

CTFSHOW-WEB入门

一、信息收集

web1

简单的信息收集入门，F12查看源代码

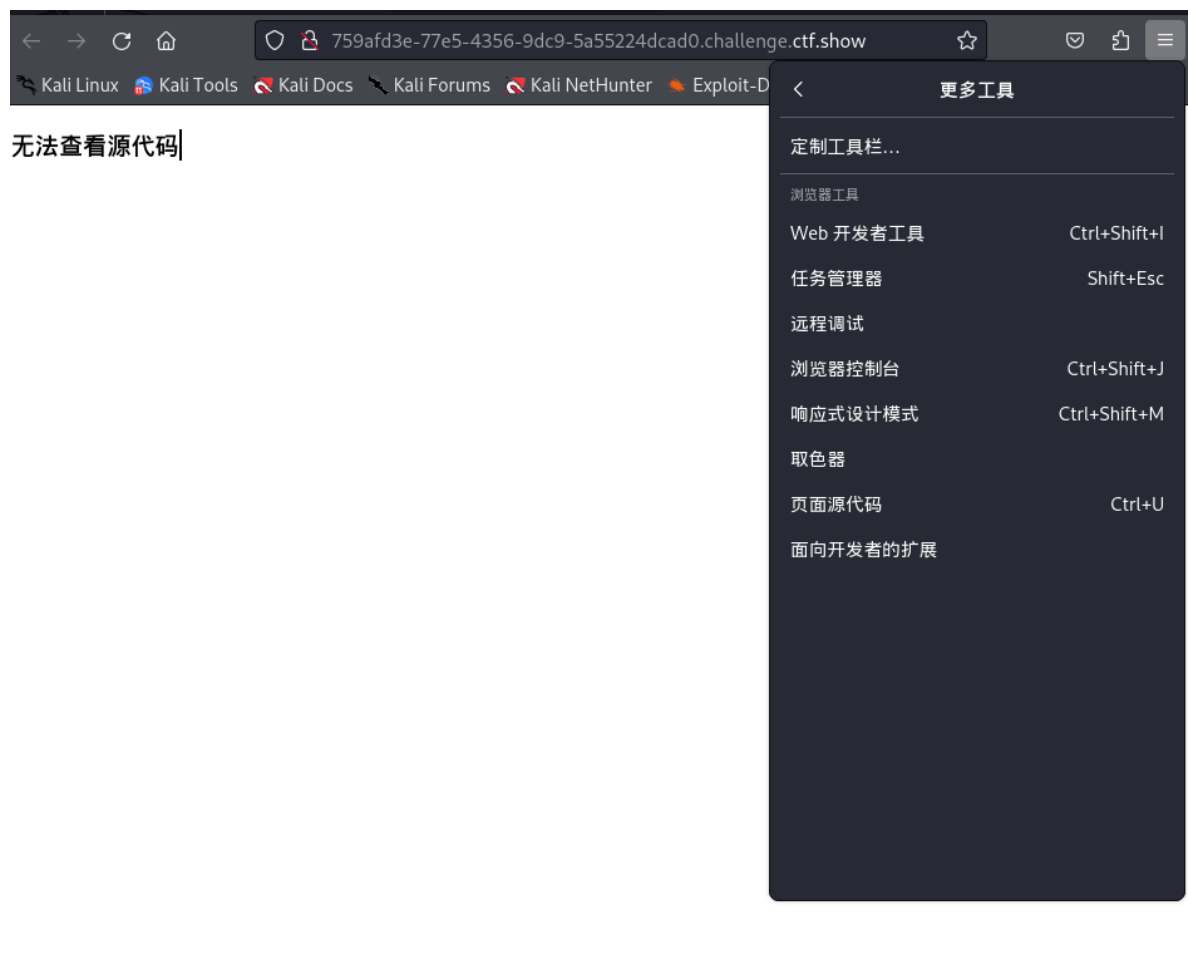
```
<!--  
# -*- coding: utf-8 -*- # @Author: hlxa # @Date: 2020-09-01 13:45:32 # @Last Modified by: hlxa # @Last Modified time:  
2020-09-02 03:12:48 # @email: hlxa@ctfer.com # @link: https://ctfer.com  
-->  
<!DOCTYPE html>  
<html>  
  <head></head>  
  <body>  
    <h3>web1:where is flag?</h3>  
    <!-- ctfshow{eb6fbe89-7dae-4a99-93b0-b0e8d9d15cc3}-->  
  </body>  
</html>
```

html > body

发现flag

web2

进去发现F12和右键被禁用，



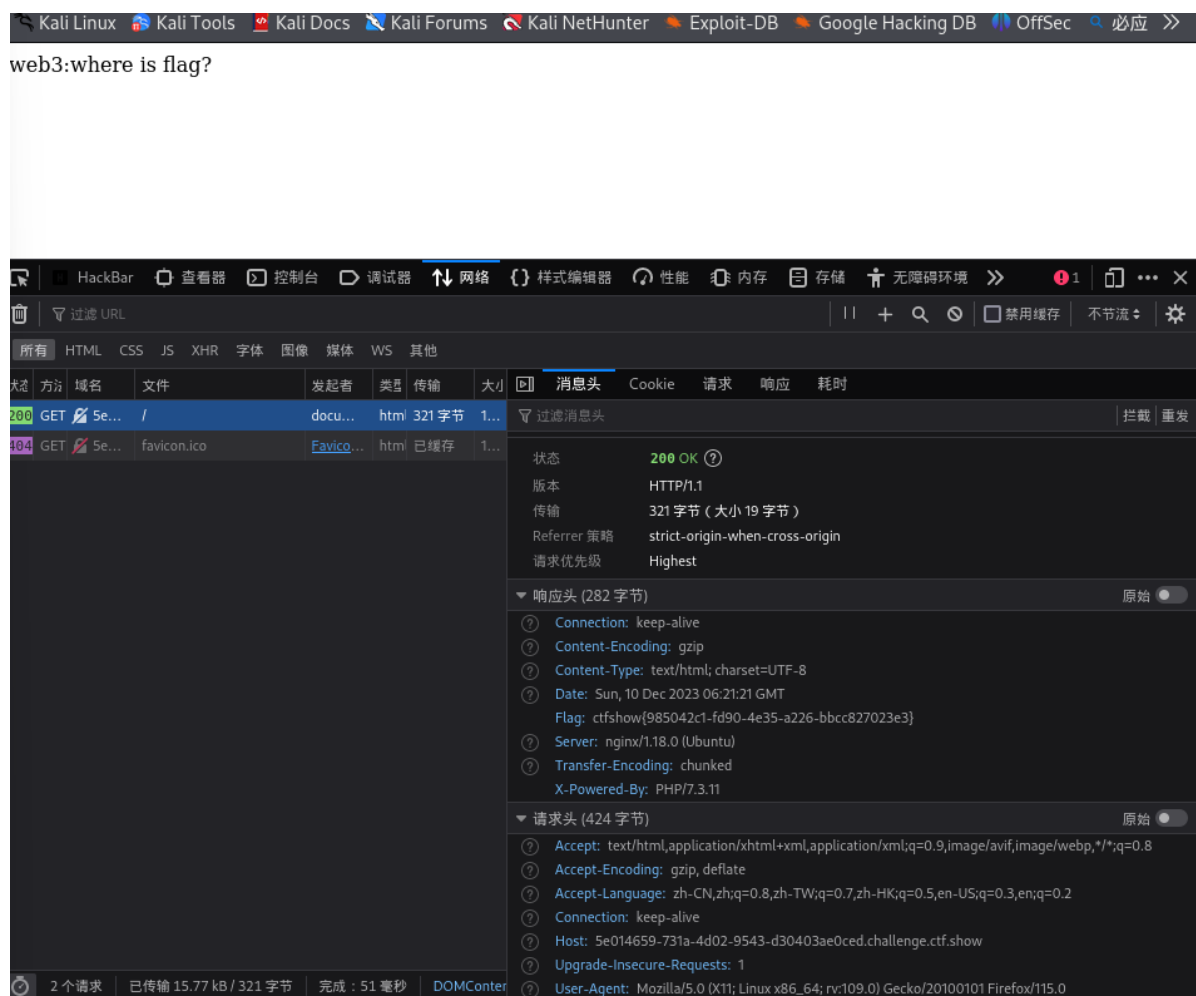
在火狐浏览器中，可以打开应用程序菜单>更多工具>页面源代码（或者直接快捷键ctrl+u），查看源代码

```
11
12 <!DOCTYPE HTML>
13 <html>
14 <head>
15 <meta charset="utf-8">
16 <title>CTFshow 新手入门题目 </title>
17 <script type="text/javascript">
18   window.oncontextmenu = function(){return false};
19   window.onselectstart = function(){return false};
20   window.onkeydown = function(){if (event.keyCode==123){event.keyCode=0;event.returnValue=false}
21 </script>
22 </head>
23 <body>
24   <h3>无法查看源代码</h3>
25   <!-- ctfshow{ac741438-f970-4741-8425-80c7a3f5af97} -->
26 </body>
27 </html>
```

获得flag

web3

题目提示可以抓包，可以是浏览器工具进行查看请求包



在响应头中发现flag

web4

题目提示了robots,

如何判断是robots.txt

1) dirsearch扫描一下网站

```

(kali㉿kali)-[~]
$ dirsearch -u http://9ec9891a-f61a-49b4-b051-103128cab1ce.challenge.ctf.sh
OW
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/lat
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_9ec9891a-f61a-49b4-b051-103128cab1ce.cha
llenge.ctf.show/_23-12-10_14-34-21.txt

Target: http://9ec9891a-f61a-49b4-b051-103128cab1ce.challenge.ctf.show/

[14:34:21] Starting:
[14:34:43] 200 - 40B - /robots.txt

Task Completed

