

Fortify on Demand Security Review

Tenant: Surgimap
Application: <https://staging.surgimap.com/angular-access/>
Release: <https://staging.surgimap.com/angular-access/>
Latest Analysis: 2018/02/27 02:29:01 PM
Latest Assessment Type: Dynamic Basic Assessment (remediation)

Executive Summary

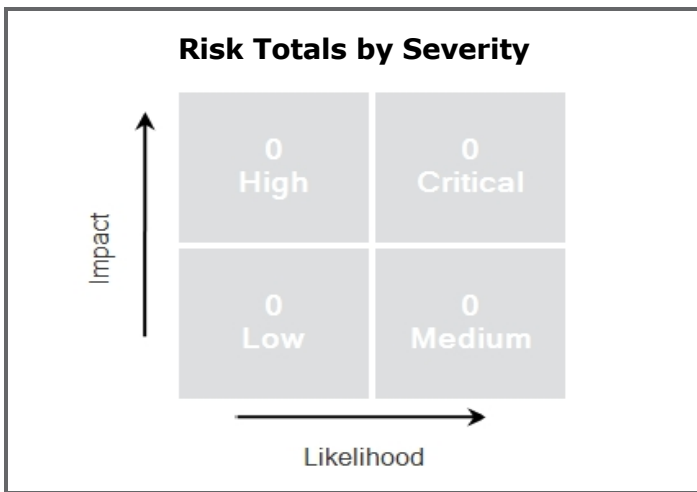
Tenant: Surgimap
 Application: <https://staging.surgimap.com/angular-access/>
 Release: <https://staging.surgimap.com/angular-access/>
 Business Criticality: High
 SDLC Status: QA/Test
 Static Analysis: ---
 Date:
 Dynamic Analysis: 2018/02/27
 Date:

Fortify on Demand Security Rating

★★★★★

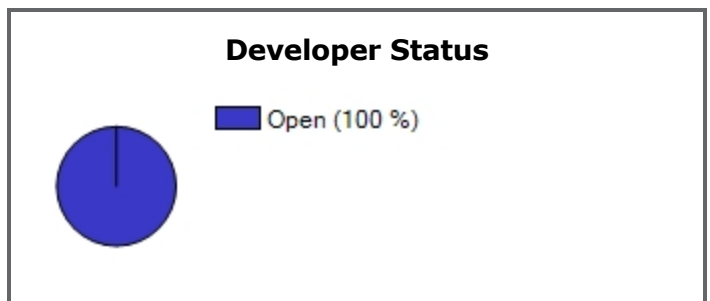
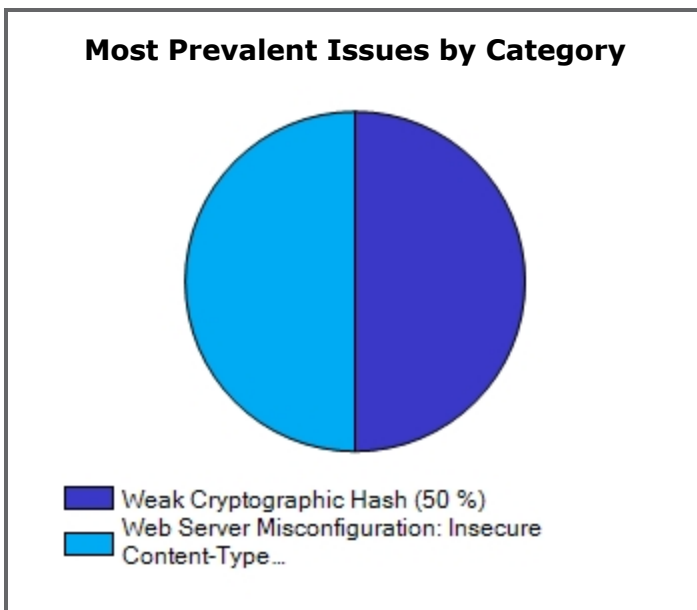
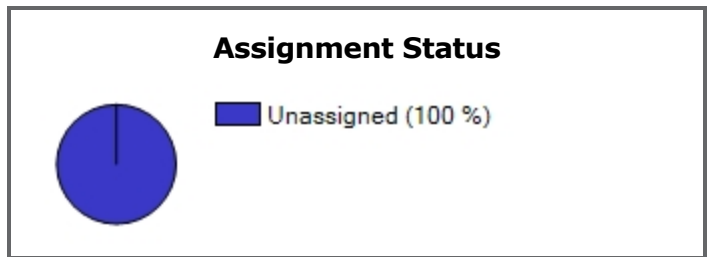
2 issues Status: Pass

Static: ❌ Dynamic: ✔️



Issue Status






New	Existing	Reopened
2	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 projects that undergo a Fortify on Demand security review, which analyzes a project for a variety of software security vulnerabilities.
	Fortify on Demand awards two stars to projects that undergo a Fortify on Demand security review that identifies no high likelihood / 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 projects that undergo a Fortify on Demand security review that identifies no low likelihood / 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 projects that undergo a Fortify on Demand security review that identifies no high likelihood / 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 to projects that undergo a Fortify on Demand 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.

Fortify on Demand Remediation Effort Estimate

Major Remediation

Major remediation effort issues must often be addressed at multiple locations to fix the root problem.

Minor Remediation

Minor remediation effort issues can typically be addressed at the location of the root problem.