# CTF信息搜集/泄露

原创

Skn1fe 于 2021-02-24 16:49:14 发布 845 收藏 2
文章标签： php 安全

## 文章目录

本文以ctf.show网站题目为例，总结ctf中的信息泄露姿势

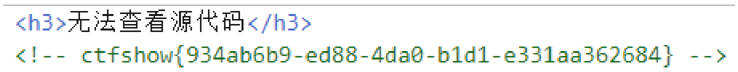
---

## 注释未删除

```
<h3>web1:where is flag?</h3>
<!-- ctfshow{86b423f4-6286-4854-a7c1-7a1f63a8004f} -->
```

## js前台拦截绕过

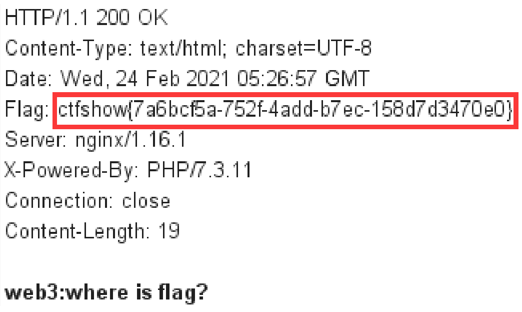
js禁止了右键和F12，手动呼出开发者工具即可



```
<h3>无法查看源代码</h3>
<!-- ctfshow{934ab6b9-ed88-4da0-b1d1-e331aa362684} -->
```

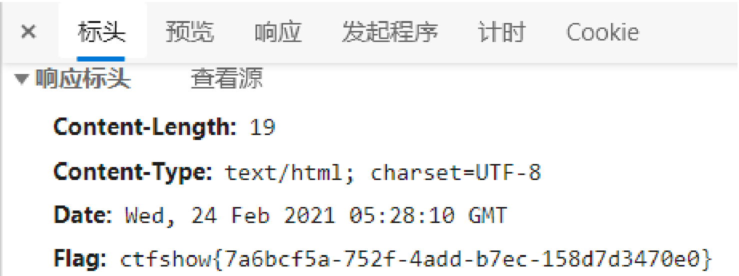
## 响应头

burp抓包或者F12查看



```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Wed, 24 Feb 2021 05:26:57 GMT
Flag: ctfshow{7a6bcf5a-752f-4add-b7ec-158d7d3470e0}
Server: nginx/1.16.1
X-Powered-By: PHP/7.3.11
Connection: close
Content-Length: 19

web3:where is flag?
```



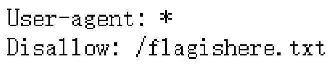
**Content-Length:** 19

**Content-Type:** text/html; charset=UTF-8

**Date:** Wed, 24 Feb 2021 05:28:10 GMT

**Flag:** ctfshow{7a6bcf5a-752f-4add-b7ec-158d7d3470e0}

## robots.txt泄露

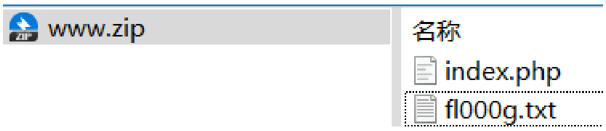


```
User-agent: *
Disallow: /flagishere.txt
```

## phps源码泄露

访问/index.phps

## www.zip源码泄露



有时候给的文件内容是假flag，要去网站目录找
访问/fl000g.txt

## .git泄露

版本控制很重要，但不要部署到生产环境更重要。

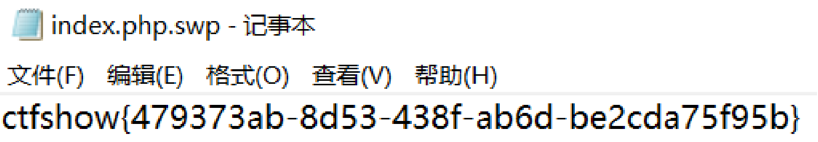
```
sudo python GitHack.py -u http://1525f5c6-9693-4c82-9ee8-79213253e147.chall.ctf.show:8080/.git
```

