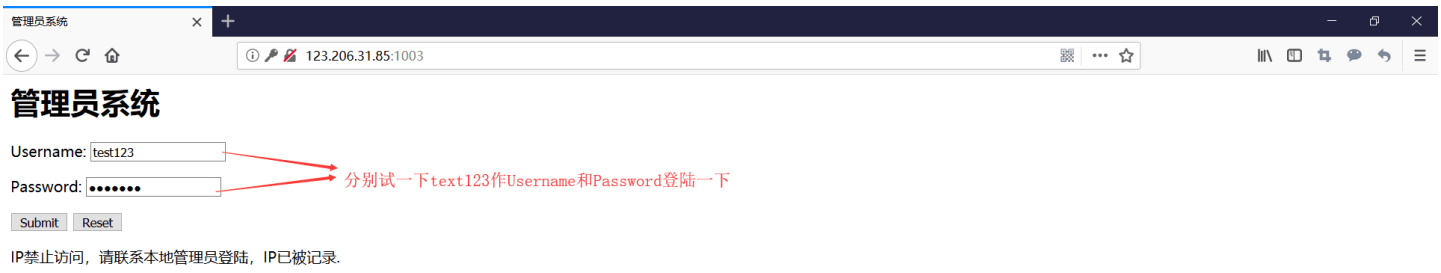








得到了一个**test123**的字符串，那就试一试会不会是用户名和密码



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

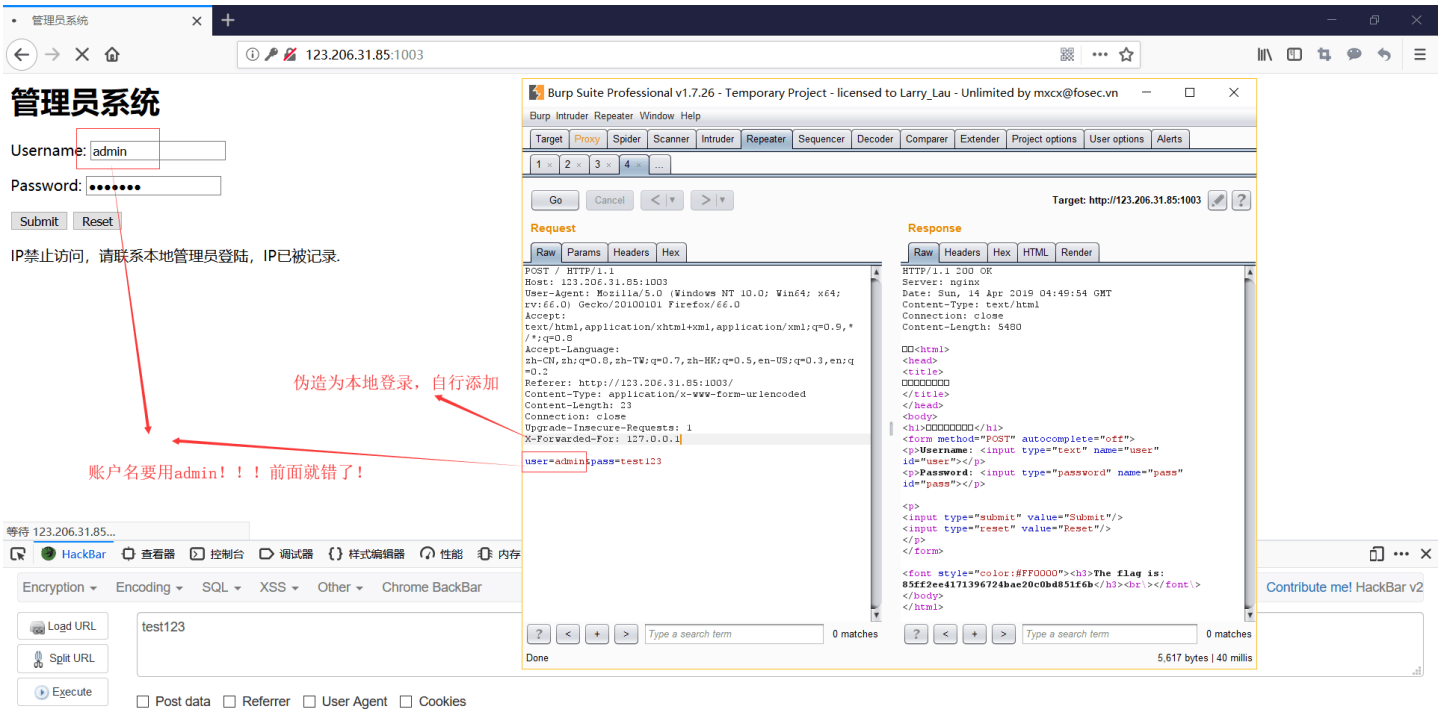
用burpsuite抓包，传递给repeater后在row那一栏下方添加X-Forwarded-For：127.0.0.1

