

# ctf.show web入门

原创

[echo&once](#) 于 2022-01-21 23:30:14 发布 1721 收藏

文章标签: [前端](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/midaxin/article/details/122607883>

版权

目录

## 信息收集

web1: **【where is flag】**

web2: **【无法查看源代码】**

web3: **【where is flag】**

web4: **【robots】**

web5: **【phps文件泄露】**

web6: **【网站源码泄露】**

web7: **【git】**

web8: **【svn泄露】**

web9: **【vim缓存泄露】**

web10: **【cookie】**

web11: **【域名解析】**

web12: **【网站公开信息=管理员常用密码】**

web13: **【技术文档里的敏感信息】**

web14: **【editor】**

web15: **【公开的邮箱】**

web16: **【探针】**

web17: **【sql备份文件】**

web18: **【unicode转码】**

web19: **【密码放在前端】**

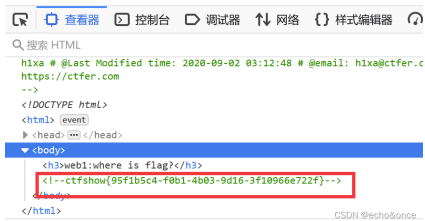
web20: **【数据库文件泄露】**

---

## 信息收集

web1: **【where is flag】**

## 打开开发者工具



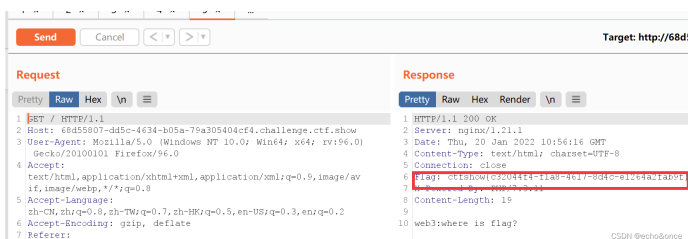
## web2: 【无法查看源代码】

ctrl+u或者开发者工具,都可以



## web3: 【where is flag】

直接抓包, 查看响应包



## web4: 【robots】

**Robots协议**:也称为爬虫协议、机器人协议等,其全称为“网络爬虫排除标准”,它通常是一个叫做robots.txt的文本文件,一般放在网站的根目录下。网站通过Robots协议告诉搜索引擎哪些页面可以抓取,哪些页面不能抓取。

先抓包,发现响应包里面并没有flag,查看网站下有没有robots.txt,发现有,并发现flag存放位置继续访问改文件即可得到flag

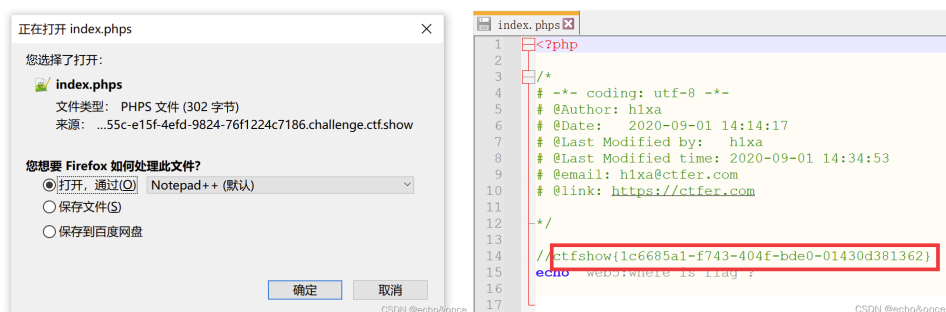


## web5: 【phps文件泄露】

.phps为后缀:**phps文件就是php的源代码文件**,通常用于提供给用户(访问者)查看php代码,因为用户无法直接通过Web浏览器看到php文件的内容,所以需要phps文件代替。只要不用php等已经在服务器中注册过的MIME类型为文件即可,但为了国际通用,所以才用了phps文件类型。

直接访问url/index.php可以下载网站的php源代码文件,打开即可。

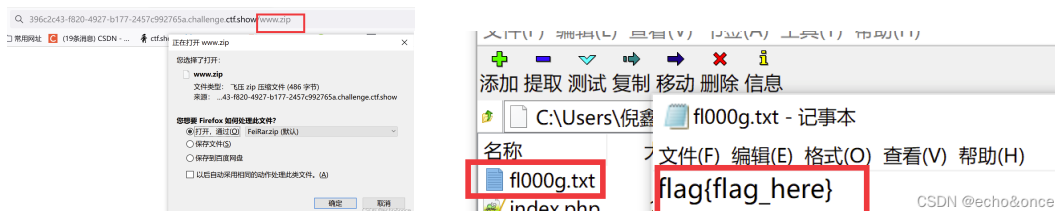
**MIME类型：**MIME类型就是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。