```

扫描得到/robots.txt

2) 题做得多了就可以判断出robots.txt

```

User-agent: *
Disallow: /flagishere.txt

```

HackBar 查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 ... X

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL ENCODING

URL

http://9ec9891a-f61a-49b4-b051-103128cab1ce.challenge.ctf.show/robots.txt|

输入后，提示一个地址/flagishere.txt

跟进去看看

```

ctfshow{48787d8c-6dd2-4f6f-a0cc-366c98e0b25e}

```

HackBar 查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL

URL

http://9ec9891a-f61a-49b4-b051-103128cab1ce.challenge.ctf.show/flagishere.txt

得到flag

web5

dirsearch简单扫一下没扫到

题目提示phps源码泄露

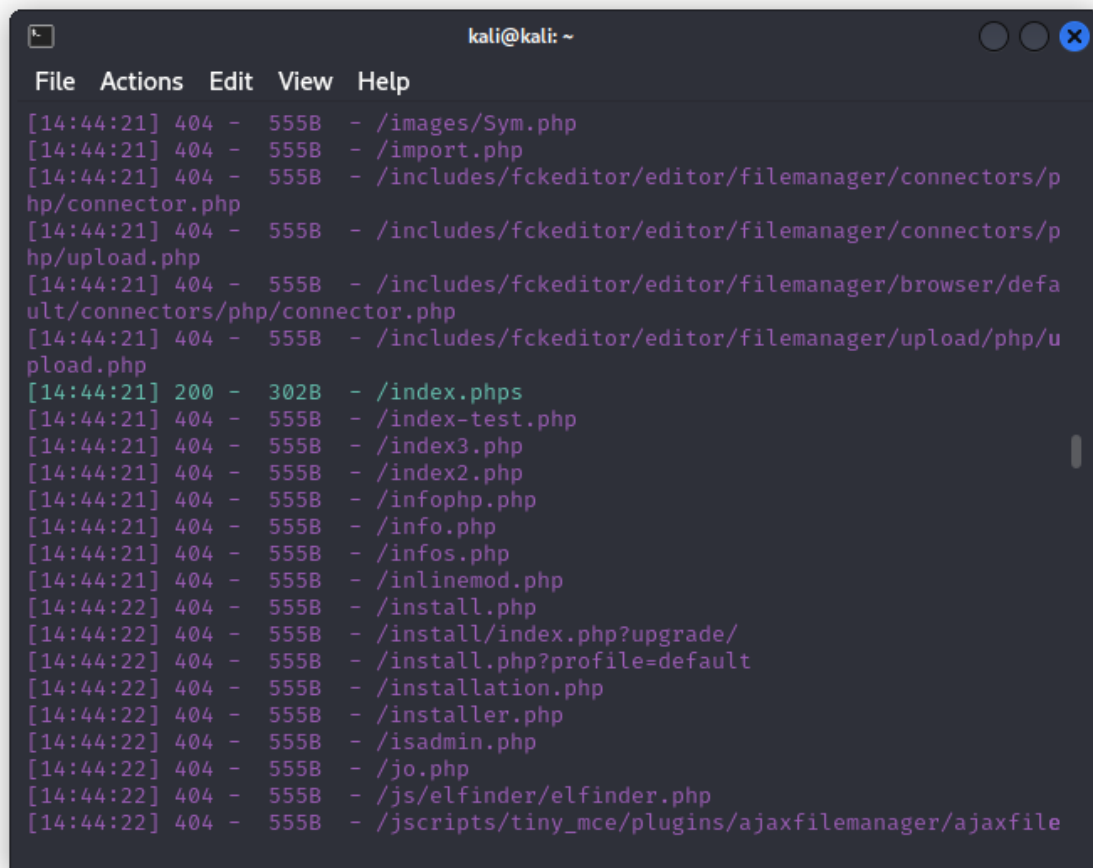
有关源码泄露的知识在下面博客

<https://www.cnblogs.com/Lmg66/p/13598803.html>

于是针对性的扫描一下phps

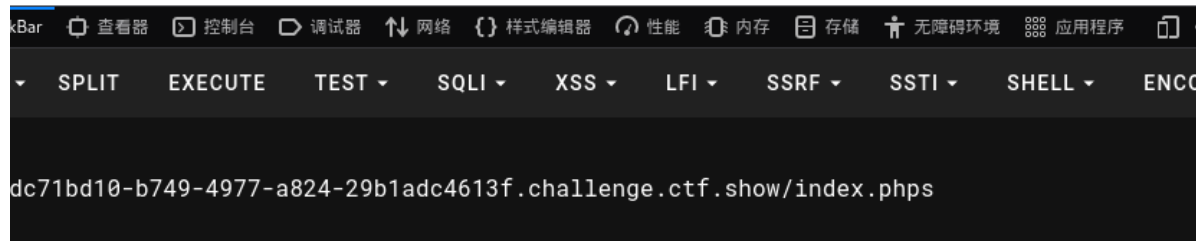
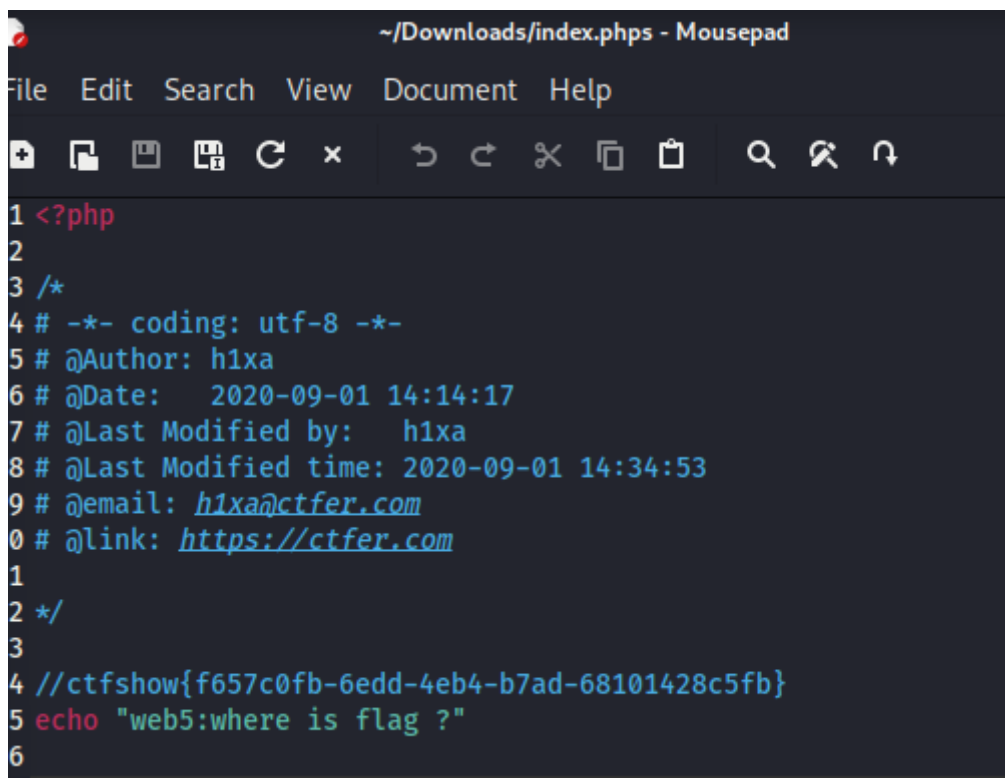
```
dirsearch -u <URL> -e <phps>
```

flag ?



```
kali@kali: ~  
File Actions Edit View Help  
[14:44:21] 404 - 555B - /images/Sym.php  
[14:44:21] 404 - 555B - /import.php  
[14:44:21] 404 - 555B - /includes/fckeditor/editor/filemanager/connectors/p  
hp/connector.php  
[14:44:21] 404 - 555B - /includes/fckeditor/editor/filemanager/connectors/p  
hp/upload.php  
[14:44:21] 404 - 555B - /includes/fckeditor/editor/filemanager/browser/defa  
ult/connectors/php/connector.php  
[14:44:21] 404 - 555B - /includes/fckeditor/editor/filemanager/upload/php/u  
pload.php  
[14:44:21] 200 - 302B - /index.php  
[14:44:21] 404 - 555B - /index-test.php  
[14:44:21] 404 - 555B - /index3.php  
[14:44:21] 404 - 555B - /index2.php  
[14:44:21] 404 - 555B - /info.php.php  
[14:44:21] 404 - 555B - /info.php  
[14:44:21] 404 - 555B - /infos.php  
[14:44:21] 404 - 555B - /inlinemod.php  
[14:44:22] 404 - 555B - /install.php  
[14:44:22] 404 - 555B - /install/index.php?upgrade/  
[14:44:22] 404 - 555B - /install.php?profile=default  
[14:44:22] 404 - 555B - /installation.php  
[14:44:22] 404 - 555B - /installer.php  
[14:44:22] 404 - 555B - /isadmin.php  
[14:44:22] 404 - 555B - /jo.php  
[14:44:22] 404 - 555B - /js/elfinder/elfinder.php  
[14:44:22] 404 - 555B - /jscripts/tiny_mce/plugins/ajaxfilemanager/ajaxfile
```

发现/index.php

[打开查看](#)

发现flag

老规矩扫描一下

```
(kali㉿kali)-[~]
$ dirsearch -u http://1dcfca2b-8e23-447d-8aee-64ec4019fb6a.challenge.ctf.show/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_1dcfca2b-8e23-447d-8aee-64ec4019fb6a.challenge.ctf.show/__23-12-10_14-51-45.txt

Target: http://1dcfca2b-8e23-447d-8aee-64ec4019fb6a.challenge.ctf.show/

[14:51:45] Starting:
[14:52:13] 200 - 486B - /www.zip

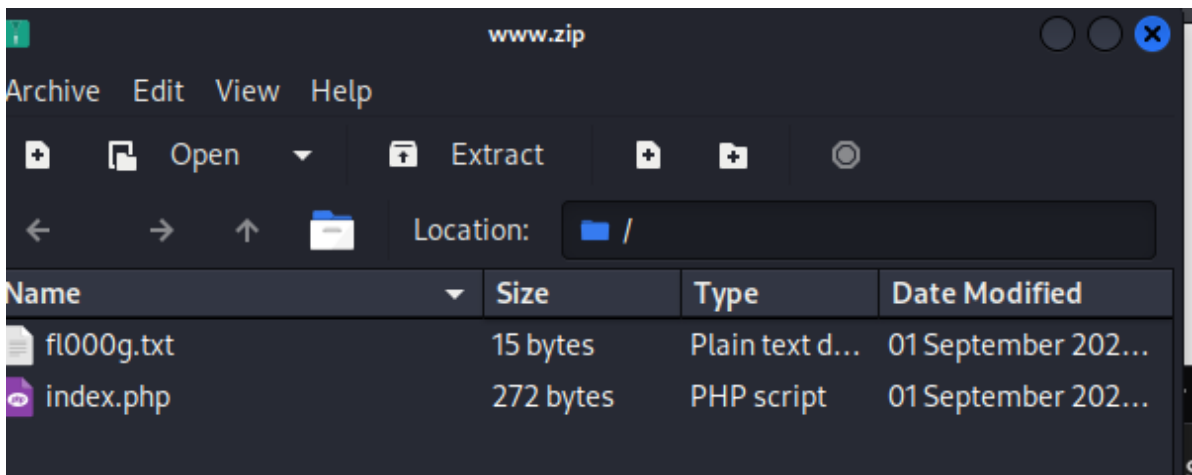
Task Completed
```

发现/www.zip,



下载www.zip,并打开查看

发现目录下两个文件



分别查看

index.php

```
~/.cache/fr-xfuaHU/index.php - Mousepad
File Edit Search View Document Help
[Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1 |<?php
2
3 /*
4 # -*- coding: utf-8 -*-
5 # @Author: h1xa
6 # @Date: 2020-09-01 14:37:13
7 # @Last Modified by: h1xa
8 # @Last Modified time: 2020-09-01 14:42:44
9 # @email: h1xa@ctfer.com
10 # @link: https://ctfer.com
11
12 */
13 //flag in fl000g.txt
14 echo "web6:where is flag?"
15 ?>
```

