

Bugku bugku导航 writeup

原创

[n1109964492](#) 于 2020-03-21 15:26:12 发布 593 收藏

分类专栏: [ctf](#) 文章标签: [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/n1109964492/article/details/105010438>

版权



[ctf 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

第一次写文章, 如果有什么问题欢迎大家指出

Challenge 91 Solves

bugku导航

150

<http://123.206.87.240:9006/>

flag在根目录

Flag Submit

<https://blog.csdn.net/n1109964492>

打开上面的链接显示这样

CTF社区 CTF社

[设为首页](#) [加入收藏](#) [新建页面](#)

首页 娱乐休闲 生活服务 电脑网络 文化教育 地方服务 国外网站 其他类别

邮箱快速登录 百度 搜索 热门关键词

欢迎您: qweasd 管理我的收藏 添加收藏网址

网站动态 国内新闻 国际新闻

Get ADOBE FLASH PLAYER

Baidu 百度

Sina 新浪网



娱乐休闲

<https://blog.csdn.net/n1109964492>

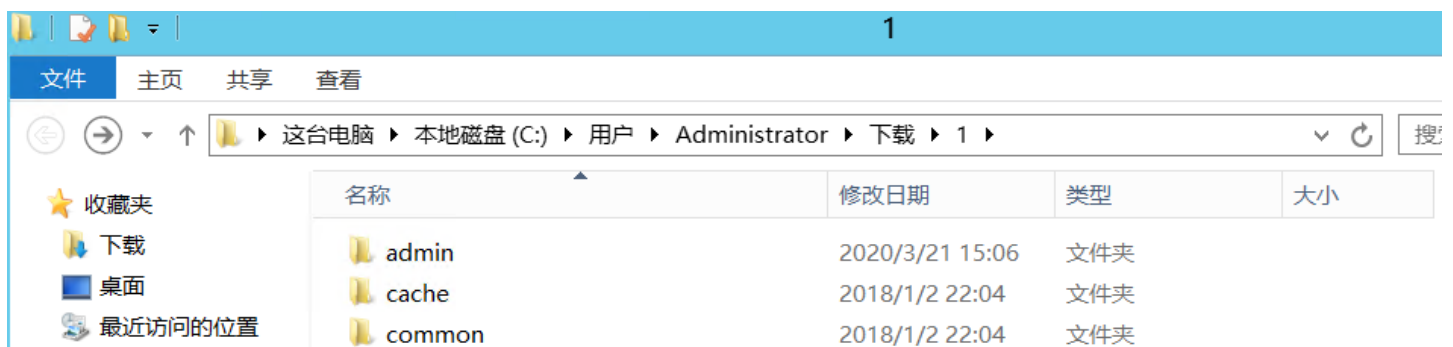
第一步，我们先用扫描器扫描该网站有没有什么敏感文件或资源

```

root@kali: ~/dirsearch-master
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: ~ x root@kali: ~ x root@kali: ~/dirsearch-... x
Target: http://123.206.87.240:9006/
[14:55:48] Starting:
[14:56:03] 301 - 178B - /admin -> http://123.206.87.240:9006/admin/
[14:56:04] 200 - 17B - /admin/
[14:56:04] 200 - 17B - /admin/?/login
[14:56:05] 200 - 17B - /admin/index.php
[14:56:06] 200 - 3KB - /admin/login.php
[14:56:06] 200 - 925B - /admin/upload.php
[14:56:22] 200 - 2MB - /1.zip
[14:56:25] 301 - 178B - /cache -> http://123.206.87.240:9006/cache/
[14:56:29] 301 - 178B - /common -> http://123.206.87.240:9006/common/
[14:56:29] 200 - 6B - /config.xml
[14:56:31] 301 - 178B - /data -> http://123.206.87.240:9006/data/
[14:56:40] 301 - 178B - /include -> http://123.206.87.240:9006/include/
[14:56:42] 200 - 56KB - /index.html
[14:56:48] 301 - 178B - /member -> http://123.206.87.240:9006/member/
[14:56:48] 200 - 3KB - /member/
[14:56:48] 200 - 365B - /member/login.php
[14:56:59] 200 - 91B - /robots.txt
[14:57:06] 301 - 178B - /templates -> http://123.206.87.240:9006/templates/
[14:57:06] 301 - 178B - /templates_c -> http://123.206.87.240:9006/templates_c/
[14:57:08] 301 - 178B - /upload -> http://123.206.87.240:9006/upload/

```

我们发现扫出了1个admin、1.zip、robots.txt等等敏感文件目录
 然后我们访问1.zip把该文件下载过来，然后下载解压后发现这个是该网站的源代码
 这个时候，我们在看一下上面的题目提示，flag在根目录，是的，我们发现了这个东西



名称	日期	类型	大小
data	2018/1/2 22:04	文件夹	
include	2020/3/21 15:06	文件夹	
member	2018/1/2 22:04	文件夹	
player	2018/1/2 22:04	文件夹	
slogo	2020/3/21 15:06	文件夹	
sort	2020/3/21 15:06	文件夹	
templates	2018/1/2 22:04	文件夹	
templates_c	2018/1/2 22:04	文件夹	
update	2018/1/2 22:04	文件夹	
config.xml	2018/1/2 22:04	XML 文档	2 KB
flag-asd.txt	2018/1/2 22:04	文本文档	0 KB
index.html	2018/1/2 22:04	Chrome HTML D...	56 KB
is_installed.lock	2018/1/2 22:04	LOCK 文件	1 KB
robots.txt	2018/1/2 22:04	文本文档	1 KB

17 个项目 | 选中 1 个项目 0 字节

<https://blog.csdn.net/n1109964492>

在本地打开该文件是没有任何东西的，但是我们在浏览器上访问该文件，就显示出flag了

← → ↻ ⓘ 不安全 | 123.206.87.240:9006/flag-asd.txt

flag {NusWJjsw90-SDADSADAA}