CTFHUB-Http协议

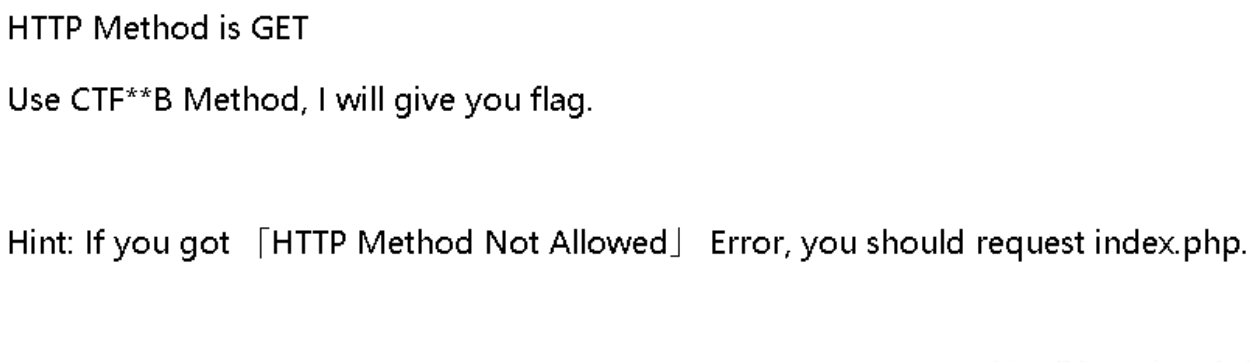
原创

熊是本熊 于 2021-03-11 20:27:06 发布 250 收藏

CTFHUB-请求方式

关于http请求的方法和其他知识就看这个链接：

1.HTTP Method 是可以自定义的，并且区分大小写，直接用 CTFHUB 方法请求 index.php 即可拿到 flag。



windows打开cmd输入：curl -v -X CTFHUB http://challenge-d2ecdef791f4e8ee.sandbox.ctfhub.com:10080/index.php就可以得到flag。
curl命令见：https://www.cnblogs.com/guixiaoming/p/8507268.html

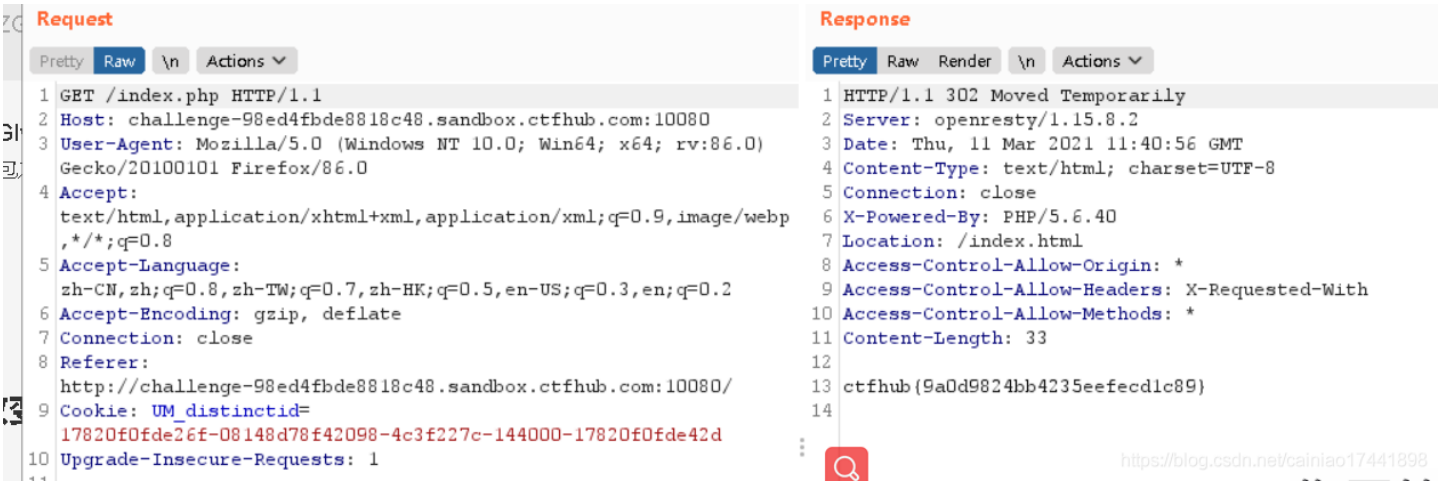
```
<
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8"/>
    <title>CTFHub HTTP Method</title>
</head>
<body>

good job! ctfhub{7e6976b81abc6c50b9b1f000}

</body>
</html>
* Connection #0 to host challenge-d2ecdef791f4e8ee.sandbox.ctfhub.com left intact
```