## .svn泄露

直接访问/.svn

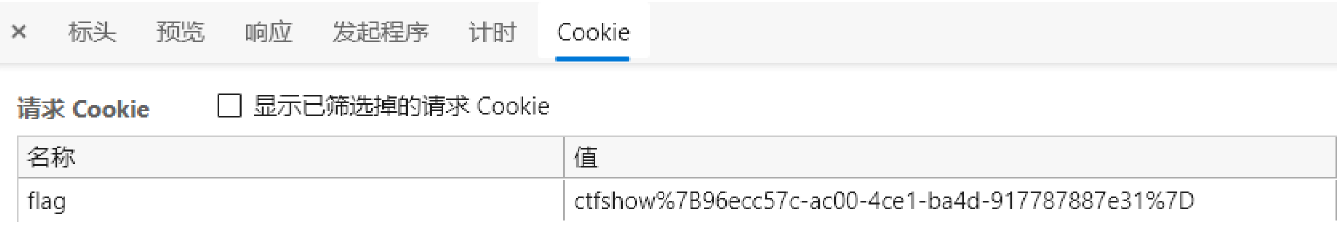
## vim泄露

vim在保存出错的情况下会产生.swp文件



ctfshow{479373ab-8d53-438f-ab6d-be2cda75f95b}

## cookie泄露



**请求 Cookie** ☐ 显示已筛选掉的请求 Cookie

| 名称 | 值 |
|---|---|
| flag | ctfshow%7B96ecc57c-ac00-4ce1-ba4d-917787887e31%7D |

