

Ctfhub解题 彩蛋

原创

一个平凡de人  于 2021-03-21 22:59:04 发布  925  收藏 1

分类专栏: [《从0到1: CTFer成长之路》](#)

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_46703850/article/details/115057546

版权



[《从0到1: CTFer成长之路》](#) 专栏收录该内容

39 篇文章 20 订阅

订阅专栏

Ctfhub解题 彩蛋

1. 首页
2. 公众号
3. 题目入口
4. Writeup
5. 工具
6. 赛事
7. 真题
8. 投稿提交

介绍: 记录解题过程

1. 首页

听说在首页的某个地方隐藏了一个flag, 可能在*.ctfhub.com中, 不妨先找到flag再来开题

1. 访问并查看源码

```
view-source:https://api.ctfhub.com/#/index
```

```
<div id="container">
  <h1>Welcome to CTFHub!</h1>

  <div id="body">
    <p>CTFHub 是一个CTF爱好者的聚集地，提供题目练习，赛事跟踪等服务</p>
    <code style="color: #f9f9f9;">You found it, give your's FLAG: </br>ctfhub{c18732f48a96c40d40a06e74b1305706}</code>
  </div>

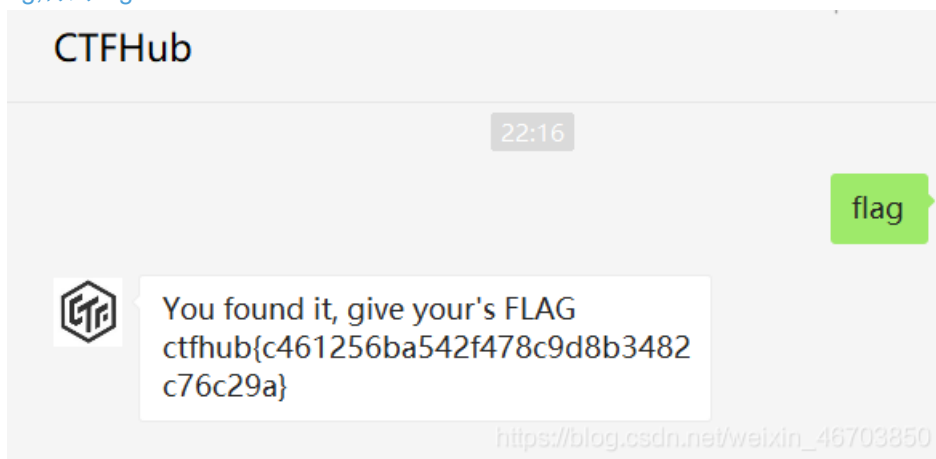
  <p class="footer">Page rendered in <strong>0.0013</strong> seconds.</p>
</div>

</body>
</html>
```

2. 公众号

在CTFHub微信公众号上签到可获得更多金币。听说在微信公众号上也有个彩蛋，去看看吧

1. 关注公众号，回复flag,得到flag



3. 题目入口

在某个题目的入口上也有一个哦

做题时缘分相遇

请求

名称	值
POST	/flag.php HTTP/1.1
主机	127.0.0.1:80
Content-Length	36
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1
Origin	http://challenge-94eba7626772d638.sandbox.ctfhub.com:10080
Content-Type	application/x-www-form-urlencoded
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Referer	http://challenge-94eba7626772d638.sandbox.ctfhub.com:10080/
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.9
Connection	关闭

1 key=868458d11163852eddbbc4ec345aeb24

响应

```
31  止住勿钢化
32  </strong>
33  , 请稍等片刻即可访问
34  </div>
35  <div class="alert alert-warning">
36  环境<strong>
37  已到期
38  </strong>
39  , 当前环境将保留5分钟, 请尽快续期即可恢复访问
40  </div>
41  <div class="alert alert-danger">
42  环境<strong>
43  已销毁
44  </strong>
45  , 请重新开启题目环境
46  </div>
47  <span style="color:#e9ecef">You found it, give your's FLAG:
48  ctfhub{b644d27a30b450b2f170c4f19ef1dd85fb1efc5d}</span>
49  </div>
50  </div>
51  </body>
52  </html>
```

