

Security Findings of Project "aes"

Analysis Date: 2020-03-07 03:02:37

Analyzed Workspace:

Packages:	1	Total LOC:	49
Classes:	1	No. of Bytecode Instructions:	215

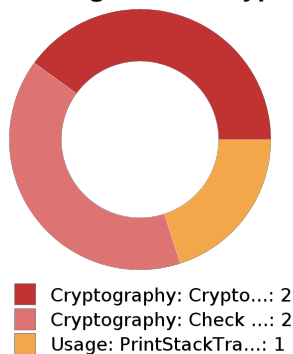
Computed Call Graph:

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

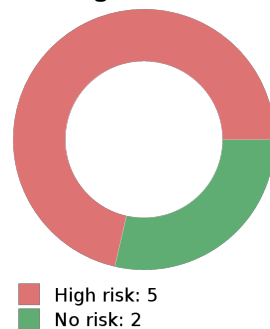
Findings in List:

All Findings:	7	Problematic Findings:	5
---------------	---	-----------------------	---

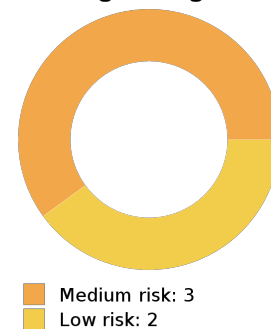
Finding Problem Types:



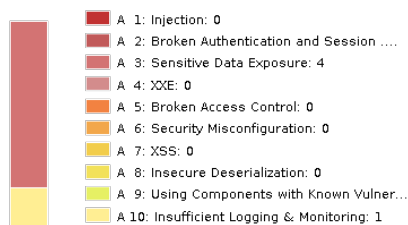
Finding Classifications:



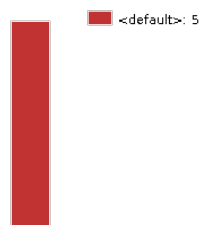
Finding Ratings:



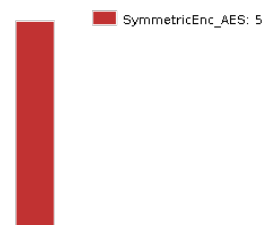
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	6	Problem Type:	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-03-07 03:02:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):24		
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_KeyGeneratorGetInstance'.</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_KeyGeneratorGetInstance':</p> <pre>static javax.crypto.KeyGenerator javax.crypto.KeyGenerator.getInstance(java.lang.String, ***)</pre>		

Finding ID:	7	Problem Type:	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-03-07 03:02:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):35		
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>		

Findings List

Finding ID:	4	Problem Type:	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	Date:	2020-03-07 03:02:37 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):24		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms Used in Project'. Declared in: javax.crypto.KeyGenerator Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms Used in Project': static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)		

Finding ID:	5	Problem Type:	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	Date:	2020-03-07 03:02:37 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):35		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms Used in Project'. Declared in: javax.crypto.Cipher Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms Used in Project': static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)		

Finding ID:	1	Problem Type:	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
Classification:	Warning	Date:	2020-03-07 03:02:37 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):24		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider'. Declared in: javax.crypto.KeyGenerator Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider': static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)		

Findings List

Finding ID:	2	Problem Type:	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
Classification:	Warning	Date:	2020-03-07 03:02:37 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):35		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider'. Declared in: javax.crypto.Cipher Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider': static javax.crypto.** javax.crypto.**.getInstance(java.lang.String)		

Finding ID:	3	Problem Type:	Usage: PrintStackTrace (Special Code)
Classification:	Warning	Date:	2020-03-07 03:02:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AES.java (<Source Code>):46		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	An identified location for problem type 'Usage: PrintStackTrace'. Declared in: java.security.GeneralSecurityException Matching pattern in special code kind 'Usage: PrintStackTrace': public void java.lang.Throwable.printStackTrace()		