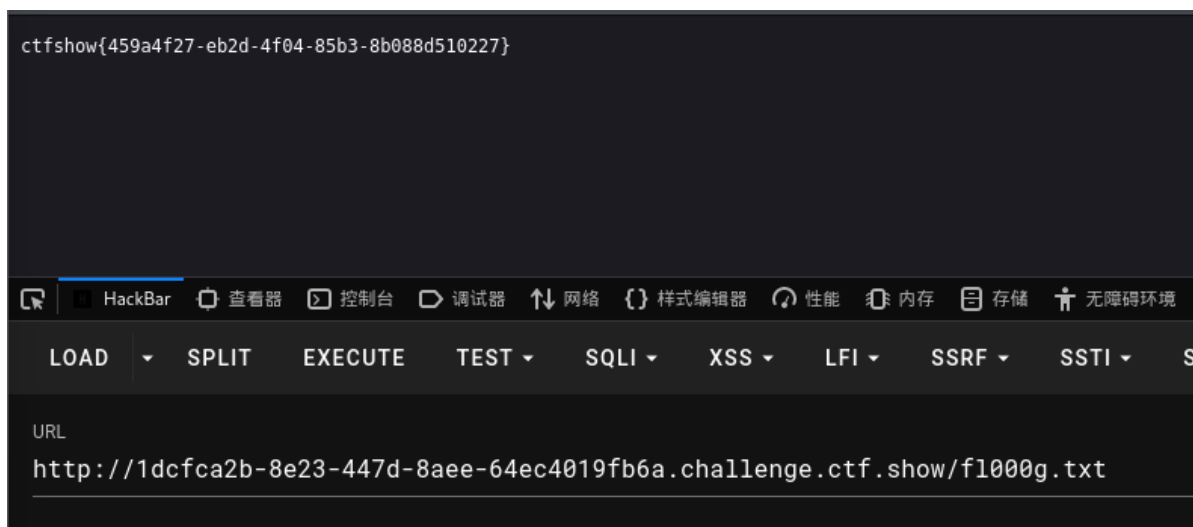
提示flag in fl000g.txt

打开fl000g.txt

发现flag{flag_here}

但是不是规定的格式，尝试提交一下，果然不对

猜测fl000g.txt可以在网站里打开，果然



得到flag

web7

扫一下


```
[15:13:17] Starting:
[15:13:18] 200 - 46B - /.git/
[15:13:18] 301 - 169B - /.git → http://d4c1c44d-74ee-45a3-90a8-da9da1a8a
410.challenge.ctf.show/.git/
##### 1 75% 8666/11460 383/s jcb:1/1 errors:0
```

发现/.git/

[进入查看](#)

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking

发现flag

web8

一个字。扫！

发现/.svn

```
L$ dirsearch -u http://edf9cfc5-e24b-4eb7-9454-ffb940ea5029.challenge.ctf.show/
```

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:  
pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html  
from pkg_resources import DistributionNotFound, VersionConflict
```

```
chir_ (ZCII-(I) v0.4.3
```

Extensions: php, aspx, jsp, html, js | **HTTP method:** GET | **Threads:** 25
Wordlist size: 11460

Output File: /home/kali/reports/http_edf9cfc5-e24b-4eb7-9454-ffb940ea5029.challenge.ctf.show/__23-12-10_15-16-53.txt

Target: http://edf9cfc5-e24b-4eb7-9454-ffb940ea5029.challenge.ctf.show/

[15:16:53] Starting:
[15:16:57] 301 - 169B - /.svn → http://edf9cfc5-e24b-4eb7-9454-ffb940ea5029.challenge.ctf.show/.svn/
[15:16:57] 200 - 46B - /.svn/

进入看一下

```
ctfshow{f630b049-99f5-4c2f-bcfc-f63fdc7401f9}
```



发现flag

web9

插入一个知识点关于vim

vim缓存泄露，在使用vim进行编辑时，会产生缓存文件，操作正常，则会删除缓存文件，如果意外退出，缓存文件保留下来，这时可以通过缓存文件来得到原文件，以index.php来说，第一次退出后，缓存文件名为.index.php.swp，第二次退出后，缓存文件名为.index.php.swo，第三次退出后文件名为.index.php.swn

这个可以利用dirsearch用字典扫出来

但是我不会（等我写完wp再说）

//因为字典里没有.php.swp所以扫描不到

字典加入后，可以扫到

```
(root@kali)~[~]
# dirsearch -u http://d1b590e5-c8a4-4dc6-b00b-5f753c9fc672.challenge.ctf.sh
ow/ -e*
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/lat
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

dirsearch v0.4.3

Extensions: php, jsp, asp, aspx, do, action, cgi, html, htm, js, tar.gz
HTTP method: GET | Threads: 25 | Wordlist size: 14597

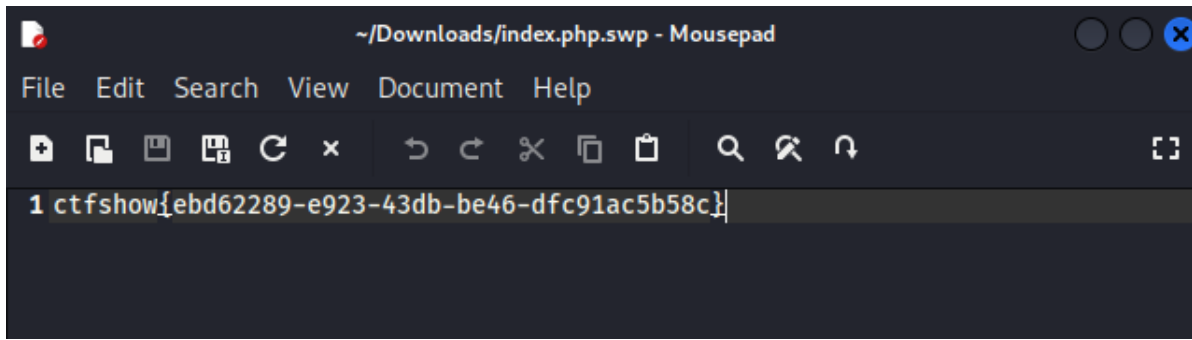
Output File: /root/reports/http_d1b590e5-c8a4-4dc6-b00b-5f753c9fc672.challeng
e.ctf.show/__23-12-10_18-00-11.txt

Target: http://d1b590e5-c8a4-4dc6-b00b-5f753c9fc672.challenge.ctf.show/

[18:00:11] Starting:
[18:00:31] 200 - 45B - /index.php.swp
```

所以我是猜到可能是index产生的缓存文件，猜测出index.php.swp

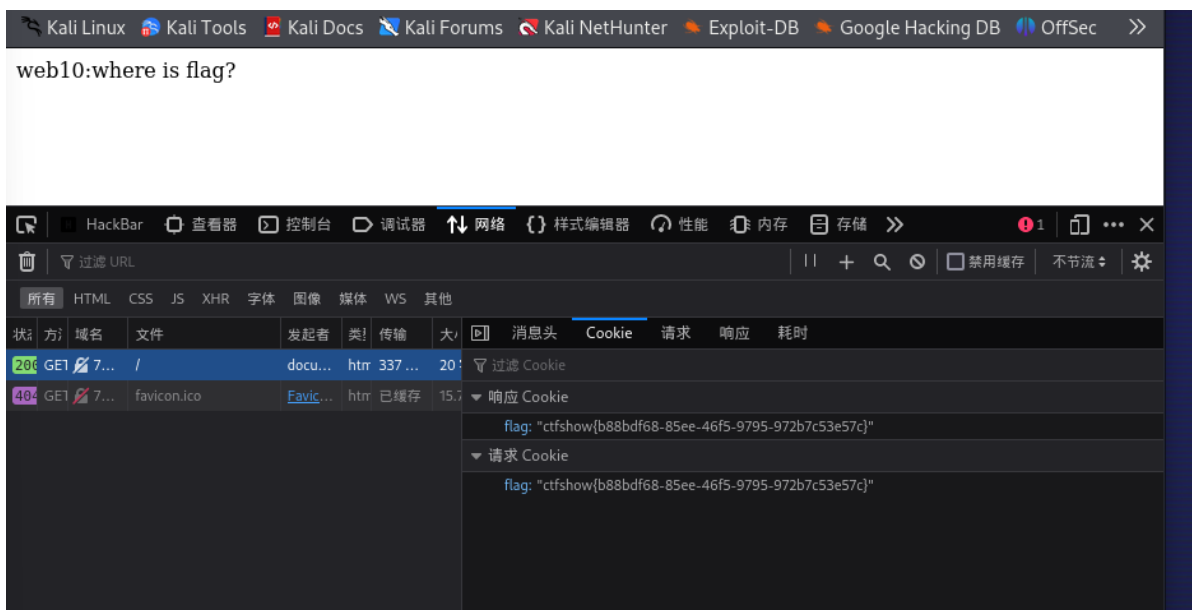
进入后下载打开



得到flag

web10

根据提示，查看cookie



发现flag

*web11

未做到

web12

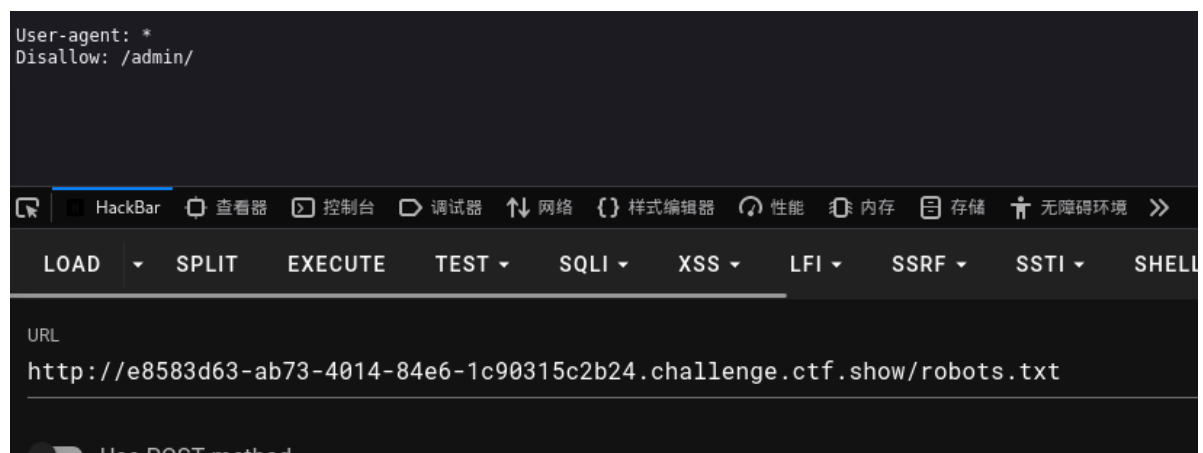
扫