## web6: 【网站源码泄露】

**原因：**一般网站管理员在日常维护中，总会把网站源码给备份一下，防止网站出现问题时，能马上恢复使用，不过一般的管理员安全意识不高，在备份的时候，会使用一些常见的压缩备份名，而且不光使用常见的备份名字，大多的管理还会把备份好的源码直接放在网站根目录里

常见备份文件后缀：`.rar` `.zip` `.7z` `.tar` `.gz` `.bak` `.txt` `.old` `.temp`



ctfshow{fb251b9c-8388-46cc-b983-ce4257ce6c30}

CSDN @echo&once

## web7: 【git】

1) git:Git是目前世界上最先进的**分布式版本控制系统**，可以记录文件的每一次改动

2) **版本库：**简单理解为一个目录，这个目录里面的所有文件都能被git管理起来，每个文件的删除、修改都能被git追踪。

3) **git版本控制主要作用：**

- 记录文件的所有历史变化
- 错误恢复到某个历史版本
- 多人协作开发编辑同一个文件

3) **.git文件导致源码泄露原理：**开发人员在开发时，常常会先把源码提交到远程托管网站（如github），最后再从远程托管网站把源码放到服务器的web目录下，攻击者可以利用这个目录，去下载.git如隐藏文件夹，如果忘记把.git文件删除，就造成此漏洞。利用.git文件恢复网站的源码，而源码里可能会有数据库的信息。

5) 如果在文件夹中存在了index.php文件的情况，一般服务器会默认直接解析这个文件，删除index.php以后，就会出现该文件夹中全部的可访问文件目录了（？？）



### web8: 【svn泄露】

1) **svn**: **SVN是源代码版本管理软件**。使用SVN管理本地代码过程中，会生成一个名为.svn的隐藏文件夹，其中包含重要的源码信息。原因：**网站管理员在发布代码时，没有使用导出功能，直接进行复制粘贴**。这就使.svn隐藏文件夹被暴露于外网环境，黑客可以借助其中包含的用于版本信息追踪的‘entries’文件，逐步摸清站点结构。”（可以利用.svn/entries文件，获取到服务器源码、svn服务器账号密码等信息）