大家的flag应该都一样吧,试试我的

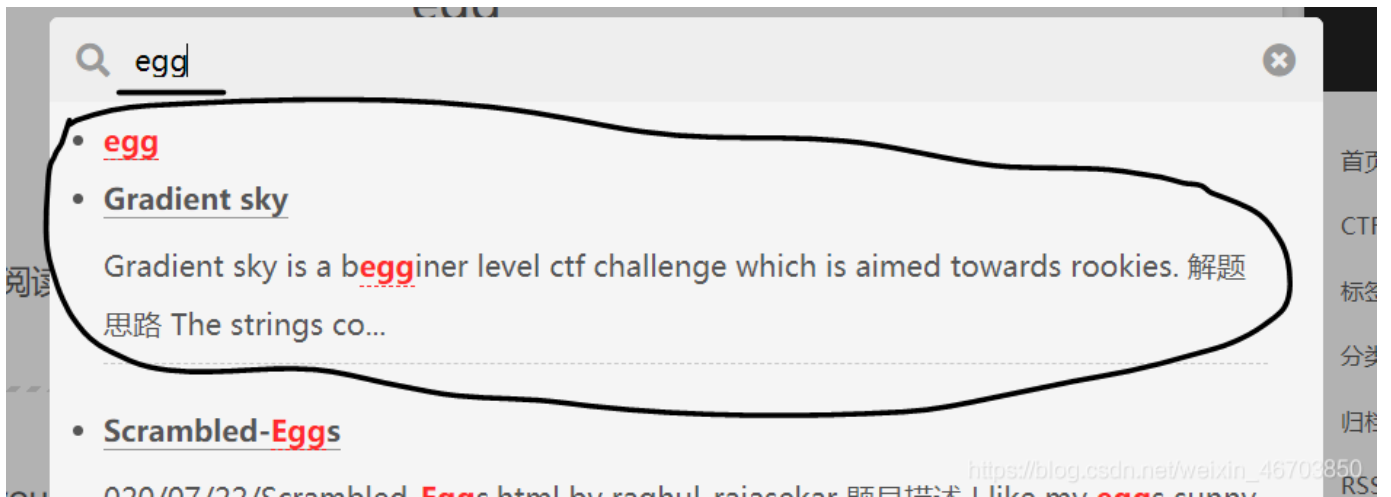


```
ctfhub{b644d27a30b450b2f170c4f19ef1dd85fb1efc5d}
```

