

## Security Findings of Project "BlowfishCBCPKCS5Padding"

**Analysis Date:** 2020-03-07 03:20:28

### Analyzed Workspace:

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

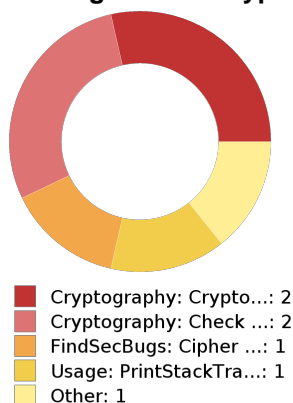
### Computed Call Graph:

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

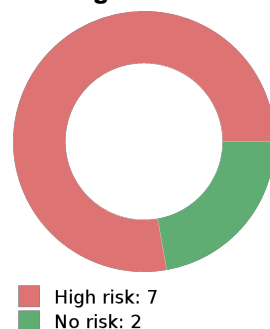
### Findings in List:

All Findings:	9	Problematic Findings:	7
---------------	---	-----------------------	---

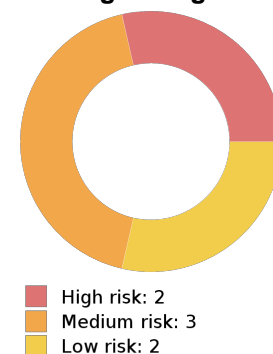
#### Finding Problem Types:



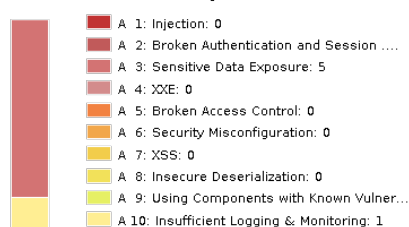
#### Finding Classifications:



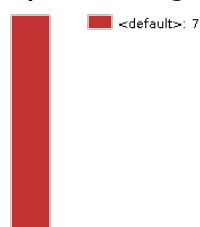
#### Finding Ratings:



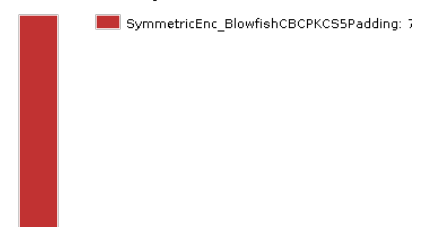
#### OWASP Top 10 2017



#### Hot Spots (Packages)



#### Hot Spots (Classes)



## Findings List

<b>Finding ID:</b>	6	<b>Problem Type:</b>	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	5.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):18		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	no comment		
<b>Description:</b>	<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_KeyGeneratorGetInstance'.</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: <a href="https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html">https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html</a></p> <p>Matching pattern in protocol check kind 'AnyAlgorithm_KeyGeneratorGetInstance':</p> <pre>static javax.crypto.KeyGenerator javax.crypto.KeyGenerator.getInstance(java.lang.String, ***)</pre>		

<b>Finding ID:</b>	7	<b>Problem Type:</b>	Cryptography: Check that only allowed crypto algorithms are used (Protocol Check Findings)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	5.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):27		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	no comment		
<b>Description:</b>	<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: <a href="https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html">https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html</a></p> <p>Matching pattern in protocol check kind 'AnyAlgorithm_CipherConstruction':</p> <pre>static javax.crypto.Cipher javax.crypto.Cipher.getInstance(java.lang.String, ***)</pre>		

### Findings List

<b>Finding ID:</b>	<b>4</b>	<b>Problem Type:</b>	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
<b>Classification:</b>	Information	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	0.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):18		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	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)		

<b>Finding ID:</b>	<b>5</b>	<b>Problem Type:</b>	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
<b>Classification:</b>	Information	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	0.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):27		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	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)		

<b>Finding ID:</b>	<b>1</b>	<b>Problem Type:</b>	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	1.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):18		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	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

<b>Finding ID:</b>	<b>2</b>	<b>Problem Type:</b>	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	1.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):27		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	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)		

<b>Finding ID:</b>	<b>9</b>	<b>Problem Type:</b>	FindSecBugs: Cipher is susceptible to Padding Oracle (SpotBugs Security Issues)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	8.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):27		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	A finding identified by the external 'SpotBugs' plugin: The cipher is susceptible to padding oracle attacks  - In method SymmetricEnc_BlowfishCBCPKCS5Padding.main(String[])		

<b>Finding ID:</b>	<b>3</b>	<b>Problem Type:</b>	Usage: PrintStackTrace (Special Code)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	5.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):38		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	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()		

### Findings List

<b>Finding ID:</b>	8	<b>Problem Type:</b>	FindSecBugs: Cipher with no integrity (SpotBugs Security Issues)
<b>Classification:</b>	Warning	<b>Date:</b>	2020-03-07 03:20:28 - new
<b>Rating:</b>	8.00	<b>Reviewed State:</b>	Not Reviewed
<b>Location:</b>	SymmetricEnc_BlowfishCBCPKCS5Padding.java (<Source Code>):27		
<b>Tags:</b>	no tags assigned		
<b>Comment:</b>	<i>no comment</i>		
<b>Description:</b>	A finding identified by the external 'SpotBugs' plugin: The cipher does not provide data integrity  - In method SymmetricEnc_BlowfishCBCPKCS5Padding.main(String[])		