CTFHUB- 302跳转

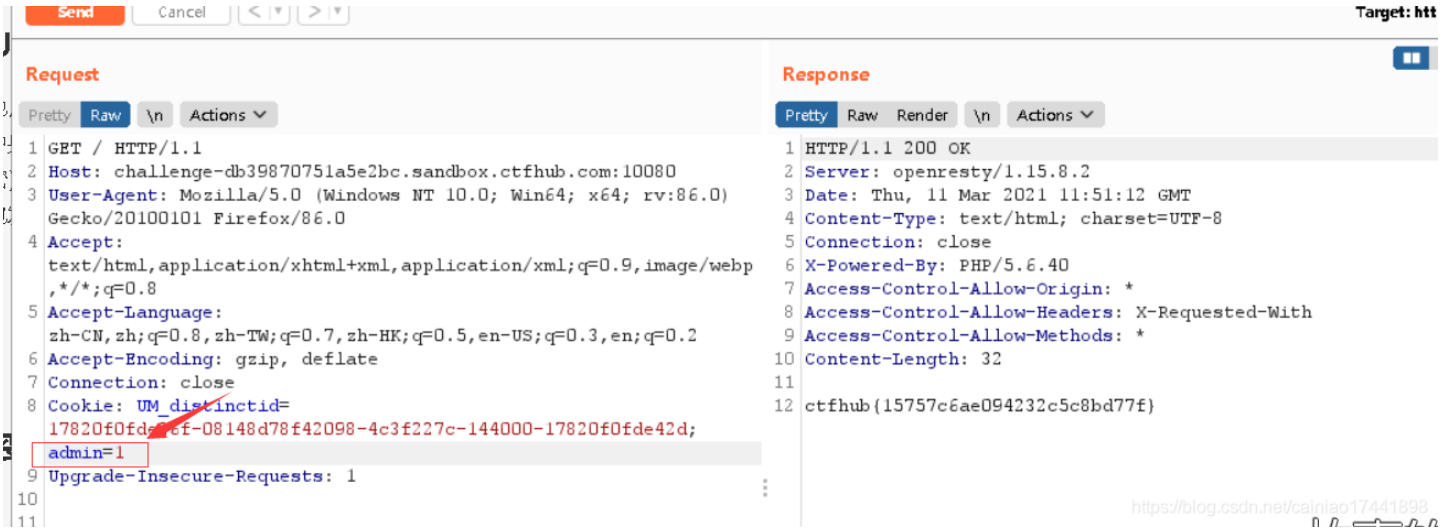
查看源码发下Give me flag重定向给了index.php
用burpsuite抓包之后发给repeater,就行了



