

Security Findings of Project "basecase"

Analysis Date: 2020-03-10 14:40:25

Analyzed Workspace:

| | | | |
|-----------|---|-------------------------------|----|
| Packages: | 1 | Total LOC: | 22 |
| Classes: | 1 | No. of Bytecode Instructions: | 63 |

Computed Call Graph:

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

Findings in List:

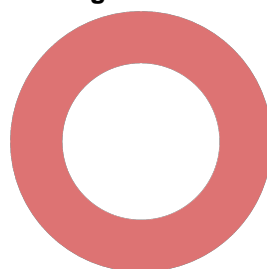
| | | | |
|---------------|---|-----------------------|---|
| All Findings: | 2 | Problematic Findings: | 2 |
|---------------|---|-----------------------|---|

Finding Problem Types:



■ Cryptography: Constr...: 2

Finding Classifications:



■ High risk: 2

Finding Ratings:

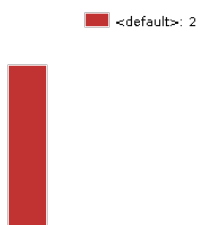


■ Medium risk: 2

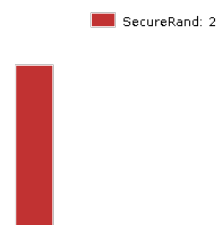
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

| | | | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------|
| Finding ID: | 1 | Problem Type: | Cryptography: Construction of Secure Random Number Generator (Protocol Check Findings) |
| Classification: | Warning | Date: | 2020-03-10 14:40:25 - new |
| Rating: | 5.00 | Reviewed State: | Not Reviewed |
| Location: | SecureRand.java (<Source Code>):10 | | |
| Tags: | no tags assigned | | |
| Comment: | <i>no comment</i> | | |
| Description: | <p>An identified location for problem type 'Cryptography: Construction of Secure Random Number Generator'.</p> <p>The seed data being used is not guaranteed to be strongly random.</p> <p>Violated protocol: Construction of a Strong Random Number Generator</p> <p>Protocol description:</p> <p>Constructing a strong random number generator.</p> <p>Matching pattern in protocol check kind 'SetStronglyRandomSeed':</p> <p>void java.security.SecureRandom.setSeed(byte[])</p> | | |

| | | | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------|
| Finding ID: | 2 | Problem Type: | Cryptography: Construction of Secure Random Number Generator (Protocol Check Findings) |
| Classification: | Warning | Date: | 2020-03-10 14:40:25 - new |
| Rating: | 5.00 | Reviewed State: | Not Reviewed |
| Location: | SecureRand.java (<Source Code>):11 | | |
| Tags: | no tags assigned | | |
| Comment: | <i>no comment</i> | | |
| Description: | <p>An identified location for problem type 'Cryptography: Construction of Secure Random Number Generator'.</p> <p>The seed data being used is not guaranteed to be strongly random.</p> <p>Violated protocol: Construction of a Strong Random Number Generator</p> <p>Protocol description:</p> <p>Constructing a strong random number generator.</p> <p>Matching pattern in protocol check kind 'SetStronglyRandomSeed':</p> <p>void java.security.SecureRandom.setSeed(byte[])</p> | | |