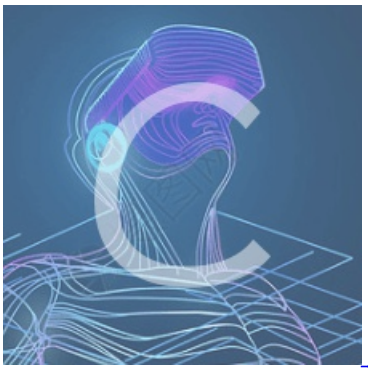
Ctfhub 彩蛋

原创

crazy0xf5 于 2021-05-29 10:42:32 发布 192 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_40470232/article/details/117378720



01 首页

首页

所需金币：30　　题目状态：已解出　　解题奖励：金币:150 经验:10

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

暂无数据

域名： ctfhub.com 开始

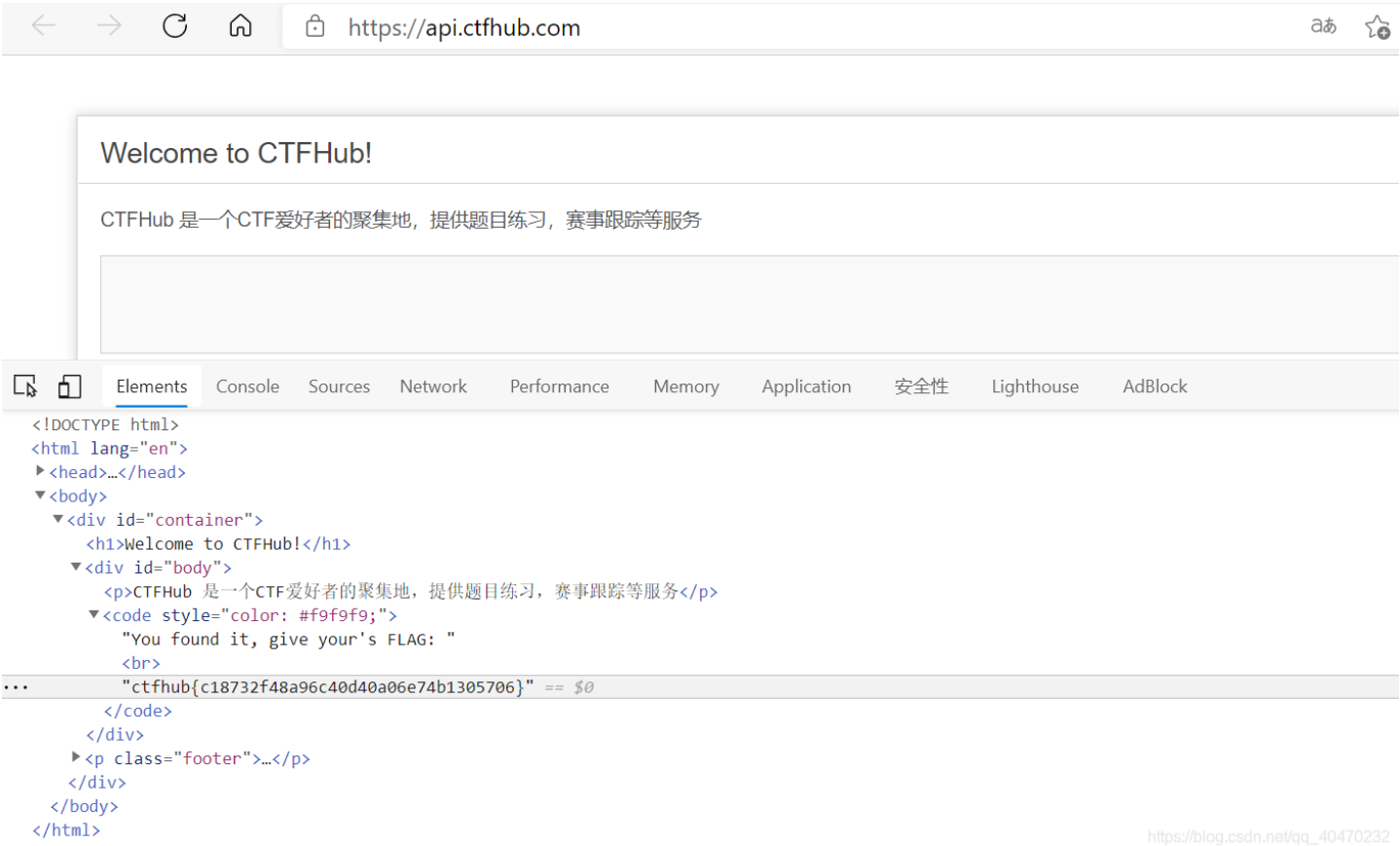
171.ctfhub.com

查询成功：www.ctfhub.com-27.152.185.98

查询成功：admin.ctfhub.com-30.0.10.101

查询成功：email.ctfhub.com-119.147.4.33

查询成功：api.ctfhub.com-47.114.158.30
查询成功：static.ctfhub.com-27.152.185.99
查询成功：proxy.ctfhub.com-47.98.148.7
查询成功：ldap.ctfhub.com-30.0.10.11
查询成功：git.ctfhub.com-30.0.10.12
查询成功：jenkins.ctfhub.com-30.0.10.13



