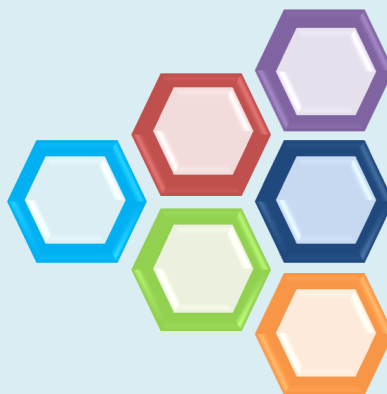


SecureFirst

SECUREFIRST SOLUTIONS



Develop Phase

ApplicationName_v0.1

Reported on: January, 27 2017

Version: **1.0**

Prepared by:




Raghavendra

SDFTwo

Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Table of Contents




Objective.....	3
In-scope and Out of Scope.....	4
Project Details	5
Executive Summary	6
Security Assessment Approach.....	7
Findings & Fix Recommendations	8



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Objective

This report contains the Develop Phase generated for ApplicationName_v0.1.



This report documents the various Security Vulnerabilities prevailing at the code level in the Application and their respective fix recommendations to be put in-place during the 'Development' Phase of the Software Development Life Cycle (SDLC). This report contains the: Security Vulnerabilities that are categorized under the Open Web Application Security Projects (OWASP) Top Ten Vulnerabilities 2013 version and the fix recommendations are provided by the Security Assessor, in-line with the Organization's Secure Development Standards (if any).



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



In-scope and Out of Scope

Below are the list of In-scope and Out of Scope.

In-scope: inscope here




Out of Scope: Any other details not covered under in-scope.



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016




Project Details




description here



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Executive Summary

A Total of 5 security vulnerabilities were identified during the security assessment conducted in the 'Develop Phase' for ApplicationName_v0.1. Below table contains the vulnerability split-up against the Severity.