```
extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_e8583d63-ab73-4014-84e6-1c90315c2b24.ch
allenge.ctf.show/__23-12-10_16-21-17.txt

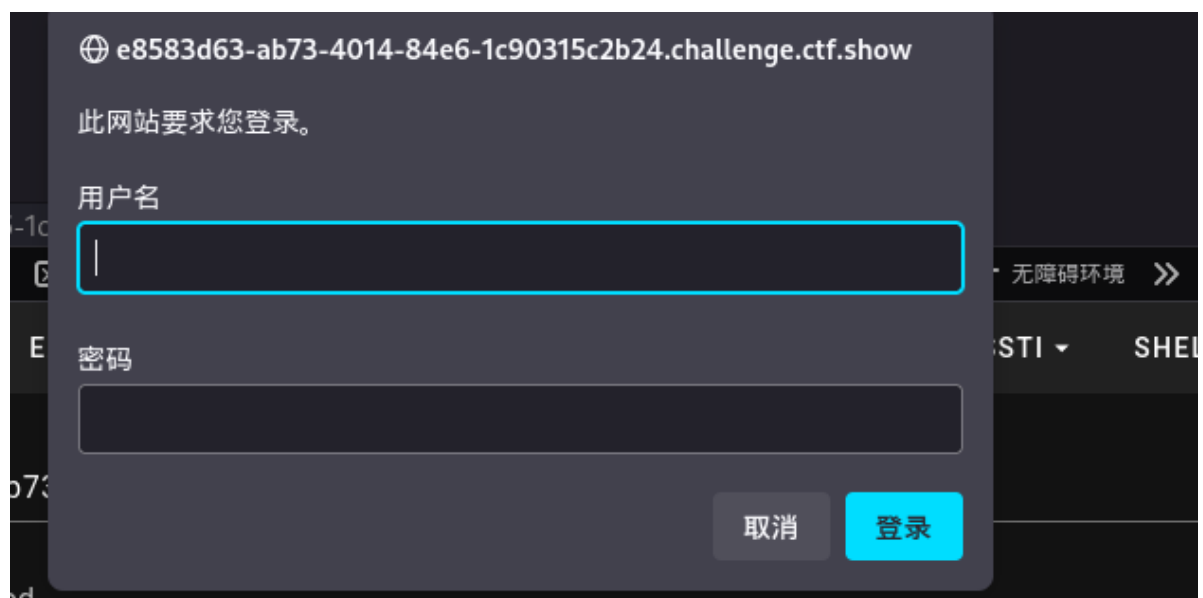
Target: http://e8583d63-ab73-4014-84e6-1c90315c2b24.challenge.ctf.show/
e8583d63-ab73-4014-84e6-1c90315c2b24.challenge.ctf.show/robots.txt
[16:21:17] Starting:
[16:21:19] 301 - 169B - /js → http://e8583d63-ab73-4014-84e6-1c90315c2b
24.challenge.ctf.show/js/
[16:21:24] 301 - 169B - /admin -> http://e8583d63-ab73-4014-84e6-1c90315
2b24.challenge.ctf.show/admin/
[16:21:24] 401 - 42B - /admin/
[16:21:24] 401 - 42B - /admin/index.php
[16:21:30] 301 - 169B - /css → http://e8583d63-ab73-4014-84e6-1c90315c2
24.challenge.ctf.show/css/
[16:21:32] 301 - 169B - /fonts → http://e8583d63-ab73-4014-84e6-1c90315
2b24.challenge.ctf.show/fonts/
[16:21:33] 301 - 169B - /images → http://e8583d63-ab73-4014-84e6-1c9031
5c2b24.challenge.ctf.show/images/
[16:21:33] 403 - 555B - /images/