2) .svn漏洞利用:添加网站url在被利用的网址后面加 /.svn/entries，列出网站目录，甚至下载整站。

3)漏洞修复方法：在web服务器配置文件中增加一段代码，过滤到.svn文件，返回404

4) 防御：开发人员在使用SVN时，严格使用导出功能。禁止直接复制代码。

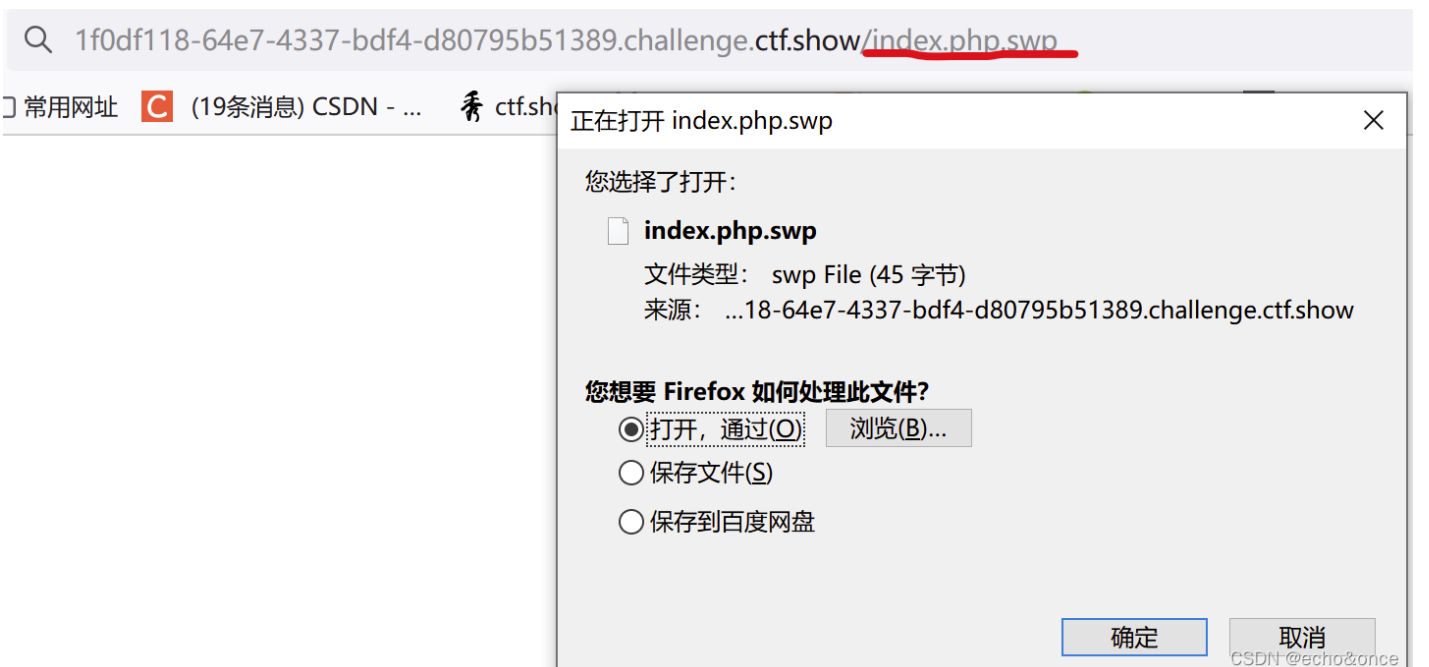
查看隐藏的文件夹即可得到flag

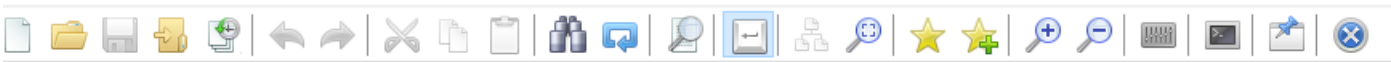


### web9: 【vim缓存泄露】

1) **vim**: vim是linux自带且常用的文件编辑器，vim在编辑时会生成一个隐藏的临时文件。当vim异常退出时这个文件就会被保留下来，产生缓存文件，缓存会一直停留在服务器上，引起源码泄露，第一次产生的缓存文件后缀为.swp，后面会产生swo，vim中的swp即swap文件，在编辑文件时产生，它是隐藏文件，如果原文件名是submit，则它的临时文件——.submit.swp如果文件正常退出，则此文件自动删除。

2) index.php:入口文件





1 ctfshow{9320918c-95bf-45fd-8489-43a062018e82}

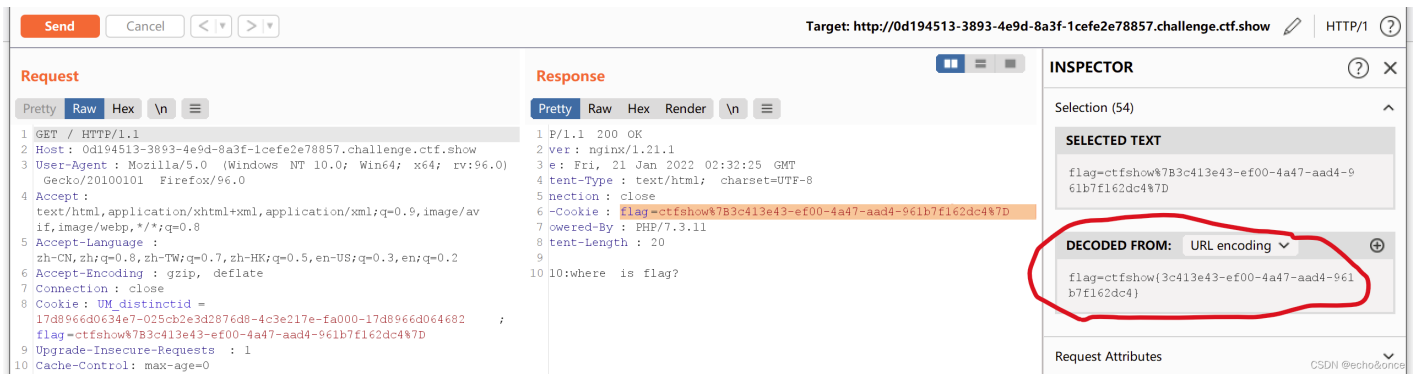
CSDN @echo&once

### web10: 【cookie】

1) Cookie是在浏览器访问WEB服务器的某个资源时，由WEB服务器在HTTP响应消息头中附带传送给浏览器的一个小文本文件。上网时都是使用无状态的HTTP协议传输出数据，这意味着客户端与服务端在数据传送完成后就会中断连接。这时我们就需要一个一直保持会话连接的机制。在session出现前，cookie就完全充当了这种角色。也就是，cookie的小量信息能帮助我们跟踪会话。一般该信息记录用户身份

