

# bugku-writeup-web-本地管理员

原创

dark2019 于 2021-06-14 14:58:20 发布 53 收藏

分类专栏: [信息安全](#) 文章标签: [信息安全](#) [web](#)

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\\_22597955/article/details/117904490](https://blog.csdn.net/qq_22597955/article/details/117904490)

版权



[信息安全](#) 专栏收录该内容

53 篇文章 1 订阅

订阅专栏

“bugku-web本地管理员 解题思路记录。”

题目: 本地管理员

本地管理员

WEB

已解决

分数: 15

金币: 2

题目作者: [harry](#)

一血: [dotast](#)

一血奖励: 1金币

解决: 3510

提示:

描述: 本地管理员

启动场景

[https://blog.csdn.net/qq\\_22597955](https://blog.csdn.net/qq_22597955)

01—解码

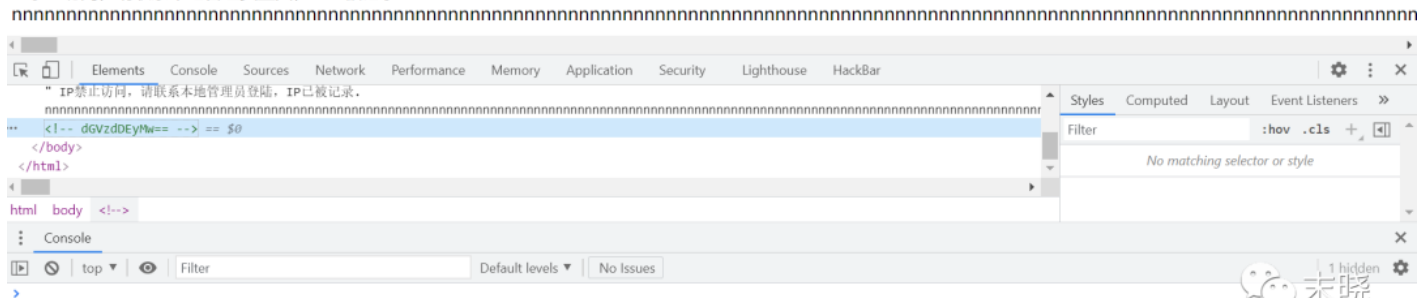
按F12查看源码, 发现登陆密码。

# 管理员系统

Username:

Password:

IP禁止访问, 请联系本地管理员登陆, IP已被记录.



使用**base64**在线工具解码, 得到密码为test123。



## 02—本地登陆

输入用户名: admin, 密码: test123, 提示无法登陆, 并显示“IP禁止访问, 请联系本地管理员登陆, IP已被记录”。可以推断需要本地登陆, 因此, 打开**Burp suite**抓包, 在Proxy查看HTTP history。

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	P	Cookies	Time	Listener port
111	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	931	JSON					104.26.8.142		12:34:32 14 ...	8080
112	https://incoming.telemetry.mozilla.org	POST	/submit/active-stream/sessions/17643...			200	236	text					52.27.200.224		12:34:32 14 ...	8080
113	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	927	JSON					104.26.8.142		12:34:32 14 ...	8080
114	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	925	JSON					104.26.8.142		12:34:32 14 ...	8080
115	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	925	JSON					104.26.8.142		12:34:32 14 ...	8080
116	http://114.67.246.176:17785	GET	/favicon.ico			404	470	HTML	ico	404 Not Found			114.67.246.176		12:36:57 14 ...	8080
117	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	933	JSON					104.26.8.142		12:36:57 14 ...	8080
118	http://114.67.246.176:17785	POST	/			200	5684	HTML		Flag is: flag{c6ca1cfaedc39b8ecd933ad679661}			114.67.246.176		12:36:58 14 ...	8080
119	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	927	JSON					104.26.8.142		12:37:07 14 ...	8080
120	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	935	JSON					104.26.8.142		12:37:07 14 ...	8080
121	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	927	JSON					104.26.8.142		12:37:07 14 ...	8080
122	https://api.shodan.io	GET	/dns/resolve?key=MM72AkzHXDhpCBP...			503	931	JSON					104.26.8.142		12:37:07 14 ...	8080

```

Request / Response
Raw Params Headers Hex
POST / HTTP/1.1
Host: 114.67.246.176:17785
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://114.67.246.176:17785
Connection: close
Referer: http://114.67.246.176:17785/
Upgrade-Insecure-Requests: 1

user=admin&pass=test123
    
```



发送到Repeater，添加本地代理X-Forwarded-For: 127.0.0.1，然后Go,查看Response，显示flag。

The screenshot shows the Repeater tool with a request and response. The request is a POST to http://114.67.246.176:17785 with headers including 'X-Forwarded-For: 127.0.0.1' and body 'user=admin&pass=test123'. The response is a 200 OK HTML page from Apache/2.4.7 (Ubuntu) with a flag: 'The flag is: flag{c6ca1cfaedc39b8ecd933ad679661}'.

又打通了一关哟，题目里面线索很多，细心去发现，flag就在眼前。