[16:21:34] 403 - 555B - /js/
[16:21:41] 200 - 32B - /robots.txt
```

打开robots.txt



提示admin

打开



猜测用户名admin

寻找密码

题目提示

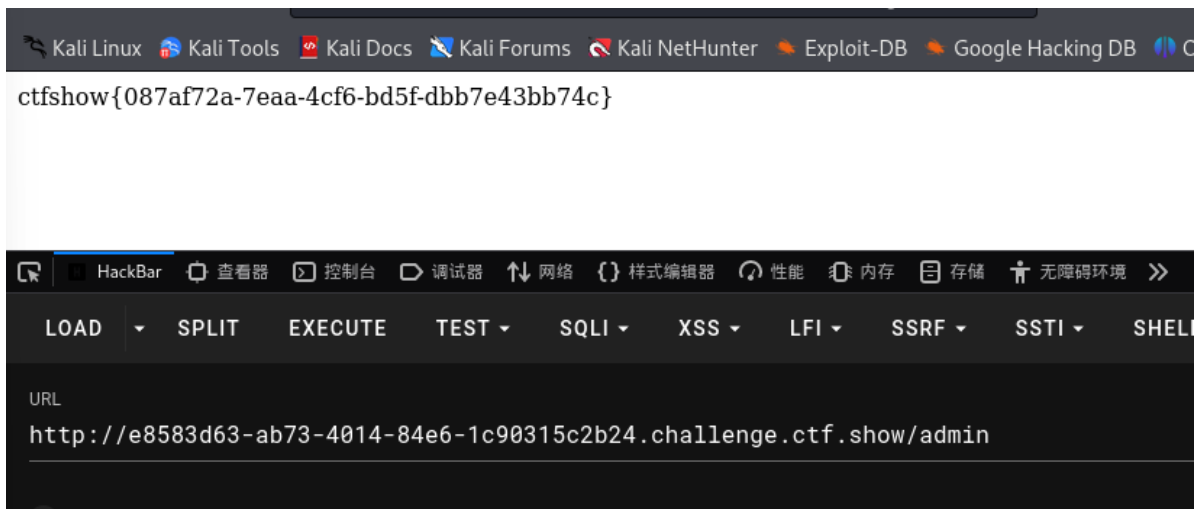
有时候网站上的公开信息，就是管理员常用密码

查看网页信息

Help Line Number : 372619038

发现一串数字

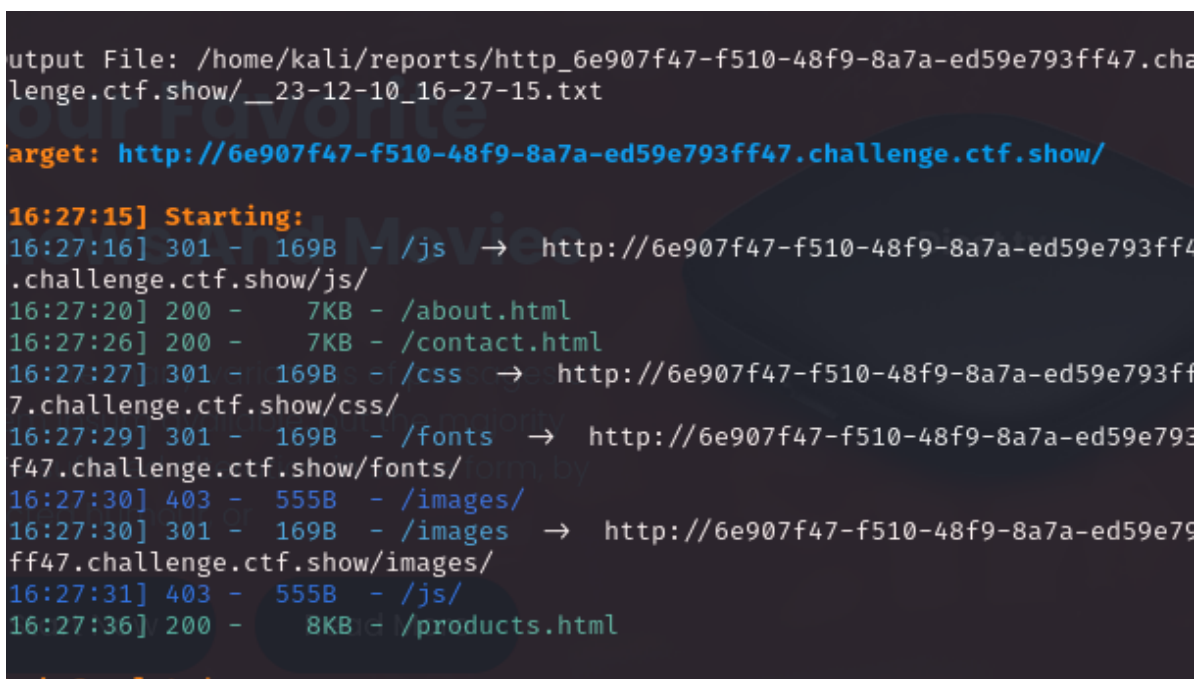
试一下，登陆成功



发现flag

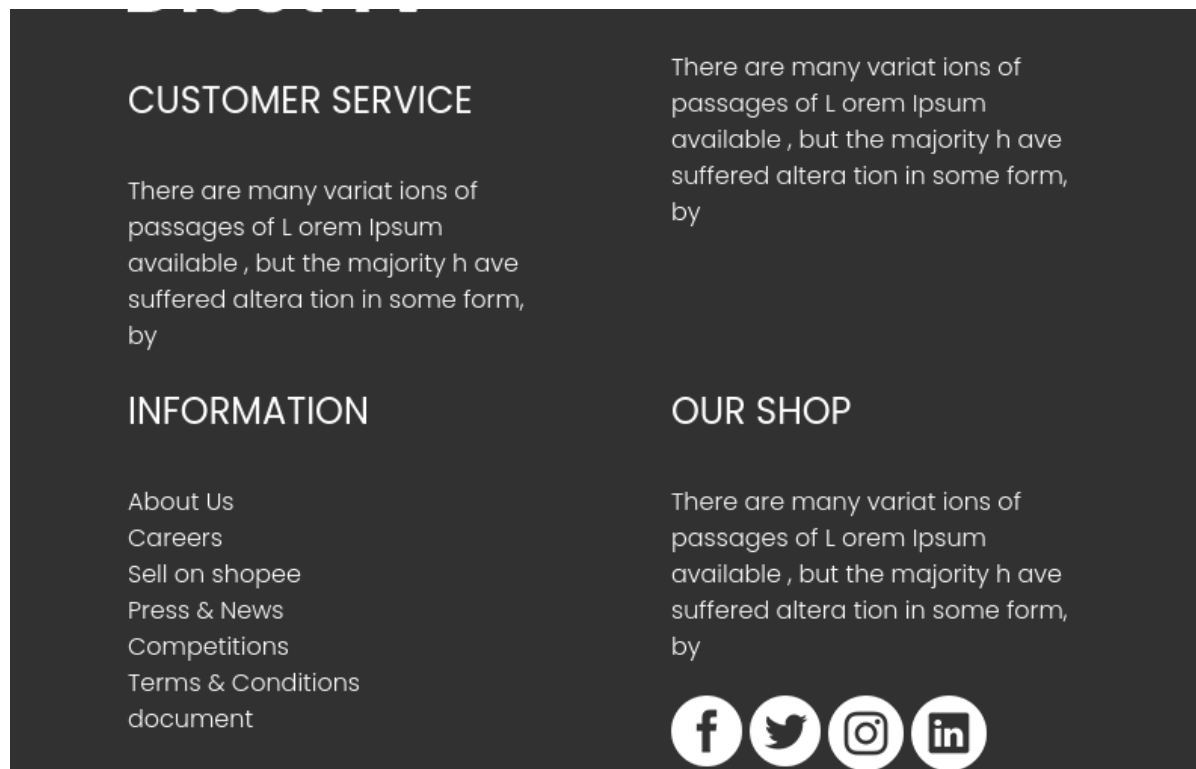
web13

s



发现几个可疑网站，打开未发现有用线索

检查网站



发现document可以点进去

● 登陆

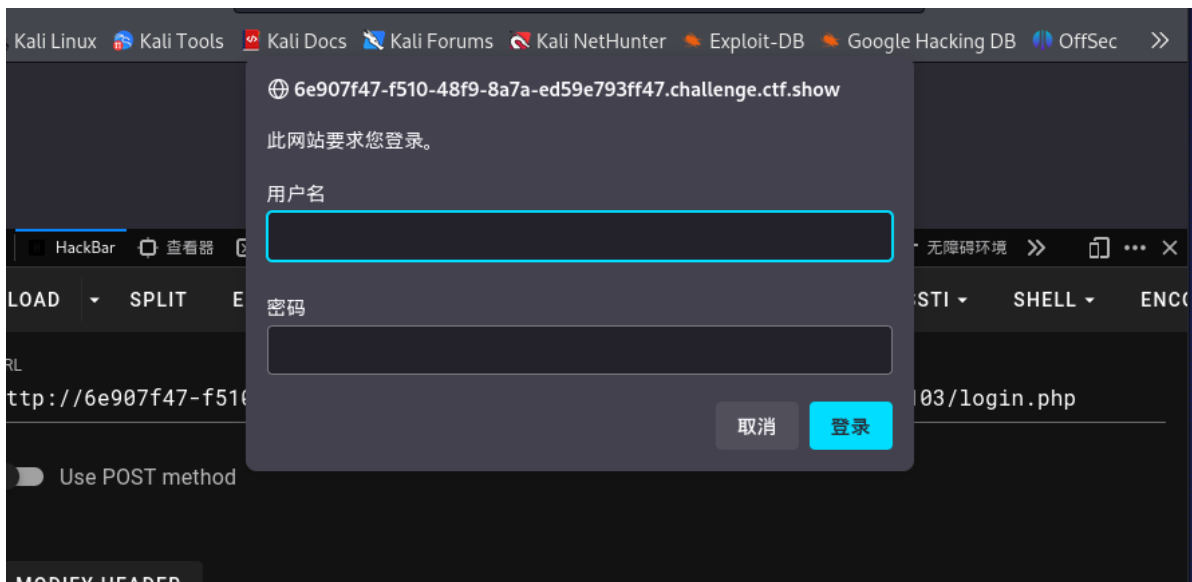
默认后台地址: <http://your-domain/system1103/login.php>

默认用户名: admin

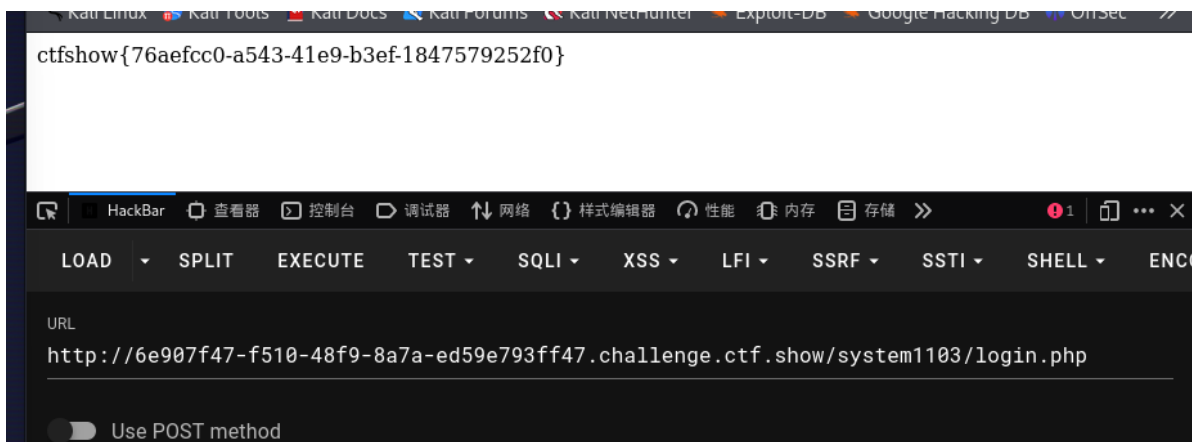
默认密码: admin1103

在文档末尾发现线索

尝试进行登录



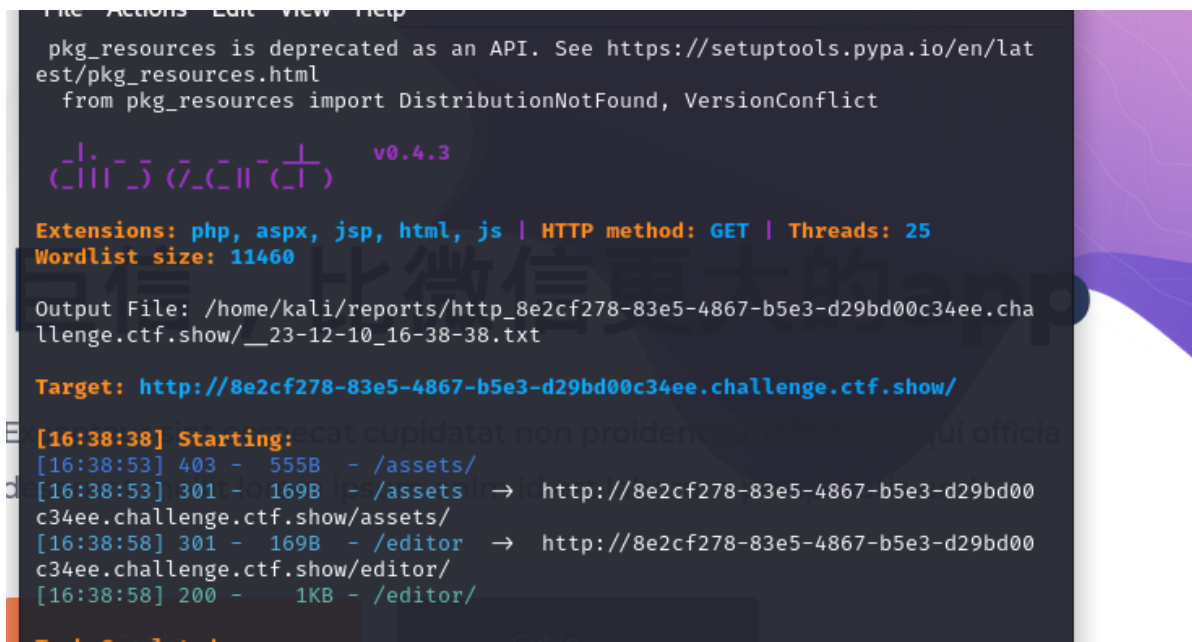
登陆成功



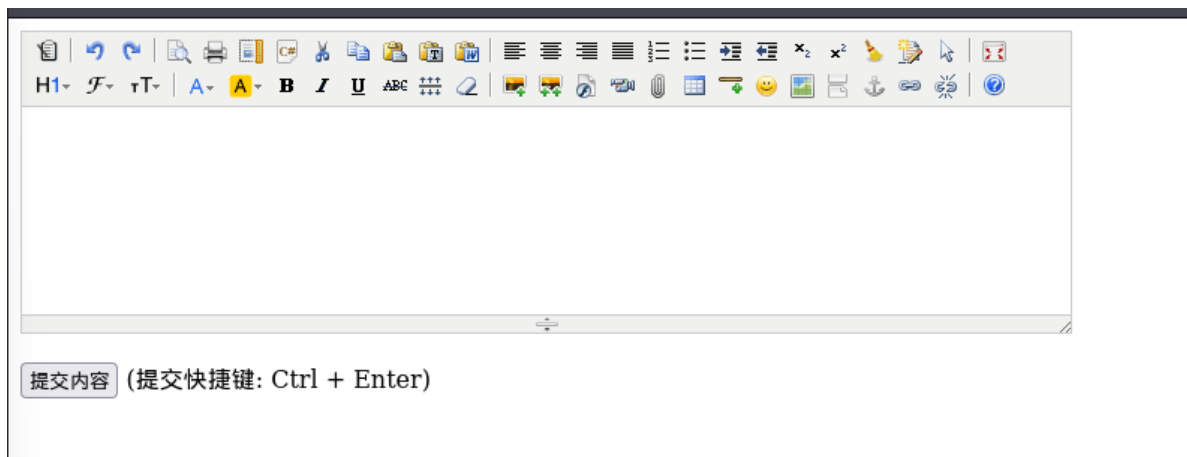
获得flag

web14

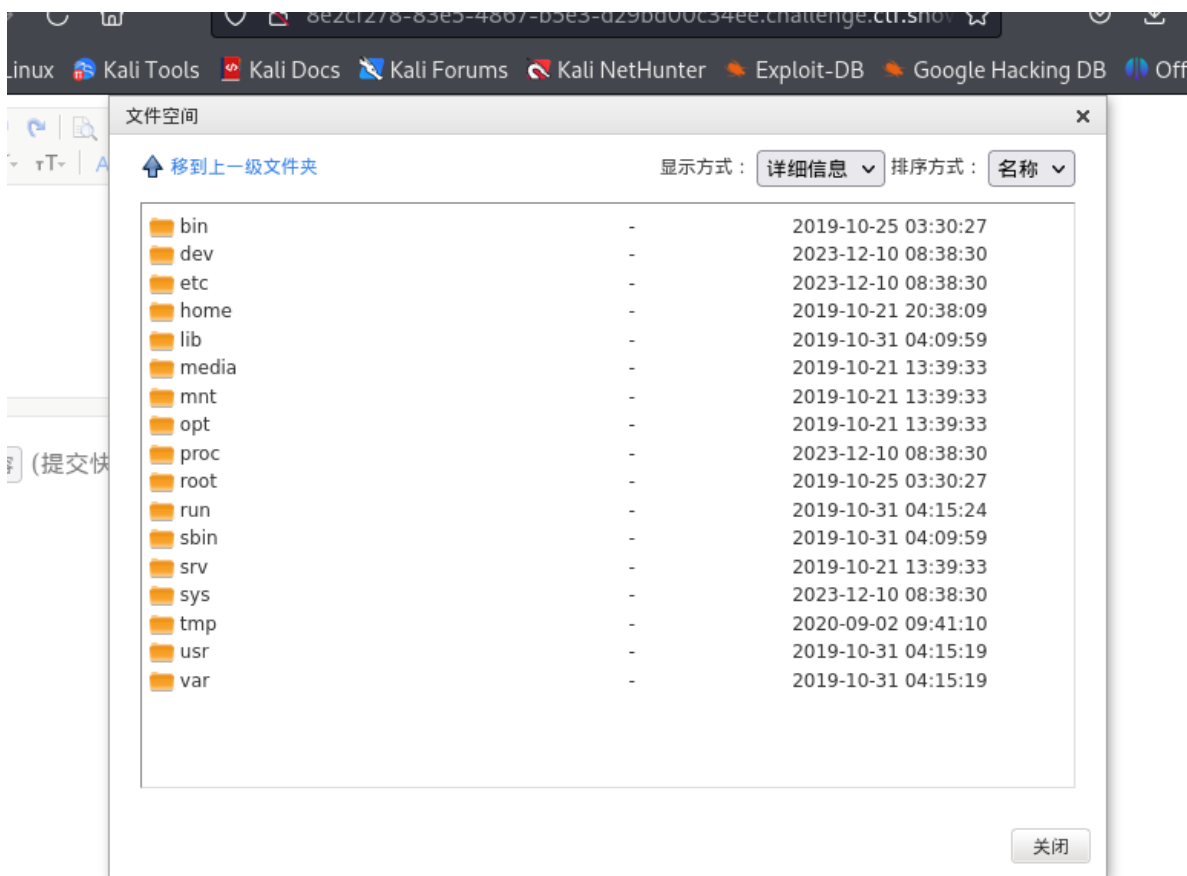
猜猜我要干啥



惊喜, 进入/editor看看

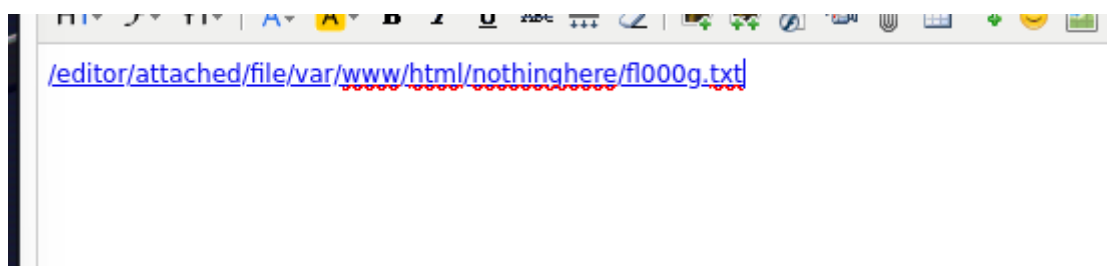


文件上传? 不能够啊, 研究一下

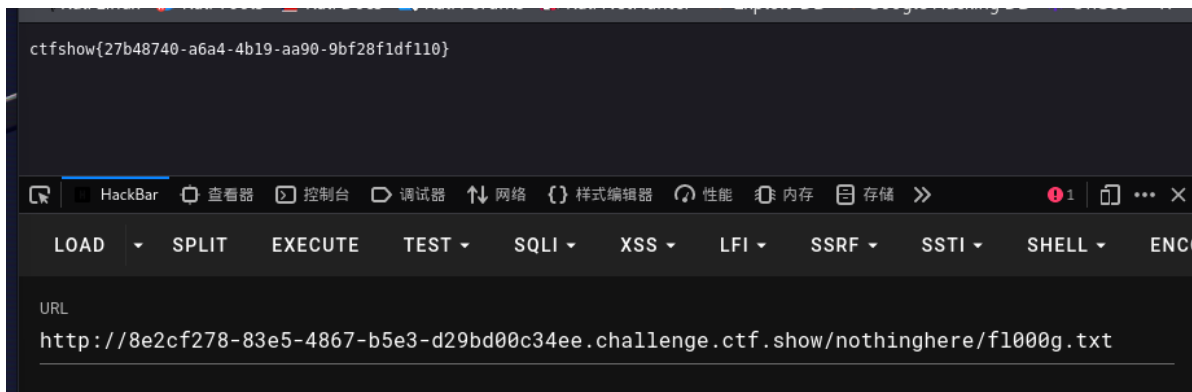


发现文件空间

检查一下



发现fl000g.txt想办法打开

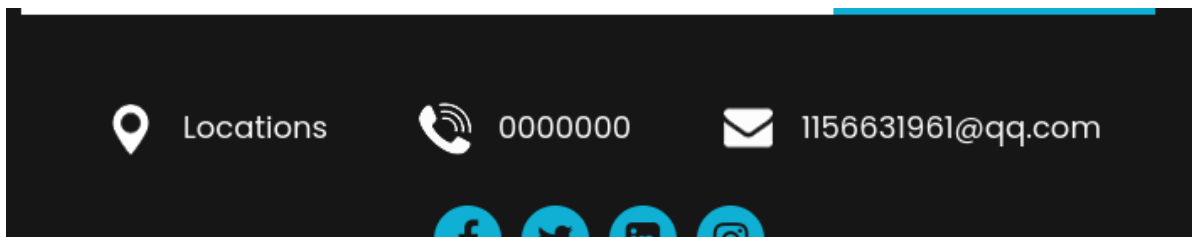


得到flag

