

# BUUCTF [RootersCTF2019] ImgXweb

原创

Senimo\_ 于 2020-12-16 11:57:36 发布 240 收藏

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [BUUCTF RootersCTF2019](#) [ImgXweb writeup](#) [CTF](#)

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\\_44037296/article/details/111249777](https://blog.csdn.net/weixin_44037296/article/details/111249777)

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

65 篇文章 9 订阅

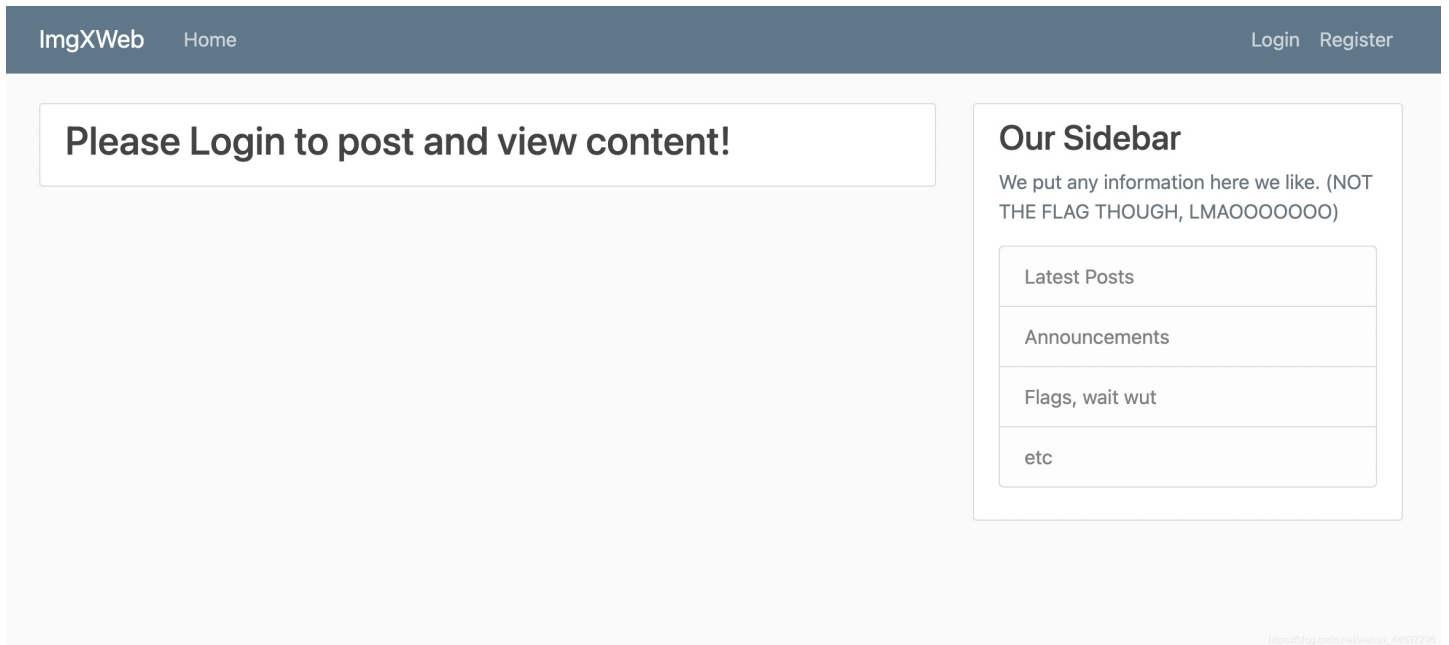
订阅专栏

## BUUCTF [RootersCTF2019] ImgXweb

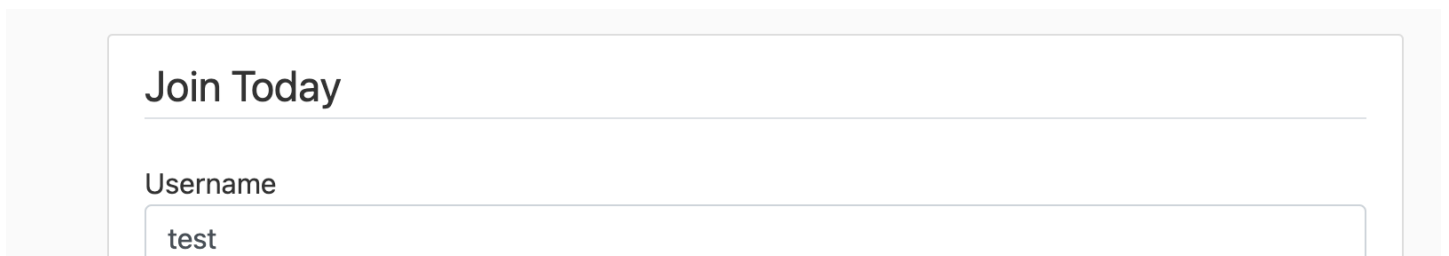
考点:

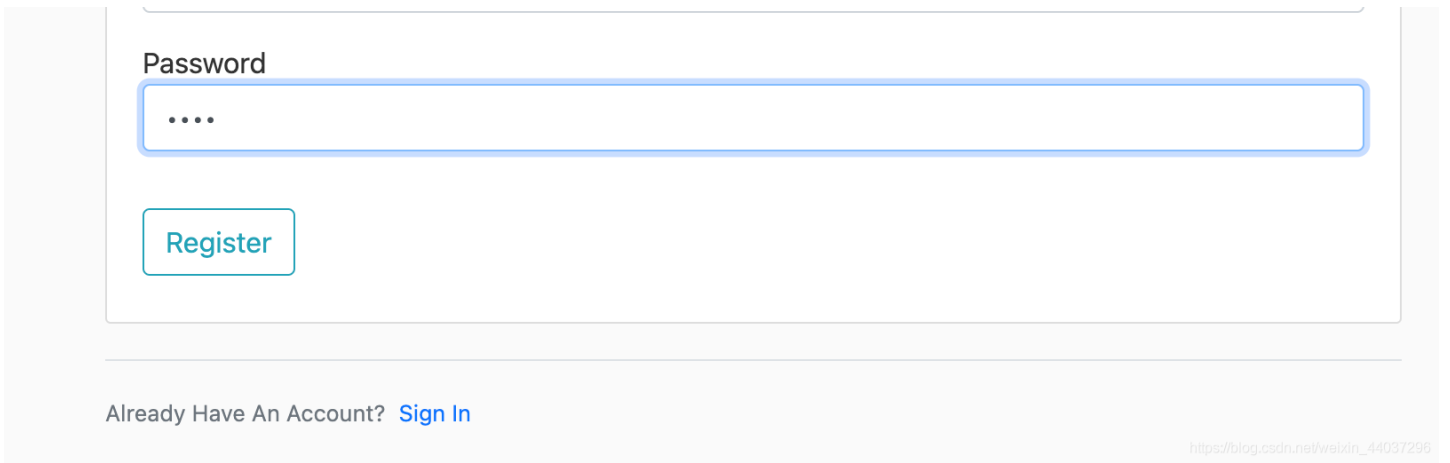
1. **JWT**编码解码
2. 伪造**session**

启动环境:



提示登录查看内容, 首先注册并登陆:





登陆成功后可以上传文件，并提示最大为 **1M**：



尝试传入一句话木马等内容：

## Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

https://img.cdn.net/waixin\_44037296

上传文件均显示服务器错误，可能不是文件上传漏洞，再次收集信息：  
发现网站存在 **robots.txt**：

```
User-agent: *  
Disallow: /static/secretkey.txt
```

访问得到：

```
you-will-never-guess
```

给出了SECRET\_KEY的值，猜测为session伪造，查看session:

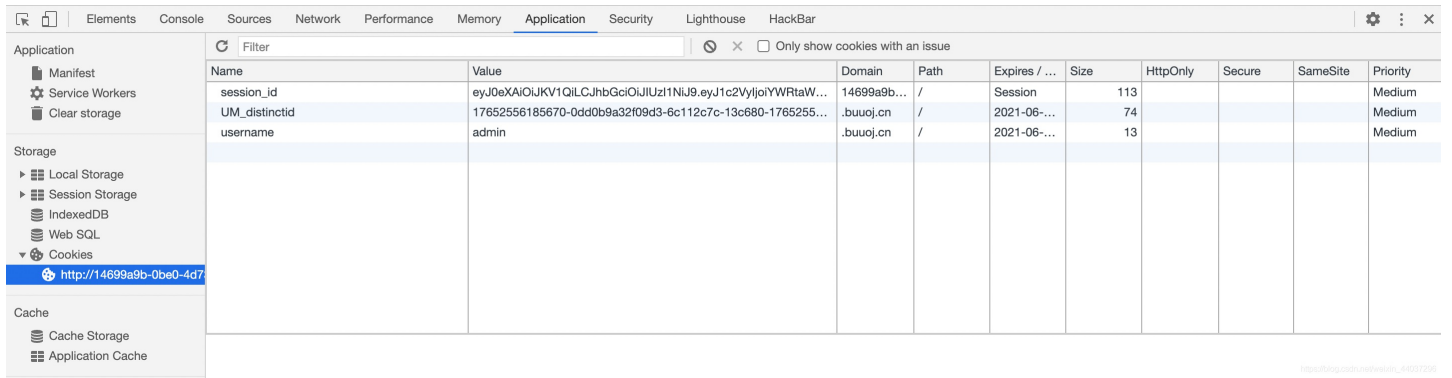
Name	Headers	Preview	Response	Initiator	Timing	Cookies
2b90a6b9-e3bc-4b5f-ac16-5...	vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9					
main.css	<b>Accept-Encoding:</b> gzip, deflate					
bootstrap.min.css	<b>Accept-Language:</b> zh-CN,zh;q=0.9					
data:image/svg+xml;...	<b>Cache-Control:</b> max-age=0					
	<b>Connection:</b> keep-alive					
	<b>Cookie:</b> username=admin; UM_distinctid=17652556185670-0dd0b9a32f09d3-6c112c7c-13c680-176525561861469; session_id=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaGVhZCJ9.bDVu04cvIiwibY7K0ZoqzvPiIL2CKyF4loApBGUCf1Fo					
	<b>Host:</b> 2b90a6b9-e3bc-4b5f-ac16-5eccb5019bc5.node3.buuoj.cn					
	<b>Referer:</b> http://2b90a6b9-e3bc-4b5f-ac16-5eccb5019bc5.node3.buuoj.cn/login					
	<b>Upgrade-Insecure-Requests:</b> 1					
	<b>User-Agent:</b> Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36					
4 requests	3.2 kB transferred					<a href="https://blog.csdn.net/weixin_44037296">https://blog.csdn.net/weixin_44037296</a>