2) 原理：客户端请求服务器时，如果服务器需要记录该用户状态，就使用response向客户端浏览器颁发一个Cookie。而客户端浏览器会把Cookie保存起来。当浏览器再请求服务器时，浏览器把请求的网址连同该Cookie一同提交给服务器。服务器通过检查该Cookie来获取用户状态

抓包查看响应头中的cookie，发现flag格式不太对，用url解码后得到flag[bp自带了编码解码工具]



### web11: 【域名解析】

打开dbcha.com输入想要解析的域名即可

域名也可以隐藏信息！！！！



dns域名解析中添加各项解析记录:



1) A记录/ip记录 [只有IP]: 将域名指向一个IPv4地址

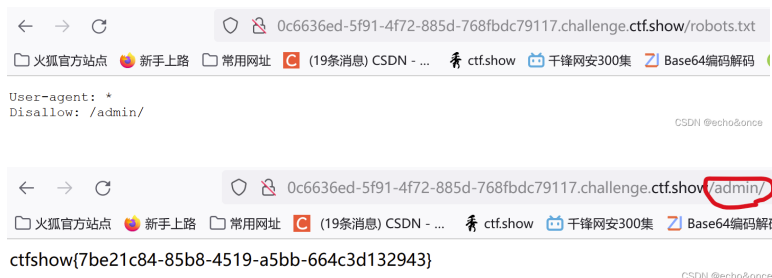
2) **CNAME记录**: 如果将域名指向一个域名, 实现与被指向域名相同的访问效果, 需要增加CNAME记录。这个



域名一般是主机服务商提供的一个域名

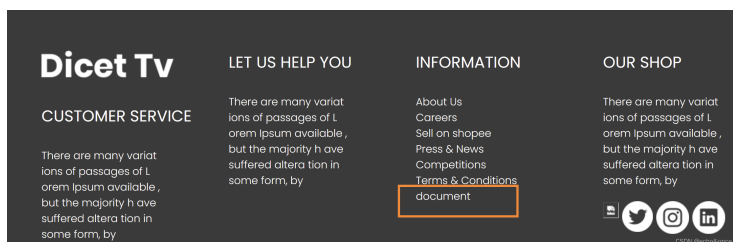
## web12: 【网站公开信息=管理员常用密码】

根据提示, 查看robots.txt看到用户名为admin, 页面最下方电话号码即为密码, 登录即得到flag



## web13: 【技术文档里的敏感信息】

发现只有document有链接, 点进去看看



### ● 登陆

默认后台地址: <http://your-domain/system1103/login.php>

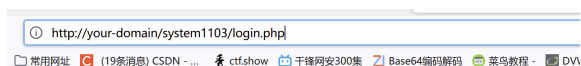
默认用户名: admin

默认密码: admin1103

CSDN @echo&once

打开登录地址连接发现无法访问, 因为开发系统或者这个技术文档, 并不是一个人用, 他们面向的域名会不一样, your-domain代表部署后的地址

your-domain:网域, 在这里应该是ctfshow的地址, 故修改



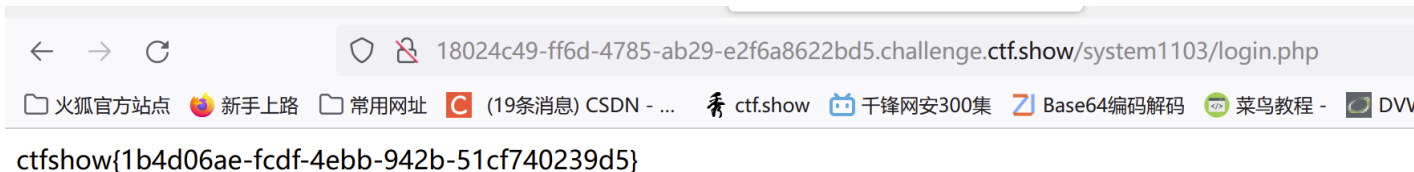
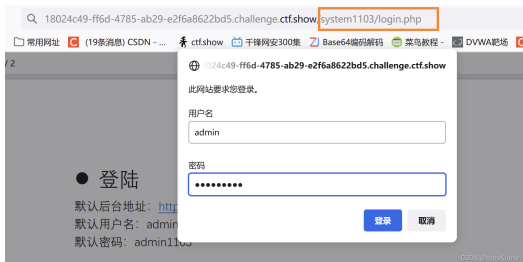
呃...找不到此网站。