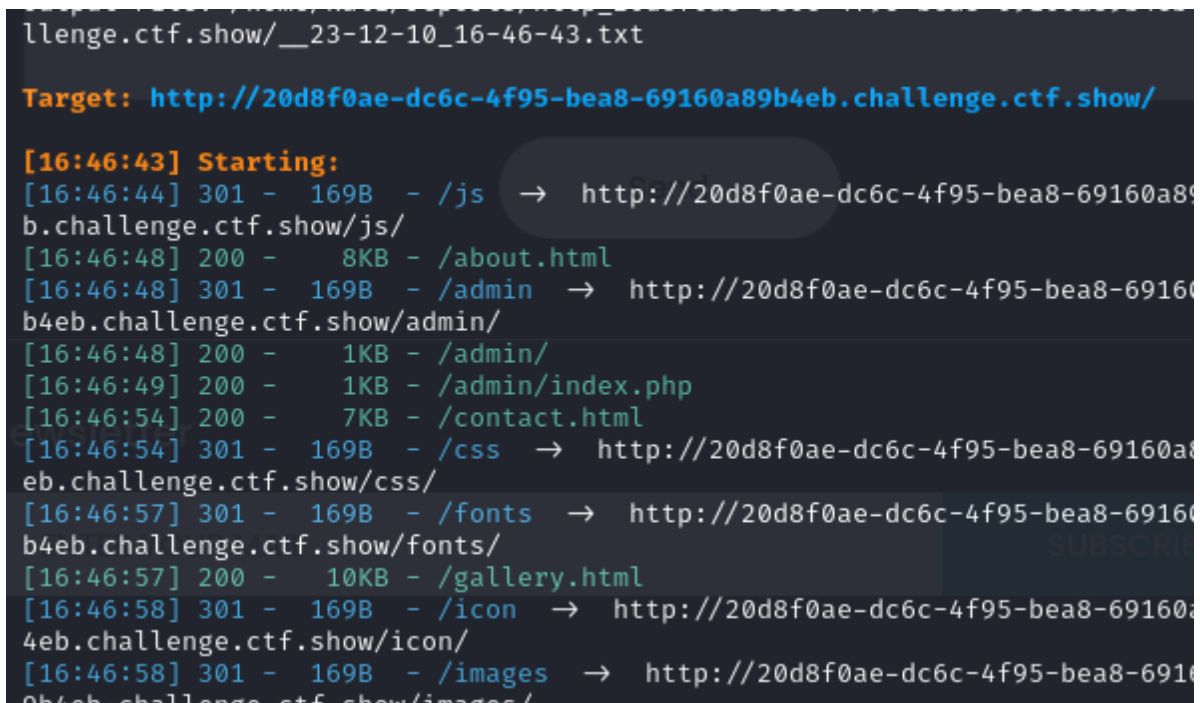
web15

检查网站

发现疑似有用信息1156631961@qq.com



S



发现登陆界面

进去看看

后台登录系统

admin

密码

 此连接不安全。在此页面输入的登录信息可以被窃取。详细了解

登录

忘记密码

密码？忘记密码看看

忘记密码

我的所在地是哪个城市？

密保答案

提交

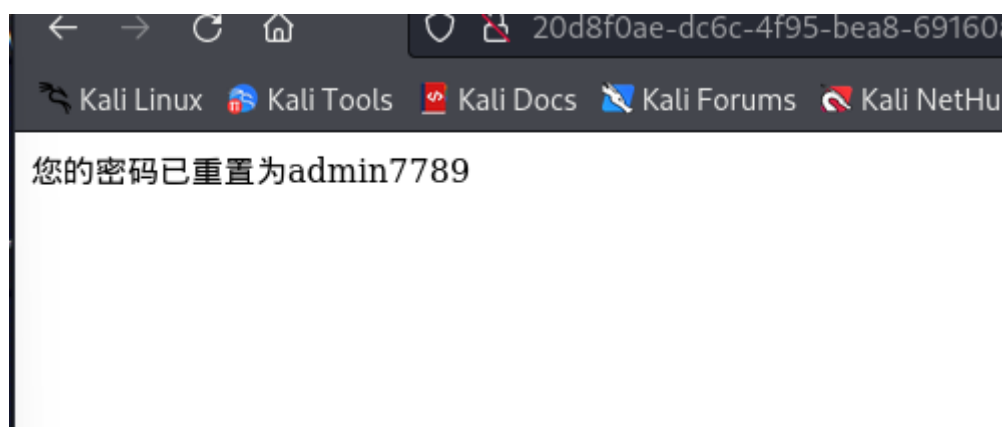
返回登陆

你在哪个城市？根据我天狗的经验，qq号可以看位置*（电脑端看不到，手机端可以）

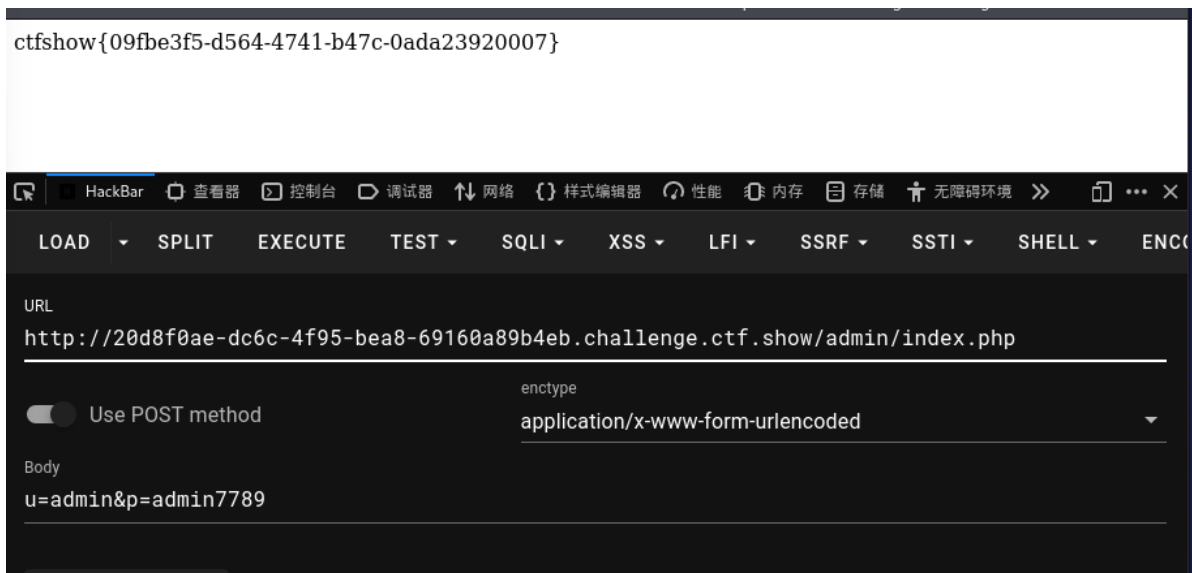


发现在西安

提交后，密码被重置



登陆试试



获得flag

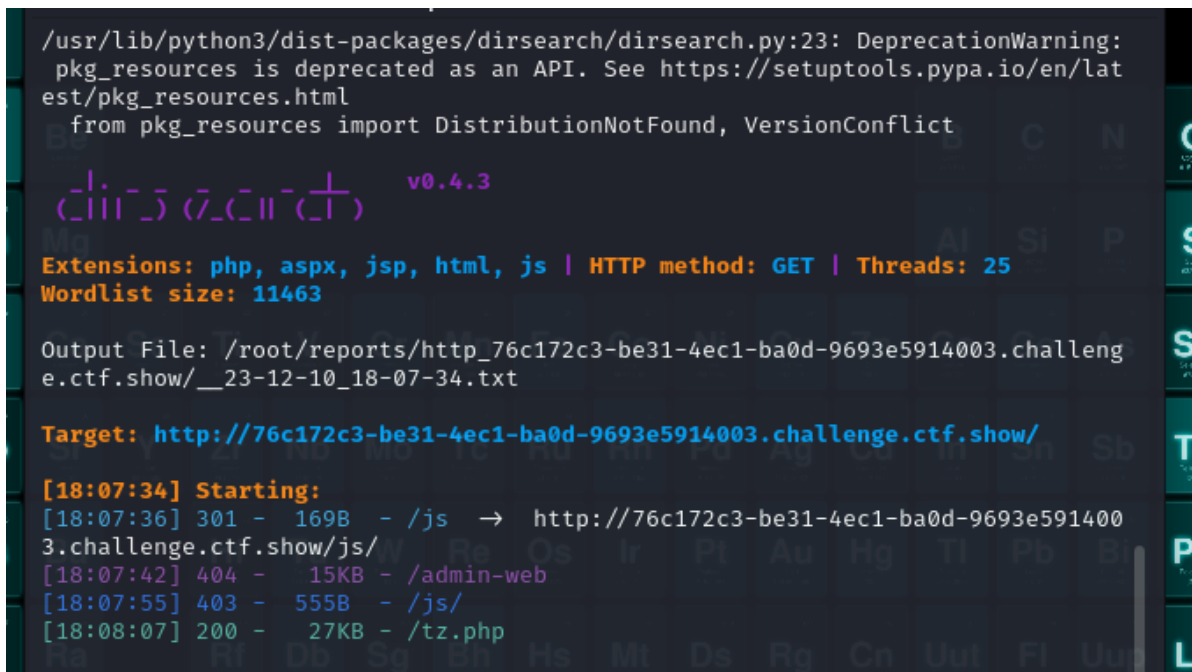
web16

题目中提到探针了解一下先

[\[php探针存在xss漏洞_php探针漏洞-CSDN博客\]](#)

提到探针格式为tz.php

用dirsearch没扫出来（和web9一样，字典里没有，加入后也可以扫到）



用御剑扫出来了、



进入tz.php看一下

PHP已编译模块检测		
Core date libxml openssl pcre sqlite3 zlib ctype curl dom fil hash iconv json mbstring SPL PDO pdo_sqlite session posix read Phar tokenizer xml xmlreader xmlwriter mysqlnd cgi-fcgi mysqli		
PHP相关参数		
PHP信息 (phpinfo) :	PHPINFO	PHP版
PHP运行方式 :	FPM-FCGI	脚本占
PHP安全模式 (safe_mode) :	×	POST
上传文件最大限制 (upload_max_filesize) :	2M	浮点型
脚本超时时间 (max_execution_time) :	30秒	socket
PHP页面根目录 (doc_root) :	×	用户根
dl()函数 (enable_dl) :	×	指定包
