ctf.show web入门

原创

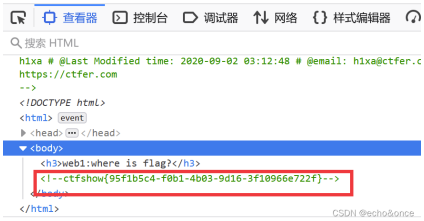
echo&once 于 2022-01-21 23:30:14 发布 1721 收藏
文章标签： 前端

目录

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。

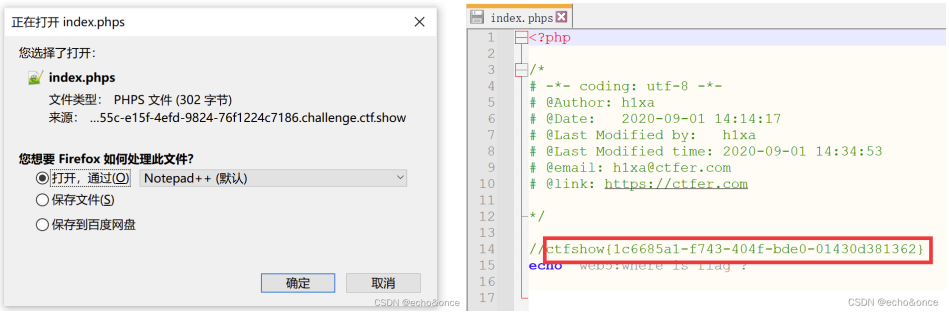
先抓包，发现响应包里面并没有flag,查看网站下有没有robots.txt,发现有，并发现flag存放位置继续访问改文件即可得到flag

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，所以需要用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.phps可以下载网站的php源代码文件,打开即可。

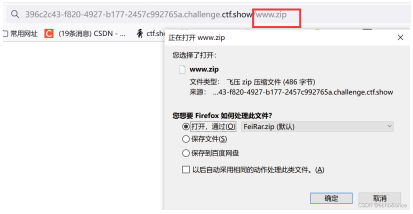
MIME类型：MIME类型就是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式.

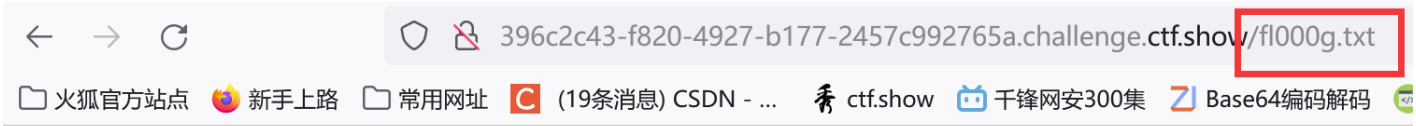


web6:【网站源码泄露】

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，能马上的恢复使用，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，大部分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

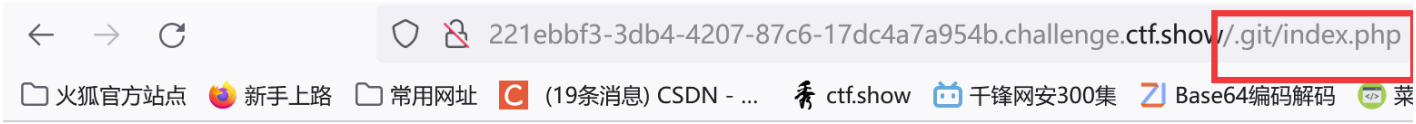
2）版本库：简单理解为一个目录，这个目录里面的所有文件都能被git管理起来，每个文件的删除、修改都能被git追踪。

