ZAP Scanning Report

Sites: http://localhost:8082 http://localhost:8081 http://localhost:8080

Generated on Thu, 8 Aug 2024 01:52:58

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2

Alerts

Name	Risk Level	Number of Instances
.htaccess Information Leak	Medium	1
Spring Actuator Information Leak	Medium	1

Alert Detail

Medium	.htaccess Information Leak
Description	htaccess files can be used to alter the configuration of the Apache Web Server software to enable/disable additional functionality and features that the Apache Web Server software has to offer.
URL	http://localhost:8081/UI/acsrf/action/addOptionToken/.htaccess
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	1
Solution	Ensure the .htaccess file is not accessible.
Reference	https://developer.mozilla.org/en-US/docs/Learn/Server-side/Apache_Configuration_htaccess https://httpd.apache.org/docs/2.4/howto/htaccess.html
CWE Id	94
WASC Id	14
Plugin Id	40032

Medium	Spring Actuator Information Leak
	Spring Actuator for Health is enabled and may reveal sensitive information about this application. Spring Actuators can be used for real monitoring purposes, but should be used

Description	with caution as to not expose too much information about the application or the infrastructure running it.
URL	http://localhost:8082/actuator/health
Method	GET
Attack	
Evidence	{"status":"UP"}
Other Info	
Instances	1
Solution	Disable the Health Actuators and other actuators, or restrict them to administrative users.
Reference	https://docs.spring.io/spring-boot/docs/current/actuator-api/htmlsingle/#overview
CWE Id	215
WASC Id	13
Plugin Id	40042