Fortify Standalone Report Generator

OWASP Top 10 2017

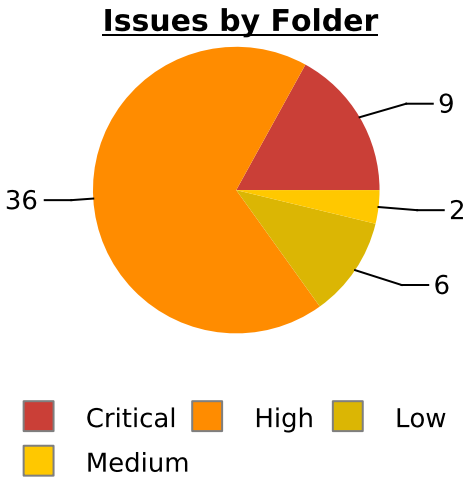
Blockchain-Bless_Transformation_Non_DHL_Fortify

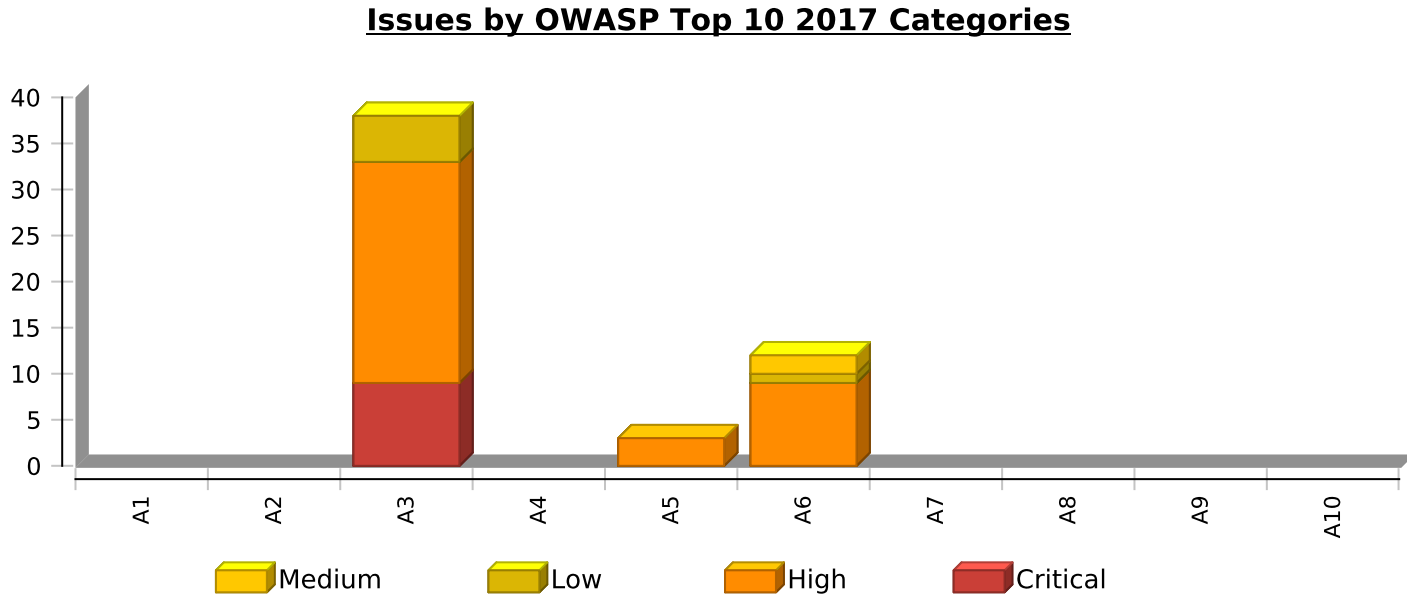
Table of Contents

Executive Summary

The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Project Name:	Blockchain-Bless_Transformation_Nor
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present
Remediation Effort (Hrs):	5.4





* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	Sep 26, 2023 2:34 PM	**Engine Version:**	23.1.0.0136
Host Name:	czcholspc000080	**Certification:**	VALID
Number of Files:	345	**Lines of Code:**	31,062

Rulepack Name	Rulepack Version
Fortify Secure Coding Rules, Community, Cloud	2023.2.0.0007
Fortify Secure Coding Rules, Community, Universal	2023.2.0.0007
Fortify Secure Coding Rules, Core, Cloud	2023.2.0.0007
Fortify Secure Coding Rules, Core, JavaScript	2023.2.0.0007
Fortify Secure Coding Rules, Core, Python	2023.2.0.0007
Fortify Secure Coding Rules, Core, Universal	2023.2.0.0007
Fortify Secure Coding Rules, Extended, Configuration	2023.2.0.0007
Fortify Secure Coding Rules, Extended, Content	2023.2.0.0007
Fortify Secure Coding Rules, Extended, JavaScript	2023.2.0.0007

Issue Breakdown

The following table summarizes the number of issues identified across the different OWASP Top 10 2017 categories and broken down by Fortify Priority Order.

