

Security Findings of Project "aesStringReplace"

Analysis Date: 2020-03-07 08:46:22

Analyzed Workspace:

Packages:	1	Total LOC:	13
Classes:	1	No. of Bytecode Instructions:	29

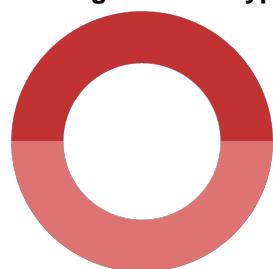
Computed Call Graph:

Classes not in Call Graph:	0	Methods not in Call Graph:	0
----------------------------	---	----------------------------	---

Findings in List:

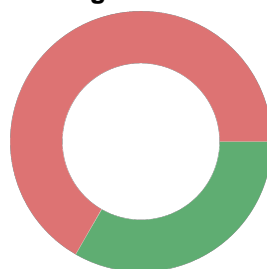
All Findings:	3	Problematic Findings:	2
---------------	---	-----------------------	---

Finding Problem Types:



■ Cryptography: Crypto...: 1
■ Cryptography: Check ...: 1

Finding Classifications:



■ High risk: 2
■ No risk: 1

Finding Ratings:

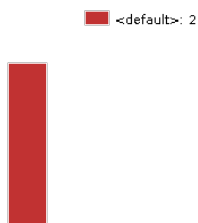


■ Medium risk: 1
■ Low risk: 1

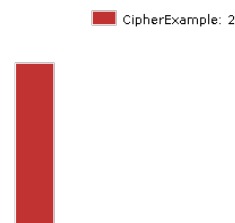
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	3	Problem Type:	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-03-07 08:46:22 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Cryptography: Check that only allowed crypto algorithms are used'.</p> <p>The protocol check detected something wrong when encountering symbol 'AnyAlgorithm_CipherConstruction':</p> <p>Only AES is allowed as algorithm for encryption or decryption.</p> <p>Violated protocol: Check Allowed Cryptography Algorithms</p> <p>Protocol description:</p> <p>Allow only a given set of cryptography algorithm names where algorithm names are expected.</p> <p>The algorithm names are configured via constant value constraint variables.</p> <p>Names to be checked against can be found here: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html</p> <p>Matching pattern in protocol check kind 'AnyAlgorithm_CipherConstruction':</p> <pre>static javax.crypto.Cipher javax.crypto.Cipher.getInstance(java.lang.String, ***)</pre>		

Finding ID:	2	Problem Type:	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	Date:	2020-03-07 08:46:22 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Cryptography: Cryptographic Algorithms Used in Project'.</p> <p>Declared in: javax.crypto.Cipher</p> <p>Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms Used in Project':</p> <pre>static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)</pre>		

Finding ID:	1	Problem Type:	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
Classification:	Warning	Date:	2020-03-07 08:46:22 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider'.</p> <p>Declared in: javax.crypto.Cipher</p> <p>Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider':</p> <pre>static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)</pre>		

Findings List