

CTFHub 彩蛋

原创

CN天狼  已于 2022-02-15 18:26:50 修改  907  收藏

分类专栏: [CTF](#) 文章标签: [网络安全](#) [html5](#) [web安全](#) [安全](#)

于 2022-02-15 16:10:10 首次发布

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/qq_62414126/article/details/122946603

版权



[CTF 专栏收录该内容](#)

35 篇文章 0 订阅

订阅专栏

ctfhub彩蛋

[工具 彩蛋](#)

[首页 彩蛋](#)

[题目入口 彩蛋](#)

[公众号](#)

[投稿提交 彩蛋](#)

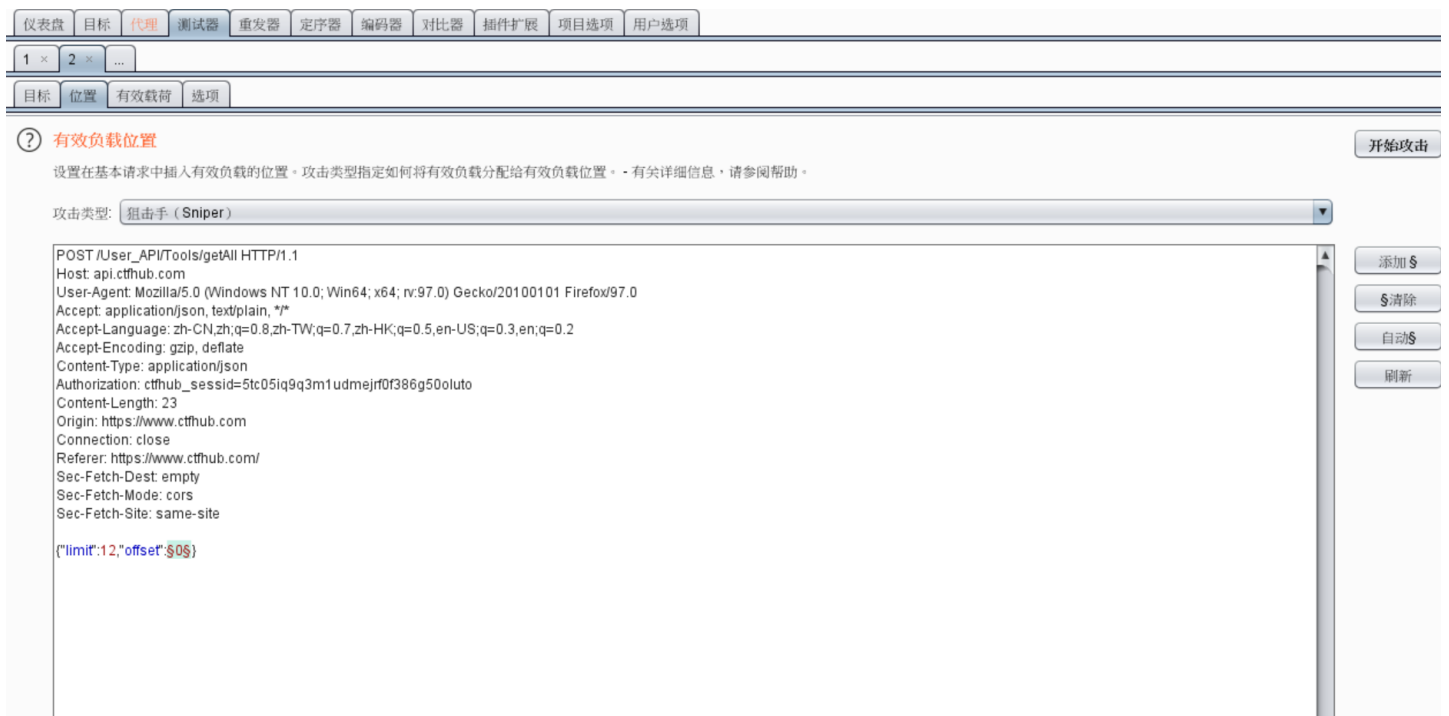
[其他彩蛋](#)

工具 彩蛋

一开始的想法是工具一共有8页, 想抓个包改下看看有没有第九页

抓包后发现不管哪一页limit都是12 但offset在变化

于是



The screenshot shows the Burp Suite interface. At the top, there are various tool tabs like '仪表盘', '目标', '代理', '测试器', etc. Below the tabs, there are buttons for '1 x', '2 x', and '...' indicating the number of requests. The main area shows a request details for '有效负载位置' (Effective Load Position). The request is a POST to '/User_API/Tools/getAll HTTP/1.1' with headers including Host, User-Agent, Accept, and Authorization. The body of the request is shown in a text area with the following payload: `{"limit":12,"offset":0}`. On the right side, there are buttons for '开始攻击', '添加 \$', '\$清除', '自动\$', and '刷新'.