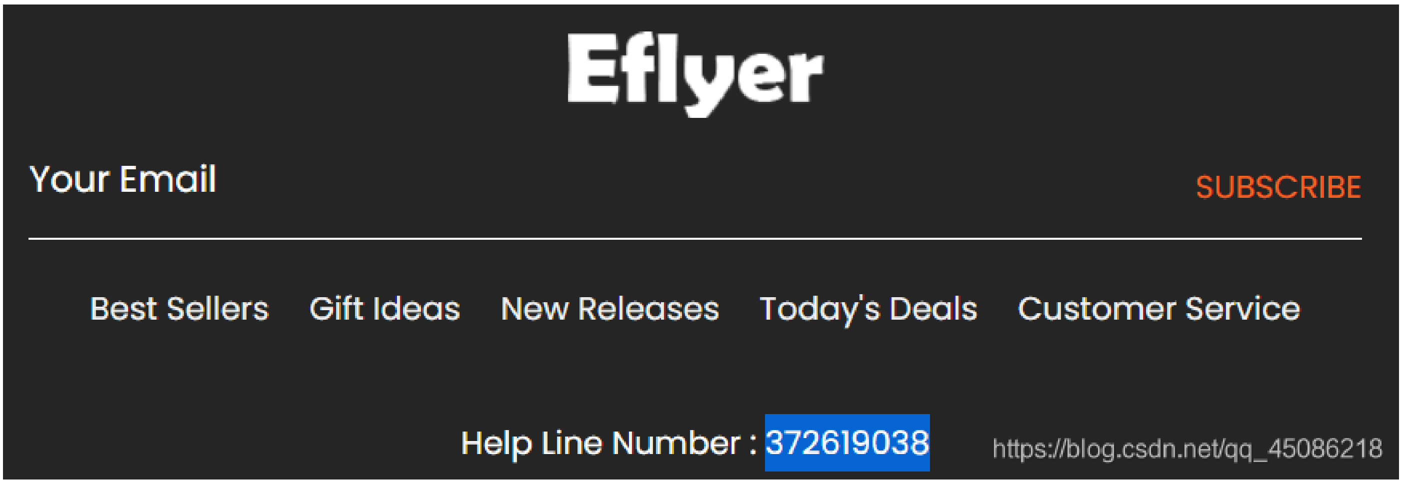
## 域名信息

域名其实也可以隐藏信息，比如ctfshow.com 就隐藏了一条信息
阿里云网站运维检测平台

| | | | |
|---|---|---|---|
| DNS服务商: | f1g1ns1.dnspod.net, f1g1ns2.dnspod.net<br>(未使用阿里云解析DNS) | 本地DNS检测: | 点击下载本地检测工具 |
| DNS服务商解析结果: | A<br>111.231.70.44<br>TXT<br>flag{just_seesee} | 223.5.5.5解析结果: | A<br>111.231.70.44<br>TXT<br>flag{just_seesee} |
| 递归解析追踪: | ✓ 域名递归解析正常 | TTL生效时间: | 域名TTL生效时间为 600 秒<br>提示：如果域名记录修改不久，请等待TTL生效时间后再次检测 |

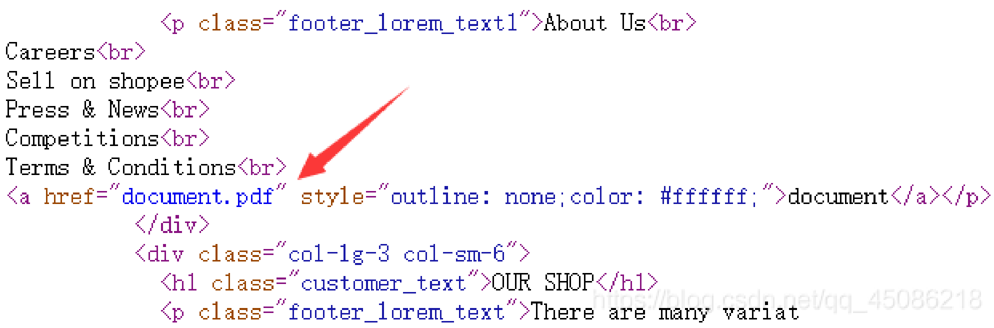
## 网页特殊信息

有时候网站上的公开信息，就是管理员常用密码



Help Line Number : 372619038

## 观察< a href="">标签



```
            <p class="footer_lorem_text1">About Us<br>
Careers<br>
Sell on shopee<br>
Press & News<br>
Competitions<br>
Terms & Conditions<br>
<a href="document.pdf" style="outline: none;color: #ffffff;">document</a></p>
          </div>
          <div class="col-lg-3 col-sm-6">
            <h1 class="customer_text">OUR SHOP</h1>
            <p class="footer_lorem_text">There are many variat
```

可以得到默认用户密码等信息

## 登陆

默认后台地址：http://your-domain/system1103/login.php
默认用户名：admin
默认密码：admin1103

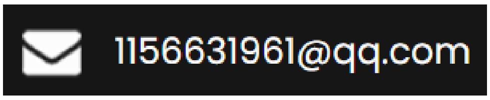
## 默认配置

网页默认存放在/var/www/html/# 常用网页目录

/admin/
/login/
/system/
/manage/
/guanli/
/admin/login.php
/admin/admin_login.php
/admin/adminlogin.php

## 社会工程学

公开的信息比如邮箱，可能造成信息泄露，产生严重后果


1156631961@qq.com


1156631961

所在地:中国，浙江，杭州

红蓝信安

在西安

## 探针泄露

对于测试用的探针，使用完毕后要及时删除，可能会造成信息泄露

/tz.php 版本是雅黑PHP探针

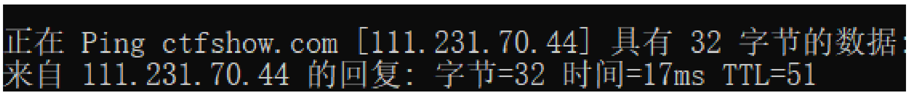
| 服务器参数 | | | |
|---|---|---|---|
| 服务器域名/IP地址 | www-data - localhost(172.12.44.200) 你的IP地址是：[redacted] | | |
| 服务器标识 | Linux 12e5214f83a3 4.15.0-134-generic #138-Ubuntu SMP Fri Jan 15 10:52:18 UTC 2021 x86_64 | | |
| 服务器操作系统 | Linux 内核版本：4.15.0-134-generic | 服务器解译引擎 | nginx/1.16.1 |
| 服务器语言 | zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6 | 服务器端口 | 80 |
| 服务器主机名 | 12e5214f83a3 | 绝对路径 | /var/www/html |
| 管理员邮箱 | | 探针路径 | /var/www/html/tz.php |