	Folder	Issues	Audited	Effort (Hrs)
A1 Injection		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
A2 Broken Authentication		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
A3 Sensitive Data Exposure		**38**	**0**	**3.9**
	Critical	9	0	
	High	24	0	
	Medium	0	0	
	Low	5	0	
A4 XML External Entities (XXE)		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
A5 Broken Access Control		**3**	**0**	**0.4**
	Critical	0	0	
	High	3	0	
	Medium	0	0	
	Low	0	0	
A6 Security Misconfiguration		**12**	**0**	**1.2**
	Critical	0	0	
	High	9	0	
	Medium	2	0	
	Low	1	0	
A7 Cross-Site Scripting (XSS)		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
A8 Insecure Deserialization		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	

	Folder	Issues	Audited	Effort (Hrs)
A8 Insecure Deserialization		**0**	**0**	**0.0**
	Low	0	0	
A9 Using Components with Known Vulnerabilities		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
A10 Insufficient Logging and Monitoring		**0**	**0**	**0.0**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	

NOTE:
1. Reported issues in the above table may violate more than one OWASP Top 10 2017 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.
2. For the same reason, the Project-level remediation effort total shown in the Executive Summary removes the effect of any duplication and may be smaller than the sum of the remediation effort per individual category.
3. Similarly, the remediation effort per external category is not intended to equal the sum of the remediation effort from the issue details section since individual files may contain issues in multiple Fortify priorities or audit folders.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by OWASP Top 10 2017, Folder, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

A1 Injection

OWASP Top 10 Application Security Risks, A1:2017 states: "Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization."

No Issues

A2 Broken Authentication

OWASP Top 10 Application Security Risks, A2:2017 states: "Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently."

No Issues

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Credential Management: Hardcoded API Credentials ***Remediation Effort(Hrs): 0.3***	**Critical**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.DataTransformer.xUnitTests.Configs

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/DataTransformer/xUnitTests/Configs/DummyHTTPOutConfig.json:3	**Sink:** **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API.test

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:20	**Sink:** **Enclosing Method:** () **Source:**	SCA

Key Management: Hardcoded Encryption Key ***Remediation Effort(Hrs): 0.2***	**Critical**

Package: .src.WebBase.configuration

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/DataTransformer-V2/src/WebBase/configuration/private.pem:1	**Sink:** **Enclosing Method:** () **Source:**	SCA

OpenAPI Misconfiguration: Missing Global Security Requirement ***Remediation Effort(Hrs): 0.1***	**Critical**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/swagger-spec.json:1	**Sink:** ConfigMap **Enclosing Method:** () **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

OpenAPI Misconfiguration: Missing Operation Security Requirement *Remediation Effort(Hrs): 0.1*	Critical

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/Kalmar_Lobster/API/swagger-spec.json:1	**Sink:** ConfigMap **Enclosing Method:** () **Source:**	SCA

Password Management: Hardcoded Password *Remediation Effort(Hrs): 0.6*	Critical

Package: .src.Web.Bless.Modules.Auth

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer-V2/src/Web.Bless/Modules/Auth/DummyRepository.cs:11	**Sink:** **Enclosing Method:** () **Source:**	SCA

Package: .src.Web.DutyDrawback.Modules.Auth

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer-V2/src/Web.DutyDrawback/Modules/Auth/DummyRepository.cs:11	**Sink:** **Enclosing Method:** () **Source:**	SCA

Package: .src.Web.Kenya.Modules.Auth

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer-V2/src/Web.Kenya/Modules/Auth/DummyRepository.cs:11	**Sink:** **Enclosing Method:** () **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.6***	**Critical**

Package: .src.WebBase.Modules.Auth

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer-V2/src/WebBase/Modules/Auth/DummyRepository.cs:9	**Sink:** **Enclosing Method:** () **Source:**	SCA

Password Management: Password in Comment ***Remediation Effort(Hrs): 0.5***	**Low**