显示错误信息 (display_errors) :	√	自定义
数据反斜杠转义 (magic_quotes_gpc) :	×	"<?...>
"<% %>"ASP风格标记 (asp_tags) :	×	忽略重
忽略重复的错误源 (ignore_repeated_source) :	×	报告内
自动字符串转义 (magic_quotes_gpc) :	×	外部字
打开远程文件 (allow_url_fopen) :	√	声明a
Cookie 支持 :	√	拼写格
高精度数学运算 (BCMath) :	×	PREL
PDF文档支持 :	×	SNMF
VMailMail邮件处理 :	×	Curl去

点开来PHPINFO

检索页面

PHP_SHA256	657cf6464bac28e9490c59c07a2cf7bb76c200f09cfadf6e44ea64e95fa01021
FLAG	ctfshow{61f08e51-ea07-4a9c-97fe-c5c71a45c5b8}
USER	www-data

flag ^ v 高亮全部(A) 区分大小写(C) 匹配变音符号(I) 全词匹配(W) 搜索

得到flag

web17

S

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_5a758586-9260-4d8a-b986-697f5db0bc3a.cha
llenge.ctf.show/__23-12-10_17-13-29.txt

Target: http://5a758586-9260-4d8a-b986-697f5db0bc3a.challenge.ctf.show/

[17:13:29] Starting:
[17:13:42] 200 - 934B - /backup.sql
[17:13:50] 301 - 185B - /images → http://5a758586-9260-4d8a-b986-697f5db
0bc3a.challenge.ctf.show/images/
[17:13:50] 403 - 571B - /images/

Task Completed
```

