Fortify Software

Fortify WebInspect Agent Rulepack Kit Guide

Version 23.1.0

Document Release Date: May 2023

Software Release Date: May 2023

Introduction

This document describes the detection capabilities of Micro Focus Fortify WebInspect Agent Rulepack Kit. The Fortify WebInspect Agent Rulepack Kit runs atop Fortify's Runtime Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

There are four major types of rules in Fortify WebInspect Agent Rulepack Kit, the details of these rules will be discussed in the following sections.

1. Vulnerability Rules
2. Attack Surface Rules
3. Trace Rules
4. Platform Rules

Output from vulnerability rules will be logged to Runtime Agent event log (if configured) in standard Micro Focus Fortify WebInspect Agent event log format. However, attack surface and

trace rules will only be sent to Fortify WebInspect and will not be logged in event log. Platform rules do not generate any events.

Attack Surface Rules

Attack Surface Rules is used to report the list of the available web pages and URLs to Micro Focus Fortify WebInspect. Fortify WebInspect can then use this information to find hidden pages or pages that the crawler failed to find.

Supported attack surfaces are:

Java	**.NET**
Tomcat/WebSphere JAX-RS	IIS WCF

Vulnerability Rules

Vulnerability rules improve Micro Focus Fortify WebInspect scanning by:

1. Reporting security vulnerabilities that Fortify WebInspect does not typically find. For example, Fortify WebInspect might not be able to find certain types of Blind SQL Injection while Fortify WebInspect Agent intercepts all SQL database operations, will be able to detect it.
2. Reporting code level details to Fortify WebInspect. For example, in the case of a Cross-site Scripting attack, Fortify WebInspect Agent can report the user source file name, line number and any other related stack traces which are very useful to developers when fixing the vulnerability reported.

Fortify WebInspect Agent sends the attack string being used in each request to Fortify WebInspect Agent in a custom HTTP header. Most vulnerability rules detect vulnerabilities by comparing the security sensitive parameter or argument with the Fortify WebInspect provided attack vector. For example, for SQL Injection rules, the monitor will check if the SQL query string contains the attack vector, which may be “`' or 1=1 --`”.

Both Java and .NET Fortify WebInspect Agent Rulepack Kits can detect the following vulnerabilities:

- Arbitrary File Upload
- Command Injection
- Credit Card Number Disclosed
- Cross-Site Scripting
- Dangerous File Inclusion: Local
- Dangerous File Inclusion: Remote
- Denial of Service: Parse Double
- Insecure Randomness
- Leftover Debug Code
- Mass Assignment: Insecure Binder Configuration
- Open Redirect
- Privacy Violation: Credit Card Number
- Privacy Violation: Social Security Number
- SQL Injection
- Social Security Number Disclosed
- Value Shadowing
- XML External Entity Injection
- XML Entity Expansion Injection

Additionally, the Java Fortify WebInspect Agent Rulepack Kit can detect the following vulnerabilities:

- ClassLoader Manipulation: Struts
- Header Manipulation: IMAP
- Header Manipulation: SMTP
- Mail Command Injection: IMAP
- Mail Command Injection: POP3
- Mail Command Injection: SMTP
- Transport Layer Protection: Insecure Mail Transmission

Trace Rules

Trace rules report various events to Micro Focus Fortify WebInspect to help Fortify WebInspect have a better insight into the application being tested. For example, a File_IO trace may notify Micro Focus Fortify WebInspect that the application is reading a particular file. Fortify WebInspect may then use the information to determine if the file operation is expected and/or if a “Path Manipulation” test should be conducted afterwards.

Both Java and .NET Fortify WebInspect Rulepack Kits can detect the following traces:

Trace Type	Operations
Database	execute, close
Attack Suggestion	N/A
Session	start, stop
File IO	open, read, write, close
Authentication	logon, logoff
Authorization	successful, failure
Unused Parameter	N/A
Network	stream
HTTP/URL Connection	init
OAuth	client_version, server_version, token, store_token, store_access_token, request
Validation Failure	struts, spring, webcontrols
autobind	trace_spring_modelattribute, trace_spring_ modelmap, trace
email	smtp_send, email_secure, smtp_command, imap_ command, pop3_command

Platform Rules

Platform rules do not detect any vulnerabilities or events but modify the application or platform to be more suitable for vulnerability scanning.

The list of all supported platform rules is as follows:

Rule	Java	.NET
Enable DEBUG in web.config*	N/A	YES

Rule	Java	.NET
Disable CAPTCHA	ReCaptcha SimpleCaptcha jCaptcha Are You A Human? NuCaptcha	ReCaptcha BotDetect NuCaptcha
Unlimited password retries	N/A	Standard MembershipProvider
Prevent accidentally changing password	N/A	Standard MembershipProvider

* DEBUG is required in order to retrieve line numbers in a stack trace.