4. Writeup

writeup中也隐藏了一个呢

1. writeup中搜索egg（彩蛋）



2. 点入得到flag

You found it, give your's FLAG

FLAG

```
1 ctfhub{0936de34af2a6dd91fbd88fead25fc877c8a4b1b}
```

本文作者: CTFHub

https://blog.csdn.net/weixin_46703850

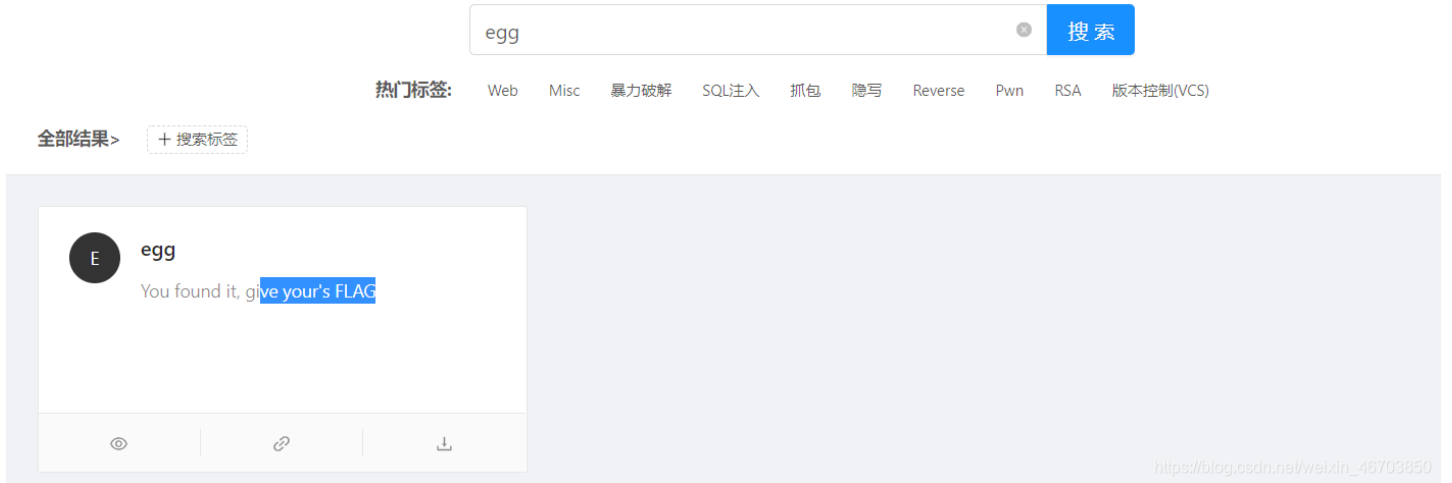
```
ctfhub{0936de34af2a6dd91fbd88fead25fc877c8a4b1b}
```

5.工具

工具中也隐藏了一个，不妨翻一翻？

1.工具中搜索egg（彩蛋）

工具



2. 复制链接地址



3. 粘贴即可得到flag

<https://www.ctfhub.com/#/ctfhub{19d9098bcd2d4e77e2c60425b3d6abf63cd0744f}>

6. 赛事

赛事中貌似也有哎

1. 赛事中搜索egg（彩蛋）,得到flag

赛事名称: 比赛形式: 比赛类型:

E egg
开始时间: 2000-02-01 00:00:00 结束时间: 2000-02-01 00:00:00

比赛形式: 线上
比赛类型: Jeopardy[解题]
比赛官网: ctfhub{70e2bc7fde5462dd49b8242a7dde88d953a858f5}

https://blog.csdn.net/weixin_46703850

7.真题

最后。来寻找隐藏在真题中的彩蛋

1. 真题中搜索egg（彩蛋）,得到flag

热门标签: Web Misc 网鼎杯 Reverse Pwn Crypto SQL注入 赛客夏令营 SSTI 2018

☆☆☆

6 12
Eggs

E egg ☆ 0 0
You found it, give your's FLAG:
ctfhub{e8c897ac0fd3b8b8771bcc84e79117e7}

https://blog.csdn.net/weixin_46703850

ctfhub{e8c897ac0fd3b8b8771bcc84e79117e7}

8.投稿提交

这次的彩蛋被不知名势力无情地打碎成好几块，现在只找到一块flag[0:6] = ctfhub，据说剩下的藏在了WP投稿和题目提交说明这里，不知名势力还留下了一句话：阅读的足够仔细就可以找到 Hint: WP投稿和提交说明在网站下方

1. 随便找个

ohhhh, 这个题还没有WriteUp, 骚年要不要来一份? [点我提交](#)

2. 最下方

隐藏的信息

```
1 flag[6:12] = "{029e0"
```

本文作者: CTFHub

https://blog.csdn.net/weixin_46703850

```
flag[6:12] = "{029e0"
```

3. Demo

模板及Demo

[下载模板](#) | [下载Demo](#)

4. file/egg_flag.txt里面:

```
flag[42:48] = aes_256_ecb_decode("c6e1d72b1102f9b96b20c1f00cc7a178d5b3f99193faaa60e53b45b9e644d782", key)
```

List item