Coding Practices and Recommendations of Spring Security for Enterprise Applications

Title	Coding Practices and Recommendations of Spring Security for Enterprise Applications
Publication Type	Conference Paper
Year of Publication	2020
Authors	Islam, M., Rahaman, S., Meng, N., Hassanshahi, B., Krishnan, P., Yao, D. D.
Conference Name	2020 IEEE Secure Development (SecDev)
Date Published	sep
Keywords	authentication, Authorization, encoding, insecure coding practices, password, pubcrawl, resilience, Resiliency, Scalability, security, security anti patterns, Security by Default, Spring security, Springs, Uniform resource locators
Abstract	Spring security is tremendously popular among practitioners for its ease of use to secure enterprise applications. In this paper, we study the application framework misconfiguration vulnerabilities in the light of Spring security, which is relatively understudied in the existing literature. Towards that goal, we identify 6 types of security anti-patterns and 4 insecure vulnerable defaults by conducting a measurement-based approach on 28 Spring applications. Our analysis shows that security risks associated with the identified security anti-patterns and insecure defaults can leave the enterprise application vulnerable to a wide range of high-risk attacks. To prevent these high-risk attacks, we also provide recommendations for practitioners. Consequently, our study has contributed one update to the official Spring security documentation while other security issues identified in this study are being considered for future major releases by Spring security community.
DOI	10.1109/SecDev45635.2020.00024
Citation Key	islam_coding_2020

security pubcrawl Resiliency Scalability authentication authorization encoding resilience password Uniform resource locators insecure coding practices security anti patterns Spring security Springs Security by Default