Security Findings of Project "baseCase"

Analysis Date: **2020-05-15 09:02:55**

Analyzed Workspace:

Packages:	1	Total LOC:	17
Classes:	1	No. of Bytecode Instructions:	30

Computed Call Graph:

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

Findings in List:

All Findings:	6	Problematic Findings:	5

Finding Problem Types:
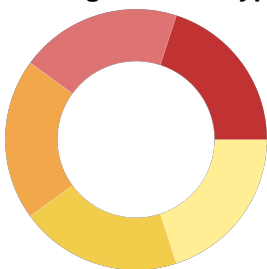
- Cryptography: Crypto...: 1
- Cryptography: Crypto...: 1
- Usage: PrintStackTra...: 1
- FindSecBugs: MD2, MD...: 1
- Other: 1

Finding Classifications:
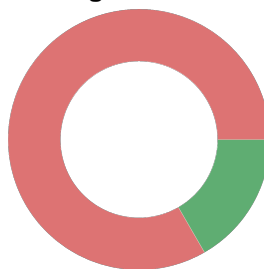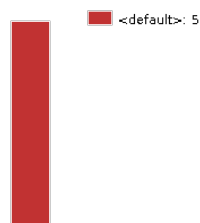
- High risk: 5
- No risk: 1

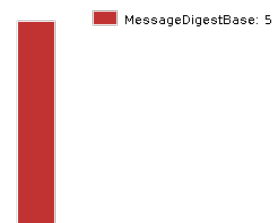**Finding Ratings:**

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

OWASP Top 10 2017

- A 1: Injection: 0
- A 2: Broken Authentication and Session ....
- A 3: Sensitive Data Exposure: 4
- A 4: XXE: 0
- A 5: Broken Access Control: 0
- A 6: Security Misconfiguration: 0
- A 7: XSS: 0
- A 8: Insecure Deserialization: 0
- A 9: Using Components with Known Vulner...
- A 10: Insufficient Logging & Monitoring: 1

Hot Spots (Packages)

- <default>: 5

Hot Spots (Classes)

- MessageDigestBase: 5

Findings List

Finding ID:	5	Problem Type:	Cryptography: Check that only allowed hash algorithms are used (Protocol Check Findings)
Classification:	Warning	Date:	2020-05-15 09:02:55 - new
Rating:	5.00	Reviewed State:	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	*no comment*		

Description: An identified location for problem type 'Cryptography: Check that only allowed hash algorithms are used'.
The protocol check detected something wrong when encountering symbol 'AnyAlgorithm_MessageDigestGetInstance'.

Violated protocol: Check Allowed Hash Algorithms
Protocol description:
Allow only a given set of hash 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_MessageDigestGetInstance':
static java.security.MessageDigest java.security.MessageDigest.getInstance(java.lang.String, ***)

Finding ID:	3	Problem Type:	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	Date:	2020-05-15 09:02:55 - new
Rating:	0.00	Reviewed State:	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	*no comment*		

Description: An identified location for problem type 'Cryptography: Cryptographic Algorithms Used in Project'.
Declared in: java.security.MessageDigest

Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms Used in Project':
static java.security.** java.security.**.getInstance(java.lang.String)

Finding ID:	1	Problem Type:	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
Classification:	Warning	Date:	2020-05-15 09:02:55 - new
Rating:	1.00	Reviewed State:	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	*no comment*		

Description: An identified location for problem type 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider'.
Declared in: java.security.MessageDigest

Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider':
static java.security.** java.security.**.getInstance(java.lang.String)

Findings List

Finding ID:	4	Problem Type:	Cryptography: Cryptographic Hashing (Protocol Check Findings)
Classification:	Warning	**Date:**	2020-05-15 09:02:55 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):10		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Cryptography: Cryptographic Hashing'. Dataflow ended in a state that was not GOOD. Violated protocol: MessageDigest Use for Cryptographic Hashing Protocol description: A MessageDigest instance is created and used for cryptographic hashing.		

Finding ID:	6	Problem Type:	FindSecBugs: MD2, MD4 and MD5 are weak hash functions (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-05-15 09:02:55 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):9		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: MD5 is not a recommended cryptographic hash function - In method MessageDigestBase.main(String[]) - Value MD5		

Finding ID:	2	Problem Type:	Usage: PrintStackTrace (Special Code)
Classification:	Warning	**Date:**	2020-05-15 09:02:55 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	MessageDigestBase.java (<Source Code>):14		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: PrintStackTrace'. Declared in: java.security.NoSuchAlgorithmException Matching pattern in special code kind 'Usage: PrintStackTrace': public void java.lang.Throwable.printStackTrace()		