# CVE-2020-11989: Apache Shiro权限绕过复现

原创<mark>hatjwe Timeline Sec</mark> 2020-11-19原文

收录于话题 #漏洞复现文章合集 70个

> 上方蓝色字体关注我们,一起学安全! 作者: hatjwe@Timeline Sec 本文字数: 1142 阅读时长: 3~4min 声明: 请勿用作违法用途,否则后果自负

### 0x01 简介

Apache

Shiro作为常用的Java安全框架,拥有执行身份验证、授权、密码和 会话管理等功能,通常会和Spring等框架一起搭配使用来开发Web 应用。

0x02 漏洞概述

 编
 号
 :
 CVE-2020-11989

 Apache
 Shiro
 1.5.3
 之前的版本中,当将Apache

 Shiro与Spring动态控制器一起使用时,精心编制的请求可能会导致
 绕过身份验证。

#### 0x03 影响版本

Apache Shiro < 1.5.3

0x04 环境搭建

我测试的demo: https://github.com/lenve/javaboy-codesamples/tree/master/shiro/shiro-starter

下载后在IDEA打开我们下载的项目文件夹 接 着 设 置 Configurations , 打 开 edit Configurations(这里我之前已经设置过了)



配 置 Configurations 点 击 加 号 添 加 spring Boot, 填写配置名称设置main class之后我们便可以运行了

🕞 Debian 7.x 64 🖞 🛛 👔 Ubuntu 64 🖞 👋 🕞 Windows 10 x64 🛛					
🔛 Ele Edit View Navigate Code Analyze Belastor Build Ran Tools VCS Winds					
shiro-web-1.4.2.jar ) org ) apache ) shiro ) web ) filter ) mgt ) 📵 PathMatchingFilterChair					
1 = Project +					
💈 🛩 📭 shire-starter C.WsentwintObig(Desktop/shire302000)/avaboy-code-samples-man					
ti → midea	+ = 0 P + < N II				
✓ ■ sre ✓ ■ main	<ul> <li>Ag spring boot</li> <li>ShiroStarterApplication</li> </ul>				
👻 🖿 java	> الله Templates				
✓ En org.javaboy.shirostarter					
MyRealm					
ShiroConfig					
ShiroStarterApplication					
ag application properties					
> Bit fast					
) target Øladesand					
🖉 shiro-starter.led					
> the External Libraries					
Scratches and Consoles					
					(tp.wttpServletRequest) getPat
5					
2					
4					
1					
*					
1					W/E MEndame
- Second S					RGA WINDOWS
🛛 g Problems 🗏 TODO 📓 Terminal 🔨 Build 📑 Java Enterprise 🔎 Spring				- FC III	netine Sec
Al files are up to-date (moments ago)					
日 P 在这里输入你要提素的内容 O 計	i 💼 📴 😰 🦛 🗰 🖉	<b>a</b>			~ 12 41 英 21:15 □

🔲 Project 👻	Pun/Dahun Configurations		
<ul> <li></li></ul>	-samples-mast		
> 🖿 idea	+ = @ <i>P</i> ▲ ∀ ₩ 8		
✓ ■ src	<ul> <li>g Spring Boot</li> </ul>		
V main	dUnnamed	Configuration Code Coverage Logs	
✓ ■ java ✓ ■ oro.javabov.shirostarter			- over time.
		Enwronment	
ShiroConfig		▼ Serine Boot	
ShiroStarterAppic			
application.propertie			
Earch by Name Project     Search by Name Project			
	Include non-project items		
Shiro-starter.ml			
Scratches and Consoles			
		Override parameters:	atto UttoSepuletRequest) getRef
		- Oxford laws de	
			Timolino Soc

Shiro主要的三个文件: ShiroConfig, LoginController, Myrealm

权限配置: ShiroConfig 其中/doLogin无需权限验证即可访问,用于登录界面 而test/文件下目录需要登陆权限认证后才可以进行访问



登陆控制: LoginController 其中设置了访问目录返回的内容



Myrealm: 其中储存着用户类信息像我们登陆所用的密码。



## 0x05 漏洞复现

IDEA运行时,我们先访问界面通过doLogin进行登陆

(这里需要注意demo中doLogin传参方式为@PostMapping()需 要改成@GetMapping())

🖄 Timeline Sec

# 我们访问界面可以看到我们设置的回显信息,那么接下来我们开始通过未授权绕过shiro控制访问到这个信息

← → C ☆ ② □ 127.0.0.1:8080/test/
 □ 火瓶首方站点 ● 新手上路 □ 常用同址 ■ 天振双11 ③ 东东南城 □ 常用同址 ④ 东东双11 ④ 东东南城 ④ 东东南城 ○ 东东南城
 ○ 京东南城 ● 东东南城
 ○ 東京南城

😳 Timeline Sec

我清除了cookie,抓包进行访问test发现需要登陆

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project option	User options
1 ×	
Send Cancel <   Y Follow redirection	Target: http://127.0.0.1:8000 🖉 🔇
Request	Response
Raw Headers Hex	Raw Headers Hex
Pretty Raw In Actions V	Pretty Raw Render In Actions V
<pre>1 GBT //est HTTP/1.1 2 Host: 17.0.0.1:0000 3 User-Agent: Mosilia/S.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefor/02.0 4 Accept: test/htal,application/shtml+mal,application/sml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: mhcft,sht;q=0.8,m-TW;q=0.7,mhK;q=0.5,m-UB;q=0.3,en;q=0.2 6 Accept-Incoding: gnip, deflate 7 Connection: close 0 Upgrade-Insecure-Requests: 1 0 </pre>	1 HTTP/1,1 302 2 Set-Cookie: JSESIONID-0FFCB421B672AAC6F66B3E49574EFEC7; Path=/: Http:nly 3 Location: http://L71.0.0.1:0000/login;jsessionid=0FECB421B672AAC6F66B3E49574EFEC7 4 Content-Length: 0 5 Date: Sat, 31 Oct 2020 10:40:36 CHT 7 8
DO matches 0 matches	©© € → Search
one	250 bytes I 156 mills