发现/.sql

进入看看



打开sql

```
21
22
23 INSERT INTO `ctfshow_secret` VALUES ('ctfshow{22da53a8-8582-4835-a883-
cd70cb5170fc}');
24
```

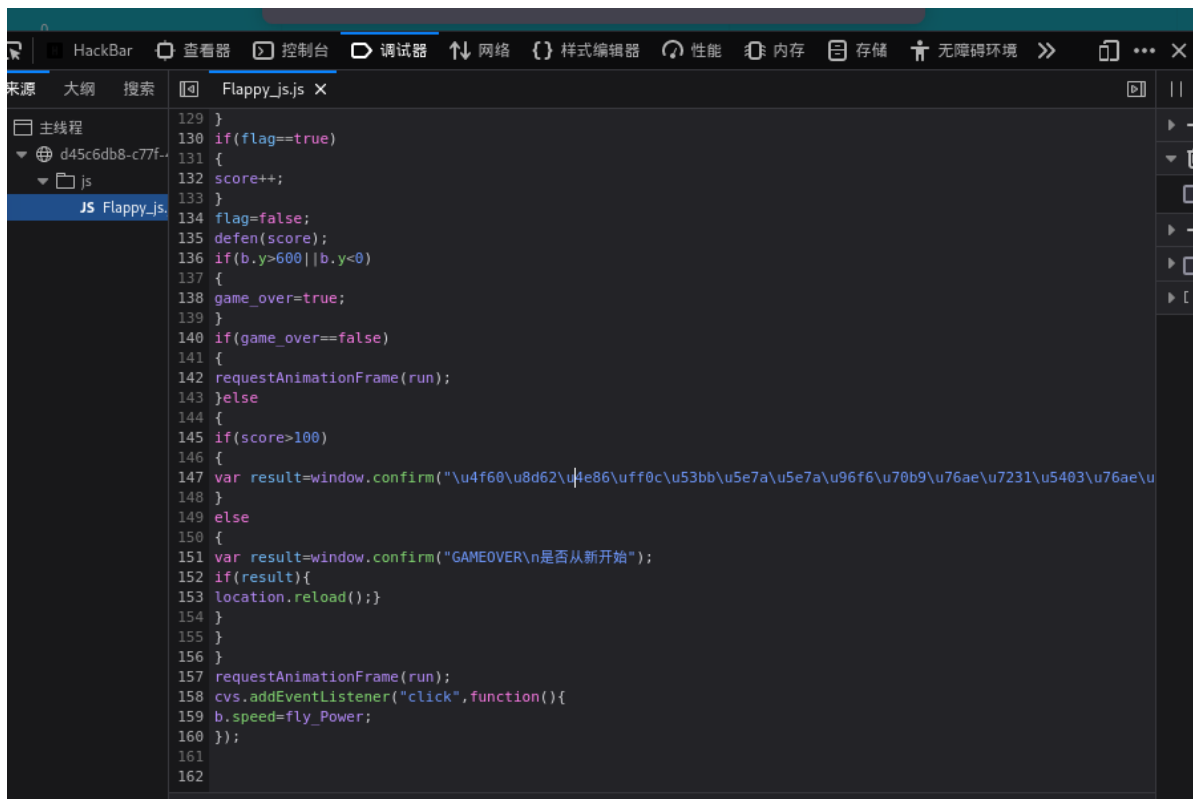
发现flag

web18

S

扫不出来

查看一下前端文件

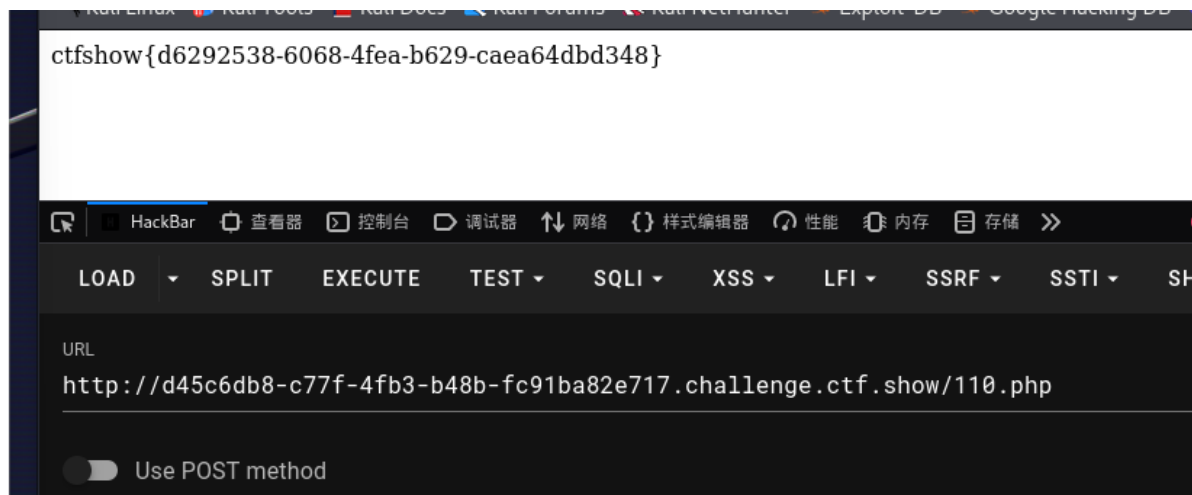


发现可疑信息

解码



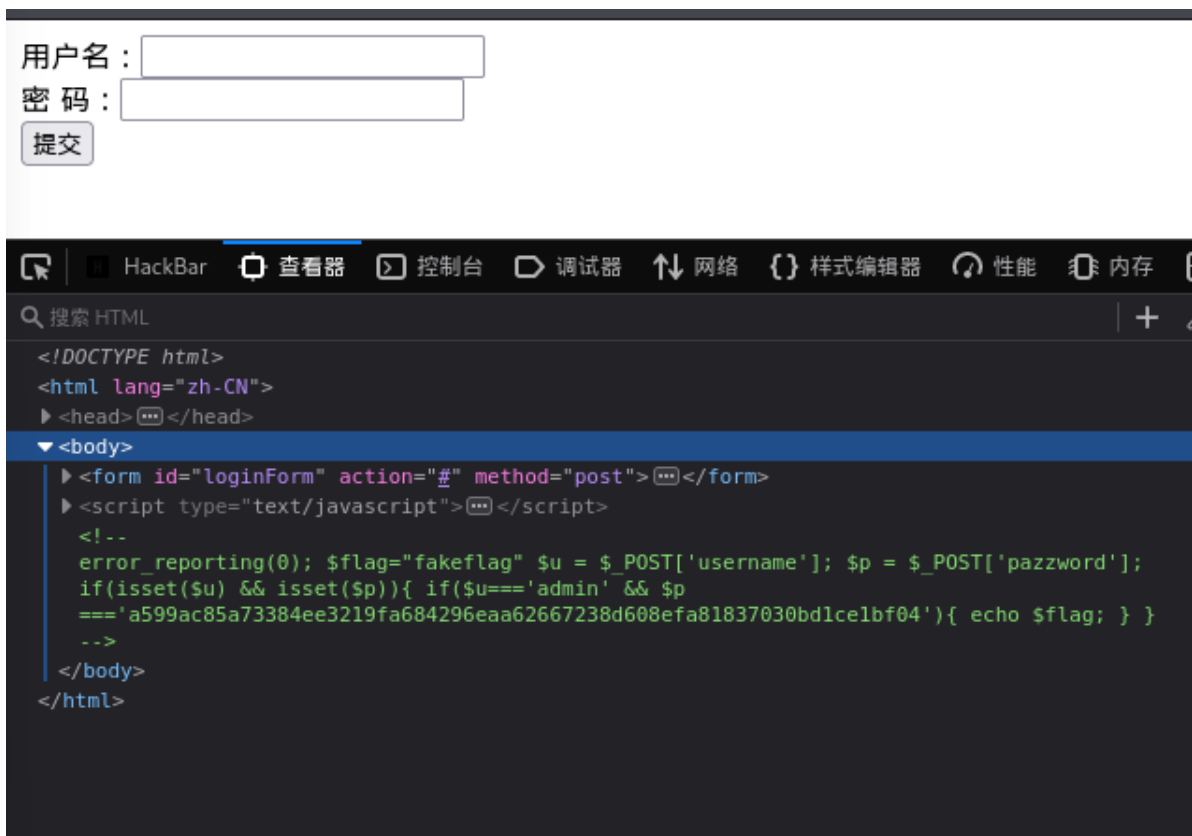
进入110.php



得到flag

web19

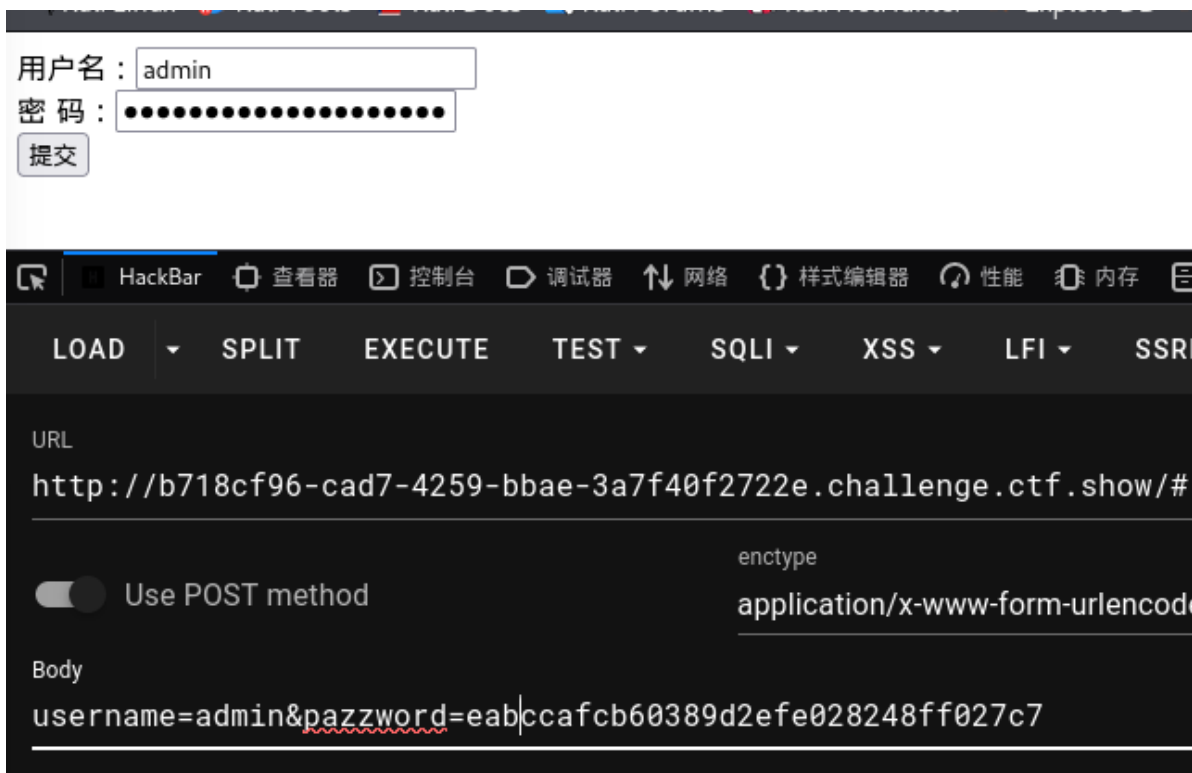
[查看原批](#)，[不不不](#)，[源码](#)



发现用户名和密码

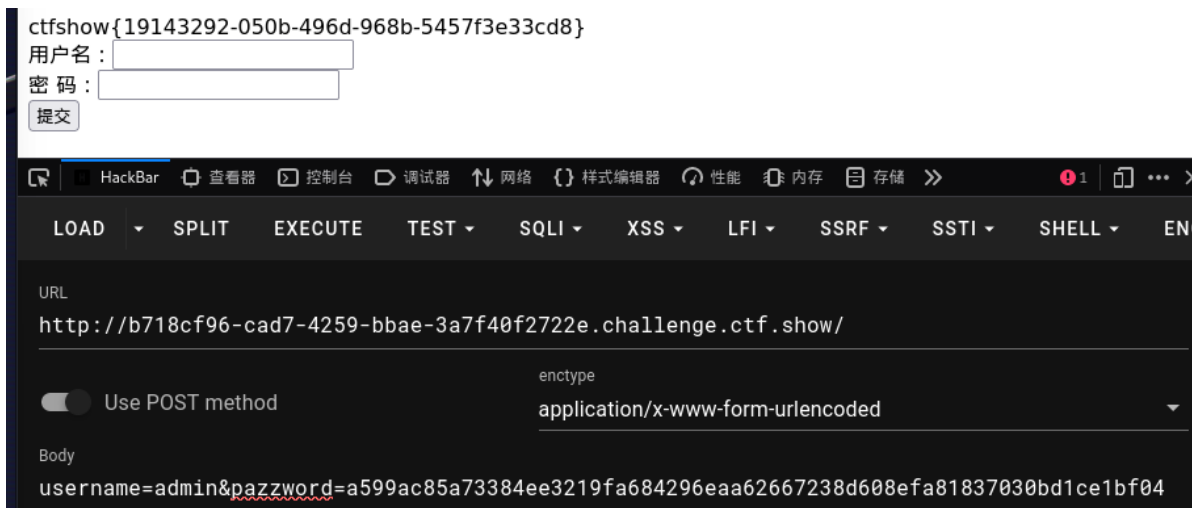
但是密码加密了

试着随便登陆一下



发现密码是经过加密后再用post传上去

我们也如此操作就不用解密了



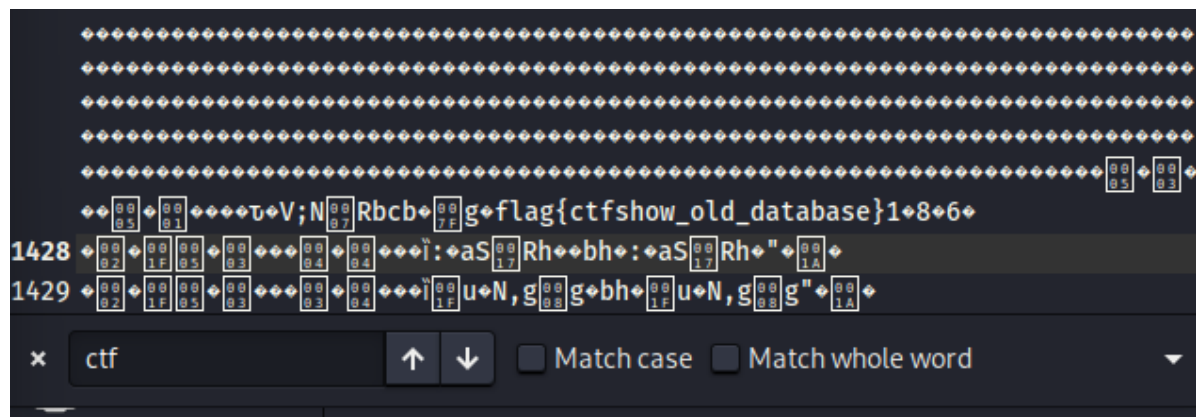
得到flag

web20

S



打开db.mdb查看（因为没有打开程序，用VIM不好查看，所以改后缀）



得到flag