这样设置参数

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

1 x 2 x ...

目标 位置 有效载荷 选项

有效载荷集 开始攻击

您可以定义一个或多个有效载荷集。有效载荷集的数量取决于“位置”选项卡中定义的攻击类型。每个有效载荷集可以使用各种有效载荷类型，并且可以以各种方式定制每种有效载荷类型。

有效载荷集： 1 有效载荷数量： 101

有效载荷类型： 数值 请求数量： 101

有效载荷选项[数字]

生成给定范围内指定格式的数字有效内容。

数字范围

类型：
 连番 随机

From: 0

To: 100

增量： 1

编号：

数字格式

基地：
 Decimal 十六进制

CSDN @CN天狼

在长度为1000到6、7千左右随便一个双击后 **点击响应** 看**响应包**

Result 88 | Intruder attack 1

Payload: 87
 Status: 200
 Length: 1802
 Timer: 109

请求 响应

原始 头 十六进制

```
[{"status":true,"msg":"u83b7u53d6u6210u529f","data":{"items":{"category":{"href":"40665","id":1,"title":"Web"},"description":"Burp Suite u662u7528u4e8e9u653bu51fbwbu5e94u7528u7a0bu5e8u7684u96c6u6210u5e73u53f0u0fcu5305u542bu4e86u8bb8u591au5de5u5177u3002Burp Suiteu4e3au8f9u4e9bu5de5u5177u9bbeu8ba1u4e86u8bb8u591au83a5u53e3u0fcu4ee5u52a0u5feb1u653bu51fbu5e94u7528u7a0bu5e8u7684u96c6u6210u5e73u53f0u3002u5240u6709u5de5u5177u90fd1u5171u4eab1u4e00u4e2au5b7u5c42u0bcu5e76u90fd1u594u740bu59f9u5e94u7684HTTPu6d98u606fu3001u6301u4e45u6027u3001u8ba4u8bc1u3001u4ee3u7406u3001u65e5u5fd7u3001u8b66u62a5u3002","download_url":"https://portswigger.net/burp/","icon_url":"https://static.ctfhub.com/tools/icon/1_45c94eed2cae20557b54914017ba6d97af1373.png?1581281078","id":1,"intro_url":"","official_url":"https://portswigger.net/burp","title":"Burp Suite"},"category":{"href":"40665","id":1,"title":"Web"},"description":"You found it, give your's FLAG","download_url":"V#vcthub(19d9098bcd2d4e77e2c60425b3d6ab63cd0744f)","icon_url":"","id":1,"intro_url":"V#vcthub(19d9098bcd2d4e77e2c60425b3d6ab63cd0744f)","official_url":"V#vcthub(19d9098bcd2d4e77e2c60425b3d6ab63cd0744f)","title":"egg"},"total":89}]
```

没有匹配

简介 题目提交
 常见问题 WriteUp 投稿
 帮助文档 友情链接
 用户协议
 法律法规

Intruder attack 1

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器：显示所有项目

| 请求 | 有效载荷 | 状态 | 错误 | 超时 | 长度 | 评论 |
|-----|------|-----|----|----|------|----|
| 98 | 97 | 200 | | | 600 | |
| 99 | 98 | 200 | | | 600 | |
| 100 | 99 | 200 | | | 600 | |
| 101 | 100 | 200 | | | 600 | |
| 99 | 98 | 200 | | | 909 | |
| 88 | 87 | 200 | | | 1802 | |
| 87 | 86 | 200 | | | 2352 | |
| 86 | 85 | 200 | | | 3222 | |
| 85 | 84 | 200 | | | 3820 | |
| 84 | 83 | 200 | | | 4387 | |
| 83 | 82 | 200 | | | 5351 | |
| 82 | 81 | 200 | | | 5849 | |

请求 响应

原始 参数 头 十六进制

```
POST /User_API/Tools/getAll HTTP/1.1
Host: api.ctfhub.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20101010 Firefox/97.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: ctfhub_session=5tc05iq9q3m1udmejrf0f386g500uto
Content-Length: 24
Origin: https://www.ctfhub.com
Connection: close
Referer: https://www.ctfhub.com/
Sar-Fatrh.Daet-amnh
```

