

Security Findings of Project "AESOFBNoPadding"

Analysis Date: 2020-03-07 03:15:37

Analyzed Workspace:

Packages:	1	Total LOC:	41
Classes:	1	No. of Bytecode Instructions:	175

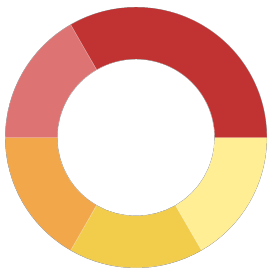
Computed Call Graph:

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

Findings in List:

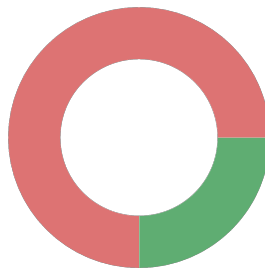
All Findings:	8	Problematic Findings:	6
---------------	---	-----------------------	---

Finding Problem Types:



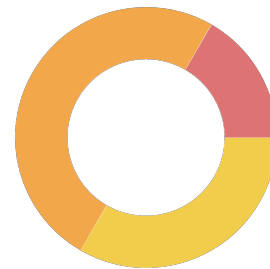
- Cryptography: Crypto...: 2
- Cryptography: AES En...: 1
- Cryptography: Check ...: 1
- Usage: PrintStackTra...: 1
- Other: 1

Finding Classifications:



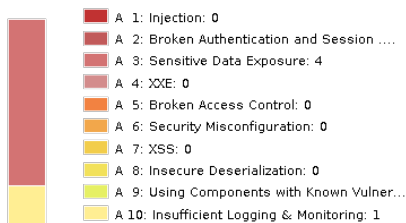
- High risk: 6
- No risk: 2

Finding Ratings:

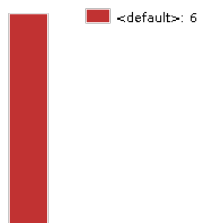


- High risk: 1
- Medium risk: 3
- Low risk: 2

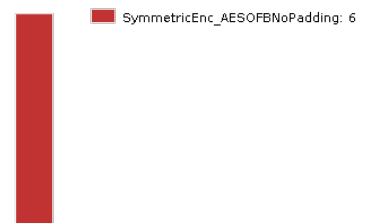
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	7	Problem Type:	Cryptography: AES Encryption (Protocol Check Findings)
Classification:	Warning	Date:	2020-03-07 03:15:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):29		
Tags:	no tags assigned		
Comment:	no comment		
Description:	<p>An identified location for problem type 'Cryptography: AES Encryption'. The protocol check detected something wrong when encountering symbol 'CipherInitializationForEncryption_IVMissing': An initialization vector should be used when encrypting.</p> <p>Violated protocol: Creation of an AES Cipher for Encryption Protocol description: Creation of a cipher for AES consists of creating an uninitialized cipher, and then initializing it properly.</p> <p>Matching pattern in protocol check kind 'CipherInitializationForEncryption_IVMissing': void javax.crypto.Cipher.init(int, java.security.Key)</p>		

Finding ID:	6	Problem Type:	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-03-07 03:15:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	no comment		
Description:	<p>An identified location for problem type 'Cryptography: Check that only allowed crypto algorithms are used'. The protocol check detected something wrong when encountering symbol 'AnyAlgorithm_CipherConstruction': Only AES is allowed as algorithm for encryption or decryption.</p> <p>Violated protocol: Check Allowed Cryptography Algorithms Protocol description: 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': static javax.crypto.Cipher javax.crypto.Cipher.getInstance(java.lang.String, ***)</p>		

Findings List

Finding ID:	4	Problem Type:	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	Date:	2020-03-07 03:15:37 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):18		
Tags:	no tags assigned		
Comment:	no comment		
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 03:15:37 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	no comment		
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 03:15:37 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):18		
Tags:	no tags assigned		
Comment:	no comment		
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 03:15:37 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):27		
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>		

Finding ID:	3	Problem Type:	Usage: PrintStackTrace (Special Code)
Classification:	Warning	Date:	2020-03-07 03:15:37 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):38		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Usage: PrintStackTrace'.</p> <p>Declared in: java.security.GeneralSecurityException</p> <p>Matching pattern in special code kind 'Usage: PrintStackTrace':</p> <pre>public void java.lang.Throwable.printStackTrace()</pre>		

Finding ID:	8	Problem Type:	FindSecBugs: Cipher with no integrity (SpotBugs Security Issues)
Classification:	Warning	Date:	2020-03-07 03:15:37 - new
Rating:	8.00	Reviewed State:	Not Reviewed
Location:	SymmetricEnc_AESOFBNoPadding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>A finding identified by the external 'SpotBugs' plugin:</p> <p>The cipher does not provide data integrity</p> <p>- In method SymmetricEnc_AESOFBNoPadding.main(String[])</p>		