

Security Findings of Project "baseCaseVariable"

Analysis Date: 2020-06-07 09:15:52

Analyzed Workspace:

Packages:	1	Total LOC:	13
Classes:	1	No. of Bytecode Instructions:	24

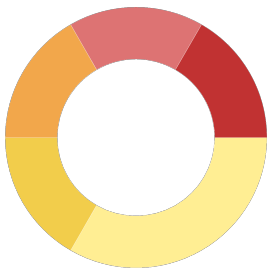
Computed Call Graph:

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

Findings in List:

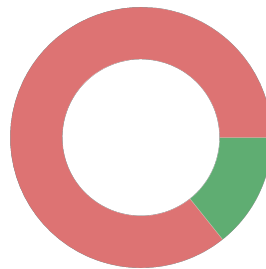
All Findings:	7	Problematic Findings:	6
---------------	---	-----------------------	---

Finding Problem Types:



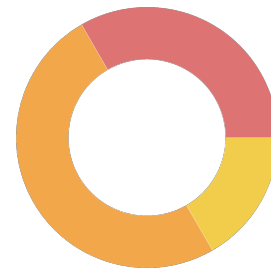
- Cryptography: AES En...: 1
- FindSecBugs: ECB mod...: 1
- Cryptography: Crypto...: 1
- Cryptography: Check ...: 1
- Other: 2

Finding Classifications:



- High risk: 6
- No risk: 1

Finding Ratings:

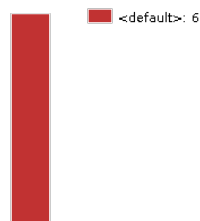


- High risk: 2
- Medium risk: 3
- Low risk: 1

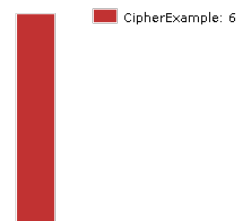
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	4	Problem Type:	Cryptography: AES Decryption (Protocol Check Findings)
Classification:	Warning	Date:	2020-06-07 09:15:52 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):11		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Cryptography: AES Decryption'. Dataflow ended in a state that was not GOOD.</p> <p>Violated protocol: Creation of an AES Cipher for Decryption Protocol description: Creation of a cipher for AES consists of creating an uninitialized cipher, and then initializing it properly, either for encryption or for decryption.</p>		

Finding ID:	5	Problem Type:	Cryptography: AES Encryption (Protocol Check Findings)
Classification:	Warning	Date:	2020-06-07 09:15:52 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):11		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	<p>An identified location for problem type 'Cryptography: AES Encryption'. Dataflow ended in a state that was not GOOD.</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>		

Findings List

Finding ID:	3	Problem Type:	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-06-07 09:15:52 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):10		
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:	2020-06-07 09:15:52 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):10		
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:	2020-06-07 09:15:52 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):10		
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

Finding ID:	7	Problem Type:	FindSecBugs: ECB mode is insecure (SpotBugs Security Issues)
Classification:	Warning	Date:	2020-06-07 09:15:52 - new
Rating:	8.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):10		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	A finding identified by the external 'SpotBugs' plugin: The cipher uses ECB mode, which provides poor confidentiality for encrypted data - In method CipherExample.main(String[])		

Finding ID:	6	Problem Type:	FindSecBugs: Cipher with no integrity (SpotBugs Security Issues)
Classification:	Warning	Date:	2020-06-07 09:15:52 - new
Rating:	8.00	Reviewed State:	Not Reviewed
Location:	CipherExample.java (<Source Code>):10		
Tags:	no tags assigned		
Comment:	<i>no comment</i>		
Description:	A finding identified by the external 'SpotBugs' plugin: The cipher does not provide data integrity - In method CipherExample.main(String[])		