Severity	Issue Count
Critical	1
High	2
Medium	1
Low	1

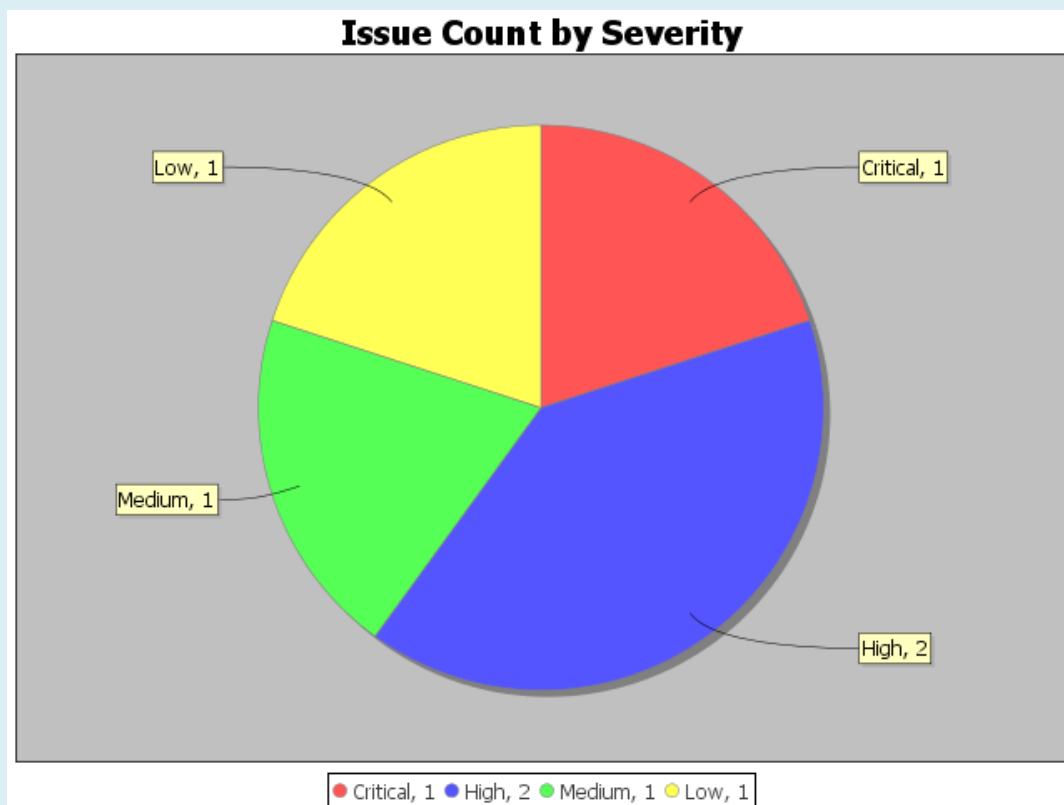


Fig.1 Number of Issues identified

Registered Office:

222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

+91 9972 6495 82
info@SecureFirstSolutions.com
www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Security Assessment Approach



During the Project Development phase, Security Advisors assist the Developers to follow the Secure Development Practices. Also, conduct Source Code reviews using the: a. Project provided source code analysis (SCA) commercial tool or the SDF recommended open source SCA tools and b. Manual Secure Code Review process (to manually identify security vulnerabilities at the code level) Capture the Tool and Manual findings in 'Develop' tab under 'Automated Scan Report' and 'Manual Secure Code Review Findings' tables.



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Findings & Fix Recommendations

Sl. No.	1	Severity	Critical
Remediation Status	Identified		
Vulnerability	Spoofing		
Description	As per the Architecture Diagram provided the Project Team, Authorization control is missing at the Application Server which will lead to Spoofing		
Mitigation	Include proper Authorization checks at the Application Server		




Sl. No.	2	Severity	High
Remediation Status	Identified		
Vulnerability	Tampering with Data		
Description	The documentation provided for System Design review contains details about the Application passing sensitive information over the URL, which will lead to Tampering of Data		
Mitigation	Sensitive information must not be part of the URL. For detailed recommendation refer SDFOne Data Protection Standards		

Sl. No.	3	Severity	High
Remediation Status	Identified		
Vulnerability	Use of vulnerable version of Adobe		
Description	As per the Architecture Diagram provided the Project Team, Authorization control is missing at the Application Server which will lead to Spoofing		
Mitigation	Include proper Authorization checks at the Application Server		

Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

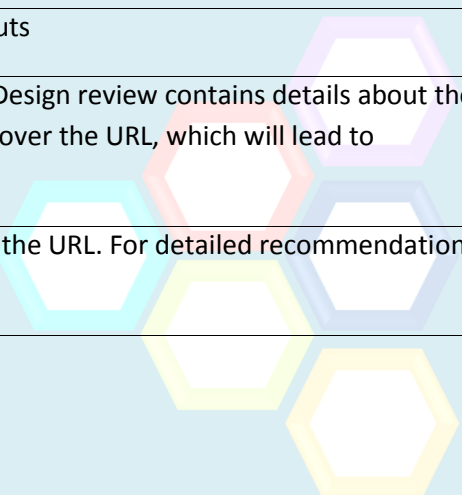
 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016



Sl. No.	4	Severity	Medium
Remediation Status	Identified		
Vulnerability	Authentication bypass		
Description	As per the Architecture Diagram provided the Project Team, Authorization control is missing at the Application Server which will lead to Spoofing		
Mitigation	Include proper Authorization checks at the Application Server		



Sl. No.	5	Severity	Low
Remediation Status	Identified		
Vulnerability	Use of outdated vulnerable version of Struts		
Description	The documentation provided for System Design review contains details about the Application passing sensitive information over the URL, which will lead to Tampering of Data		
Mitigation	Sensitive information must not be part of the URL. For detailed recommendation refer SDFOne Data Protection Standards		



Registered Office:

 222, 5th Main, 10th Cross, Padmanabhanagara,
BSK II Stage, Bengaluru – 5600 70
Karnataka. INDIA.

Contact:

 +91 9972 6495 82
 info@SecureFirstSolutions.com
 www.SecureFirstSolutions.com

© SecureFirst Solutions 2016

