Security Findings of Project "DESCBCPKCS5Padding"

Analysis Date: **2020-03-07 03:30:47**

Analyzed Workspace:

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

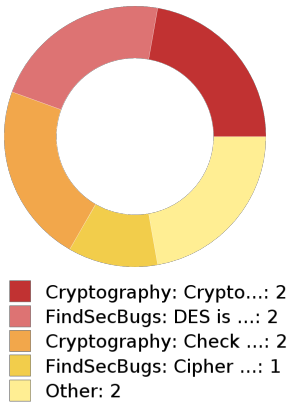
Computed Call Graph:

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

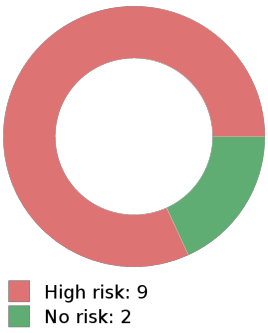
Findings in List:

All Findings:	11	Problematic Findings:	9

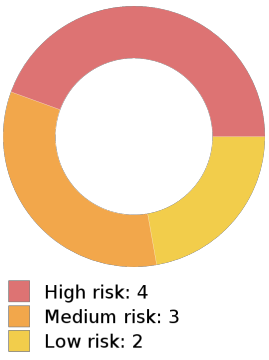
Finding Problem Types:



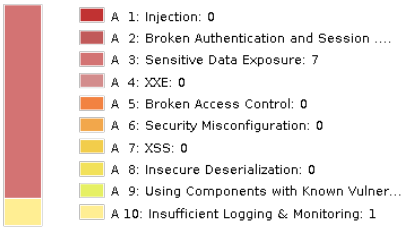
Finding Classifications:



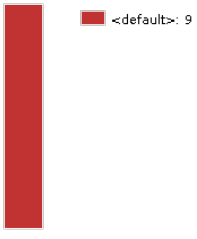
Finding Ratings:



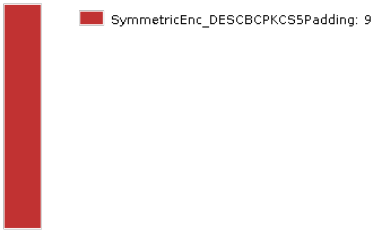
OWASP Top 10 2017



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 03:30:47 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):18		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	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_KeyGeneratorGetInstance'. Violated protocol: Check Allowed Cryptography Algorithms Protocol description: Allow only a given set of cryptography algorithm names where algorithm names are expected. The algorithm names are configured via constant value constraint variables. Names to be checked against can be found here: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html Matching pattern in protocol check kind 'AnyAlgorithm_KeyGeneratorGetInstance': static javax.crypto.KeyGenerator javax.crypto.KeyGenerator.getInstance(java.lang.String, ***)		

Finding ID:	**7**	**Problem Type:**	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	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. Violated protocol: Check Allowed Cryptography Algorithms Protocol description: Allow only a given set of cryptography algorithm names where algorithm names are expected. The algorithm names are configured via constant value constraint variables. Names to be checked against can be found here: https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html Matching pattern in protocol check kind 'AnyAlgorithm_CipherConstruction': static javax.crypto.Cipher javax.crypto.Cipher.getInstance(java.lang.String, ***)		

Findings List

Finding ID:	**4**	**Problem Type:**	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	**Date:**	2020-03-07 03:30:47 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.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 03:30:47 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.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 03:30:47 - new
Rating:	1.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.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 03:30:47 - new
Rating:	1.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):27		
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.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:	**11**	**Problem Type:**	FindSecBugs: Cipher is susceptible to Padding Oracle (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The cipher is susceptible to padding oracle attacks - In method SymmetricEnc_DESCBCPKCS5Padding.main(String[])		

Finding ID:	**9**	**Problem Type:**	FindSecBugs: DES is insecure (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):18		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: DES should be replaced with AES - In method SymmetricEnc_DESCBCPKCS5Padding.main(String[]) - Sink method javax/crypto/KeyGenerator.getInstance(Ljava/lang/String;)Ljavax/crypto/KeyGenerator; - Sink parameter 0		

Findings List

Finding ID:	**10**	**Problem Type:**	FindSecBugs: DES is insecure (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: DES should be replaced with AES - In method SymmetricEnc_DESCBCPKCS5Padding.main(String[]) - Sink method javax/crypto/Cipher.getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher; - Sink parameter 0		

Finding ID:	**3**	**Problem Type:**	Usage: PrintStackTrace (Special Code)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):38		
Tags:	no tags assigned		
Comment:	*no comment*		
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()		

Finding ID:	**8**	**Problem Type:**	FindSecBugs: Cipher with no integrity (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-03-07 03:30:47 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	SymmetricEnc_DESCBCPKCS5Padding.java (<Source Code>):27		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The cipher does not provide data integrity - In method SymmetricEnc_DESCBCPKCS5Padding.main(String[])		