---

02 公众号

此题关注公众号即可获取flag

此题只在云服务器即可抓取flag

---

03 题目入口
随便开启一个题目，抓包

`flag:ctfhub{b644d27a30b450b2f170c4f19ef1dd85fb1efc5d}`

---

03 Writeup
在Writeup里搜索egg即可拿到flag

egg

发表于 2021-01-03 | 分类于 Skill

Skill | egg

点击此处获得更好的阅读体验

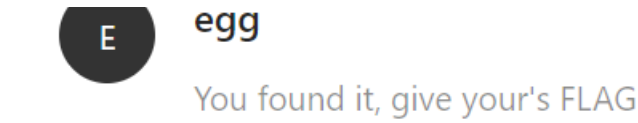
You found it, give your's FLAG

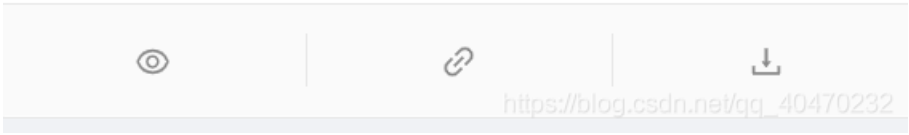
FLAG

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

---

04 工具
在工具里搜索egg即可拿到flag





复制链接即可获取flag

```
ctfhub{19d9098bcd2d4e77e2c60425b3d6abf63cd0744f}
```

---

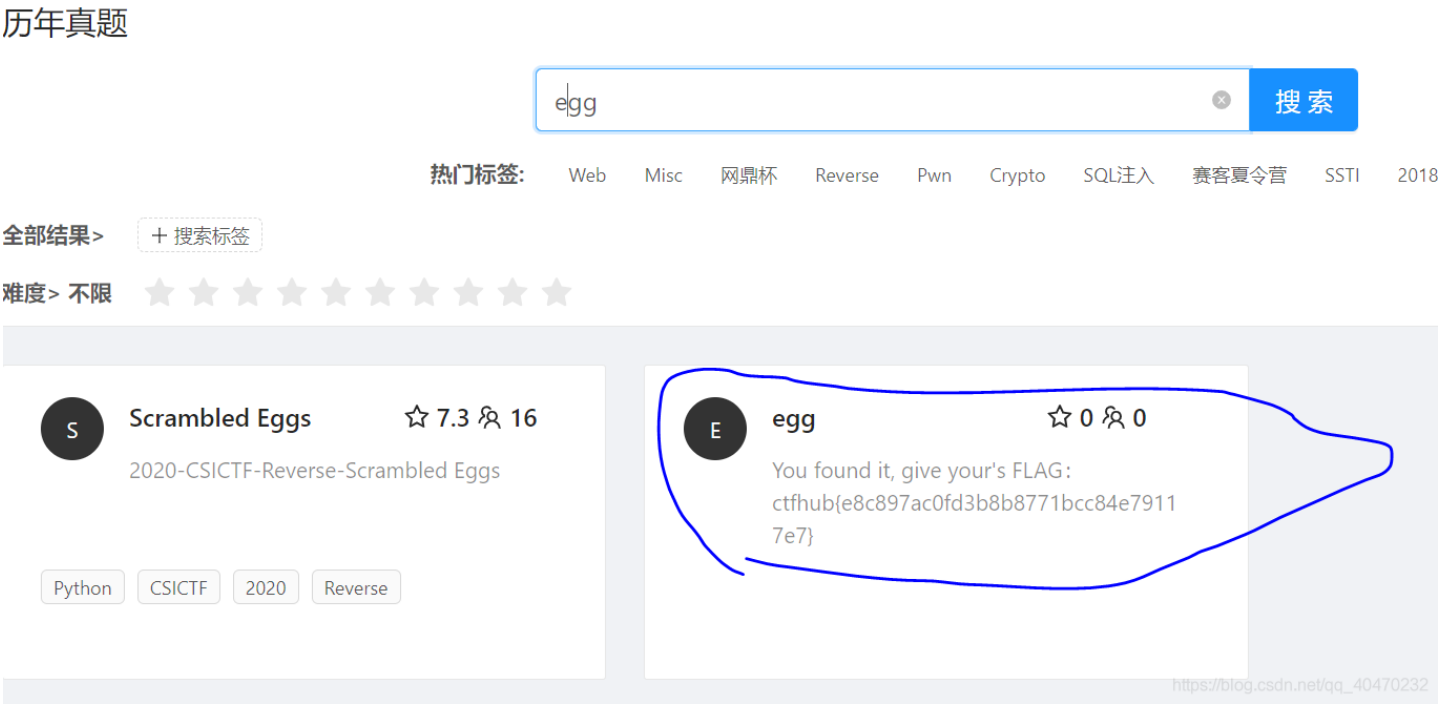
05 赛事

在赛事中搜索egg即可获取flag


```
ctfhub{70e2bc7fde5462dd49b8242a7dde88d953a858f5}
```

06 真题

在真题中搜索egg即可获取flag



`ctfhub{e8c897ac0fd3b8b8771bcc84e79117e7}`

07 投稿提交

这道题比较有意思，flag分别在不同的位置

flag[6:12]在Writeup投稿说明下方的隐藏信息中

隐藏的信息

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


flag[12:18]在题目环境提交说明下方的隐藏信息中

隐藏的信息

```
1  flag[12:18] = "2eb3a1"
```


在Writeup投稿说明页面源代码中，有一串加密字符，解码后为flag[18:24] `base64编码`

```
<p><span style="color: #fff;">ZmxhZyU1QjE4JTNBMjQlNUQlMjAlMOQlMjAlMjJlOGM0OWIlMjI=</span></p>
<h2 id="投稿奖励">投稿奖励</h2>
<ul>
<li>投稿原则上以先来后到为准，即先投稿的先审核先上线，如在审核期间有多份投稿，则使用最优质的投稿，其他则拒收</li>
<li>投稿原则上仅接受平台已有题目，若平台还没有该题目可同时提交对应环境和WP，同时提交可获得额外<code>100</code>金币奖励<br>
具体请参照<a href="https://writeup.ctfhub.com/Other/提交说明/d7098951.html">题目环境提交说明</a></li>
