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

ctfhub彩蛋

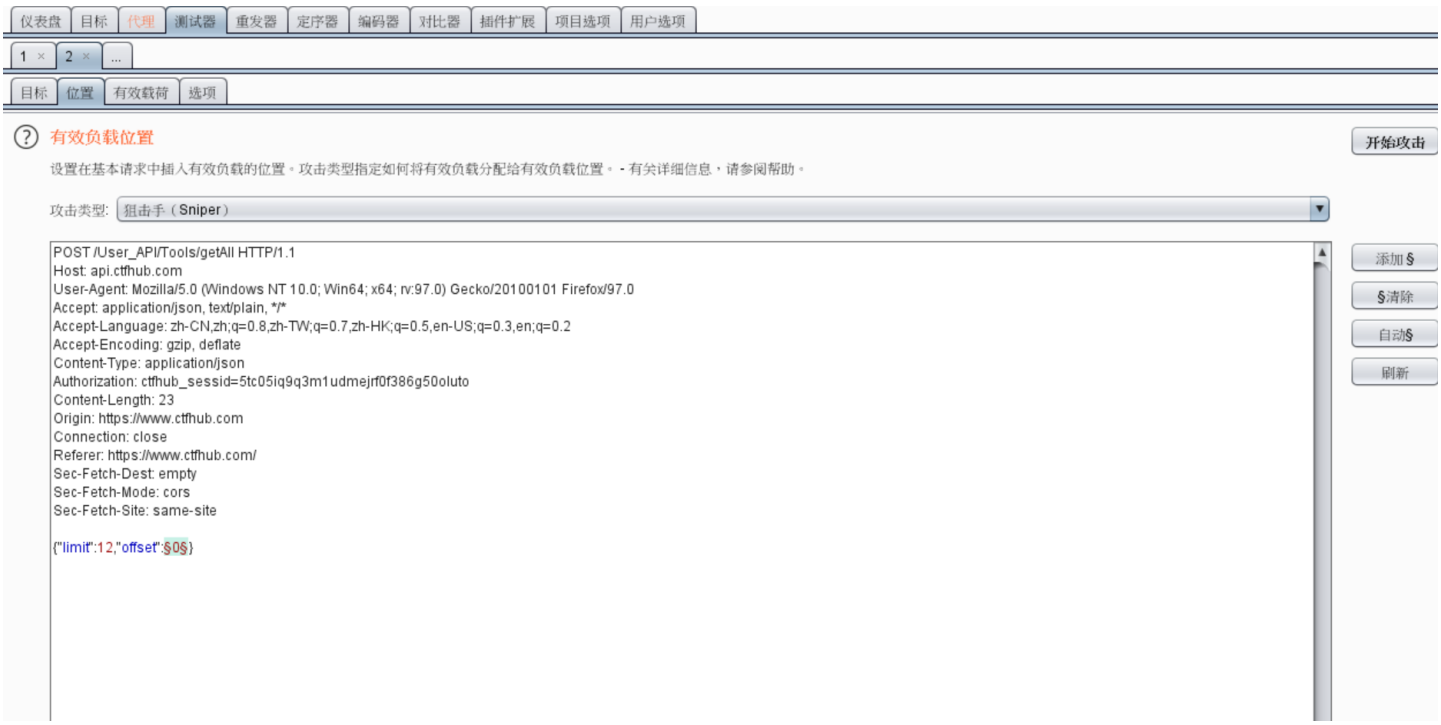
- 工具 彩蛋
- 首页 彩蛋
- 题目入口 彩蛋
- 公众号
- 投稿提交 彩蛋
- 其他彩蛋