Package: .src.modules.v1.auth

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/Kalmar_Lobster/API/src/modules/v1/auth/auth.controller.ts:118	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: .src.modules.v1.data

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/Kalmar_Lobster/API/src/modules/v1/data/db.service.ts:38	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: .src.providers

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/Kalmar_Lobster/API/src/providers/util.service.ts:7	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/Kalmar_Lobster/API/src/providers/util.service.ts:16	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Password in Comment ***Remediation Effort(Hrs): 0.5***	**Low**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFolderSplitterClient	
Location	**Analysis Info**
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/SFTPFolderSplitterClient/setting.py:42	**Sink:** Comment **Enclosing Method:** () **Source:**

Password Management: Empty Password ***Remediation Effort(Hrs): 0.6***	**High**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.DataTransformer.DPDHL.Service	
Location	**Analysis Info**
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer/DPDHL.Service/appsettings.Development.json:16	**Sink:** ConfigPair **Enclosing Method:** () **Source:**
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer/DPDHL.Service/appsettings.Production.json:16	**Sink:** ConfigPair **Enclosing Method:** () **Source:**
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer/DPDHL.Service/appsettings.Staging.json:16	**Sink:** ConfigPair **Enclosing Method:** () **Source:**
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/DataTransformer/DPDHL.Service/appsettings.json:16	**Sink:** ConfigPair **Enclosing Method:** () **Source:**

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1.7***	**High**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.DataTransformer-V2

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/DataTransformer-V2/docker-compose.yml:255	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API.test

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:51	**Sink:** FieldAccess: password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:63	**Sink:** FieldAccess: password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:87	**Sink:** FieldAccess: password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:99	**Sink:** FieldAccess: password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:110	**Sink:** FieldAccess: new_password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:123	**Sink:** FieldAccess: new_password **Enclosing Method:** lambda() **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1.7***	**High**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API.test

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:136	**Sink:** FieldAccess: new_password **Enclosing Method:** lambda() **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/test/app.e2e-spec.ts:150	**Sink:** FieldAccess: new_password **Enclosing Method:** lambda() **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.Docker

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/Docker/docker-compose.yml:37	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPClient.configuration

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPClient/configuration/sftp_config.json:7	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPClient/configuration/sftp_config.json:17	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1.7***	**High**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFileRelocator.SFTPFileRelocator.configuration

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/configuration/sftp_config.json:7	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/configuration/sftp_config.json:77	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/configuration/sftp_config.json:99	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/configuration/sftp_config_v2.json:8	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFolderSplitterClient.configuration

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/configuration/sftp_config.json:8	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/configuration/sftp_config.json:64	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

A3 Sensitive Data Exposure

OWASP Top 10 Application Security Risks, A3:2017 states: "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1.7***	**High**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFolderSplitterClient.configuration	

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/SFTPFolderSplitterClient/configuration/sftp_config.json:107	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_FortifySource/SFTPFolderSplitterClient/configuration/sftp_config.json:141	**Sink:** ConfigPair **Enclosing Method:** () **Source:**	SCA

A4 XML External Entities (XXE)

OWASP Top 10 Application Security Risks, A4:2017 states: "Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks."

No Issues

A5 Broken Access Control

OWASP Top 10 Application Security Risks, A5:2017 states: "Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc."

Path Manipulation ***Remediation Effort(Hrs): 0.5***	**High**

Package: SFTPFileRelocator.SFTPFileRelocator.s3_sftp_client

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/s3_sftp_client.py:129	**Sink:** shutil.copyfileobj() **Enclosing Method:** extract_if_gzip_file() **Source:** open() **from** SFTPFileRelocator.SFTPFileRelocator.s3_sftp_client.SFTPClient.extract_if_gzip_file() **In** jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify/Source/SFTPFileRelocator/SFTPFileRelocator/s3_sftp_client.py:128	SCA

Package: SFTPFolderSplitterClient.s3_sftp_client

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/s3_sftp_client.py:148	**Sink:** shutil.copyfileobj() **Enclosing Method:** extract_if_gzip_file() **Source:** open() **from** SFTPFolderSplitterClient.s3_sftp_client.SFTPClient.extract_if_gzip_file() **In** jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify/Source/SFTPFolderSplitterClient/s3_sftp_client.py:147	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFolderSplitterClient

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/s3_unzip_client.py:8	**Sink:** shutil.copyfileobj() **Enclosing Method:** () **Source:** open() **In** jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify/Source/SFTPFolderSplitterClient/s3_unzip_client.py:7	SCA

A6 Security Misconfiguration

OWASP Top 10 Application Security Risks, A6:2017 states: "Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion."