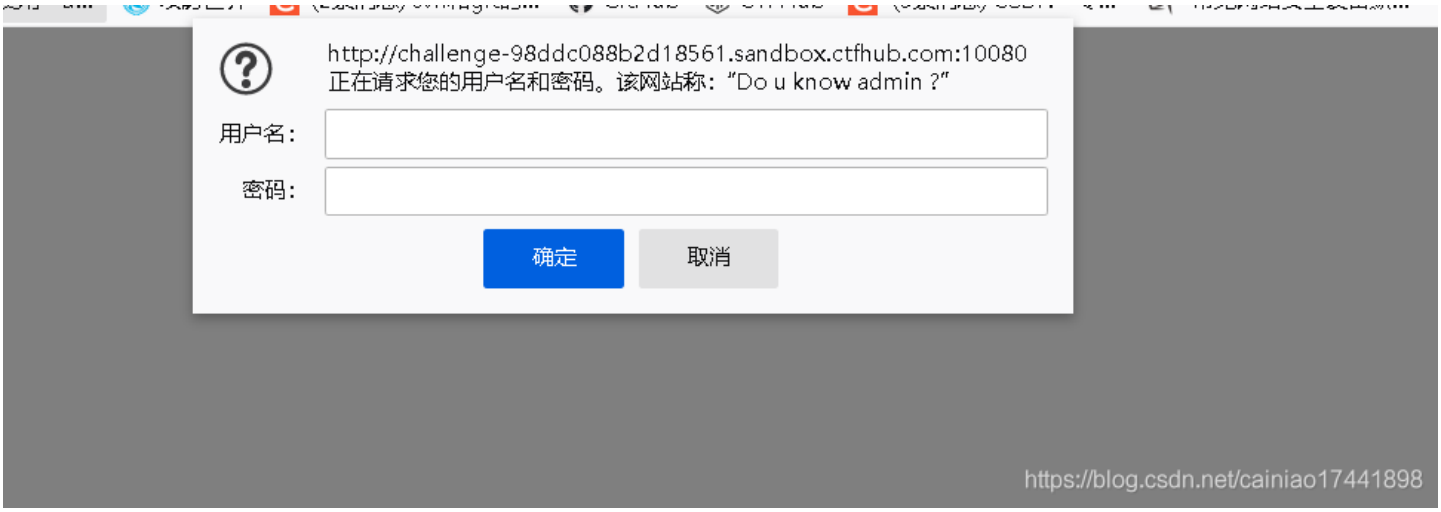
CTFHUB-Cookie

Cookie，有时也用其复数形式 Cookies。类型为“小型文本文件”，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息