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（？？）



ctfshow{1ea64472-b346-4439-a3e3-e7efc1a7a139}

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。

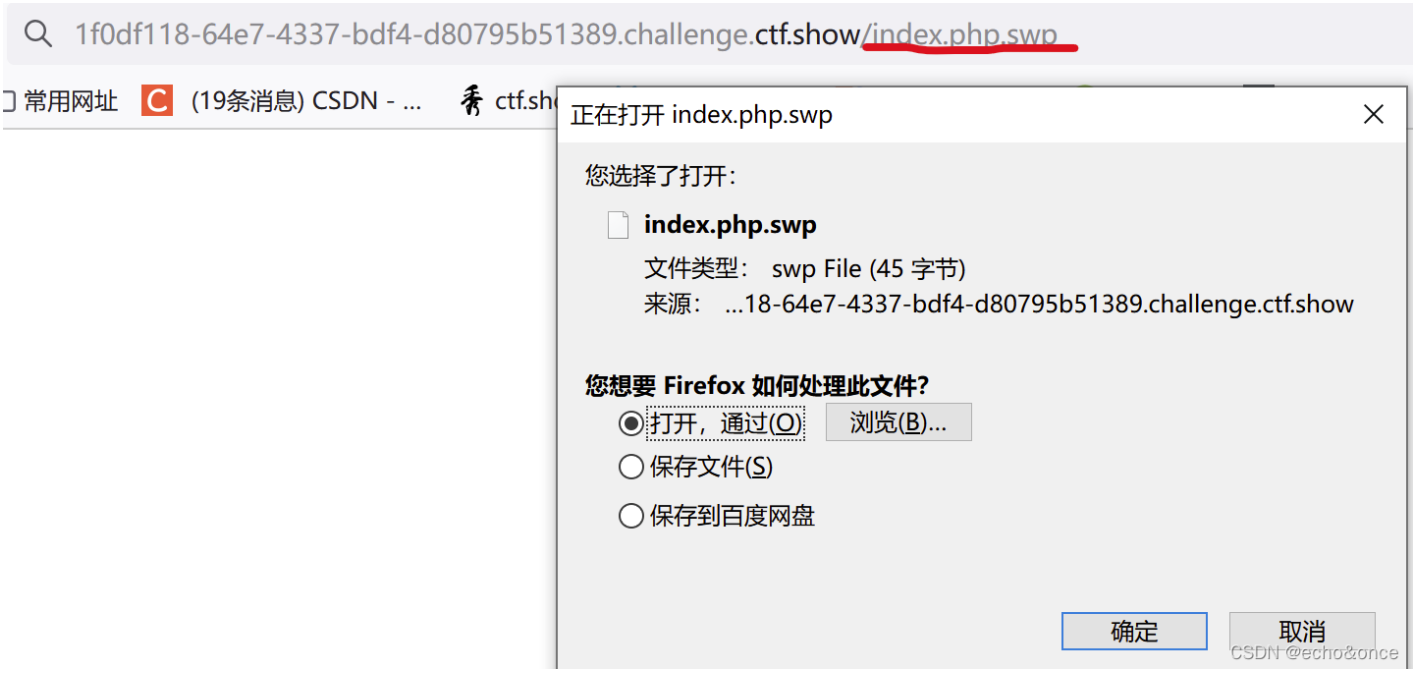
查看隐藏的文件夹即可得到flag

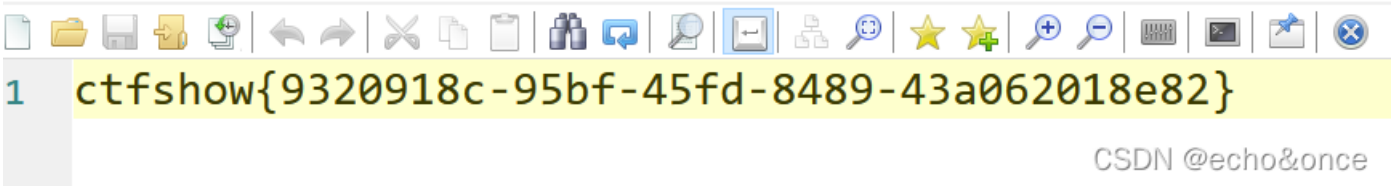
ctfshow{b0a5d8fd-bc68-422e-93ef-c2161878eb28}