我们无法连接至 your-domain 的服务器。

如果确定此网址正确, 您可以尝试:

- 过会儿再重试。
- 检查您的网络连接是否正常。
- 如果您部署有网络防火墙, 请检查 Firefox 是否已被授权访问网络。

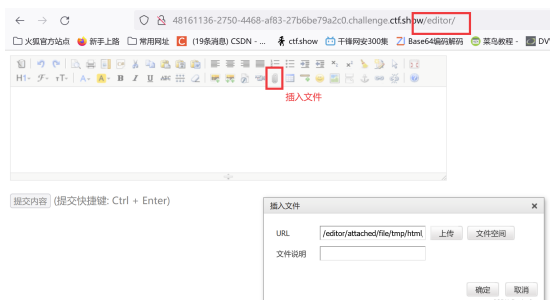
重试



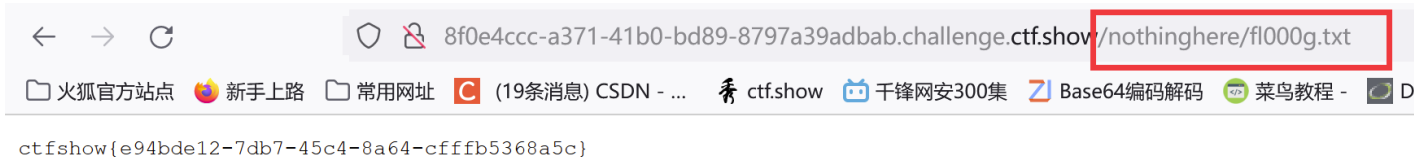
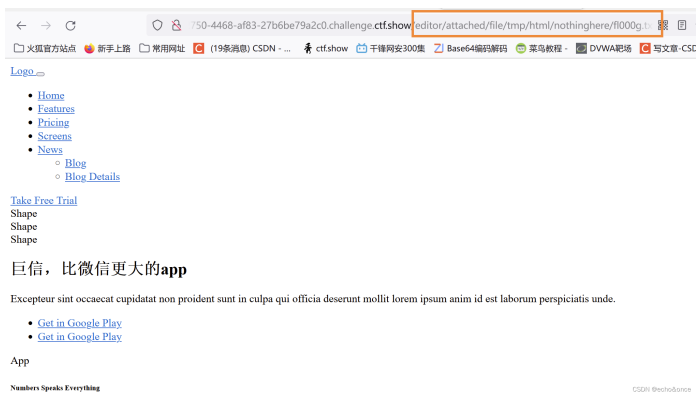
### web14: 【editor】

绝对路径是指文件在硬盘上的真实路径，而相对路径指的是相对于另一个文件来书，本文件的路径。在做web项目时应该采用相对路径，绝对路径容易造成文件的寻找失败

根据题目提示，查看编辑器editor,点开插入文件发现有文目录.....一系列操作，在tmp/html/nothinghere/fla000g.txt发现了flag

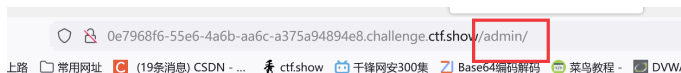


访问该文件（用绝对路径），发现并不是想要的flag,说明路径不是很正确，这里使用相对路径试试（？）



## web15: 【公开的邮箱】

根据题目提示，访问admin，发现一个登陆界面，用户名admin，密码就是首页下面的QQ邮箱（前面的web12中做过，网站公开信息很可能就是管理员常用密码），登录后显示密码错误，返回点击忘记密码，就会进行一个问题验证——所在城市；用qq去加一下QQ邮箱上面QQ发现是西安，输入，得到重置密码，登录即得到flag



