

shiro权限绕过

什么是shiro

Apache Shiro是一个强大且易用的Java安全框架，执行身份验证、授权、密码和会话管理。

使用Shiro的API，您可以快速、轻松地获得任何应用程序，从最小的移动应用程序到最大的网络和企业应用程序。

shiro权限绕过的原因

Apache Shiro是一个Java的安全管理框架，可以和spring一起使用。

shiro框架通过拦截器来实现对用户访问权限的控制和拦截。

Shiro常见的拦截器有anon,authc等。

1. anon：匿名拦截器，不需登录就能访问，一般用于静态资源，或者移动端接口。
2. authc：登录拦截器，需要登录认证才能访问的资源。

shiro权限绕过的限制条件

- 网站同时使用shiro和spring
- shiro满足特定的版本

CVE-2016-6802

shiro版本：shiro < 1.5.0

shiro与spring的URI中末尾的 / 不同导致的权限绕过

其中 * 表示匹配零个或多个字符串，/* 可以匹配/admin，但匹配不到/admin/因为*通配符无法匹配路径。

假设/admin接口设置了authc拦截器，访问/admin将会被进行权限判断，如果请求的URI为/admin/呢，/*的URL路径表达式将无法正确匹配，放行。然后进入到spring(Servlet)拦截器，而spring中/admin形式和 /admin/形式的URL访问的资源是一样的，从而导致了绕过。

CVE-2020-1957

shiro版本：shiro < 1.5.2

```
#绕过的payload
/xxx/..;/admin/
/./;/admin/
```

通过网络判断，网站处理URI时会先经过 shiro 处理，再转发到 springboot 进行路由分发工作。而在 shiro中，在对URI中的 ; 进行处理时会将URI进行截断，然后对 /xxx/.. 进行权限校验，校验通过之后再由springboot进行路由分发，然后springboot会将URI /xxx/..;/admin/ 解释为 /admin/ ,这样我们就可以成功访问到原本访问不到的接口了。

验证流程大致如下：

客户端发起请求 `/xxx/../admin/`。

shiro处理之后返回 `/xxx/..` 校验通过。

springboot处理 `/xxx/../admin/` 返回 `/admin/`。

最后访问到需要权限校验的资源。

使用vulhub搭建shiro的漏洞环境

下载vulhub离线包，docker-compose启动

(1) 启动docker服务

```
systemctl start docker
```

(2) 下载vulhub靶场

```
https://github.com/vulhub/vulhub    ##vulhub项目地址

wget https://github.com/vulhub/vulhub/archive/master.zip -O vulhub-master.zip
##下载vulhub
```

(3) 搭建fastjson漏洞环境



```
unzip vulhub-master.zip    ##解压vulhub-master.zip

cd vulhub-master/shiro/CVE-2020-1957    ##进入vulhub-master目录下

docker-compose up -d    ##使用docker-compose拉取启动shiro靶场
```

vulhub靶场启动shiro场景

访问地址：192.168.21.137:8080

  192.168.21.137:8080

Hello, World!

Login

Account info (Requires authenticated.)

shiro权限绕过漏洞利用

```
#绕过的payload  
/xxx/..;/admin/  
/..;/admin/
```

  192.168.21.137:8080/xxx/..;/admin/

Account Info Page for: World!

[Home](#)[Logout](#)