用burpsuite抓包发给repeater，把admin=0改成admin=1



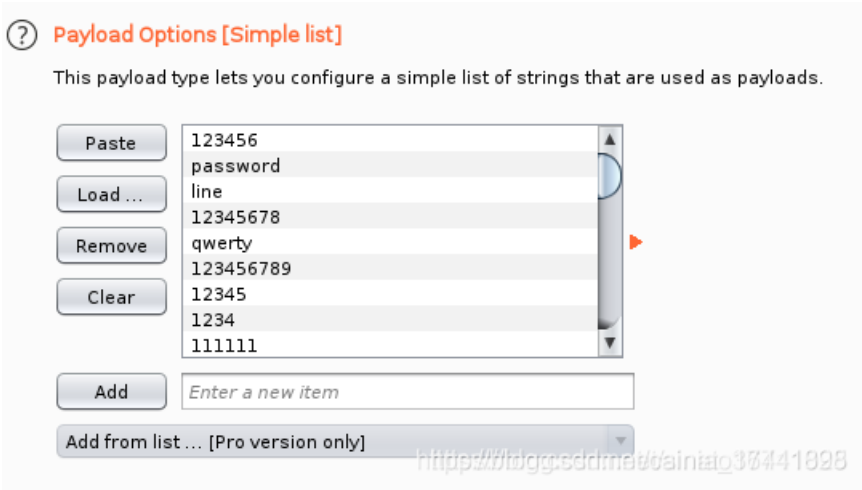
CTFHUB-基础认证

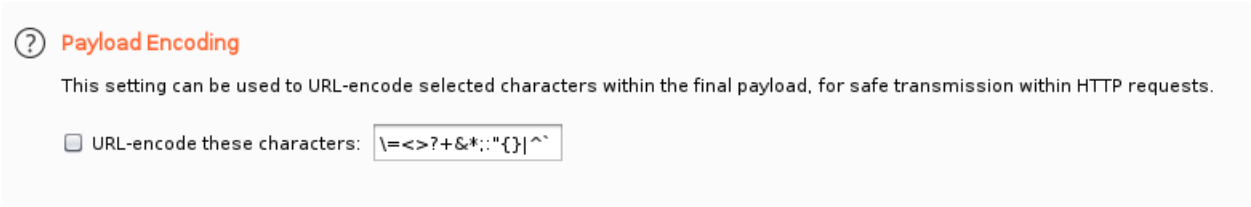


先随便猜一个密码，将其用burpsuit抓包之后发给intruder爆破。去掉那两个符号

改成这样

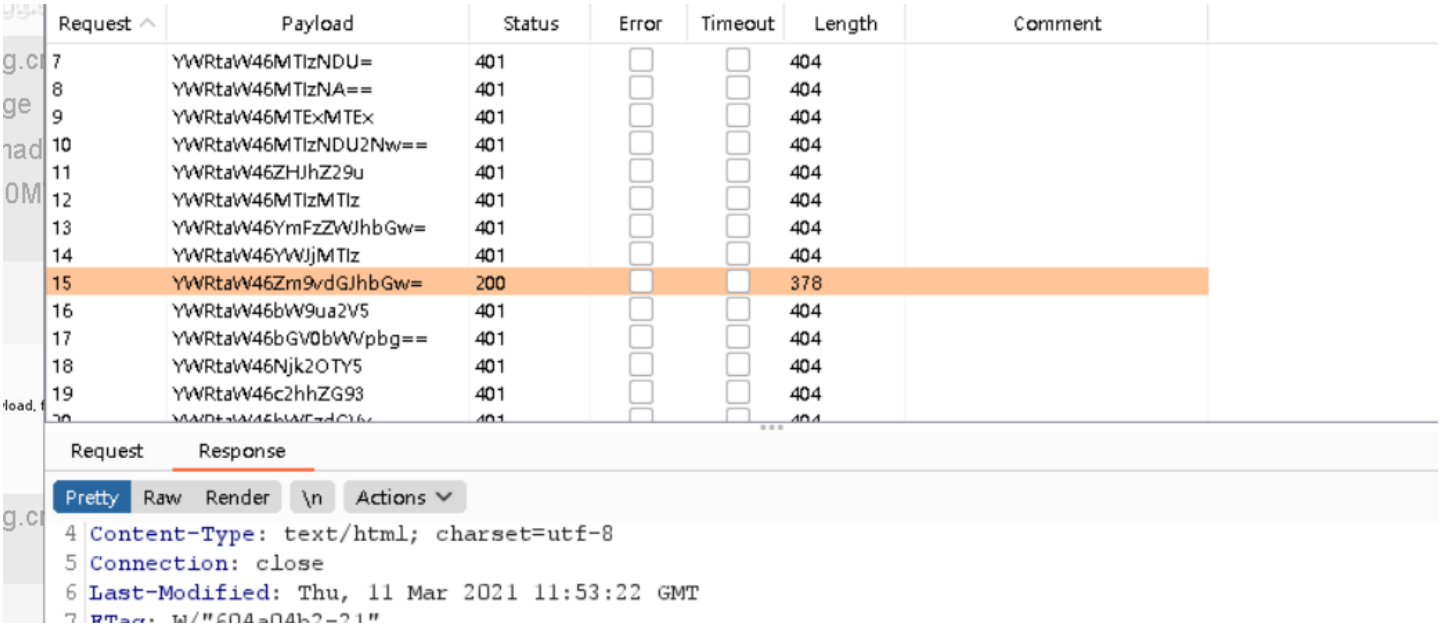
在 Payloads选项卡下，选择 Payload Type为SimpleList,然后在 Payload Options 中点击 load 加载密码字典