### 后台登录系统

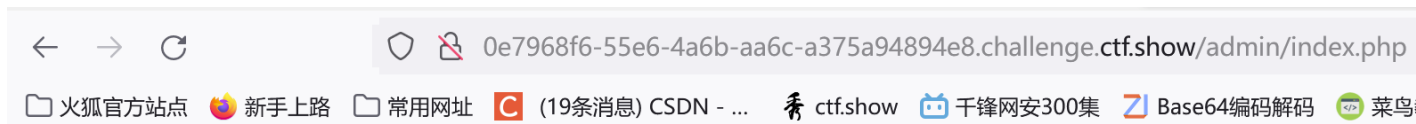
用户名

密码

登录

忘记密码

CSDN @echo&once



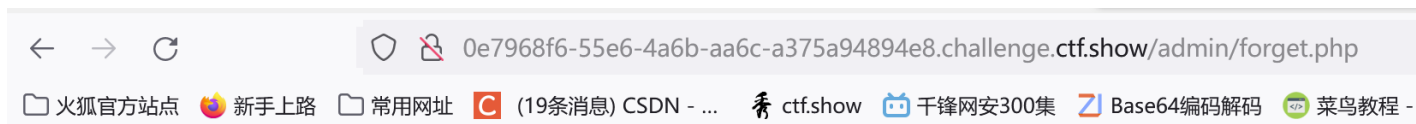
### 密码错误

CSDN @echo&once



CSDN @echo&once

CSDN @echo&once



您的密码已重置为 **admin7789**

CSDN @echo&once

admin

admin7789

登录

忘记密码

CSDN @echo&once

ctfshow{d8bea42e-2c33-48ab-8fdf-7ee4f35807fe}

CSDN @echo&once

## web16: 【探针】



**php探针：** php探针是用来探测空间、服务器运行状况和PHP信息用的，探针可以实时查看服务器硬盘资源、内存占用、网卡流量、系统负载、服务器时间等信息。

php探针的功能：

- 1、服务器环境探测：CPU、在线时间、内存使用状况、系统平均负载探测，操作系统、服务器域名、IP地址、解释引擎等；
- 2、PHP基本特征探测：版本、运行方式、安全模式及常规参数；
- 3、自定义探测：MYSQL连接测试、MAIL发信测试、函数支持情况及PHP配置参数。

根据提示，在url后面加/tz.php，发现在phpinfo初有个链接，打开，在出现的页面中查找flag即可

PHP相关参数	
PHP信息 (phpinfo) :	PHPINFO
PHP运行方式:	FPM-FCGI
PHP安全模式 (safe_mode) :	×
上传文件最大限制 (upload_max_filesize) :	2M
脚本超时时间 (max_execution_time) :	30秒
PHP页面根目录 (doc_root) :	×
allow_url_fopen (allow_url_fopen) :	×
allow_url_include (allow_url_include) :	×

6fcr4fce2-8745-4f61-ae50-a24e029d24cb\_challenge\_ctfshow/tz.php?act=phpinfo

## Environment

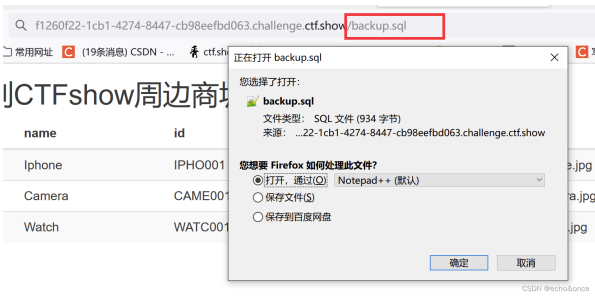
Variable	Value
PHP_EXTRA_CONFIGURE_ARGS	--enable-fpm --with-fpm-user=www-data --with-fpm-group=www-data --disable-cgi
HOSTNAME	e4115aa6a2c6
PHP_INI_DIR	/usr/local/etc/php
SHLVL	1
HOME	/home/www-data
PHP_LDFLAGS	-Wl,-O1 -Wl,--hash-style=both -pie
PHP_CFLAGS	-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_MD5	no value
PHP_VERSION	7.3.11
GPG_KEYS	CBAF69F173A0FEA4B537F470D66C9593118BCCB6 F38252826ACD957EF380D39F2F7956BC5DA04B5D
PHP_CPPFLAGS	-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_ASC_URL	https://www.php.net/get/php-7.3.11.tar.xz.asc/from/this/mirror
PHP_URL	https://www.php.net/get/php-7.3.11.tar.xz/from/this/mirror
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PHPIZE_DEPS	autoconf dpkg-dev dpkg file g++ gcc libc-dev make pkgconf re2c
PWD	/var/www/html
PHP_SHA256	657cf6464bac28e9490c59c07a2cf7bb76c200f09cfadf6e44ea64e95fa01021
FLAG	ctfshow{a75c27a6-ed53-4a69-b2fd-3c1f53e37da1}
USER	www-data

## PHP Variables

### web17: 【sql备份文件】

根据提示，访问备份的sql文件（即url+backup.sql），打开文件即可看到flag.....