## 但是当访问/;/test时我们便可以绕过shiro认证查看需要登录认证的 信息了



## 0x06 漏洞分析

根据参考文章漏洞初始成因定位到

PathMatchingFilterChainResolver的getChain函数下

该函数作用根据URL路径匹配中配置的url路径表达式来匹配输入的U RL,判断是否匹配拦截器,匹配成功将会返回响应的拦截器执行链, 让ShiroFither执行权限操作的

其中对于URL路径表达式和输入URL的匹配主要通过pathMathche s函数进行匹配。

接下来我们在IDEA中进行debug,首先在 PathMatchingFilterChainResolver.java文件中的getPathWit hinApplication(Request)处 下断点进行调试



浏览器访问: http://127.0.0.1:8080/test

我们跟进getPathWithinApplication



跟进到

org.apache.shiro.web.util.WebUtils#getPathWithinApplic ation

继续跟进到

org.apache.shiro.web.util.WebUtils#getRequestUri

获取的是我们输入的路径



跟进到

org.apache.shiro.web.util.WebUtils#normalize(decodeAn dCleanUriString(request, uri))

这里会进行判断将;后边进行截断



之后可以看到

org.apache.shiro.web.util.WebUtils#getRequestUri 获取到的是/



之后回到最开始的最开始的getPathWithinApplication往下调试 到pathMatches进行权限的判断



但我们接下来继续跟踪会发现我们直接绕过了 if (pathMatches(pathPattern, requestURI)的逻辑 跳出了shiro权限判断



最终经过getPathWithinServletMapping函数格式化处理后,得 到最终路径为**/test**,所以我们可以正常访问到该页面

Die Seit Vom Merinste Code Analyze Delaster Duild Due Tools WCS Mindow Hale	chroutarter - UriVathileiner clarr IN	aven: org roopgtramework;rongg-web/517/k/k/k/	WE I			_
ng-web-5.1.7.RELEASE.jar) org ) springframework ) web ) util ) @ UrlPathHelper ) @ getPathW				🔨 🛋 ShiroStarterApp	lication 🔻 🕨 🛍 🕵 🚱	
Project 🗸 🤤	😤 🏚 — 🥘 PathMatchingFilterC					
<ul> <li>To des stater Classicals this global signal of size (Classicals the size of size</li></ul>		<pre>bytecode version 52.0 (Jera 8) f (this.alwaysUseFullPath) {     return this.getPathNithInApplicati     else {         String rest = this.getPathNithInSe         return !-*.equals(rest) ? rest : ti     } }</pre>	on(request); rvletMapping(request); his.getPathWithinApplication(re			
<ul> <li>✓ Big resources in application,properties         ) ■ traget In traget If promotel # Adva state sinel If a transit Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial Barterial</li></ul>	72 \$ public 73 \$ 74 \$ 76 \$ 77 \$ 77 \$ 77 \$ 79 \$ 79 \$ 80 \$ 79 \$ 81 \$ 79 \$ 81 \$ 79 \$ 81 \$ 79 \$ 81 \$ 79 \$ 81 \$ 79 \$ 79 \$ 79 \$ 79 \$ 70 \$ 70 \$ 70 \$ 70 \$ 70 \$ 70 \$ 70 \$ 70	<pre>String getValuationservierApping/ tring servietPath = thi.getServietPath tring servietPath = thi.getServietPa tring servietPathWithindpe = this.get tring gat: (ServietPath:contains(SenitizedPath Dath = this.getBensiningPath(Senth path = this.getBensiningPath(SethWithing))</pre>	httparvietkequest request) in hinAppliation(request); pathh th(request); servietPath; //t etSanitizedPath(pathWithinApp); WithinApp)) { servietPath; //t izedPathWithinApp, servietPath, ithinApp, servietPath, ignoreCa	<pre>request: Sniron(tpservict lininApp: "/test" ist" request: SniroN(tpSe i sonitizedPathWithinApp: cest" sonitizedPathWithinApp: cest" sonitizedPathWithin [gnoreCase: false); se: false);</pre>		
ebug:e_ShiroStarterApplication ×						
🔒 Debugger 🛛 Console 🚜 Endpoints 🚍 🗠 土 🛓 🏦 🦮 🔤 🚟						=
Frames Variables						
<ul> <li>( → Thep-sole:000++, p * sub * (LHANNO *) + ( ↓ Y ) &gt; E the Endballege ODE</li> <li>percentional content operation ( Non-tent Kipper and point &gt; ) E particular distribution = * net *</li> <li>S = sound base + * net *</li> <li>S = sound base + * net *</li> </ul>						
R Ø g moberns :				😤 Ti	meline S	

所以当我们输入/;/test时oorg.apache.shiro.web.util.WebUtil s#normalize会将;后边进行截取

而 if (pathMatches(pathPattern, requestURI)又会错误的处理/导致逻辑绕过,以至于我们可以正常 访问需要授权的页面

### 0x07 修复方式

通过WAF检测请求的uri中是否包含%25%32%66关键词 通过WAF检测请求的uri开头是否为/;关键词 升级至Apache Shiro 1.5.3 或更高版本

参考链接:

https://www.bilibili.com/video/BV1Ca4y1L7j3?t=5 https://paper.seebug.org/1196/





阅读原文看更多复现文章

Timeline Sec 团队 安全路上,与你并肩前行 用户设置不下载评论 阅读全文

精选留言