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

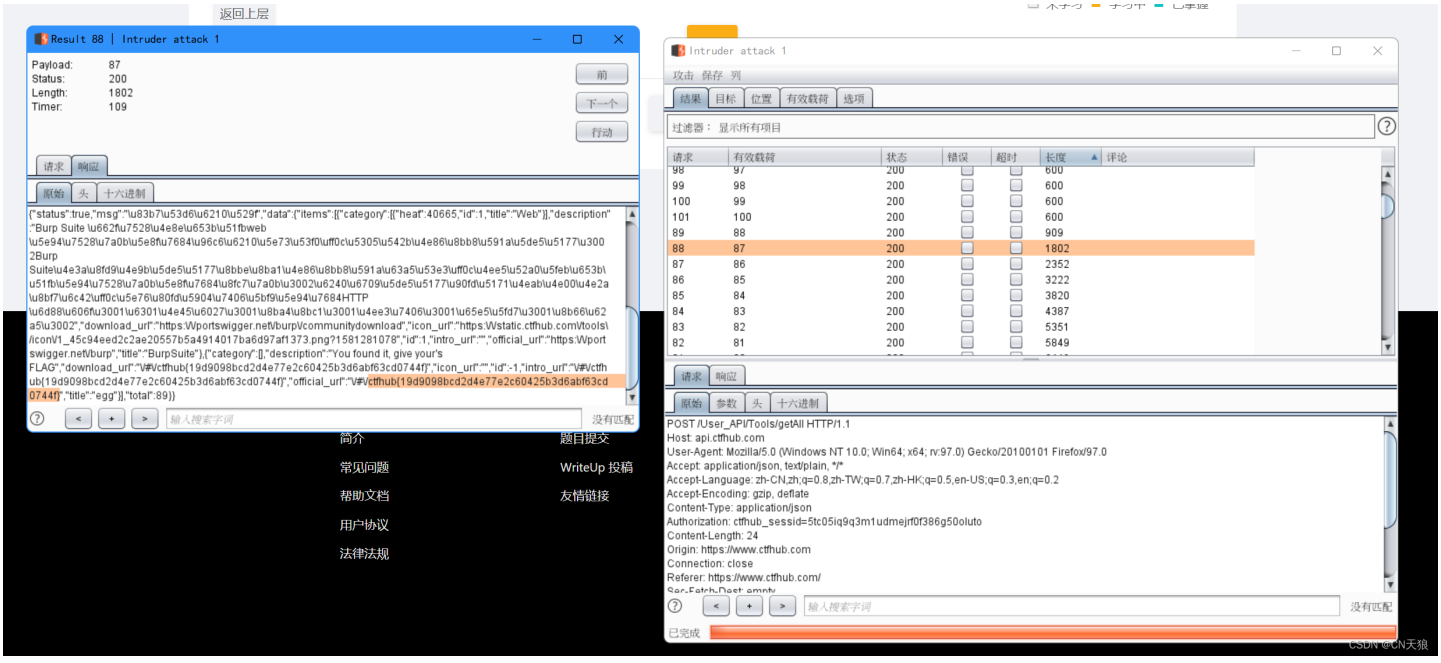
抓包后发现不管哪一页limit都是12 但offset在变化

于是



这样设置参数

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

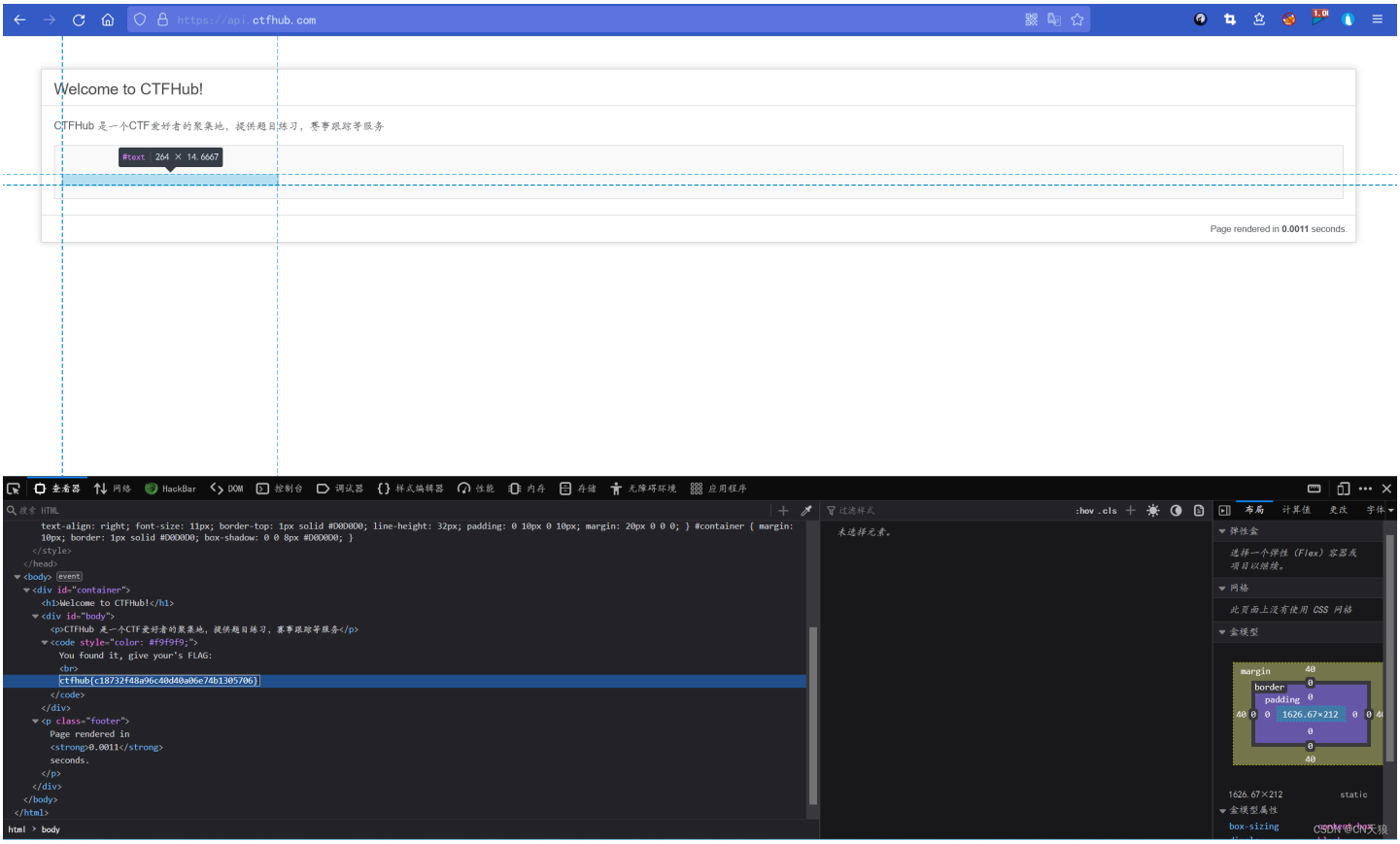


在最后一行

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anweilx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