\*.sql文件是mysql数据库导出的备份文件



```

1 CREATE DATABASE IF NOT EXISTS ctfshow;
2 USE ctfshow;
3
4 --
5 -- Table structure for table `products`
6 --
7
8 CREATE TABLE IF NOT EXISTS `products` (
9   `product_id` int(11) NOT NULL,
10  `name` varchar(100) NOT NULL,
11  `sku` varchar(10) NOT NULL,
12  `price` decimal(15,2) NOT NULL,
13  `image` varchar(50) NOT NULL,
14  PRIMARY KEY (`product_id`),
15  UNIQUE KEY `sku` (`sku`)
16  ) ENGINE=InnoDB AUTO_INCREMENT=1 DEFAULT CHARSET=utf8;
17
18 CREATE TABLE `ctfshow_secret` (
19   `secret` varchar(255) DEFAULT NULL
20  ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
21
22
23 INSERT INTO `ctfshow_secret` VALUES ('ctfshow(91f70c61-baa6-4da5-a901-123274e080bd)');
24
25 --
26 -- Dumping data for table `products`
27 --

```

## web18: 【unicode转码】

unicode编码: (统一码、万国码、单一码)，Unicode是为了解决传统字符编码方案的局限而产生的，为每种语言中的每个字符都设定了统一唯一的二进制编码【计算机只能识别二进制数字】，以实现跨语言、跨平台进行文本转换、处理的要求。

根据提示，分析源码，查看js文件：Flappy\_js.js,发现了一段不认识的编码[unicode编码]

去菜鸟工具里面将这个Unicode编码转码看看，“去110.php看看”，

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
5   <link rel="stylesheet" href="css/Flappy.css">
6   <title>Bird</title>
7 </head>
8 <body>
9   <canvas id="cvs" width="1200px" height="600px">
10    
11    
12    
13  </canvas>
14  <script type="text/javascript" src="js/Flappy_js.js"></script>
15 </body>
16 </html>
17

```

```

view-source:http://34dd99ac-7919-45a2-8157-2e4c8a8794ed.challenge.ctfshow/js/Flappy_js.js
bucket_four.draw();
bucket_five.hit(b.x,b.y);
bucket_five.update();
bucket_five.draw();
b.update(dt);
b.draw();
var flag=false;
if(b.x==bucket_one.x||b.x==bucket_two.x||b.x==bucket_three.x||b.x==bucket_four.x||b.x==bucket_five.x)
{
flag=true;
}
if(flag==true)
{
score++;
}
flag=false;
defen(score);
if(b.y>600||b.y<0)
{
game_over=true;
}
if(game_over==false)
{
requestAnimationFrame(run);
}
else
{
if(score>100)
{
var result=window.confirm("u4f60\u8d62\u4e8e\u00f0c\u53bb\u5e7a\u5e7a\u96fe\u70b9\u76ae\u7231\u5403\u76ae\u770b\u770b");
}
}

```

菜鸟工具 WEB 在线工具 SVG 编辑器 渐变色工具 图片编辑器 菜鸟教程 中文 Search.....

Unicode 转 中文 中文 转 Unicode ASCII 转 Unicode Unicode 转 ASCII 清空结果

1 \uff0c\u53bb\u5e7a\u5e7a\u96f6\u70b9\u76ae\u7231\u5403\u76ae\u770b\u770b

1 你赢了，去么么零点皮爱吃皮看看

CSDN @echo&once

6e813acb-6879-4853-9d96-3d8cfcecab35.challenge.ctf.show/110.php

火狐官方网站 新手上路 常用网址 (19条消息) CSDN - ... ctf.show 干锋网安300集 Base64编码解码

ctfshow{c273e694-6435-40d0-a390-73cbad532b22}

CSDN @echo&once

### web19: 【密码放在前端】

根据提示，查看源码，发现需要提交两个参数——用户名和密码，只要参数符合要求，就会获得flag，抓包，修改参数值，用post请求提交符合条件参数，查看响应包即可获得flag