| 服务器实时数据 | | | |
|---|---|---|---|
| 服务器当前时间 | 2021-02-24 16:27:17 | 服务器已运行时间 | 32天15小时51分钟 |
| CPU型号 [2核] | AMD EPYC 7K62 48-Core Processor \| 频率:2595.124 \| 二级缓存:512 KB \| Bogomips:5190.24 ×2 | | |
| CPU使用状况 | 0%us, 0%sy, 0%ni, 98.97%id, 0%wa, 0%irq, 1.03%softirq \| 查看图表 | | |
| 硬盘使用状况 | 总空间 49.152 G， 已用 45.602 G， 空闲 3.55 G， 使用率 92.78% | | |
| 内存使用状况 | 物理内存：共 7.633 G , 已用 6.288 G , 空闲 1.345 G , 使用率 82.38%<br>Cache化内存为 3.025 G , 使用率 39.62 % \| Buffers缓冲为 0.634 G<br>真实内存使用 2.629 G , 真实内存空闲 5.004 G , 使用率 34.45 %<br>SWAP区：共 2 G , 已使用 0.049 G , 空闲 1.951 G , 使用率 2.44 % | | |
| 系统平均负载 | 0.03 0.12 0.15 2/1311 | | |

## 真实ip

透过重重缓存，查找到ctfer.com的真实IP

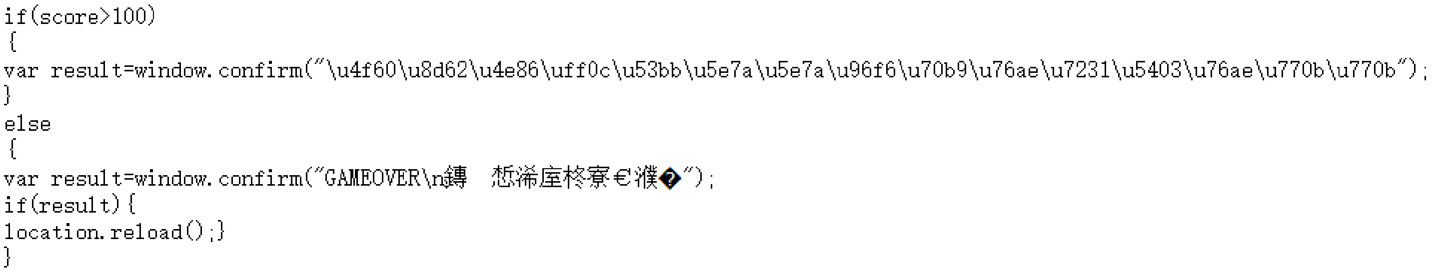
直接ping www.ctfshow.com



```
正在 Ping ctfshow.com [111.231.70.44] 具有 32 字节的数据
来自 111.231.70.44 的回复: 字节=32 时间=17ms TTL=51
```

## js小游戏

查找通关条件的语句



```
if(score>100)
{
var result=window.confirm("\u4f60\u8d62\u4e86\uff0c\u53bb\u5e7a\u5e7a\u96f6\u70b9\u76ae\u7231\u5403\u76ae\u770b\u770b");
}
else
{
var result=window.confirm("GAMEOVER\n鏄  惁瑕侀噸鏂板紑濮�");
if(result){
location.reload();}
}
```

ASCII解码

## 数据库泄露

mdb文件是早期asp+access构架的数据库文件，文件泄露相当于数据库被脱裤了。

/db/db.mdb下载数据库文件

## 目录扫描

```
sudo python3 dirsearch.py -u http://5abc68f7-ee21-4aba-8a99-40b535294c4e.chall.ctf.show:8080/ -e *
```

-s DELAY, --delay=DELAY 设置请求之间的延时