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



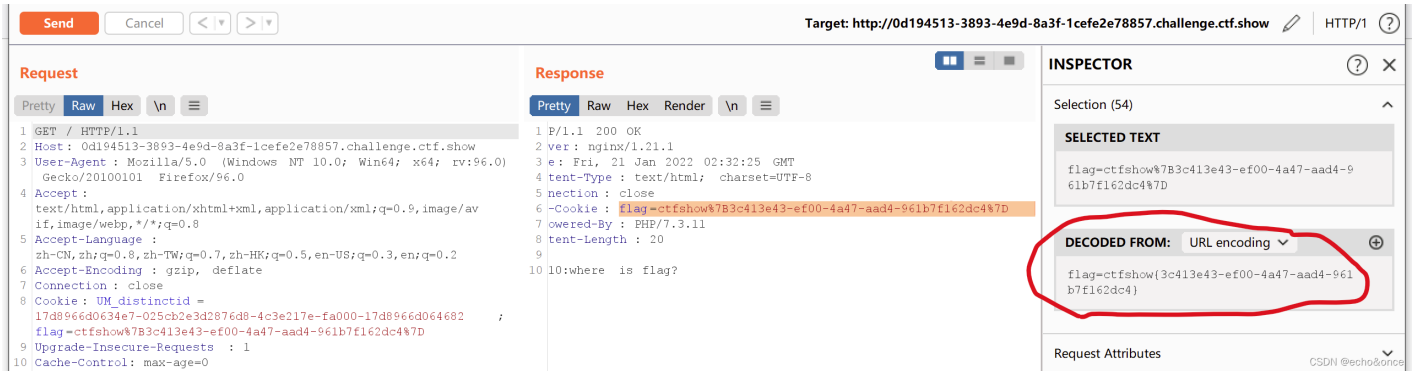


web10:【cookie】

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

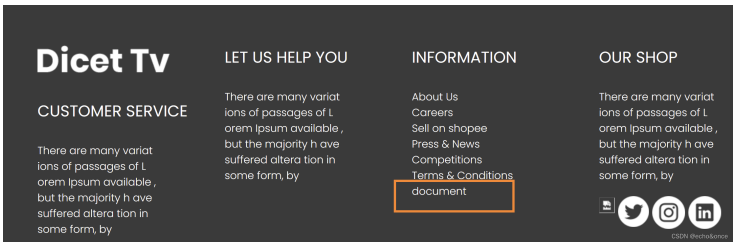
.....

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



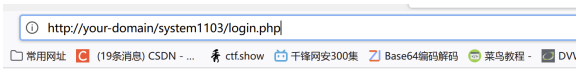
- 登陆

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

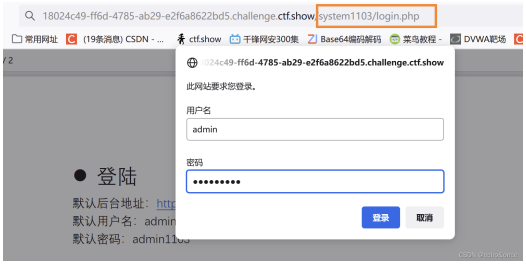
CSDN @echo&once

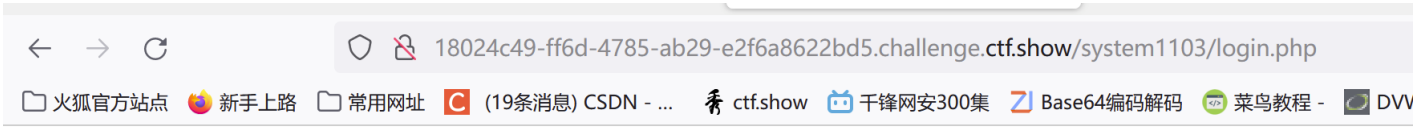
打开登录地址连接发现无法访问，因为开发系统或者这个技术文档，并不是一个人用，他们面向的域名会不一样，your-domain代表部署后的地址

your-domain:网域，在这里应该是ctfshow的地址，故修改



18024c49-ff6d-4785-ab29-e2f6a8622bd5.challenge.ctf.show/document.pdfsystem1103/login.php



