# Security Findings of Project "replaceSHA256DES"

**Analysis Date:**　　　　　　**2020-06-04 05:16:38**

## Analyzed Workspace:

| | | | |
|---|---|---|---|
| Packages: | 1 | Total LOC: | 16 |
| Classes: | 1 | No. of Bytecode Instructions: | 41 |

## Computed Call Graph:

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

## Findings in List:

| | | | |
|---|---|---|---|
| All Findings: | 4 | Problematic Findings: | 3 |

## Finding Problem Types:

- Cryptography: Crypto...: 1
- Cryptography: Crypto...: 1
- Cryptography: Check ...: 1

## Finding Classifications:
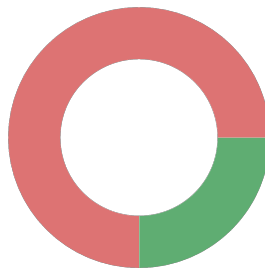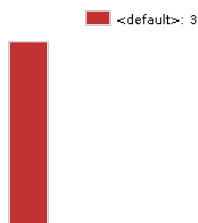
- High risk: 3
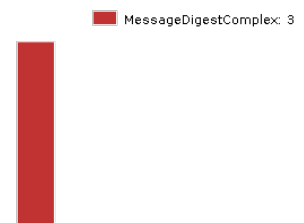- No risk: 1

## Finding Ratings:

- Medium risk: 2
- Low risk: 1

### OWASP Top 10 2017

- A 1: Injection: 0
- A 2: Broken Authentication and Session ....
- A 3: Sensitive Data Exposure: 3
- 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: 0

### Hot Spots (Packages)

- <default>: 3

### Hot Spots (Classes)

- MessageDigestComplex: 3

# Findings List

| | | | |
|---|---|---|---|
| **Finding ID:** | 4 | **Problem Type:** | Cryptography: Check that only allowed hash algorithms are used (Protocol Check Findings) |
| **Classification:** | Warning | **Date:** | 2020-06-04 05:16:38 - new |
| **Rating:** | 5.00 | **Reviewed State:** | Not Reviewed |
| **Location:** | MessageDigestComplex.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:** | 2 | **Problem Type:** | Cryptography: Cryptographic Algorithms Used in Project (Special Code) |
| **Classification:** | Information | **Date:** | 2020-06-04 05:16:38 - new |
| **Rating:** | 0.00 | **Reviewed State:** | Not Reviewed |
| **Location:** | MessageDigestComplex.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:** | 2020-06-04 05:16:38 - new |
| **Rating:** | 1.00 | **Reviewed State:** | Not Reviewed |
| **Location:** | MessageDigestComplex.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:** | **3** | **Problem Type:** | Cryptography: Cryptographic Hashing (Protocol Check Findings) |
| **Classification:** | Warning | **Date:** | 2020-06-04 05:16:38 - new |
| **Rating:** | 5.00 | **Reviewed State:** | Not Reviewed |
| **Location:** | MessageDigestComplex.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. <br><br> Violated protocol: MessageDigest Use for Cryptographic Hashing <br> Protocol description: <br> A MessageDigest instance is created and used for cryptographic hashing. | | |