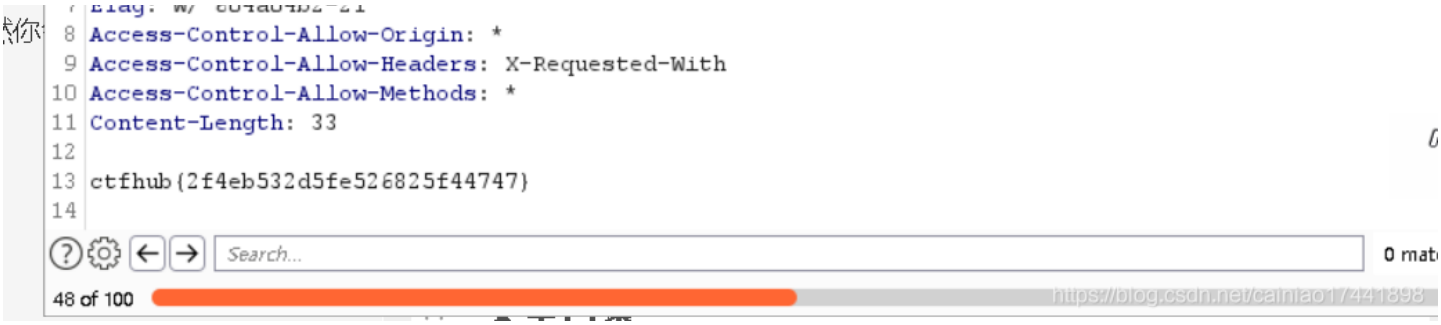




Payload Encode

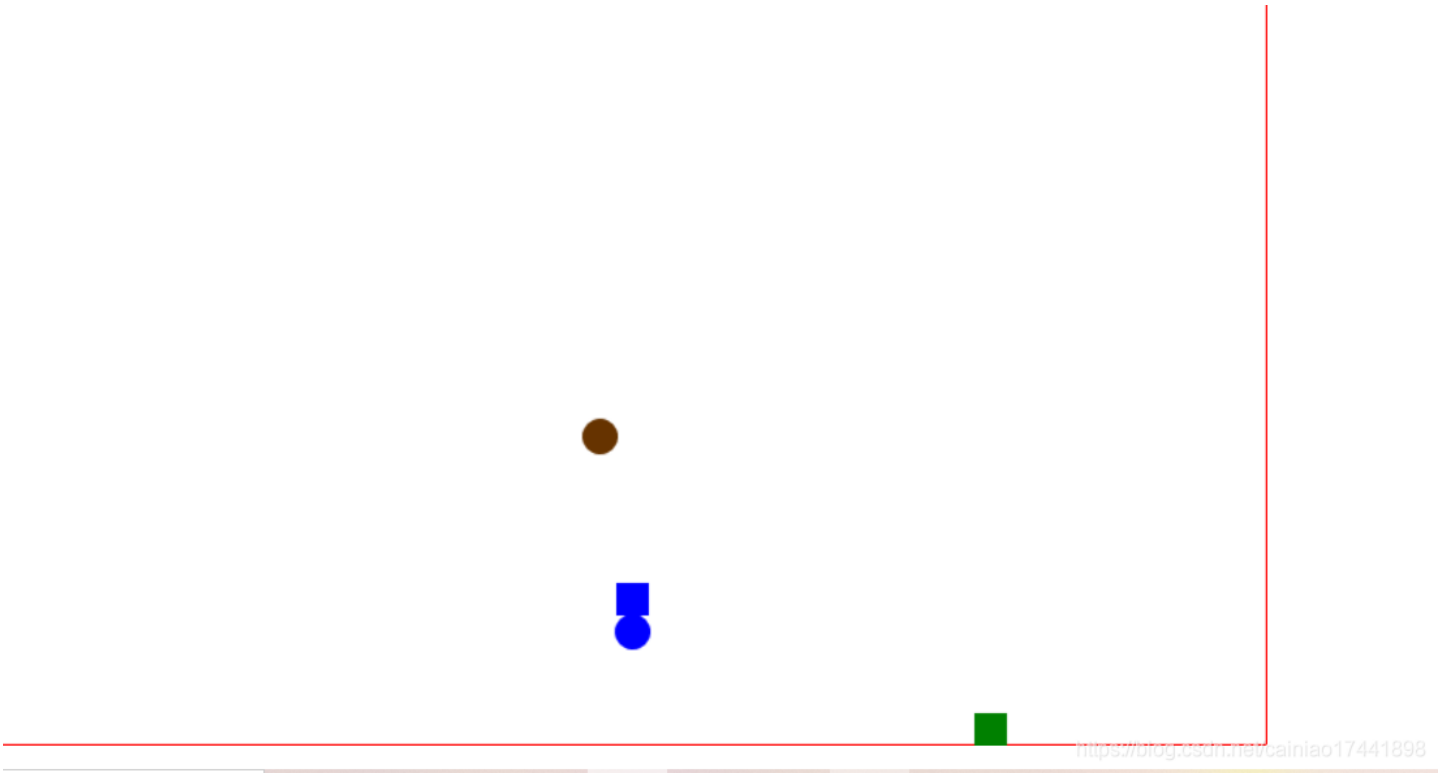
取消勾选的 URL-encode, 不然你会看到base64之后的=会被转成 %3d ， 就爆破不出来。





有个长度不一样的，查看response就有flag了。

CTFHUB-HTTP响应包源代码查看



flag就在源码里面。

```
    <canvas id="canvas" width="1000" height="700"></canvas>
    <div>
        <input id="switch" type="button" value="開始" onclick="clickSwitch()"></input><br/>
        <input id="content" type="text" value="0"></input>
    </div>
</body>
<!-- ctfhub{5e83369f0fc0bf6e36402904} -->
<script type="text/javascript">
    const WIDTH = 1000;
    const HEIGHT = 700;
    const SNACK_WIDTH = 20;
    const SNACK_HEIGHT = 20;
    //移动时间间隔
    const TIME_MOVE = 300;
    //食物刷新时间
    const TIME_FOOD = 5000;
    //食物总量
    const TOTAL_FOOD = 200;
    //石头刷新时间
    const TIME_STONE = 8000;
```

文章目录

总结

HTTP知识需要熟练。题还是比较简单的。