没有匹配

已变成

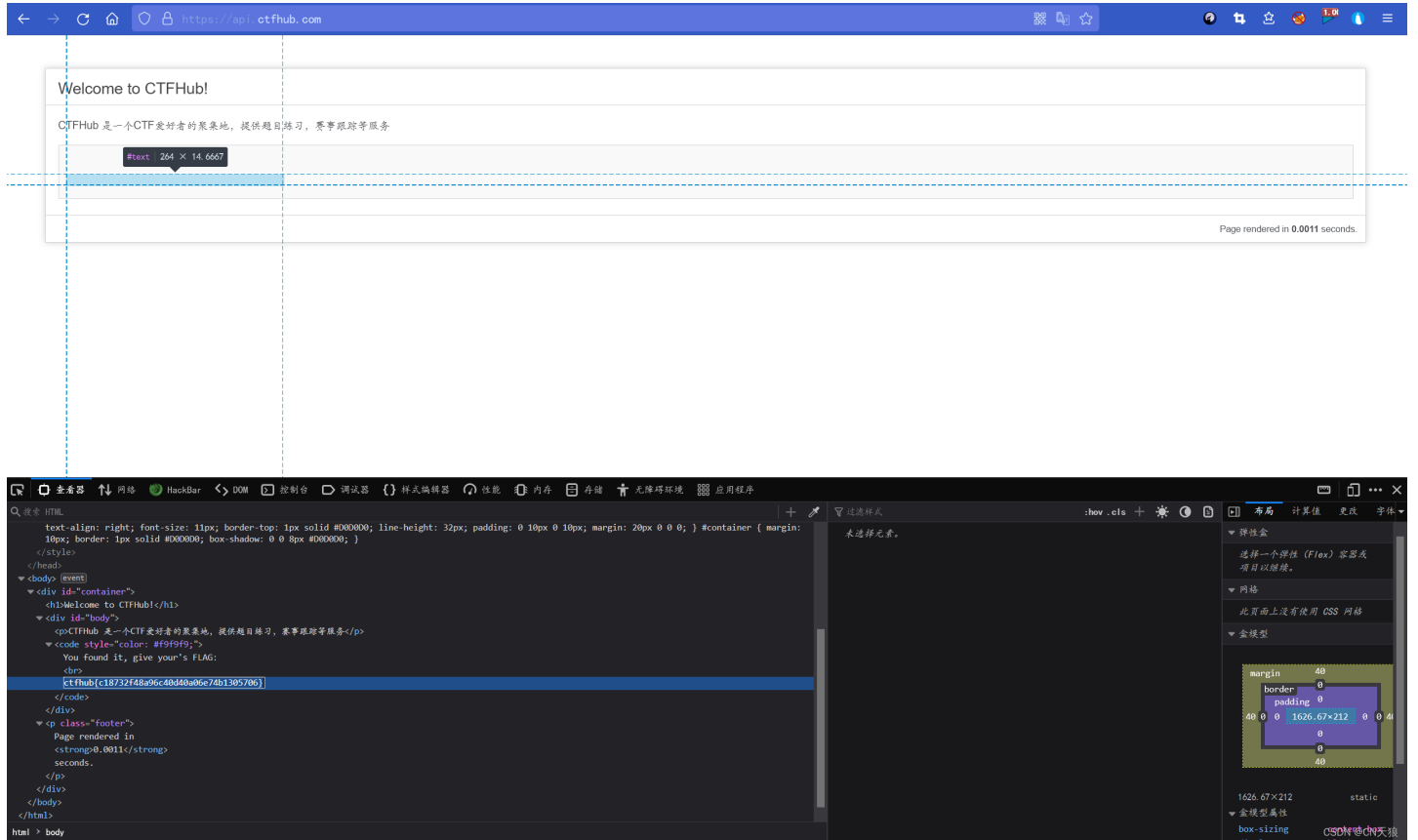
CSDN @CN天狼

在最后一行

首页 彩蛋

api中间框内隐藏着两行字

ctfhub{c18732f48a96c40d40a06e74b1305706}



题目入口 彩蛋

在web-ssrf中间那一列的某些题传参错误时会出现
详情见ctfhub-ssrfpost最后一行介绍

公众号

公众号彩蛋坑的一批！
首先要先绑定
然后点彩蛋
它提示要回复正确的关键词
我*#@%
我回复过

彩蛋 关键词 egg ctfhub CTFHub 拿来把你 CTFer 自己人

到底没想到竟然是flag

投稿提交 彩蛋

只找到了前半部分
分别在题目提交和wp提交页面的最后

```
ctfhub{029e02eb3a1
e8c49b1132b5
15b652a5f3a8
62013}
```

最后这个彩蛋剩余部分也没找到

网上搜了下才明白：感谢anweix的wp

第一行是俩页面的最后有

第二行是在俩页面源码 分别搜**奖励** 在上面那行一个是base64然后再转url 一个是hex解码

第三行是俩页面的图片隐写 丢进winhex

第四行有提示

aes 256 ecb**解码**

其他彩蛋

剩余皆可在对应页面搜索egg即可获得