<li>投稿允许转载。但请先取得文章作者的许可。平台上线时将会保留转载来源</li>
<li>投稿原则上仅接受平台不存在的WP，若平台已存在相同思路的WP会被拒收<br>
除非投稿的WP比平台上现有的更详细更深入会酌情考虑是否接收</li>
<li>若同一个题目在平台上已有WP但是用另外的思路解出，视为一篇新的WP，按照新WP的标准执行</li>
```


请将要加密或解密的内容复制到以下区域

```
flag[18:24] = "e8c49b"
```

BASE64加密　BASE64解密

在题目环境提交说明页面源代码中，有一串加密字符，解码后为flag[24:30] hex编码

```
<p><span style="color: #fff;">666c61675b32343a33305d203d202231313332623522</span></p>
<h2 id="提交奖励">提交奖励</h2>
<ul>
<li>提交原则上以先来后到为准，即先提交的先审核先上线，如在审核期间有多份相同题目提交，则使用最优质的提交，其他则拒收<br>
</li>
<li>允许提交其他比赛的题目，但请先取得原作者的许可<br>
提交至平台即视为<code>已取得原作者许可</code>，如后期产生纠纷CTFHub<code>不承担任何责任</code><br>
</li>
```

flag[24:30] = "1132b5"

UTF-8 GB2312 编码 解码

在Writeup投稿说明页面的图片中隐写了flag[30:36]

使用winhex打开图片，在图片最后发现flag

```
0000000000003B70  2D E7 E8 CE EF 01 7A 92  18 C0 88 77 1D 7A B2 8D  -.........w.z..
0000000000003B80  1A 45 15 98 0B 7A 94 B2  37 2C DE 84 39 9A 73 09  .E...z..7,9·∞.s.
0000000000003B90  6A F7 C5 F2 D3 1E 44 44  44 44 44 44 44 44 44 44  j.....DDDDDDDDDD
0000000000003BA0  44 44 44 44 44 44 8F F4  07 0F FD 74 92 1A 7D 3E  DDDDDD.....t..}>
0000000000003BB0  AD 00 00 00 00 49 45 4E  44 AE 42 60 82 66 6C 61  .....IEND.B`.fla
0000000000003BC0  67 5B 33 30 3A 33 36 5D  20 3D 20 22 31 35 62 36  g[30:36]·=·"15b6
0000000000003BD0  35 32 22                                        52"·····
```

