YII框架全版本文件包含漏洞挖掘和分析

l4yn3 / 2019-05-07 09:36:00 / 浏览数 8316 安全技术 WEB安全 顶(1) 踩(0)

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

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版本下执

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。

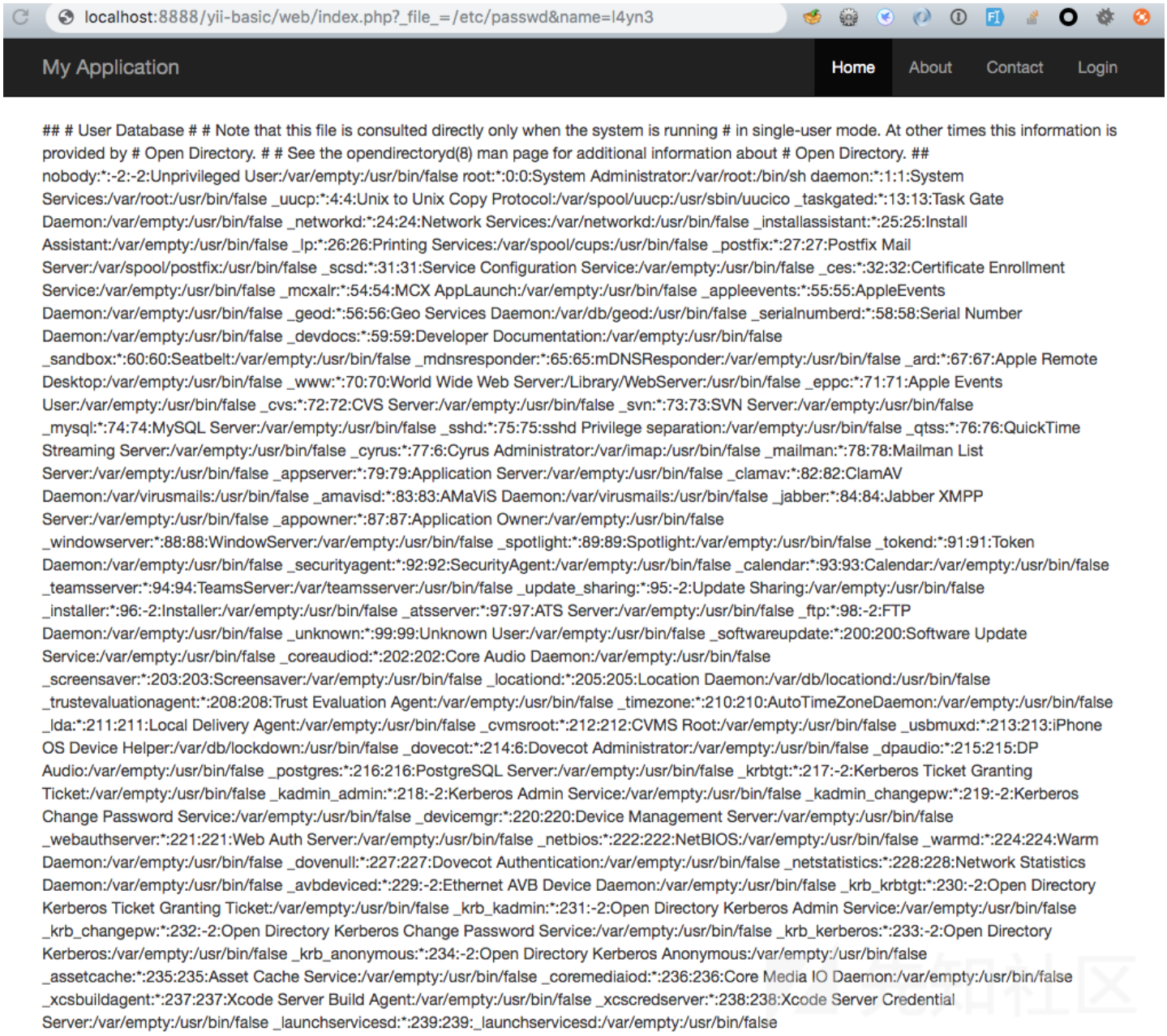
到此这个漏洞发展成了一个和 《codeigniter框架内核设计缺陷可能导致任意代码执行》 一样的漏洞。

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。



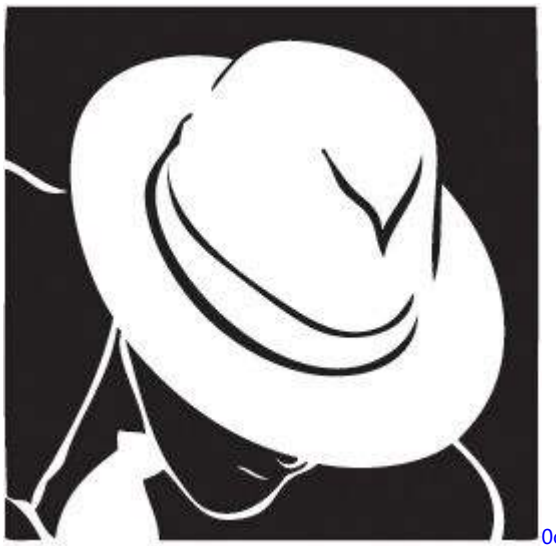
最后

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 条回复



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

Yii Version 2.0.18 貌似已经修复了

0 回复Ta

0c**** 2019-05-08 12:17:21

没修...

0 回复Ta

0c**** 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