Dockerfile Misconfiguration: Sensitive Host Directory ***Remediation Effort(Hrs): 0.1***	**Low**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.Docker	

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/Docker/Dockerfile:22	**Sink:** COPY **Enclosing Method:** () **Source:**	SCA

OpenAPI Misconfiguration: Missing Error Handling ***Remediation Effort(Hrs): 0.1***	**Medium**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.API	

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/swagger-spec.json:1	**Sink:** ConfigMap **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/API/swagger-spec.json:1	**Sink:** ConfigMap **Enclosing Method:** () **Source:**	SCA

Dockerfile Misconfiguration: Default User Privilege ***Remediation Effort(Hrs): 0.9***	**High**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.DataTransformer.DPDHL.Service	

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/DataTransformer/DPDHL.Service/Dockerfile:3	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/DataTransformer/DPDHL.Service/Dockerfile2:1	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA

A6 Security Misconfiguration

OWASP Top 10 Application Security Risks, A6:2017 states: "Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion."

Dockerfile Misconfiguration: Default User Privilege ***Remediation Effort(Hrs): 0.9***	**High**

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPClient

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPClient/Dockerfile:2	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPClient/Dockerfile-test:1	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFileRelocator.SFTPFileRelocator

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/Dockerfile:2	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFileRelocator/SFTPFileRelocator/Dockerfile-test:1	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA

Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.SFTPFolderSplitterClient

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/Dockerfile:2	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/SFTPFolderSplitterClient/Dockerfile-test:1	**Sink:** FROM **Enclosing Method:** () **Source:**	SCA

A6 Security Misconfiguration

OWASP Top 10 Application Security Risks, A6:2017 states: "Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion."

Dockerfile Misconfiguration: Dependency Confusion ***Remediation Effort(Hrs): 0.1***	**High**
Package: jenkins-remote.workspace.Blockchain-Bless.Transformation_Non_DHL_Fortify.Source.Kalmar_Lobster.Docker	

Location	Analysis Info	Analyzer
jenkins-remote/workspace/Blockchain-Bless/Transformation_Non_DHL_Fortify Source/Kalmar_Lobster/Docker/Dockerfile:16	**Sink:** RUN **Enclosing Method:** () **Source:**	SCA

A7 Cross-Site Scripting (XSS)

OWASP Top 10 Application Security Risks, A7:2017 states: "XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites."

No Issues

A8 Insecure Deserialization

OWASP Top 10 Application Security Risks, A8:2017 states: "Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks."

No Issues

A9 Using Components with Known Vulnerabilities

OWASP Top 10 Application Security Risks, A9:2017 states: "Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts."

No Issues

A10 Insufficient Logging and Monitoring

OWASP Top 10 Application Security Risks, A10:2017 states: "Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring."

No Issues

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.

Remediation Effort

The report provides remediation effort estimates. You can use these estimates to perform a relative comparison of projects and as a starting point for estimates specific to your organization. Remediation effort estimates are provided in the following report sections:

- Executive Summary
- Issue Breakdown
- Issue Details

To determine remediation effort for a collection of issues, Software Security Center weights each issue based on its category (“remediation constant”) and adds an overhead calculation based on the number of distinct files which contain the set of issues. The formula used at each report level is the same:

- Remediation Effort (in mins) = SUM(remediation constant for each issue in the set) + 6 * Number of distinct files in that set of issues.

At the lowest level of detail, issues are grouped based on Fortify category and Fortify priority OR Fortify category and folder name, depending on report options. So, for example, the Issue Details section of the report might show the remediation effort for “SQL Injection, Critical” or “SQL Injection, MyFolder”.

At the Issue Breakdown level, remediation effort is shown at the level of each external (non-Fortify) category (such as “AC-3 Access Enforcement” in the case of NIST, or “A1 Unvalidated Input” in the case of OWASP Top10). Remediation effort is calculated for the set of all issues that fall into that external category (irrespective of Fortify priority or folder name). As an example, if there are two SQL injection vulnerabilities, one critical and one medium, within the same file, the file overhead is only included once.

At the Executive Summary level, all issues of that project which are mapped to the specified external category list (such as NIST or CWE) are used in the remediation effort calculation.

Fortify recommends that you treat the different levels of remediation effort as information relevant at that level only. You cannot add up remediation effort at a lower level and expect it to match the remediation effort at a higher level.