Fortify Software Security Center

Developer Workbook

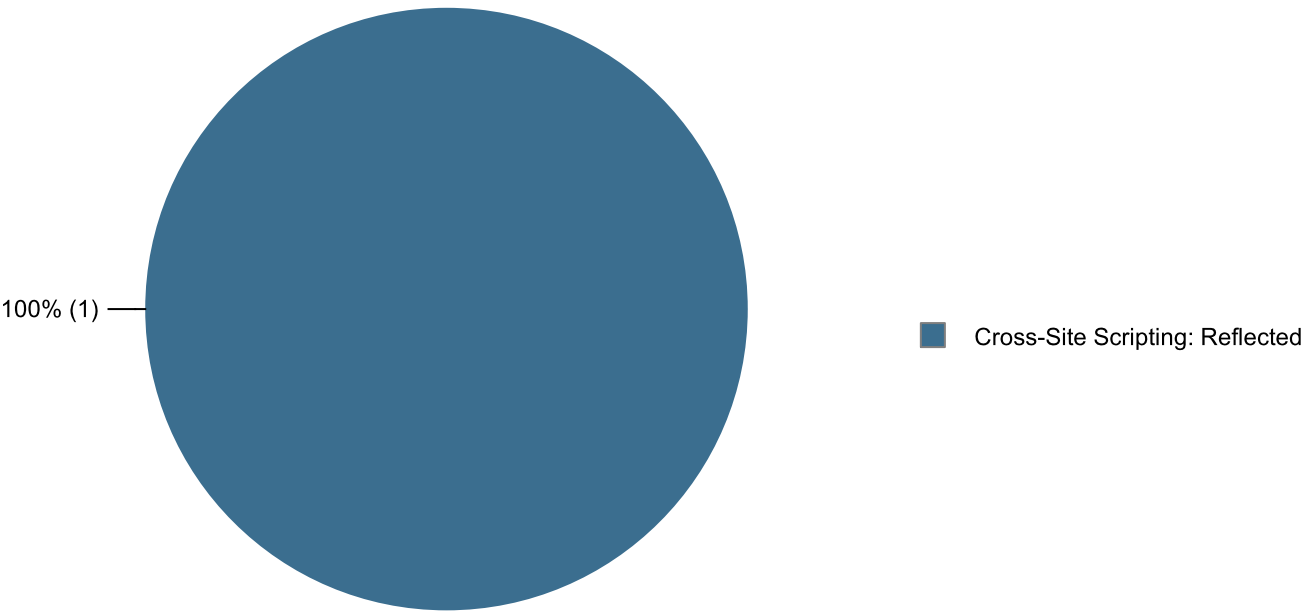demoaa - v1

Table of Contents

Executive Summary

This workbook is intended to provide all necessary details and information for a developer to understand and remediate the different issues discovered during the demoaa - v1 project audit. The information contained in this workbook is targeted at project managers and developers.

This section provides an overview of the issues uncovered during analysis.

Project Name:	demoaa
Project Version:	v1
SCA:	Results Not Present
WebInspect:	Results Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present

Issues by Priority

0 High	**1** Critical
2 Low	**0** Medium

Impact

Likelihood
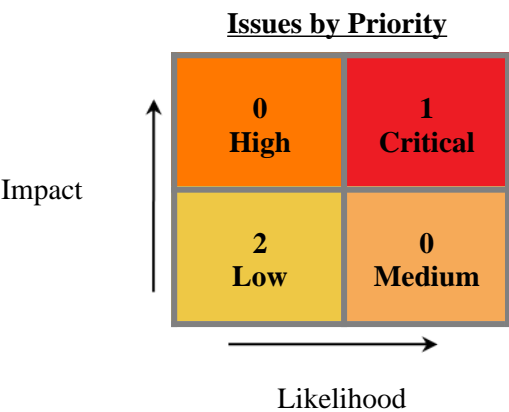
Top Ten Critical Categories

100% (1)

■ Cross-Site Scripting: Reflected

Project Description

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

WEBINSPECT

Date of Last Analysis:	Sep 27, 2016, 8:47 AM	**Engine Version:**	N/A
Host Name:	N/A	**Certification:**	NOT PRESENT
Number of Files:	N/A	**Lines of Code:**	N/A

Accessibility	Internal Network Access Required
Application Classification	<none>
Authentication System	<none>
Business Risk	High
Data Classification	<none>
Development Languages	<none>
Development Phase	Active Development
Development Strategy	Internally Developed
Interfaces	<none>
Known Compliance Obligations	<none>

Issue Breakdown by Fortify Categories

The following table depicts a summary of all issues grouped vertically by Fortify Category. For each category, the total number of issues is shown by Fortify Priority Order, including information about the number of audited issues.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	**High**	**Medium**	**Low**	
Cross-Site Scripting: Reflected	0 / 1	0	0	0	0 / 1
Web Server Misconfiguration: Insecure Content-Type	0	0	0	0 / 2	0 / 2

Results Outline

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.

About Fortify Solutions

Fortify is the leader in end-to-end application security solutions with the flexibility of testing on-premise and on-demand to cover the entire software development lifecycle. Learn more at software.microfocus.com/en-us/solutions/application-security.

Fortify Professional Services

Fortify Professional Services takes a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise (yours and ours) and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people. Learn more about Fortify Professional Services at software.microfocus.com/en-us/services/enterprise-security-consulting-services.