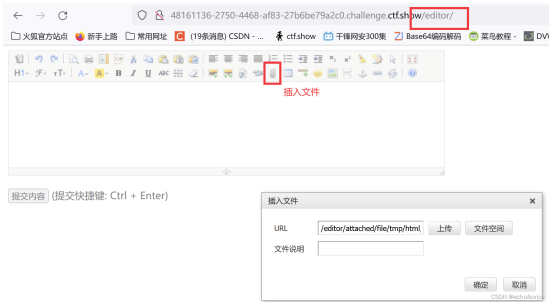


ctfshow{1b4d06ae-fcdf-4ebb-942b-51cf740239d5}

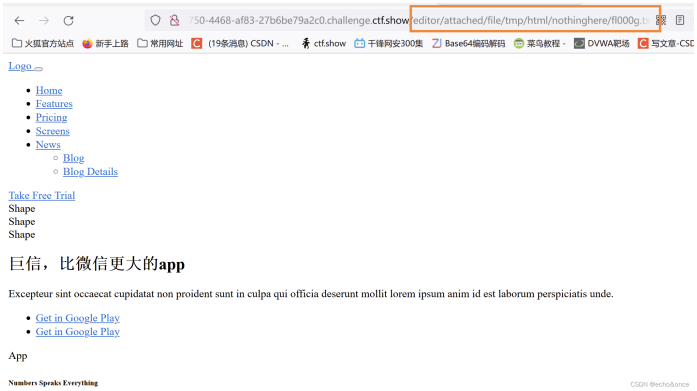
web14:【editor】

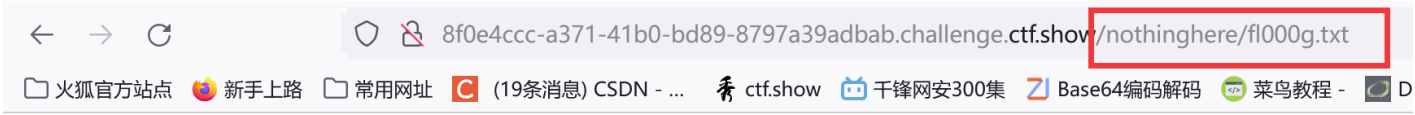
绝对路径是指文件在硬盘上的真实路径，而相对路径指的是相对于另一个文件来书，本文件的路径。在做web项目时应该采用相对路径，绝对路径容易造成文件的寻找失败

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（？）

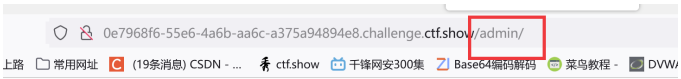


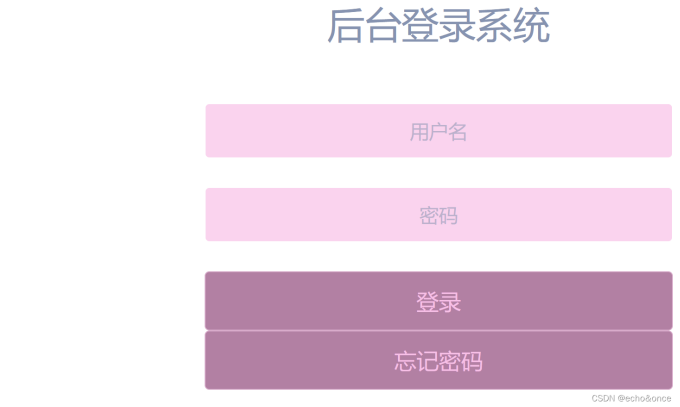


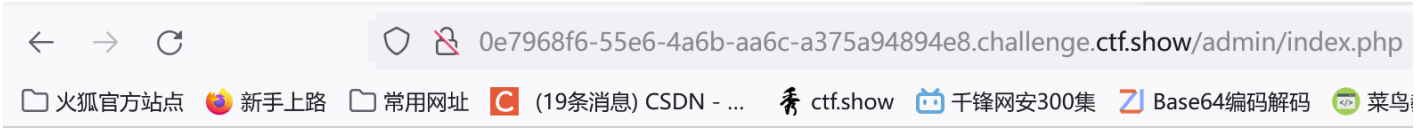
ctfshow{e94bde12-7db7-45c4-8a64-cfffb5368a5c}

