

Feeefan_W

菜的不能再菜的 vegetable 萌新

(Web2) 换头大作战

搞了好久，因为 vegetable 所以第一步搞了好久得到 不知道怎莫将 X-Forwarded-For 设置，百度发现了一些类似的 CTF 题 才知道要把 X-Forwarded-For 设置成主机 127.0.0.1 后来就一气呵成拿到 flag。第一次有点小兴奋~

1、随便输入数据提交显示: request method is error.I think POST is better

2、F12 查看源码发现: `<form action="index.php" method="get">...</form>`

3、更改 method: `<form action="index.php" method="post">...</form> == $0`

4、用 burp 抓包得到

`
https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag`

X-Forwarded-For:127.0.0.1

want=

5、将 X-Forwarded-For 设置成: 127.0.0.1 为本机地址

6、`
https://www.wikiwand.com/en/User_agent
please use Waterfox/50.0`

显示需要更

改代理，在 user agent 处添加 Waterfox/50.0

7、显示:

`
https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.bilibili.com`

再修改 Referrer: `Referer:www.bilibili.com`

`
https://www.wikiwand.com/en/HTTP_cookie
you are not admin`

8、显示

9、`Cookie: admin=0` 更改 cookie `Cookie: admin=1`

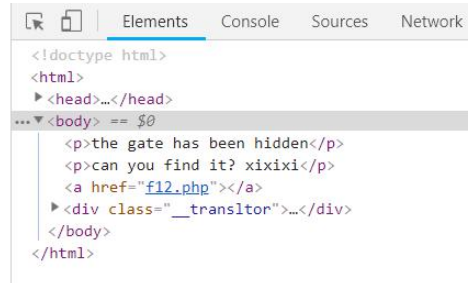
10、得到 flag `
hgame{hTtp_HeaDeR_iS_Ez}`

(Web4) can u find me?

直接 F12 查看源码 哦豁果然在这里

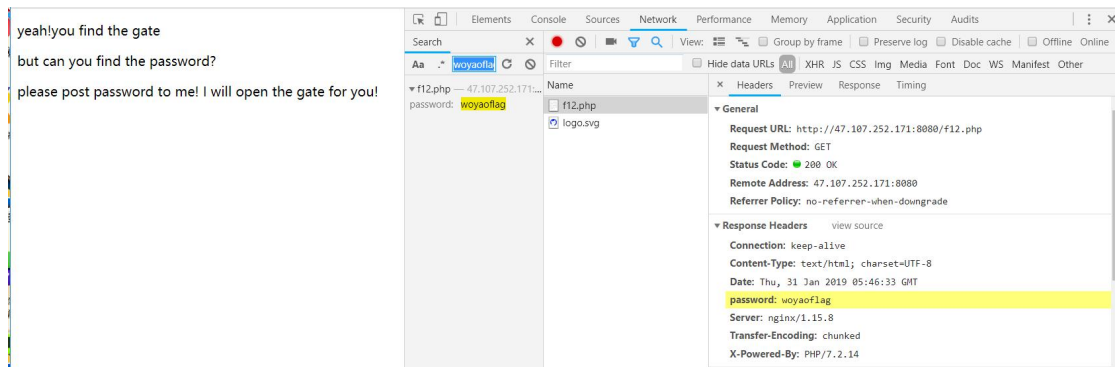
the gate has been hidden

can you find it? xixixi



```
<!doctype html>
<html>
  <head>...</head>
  <body>
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"></a>
    <div class="_transltor">...</div>
  </body>
</html>
```

进去发现需要找 password; 听说 network 里有好东西进去搜索果然有 password: woyaoflag



yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

Network tab details:

- Request URL: http://47.107.252.171:8080/f12.php
- Request Method: GET
- Status Code: 200 OK
- Remote Address: 47.107.252.171:8080
- Response Headers: password: woyaoflag

Post password? 天哪别笑我 vegetable 这个 post 的过程百度了好久终于知道了。。。



yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

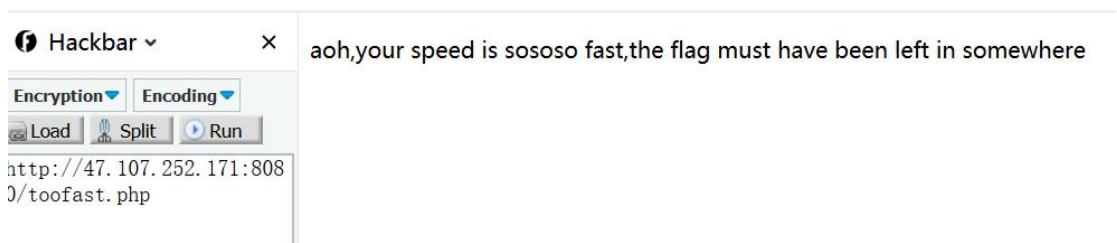
right!