```

</script>
<!--
error_reporting(0);
$flag="fakeflag"
$u = $_POST['username'];
$p = $_POST['pazzword'];
if(isset($u) && isset($p)){
    if($u=== 'admin' && $p === 'a599ac85a73384ee3219fa684296eaa62667238d608efa81837030bd1ce1bf04' ) {
        echo $flag;
    }
}

```

CSDN @echo&once

3806e6a8

火狐官方网站 新手上路 常用网址 (19条消息)

用户名: admin

密码: ●●●●●●

提交

CSDN @echo&once

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```

1 POST / HTTP/1.1
2 Host: 3806e6a8-0fdb-4e01-b1c4-06474af5328a.challenge.ctf.show
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://3806e6a8-0fdb-4e01-b1c4-06474af5328a.challenge.ctf.show/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 59
10 Origin: http://3806e6a8-0fdb-4e01-b1c4-06474af5328a.challenge.ctf.show
11 Connection: close
12 Cookie: UM_distinctid=17d8966d0634e7-025cb2e3d2876d8-4c3e217e-fa000-17d8966d064682
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&pazzword=a599ac85a73384ee3219fa684296eaa62667238d608efa81837030bd1ce1bf04

```

CSDN @echo&once

## Response

Pretty Raw Hex Render \n ☰

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.21.1
3 Date: Fri, 21 Jan 2022 14:06:28 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.11
7 Content-Length: 1813
8
9 ctFshow{7907f6b6-5235-4eab-9f15-d7ef3e52920b}
10 <!DOCTYPE html>
11 <html lang="zh-CN">
12 <head>
13 <meta charset="UTF-8">
14 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
15 <meta name="renderer" content="webkit"/>
16 <script src="js/jquery.min.js">
17 </script>
18 <script src="js/crypto.js">
19 </script>
20 <script src="js/cipher-core.js">
21 </script>
22 </head>
23 <body>
24 <div style="text-align: center;">
25 <h1>ctFshow{7907f6b6-5235-4eab-9f15-d7ef3e52920b}</h1>
26 </div>
27 </body>
28 </html>
```

## web20: 【数据库文件泄露】

1) mdb格式文件是一个数据库文件，它是Microsoft Access软件生成的一种存储格式

2) Access数据库的存储隐患是在ASP+Access应用系统中，如果获得或者猜到Access数据库的存储路径和数据库名，则该数据库就可以被下载到本地。由于Access数据库的加密机制非常简单，所以即使数据库设置了密码，解密也很容易。由于ASP程序采用的是非编译性语言，这大大降低了程序源代码的安全性。任何人只要进入站点，就可以获得源代码，从而造成ASP应用程序源代码的泄露。

3) 在数据库名称里加上#号，从URL上请求时#是请求地址和请求参数的一个分隔字符，如果知道了数据库名，直接请求的话，如：<http://www.xx.com/access#.mdb>，WEB服务器会认为请求的是access而不是access#.mdb，所以会提示找不到文件，但是URL中对于这些特殊的字符都会有一个特殊的表示方式，#的特殊表示就是%23，如<http://www.xx.com/access%23.mdb>，那么access#.mdb将会被下载。还有如果用FlashGet之类的下载工具也可以直接下载。

4) 防止数据库被下载的方法：

1.在数据库新建一个表，表名为<%safe就可以了，这样iis在解析的时候会出现500错误，数据库也就下载不了了！

注：.造成500错误常见原因有：

- ASP语法出错
- ACCESS数据库连接语句出错
- 文件引用与包含路径出错(如未启用父路径)
- 使用了服务器不支持的组件，如FSO等。

2.在你的数据库文件名后门加上#（不是扩展名，比如name#.mdb）这样iis就以为你是在请求该目录中默认的文件名，比如index.asp，如果iis找不到就会发出403禁止浏览目录的错误警告！

3.在iis中是把数据库所在的目录设为不可读，这样就可以防止被下载！这样做不会影响asp程序的正常使用

\*4.直接使用数据源 (ODBC)这样数据库就可以不用在web目录里面，从而彻底防止被下载，但是这样做你必须拥有服务器的管理员权限，但是，大部分虚拟主机用户是不可能用数据源 (ODBC)的！

4.1) IIS【建网站用的】是Internet Information Services英文全称的缩写，是一个World Wide Web server服务。IIS是一种Web(网页)服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络(包括互联网和局域网)上发布信息成了一件很容易的事。

根据题目提示，访问db/db.mdb,下载文件用记事本打开并查找flag即可