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

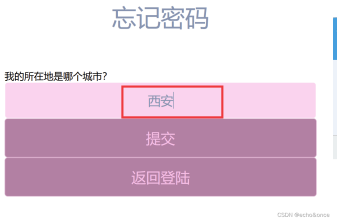


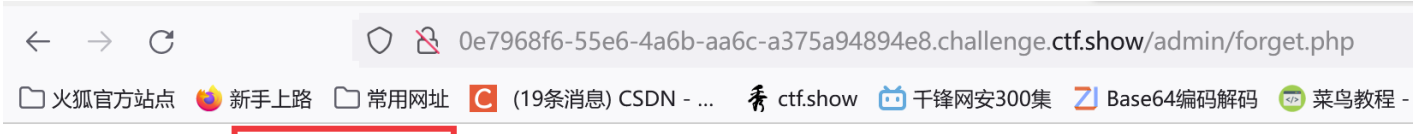




密码错误

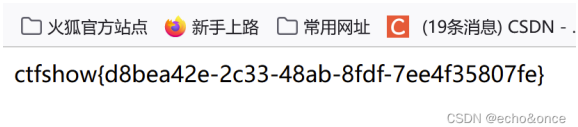
CSDN @echo&once





您的密码已重置为admin7789

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）：	×
dl()函数（enable_dl）：	×

6fc4fce2-8745-4f61-ae50-a24e029d24cb.challenge.ctf.show/tz.php?act=phpinfo

Environment

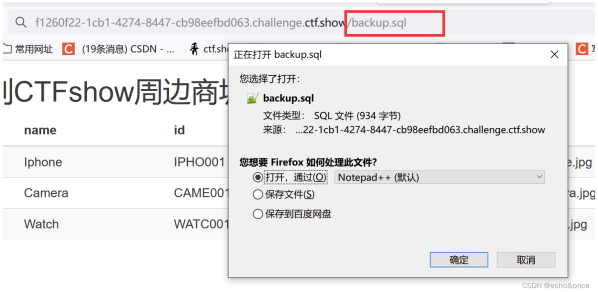
Variable	Value
PHP_EXTRA_CONFIGURE_ARGS	--enable-fpm --with-fpm-user=www-data --with-fpm-group=www-data --disable-cgi
HOSTNAME	e4115aa6a2c6
PHP_INI_DIR	/usr/local/etc/php
SHLVL	1
HOME	/home/www-data
PHP_LDFLAGS	-Wl,-O1 -Wl,--hash-style=both -pie
PHP_CFLAGS	-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -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