同样的套路在题目环境提交说明页面的图片中隐写了flag[36:42]

```
0000000000003C90  80 54 00 52 01 48 05 20  15 00 A4 02 90 0A 40 2A  .T.R.H.·......@*
0000000000003CA0  00 A9 00 A4 02 90 0A 40  2A 00 48 05 20 15 80 54  .......@*.H.·..T
0000000000003CB0  00 52 01 48 05 20 15 80  54 00 90 0A 40 2A 00 A9  .R.H.·..T...@*..
0000000000003CC0  00 A4 02 90 0A 40 2A 00  A9 00 20 15 80 54 00 52  .....@*...·..T.R
0000000000003CD0  01 FE 6D 9F 8E 69 00 00  00 18 06 F9 77 BD A4 FF  ..m..i......w...
0000000000003CE0  1C 80 07 54 01 55 40 15  50 05 C8 AB 32 79 DF B1  ...T.U@.P.õ·2y..
0000000000003CF0  57 9A 14 4D 87 00 00 00  00 49 45 4E 44 AE 42 60  W..M.....IEND.B`
0000000000003D00  82 66 6C 61 67 5B 33 36  3A 34 32 5D 20 3D 20 22  .flag[36:42]·=·"
0000000000003D10  61 35 66 33 61 38 22                            a5f3a8"·····
```

UNKNOWN 0000000000003D17: 0000000000003D17 (Synchronized with IDA View-A)

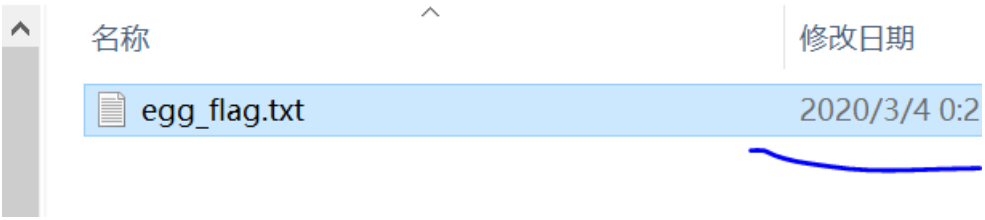
在Writeup投稿说明页面中有一个链接可以下载一个压缩包文件

模板及Demo

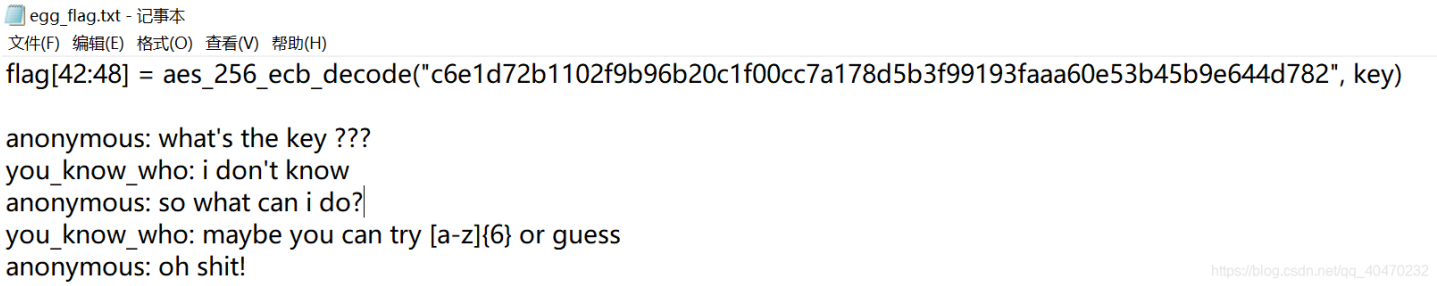
下载模板 | 下载Demo

在files文件夹中有一个egg_flag.txt

示例



里面打开内容是：



根据内容提示是AES加密 256位 而且密码是6位

```
flag[6:12] = "{029e0"
flag[12:18] = "2eb3a1"
flag[18:24] = "e8c49b"
falg[24:30] = "1132b5"
flag[30:36]= "15b652"
flag[36:42]= "a5f3a8"
flag[42:47] = "62013}"
ctfhub{029e02eb3a1e8c49b1132b515b652a5f3a862013}
```