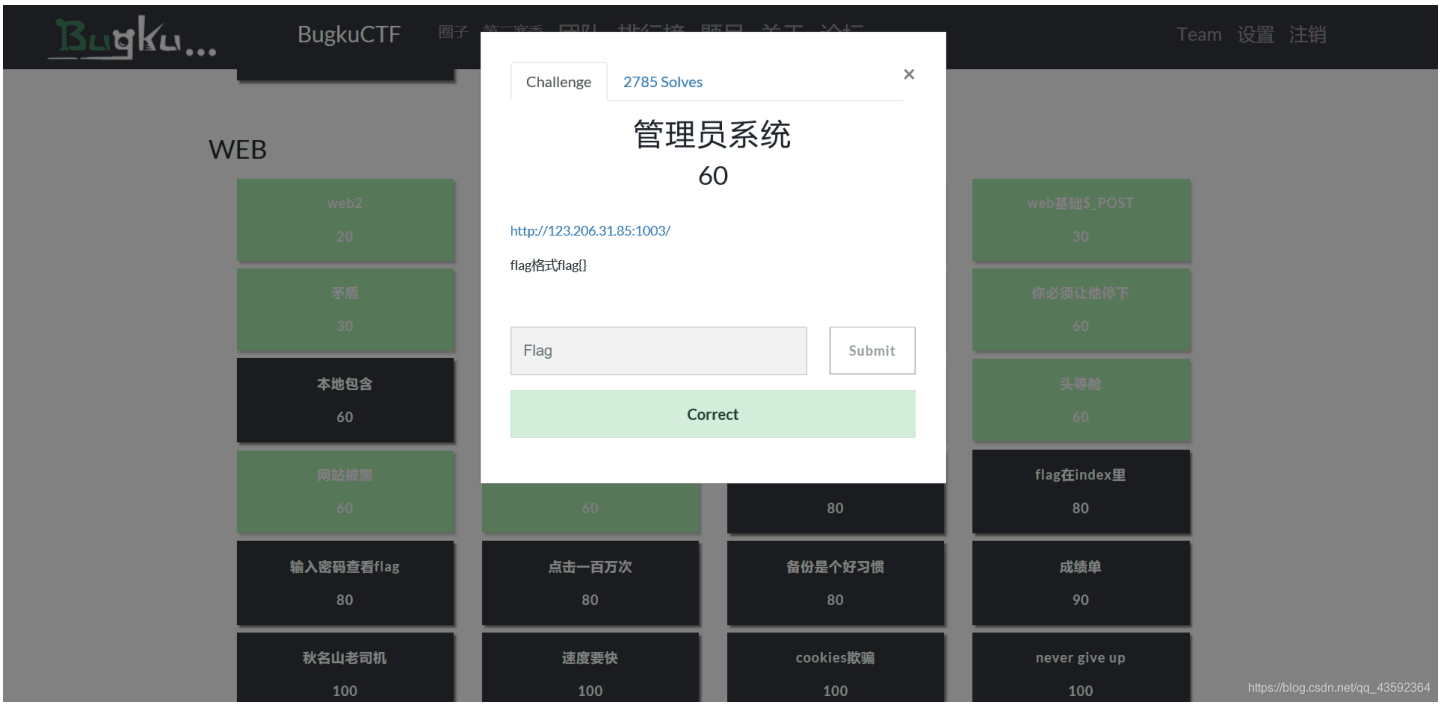
> X-Forwarded-For：127.0.0.1

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进行放包，结果得到flag





//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。