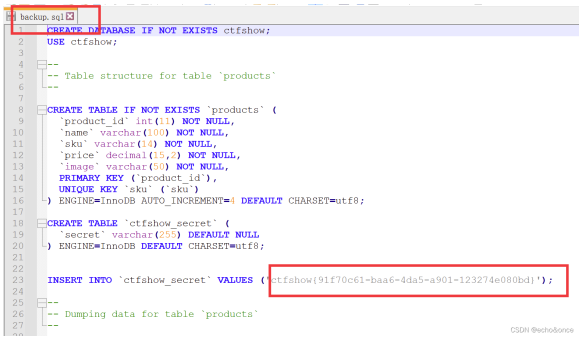
PHP Variables

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





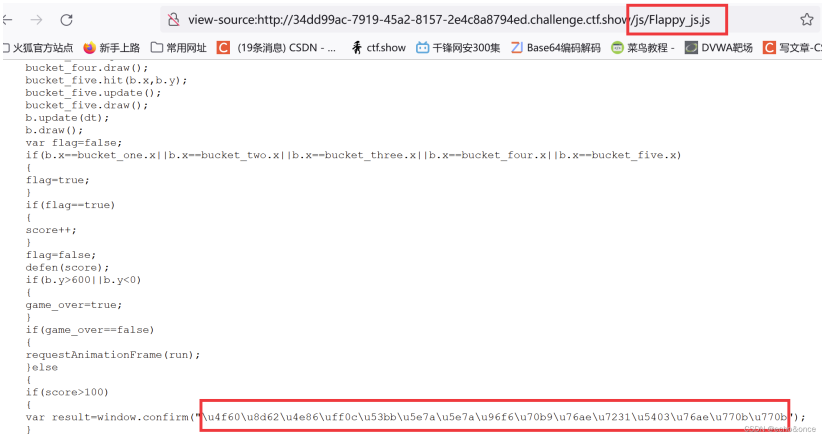
web18:【unicode转码】

unnicode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”，

```
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <link rel="stylesheet" href="css/Flappy_css.css">
    <title>Bird</title>
</head>
<body>
    <canvas id="cvs" width= "1200px" height="600px">
    <img id = "bird" src = "img/bird.png"/>
    <img id = "back1" src = "img/background.png"/>
    <img id = "back2" src = "img/background.png"/>
    </canvas>
    <script type="text/javascript" src="js/Flappy_js.js"></script>
</body>
</html>
```



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

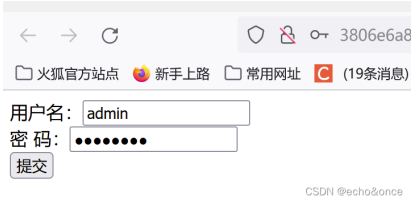
CSDN @echo&once

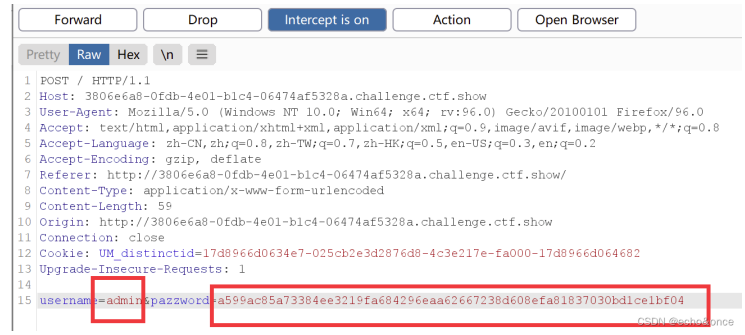
web19:【密码放在前端】

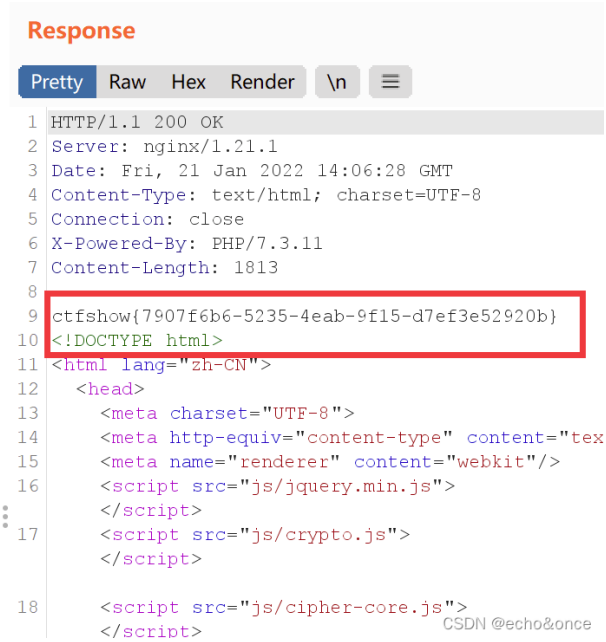
根据提示，查看源码，发现需要提交两个参数——用户名和密码，只要参数符合要求，就会获得flag，抓包，修改参数值，用post请求提交符合条件参数，查看响应包即可获得flag

```
</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







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