



## **Fortify on Demand Security Review**

Tenant:	Other_740088900_FMA_686636323
Application:	web
Release:	test
Latest Analysis:	2025/02/13 06:02:51 AM
Latest Assessment Type:	Static Assessment

## Executive Summary

Tenant: Other\_740088900\_FMA\_686636323  
Application: web  
Release: test  
Business Criticality: High  
SDLC Status: QA/Test  
Static Analysis Date: 02/13/2025  
Dynamic Analysis ---  
Date:

### Fortify on Demand Security Rating



46 issues

Status: Failed

Static:



Dynamic:



Open



Source:

Monitoring:



### Application Details

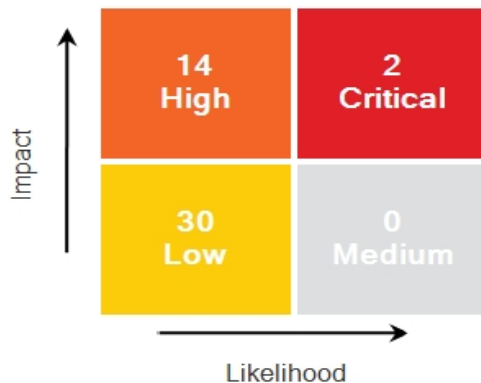
Application type: Other Development

Interface type: Web Service (SOA)

Project type: Other

Sample Application: True

#### Risk Totals by Severity



#### Issue Status

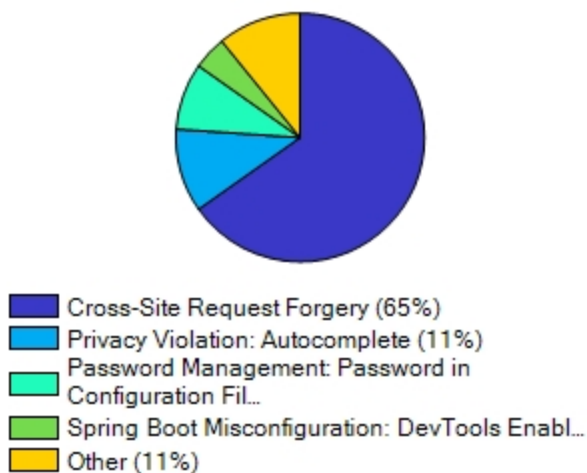
New	Existing	Reopened
27	19	0

#### Assignment Status



Assigned (2%)  
Unassigned (98%)

#### Most Prevalent Issues by Category



#### Developer Status



Open (100%)

#### Auditor Status



Pending Review (100%)

## Issue Breakdown

Issues are divided based on their impact (potential damage) and likelihood (probability of identification and exploit).

High impact / high likelihood issues represent the highest priority and present the greatest threat.

Low impact / low likelihood issues are the lowest priority and present the smallest threat.

See Appendix for more information.

Rating	Category	Test Type	
Critical	SQL Injection: MyBatis Mapper	Static As...	2
High	Password Management: Hardcoded Password	Static As...	1
High	Password Management: Password in Configuration File	Static As...	4
High	Privacy Violation: Autocomplete	Static As...	5
High	Spring Boot Misconfiguration: DevTools Enabled	Static As...	2
High	Unreleased Resource: Streams	Static As...	2
Low	Cross-Site Request Forgery	Static As...	30

## Issue Breakdown by OWASP Top 10 2017 PCI Sections 6.3, 6.5 & 6.6

The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

The PCI compliance standards, particularly sections 6.3, 6.5, and 6.6, reference the OWASP Top Ten vulnerability categories as the core categories that must be tested for and remediated.

OWASP Category	Severity			
	Critical	High	Medium	Low
A1 - Injection	2			
A2 - Broken Authentication				
A3 - Sensitive Data Exposure		10		
A4 - XML External Entities (XXE)				
A5 - Broken Access Control				
A6 - Security Misconfiguration		2		
A7 - Cross-Site Scripting (XSS)				
A8 - Insecure Deserialization				
A9 - Using Components with Known ...				
A10 - Insufficient Logging and Monito...				
Total	2	12		

## Issue Breakdown by OWASP Top 10 2021 PCI Sections 6.3, 6.5 & 6.6

The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

The PCI compliance standards, particularly sections 6.3, 6.5, and 6.6, reference the OWASP Top Ten vulnerability categories as the core categories that must be tested for and remediated.

OWASP Category	Severity			
	Critical	High	Medium	Low
A01 - Broken Access Control				30
A02 - Cryptographic Failures				
A03 - Injection	2			
A04 - Insecure Design		5		
A05 - Security Misconfiguration		6		
A06 - Vulnerable and Outdated Comp...				
A07 - Identification and Authenticatio...		1		
A08 - Software and Data Integrity Fail...				
A09 - Security Logging and Monitorin...				
A10 - Server-Side Request Forgery				
Total	2	12		30

## Issue Breakdown by Analysis Type

Issues are divided based on their impact (potential damage) and likelihood (probability of identification and exploit).

High impact / high likelihood issues represent the highest priority and present the greatest threat.

Low impact / low likelihood issues are the lowest priority and present the smallest threat.










See Appendix for more information.

Category	Static	Dynamic	Open S...	Monitor...
Cross-Site Request Forgery	30	0	0	0
Password Management: Hardcoded Password	1	0	0	0
Password Management: Password in Configuratio...	4	0	0	0
Privacy Violation: Autocomplete	5	0	0	0
Spring Boot Misconfiguration: DevTools Enabled	2	0	0	0
SQL Injection: MyBatis Mapper	2	0	0	0
Unreleased Resource: Streams	2	0	0	0
Total	46	0	0	0

## Appendix - Descriptions of Key Terminology

### Security Rating

The Fortify on Demand 5-star assessment rating provides information on the likelihood and impact of defects present within an application. A perfect rating within this system would be 5 complete stars indicating that no high impact vulnerabilities were uncovered.

Rating	
 	Fortify on Demand awards one star to applications that have undergone a security review that identifies critical (high likelihood and high impact) issues.
 	Fortify on Demand awards two stars to applications that have undergone a security review that identifies no critical (high likelihood and high impact) issues. Vulnerabilities that are trivial to exploit and have a high business or technical impact should never exist in business-critical software.
 	Fortify on Demand awards three stars to applications that have undergone a security review that identifies no high (low likelihood and high impact) issues and meets the requirements needed to receive two stars. Vulnerabilities that have a high impact, even if they are non-trivial to exploit, should never exist in business critical software.
 	Fortify on Demand awards four stars to applications that have undergone a security review that identifies no medium (high likelihood and low impact) issues and meets the requirements for three stars. Vulnerabilities that have a low impact, but are easy to exploit, should be considered carefully as they may pose a greater threat if an attacker exploits many of them as part of a concerted effort or leverages a low impact vulnerability as a stepping stone to mount a high-impact attack.
	Fortify on Demand awards five stars, the highest rating, to applications that have undergone a security review that identifies no issues.

### 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 on Demand 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.

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.

## Issue Status

### New

New issues are ones that have been identified for the first time in the most recent analysis of the application.

### Existing

Existing issues are issues that have been found in a previous analysis of the application and are still present in the latest analysis.

### Reopened

Reopened issues have been discovered in a previous analysis of the application but were not present in subsequent analyses. These issues are now present again in the most recent analysis of the application.