[click me to get flag](#)

Hackbar tool configuration:

- URL: http://47.107.252.171:8080/f12.php
- Enable Post data: ☒
- Post data: password=woyaoflag

OKOK 点进去 我的 flag 来了, 哦豁什么东西啊 Hint 里给了个 302 跳转, OK 抓包就完事了



aoh,your speed is sososo fast,the flag must have been left in somewhere

Hackbar tool configuration:

- URL: http://47.107.252.171:8080/toofast.php

啊果然在这里~

```
<body>
  <p>flag:hgame{f12_1s_aMazing111}</p>
</body>
```

(Re2) helloRe

记事本打开文件，然后就看见了。。。

Please input your key: hgame{Welc0m3_t0_R3_World!}

提交 hgame{Welc0m3_t0_R3_World!} 加 50 积分~

(Re5) Python 教室

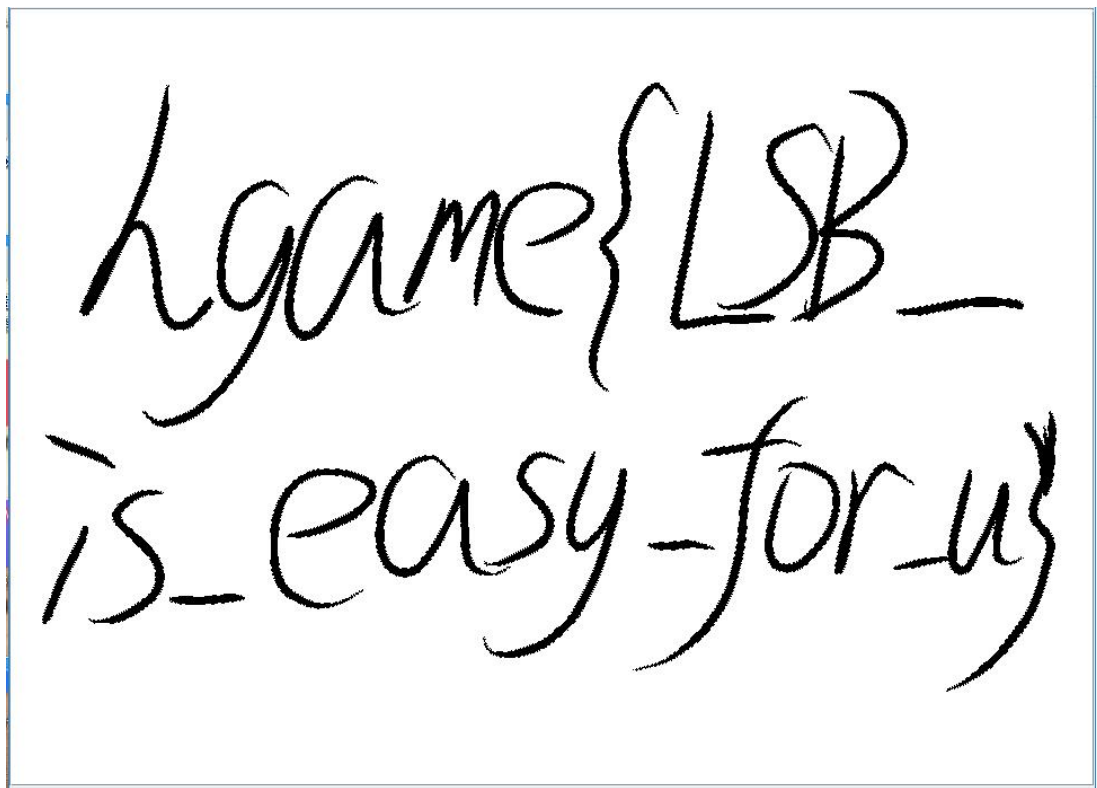
```
enc1 = 'hgame {'
enc2 = 'SGVyZV8xc18zYXN5Xw =='
enc3 = 'Pyth0n}'
```

- 1、 `first = raw_input()` 显然 第一部分就是 hgame{
 `secend = raw_input()`
- 2、 `secend = base64.b64encode(secend)` base64 解密得到 Here_1s_3asy_
 `third = raw_input()`
- 3、 `third = raw_input()` Pyth0n}

综合得到 hgame{Here_1s_3asy_Pyth0n}

(MISC1) Hidden Image in LSB

下载 hint 的工具直接拿到的 233.



(MISC2) 打字机

Google 搜图得到打字机的名称 violet typewriter 观察分辨图片代码大小写拿到 flag

Pyana{Mr_vz0Lai_ir0amPziar}

被 L 坑了很久

(CRYPTO1) Mix

先翻译摩尔斯电码

摩尔斯电码 744B735F6D6F7944716B7B6251663430657D

~~刚开始翻译出来了摩尔斯电码就疯狂提交，发现不对，后来试着看看发现可以用十六进制转换得到

base16 tKs_moyDqk{bQf40e}

然后又开始疯狂提交，当然是错的，太嫩了 因为不知道那些个密码 再后来百度找了些密码的网站，看了看懂了，还得解，看看 flag 形式应该用栅栏

栅栏 tsmYq{Q4eK_oDkbf0}，然后应该就是凯撒密码了~

凯撒 hgame{E4sY_cRypt0}~