ZAP Active Scan (3/25/24):

| Plugin | Alerts |
| --- | --- |
| Path Traversal | 0 |
| Remote File Inclusion | 0 |
| Source Code Disclosure - /WEB-INF folder | 0 |
| Heartbleed | 0 |
| Source code Disclosure - CVE-2012-1823 | 0 |
| Remote code Disclosure - CVE-2012-1823 | 0 |
| External Redirect | 0 |
| Server Side Include | 0 |
| Cross Site Scripting - ALL | 0 |
| SQL Injection - ALL | 0 |
| Log4Shell | 0 |
| Spring4Shell | 0 |
| Server Side Code injection | 0 |
| Remote OS Command Injection | 0 |
| XPath Injection | 0 |
| XML External Entity Attack | 0 |
| Generic Padding Oracle | 0 |
| Cloud Metadata Potential Exposed | 0 |
| Server Side Template Injection - ALL | 0 |
| Directory Browsing | 0 |
| Buffer Overflow | 0 |
| Format String Error | 0 |
| CRLF Injection | 0 |
| Parameter Tampering | 0 |
| ELMAH Information Leak | 0 |
| Trace.axd Information Leak | 0 |
| .htaccess Information Leak | 0 |
| .env Information Leak | 0 |
| Hidden File Finder | 0 |
| Spring Actuator Information Leak | 0 |
| XSLT Injection | 0 |
| GET for POST | 0 |
| User Agent Fuzzer | 0 |
| Script Active Scan Rules | 0 |
| SOAP Action Spoofing | 0 |
| SOAP XML Injection | 0 |