发现Cookie中存在 username=admin，并且其存在session，尝试构造 admin 的session

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaGVhZCJ9.bDVu04cvIiwibY7K0ZoqzvPiIL2CKyF4loApBGUCf1Fo
```

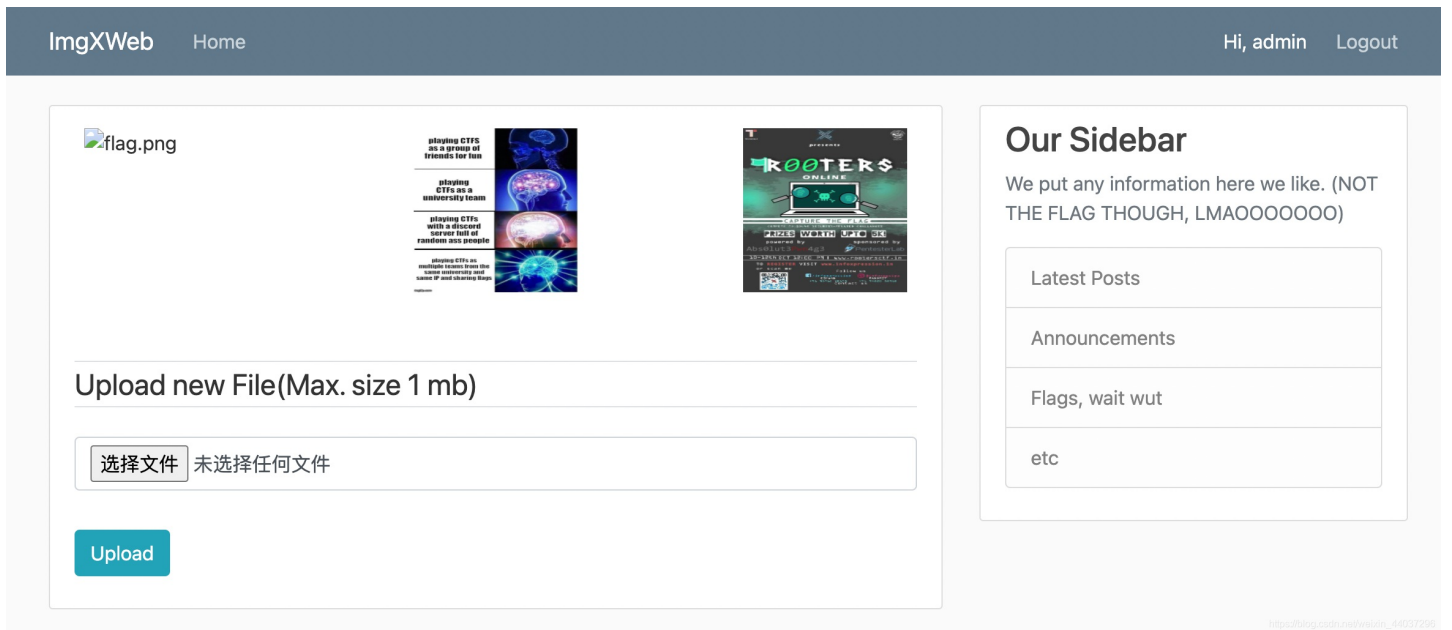


使用F12中的Application修改session的值:



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Priority
session_id	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VYljoIYWRtaW...	14699a9b...	/	Session	113				Medium
UM_distinctid	17652556185670-0dd0b9a32f09d3-6c112c7c-13c680-1765255...	.buuoj.cn	/	2021-06-...	74				Medium
username	admin	.buuoj.cn	/	2021-06-...	13				Medium

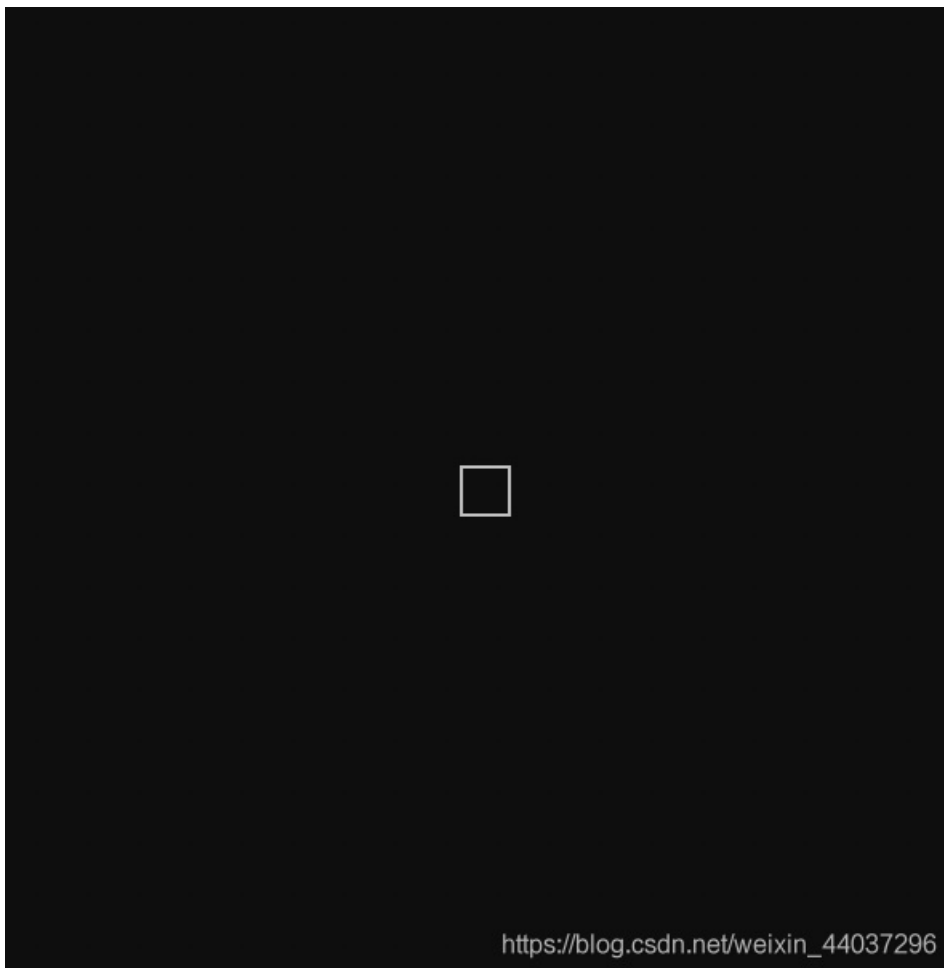
刷新页面后, 成功以 `admin` 用户身份登陆:



其中有一个: `flag.png` :

```

```



[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

新标签页访问：  
查看源码得到flag:

← → ↻ ⚠ 不安全 | view-source:14699a9b-0be0

```
1 flag{ddc0ddfa-58d8-43f1-83ff-744827e293ce}  
2
```