

Software Verification

Static Analysis Report

Team 5

201410373 고예은

201411266 김수현

201411268 김아름

Index

1. Code Inspector	3
1.1. Rules	3
1.2. Analysis Result	3
2. SonarQube	8
2.1. URL.....	8
2.2. Rules	8
2.3. Analysis Result	9
3. FindBugs.....	11
3.1. Rules	11
3.2. Analysis Result	11
4. Pmd.....	12
4.1. Rules	12
4.2. Analysis Result	12

1. Code Inspector

1.1. Rules

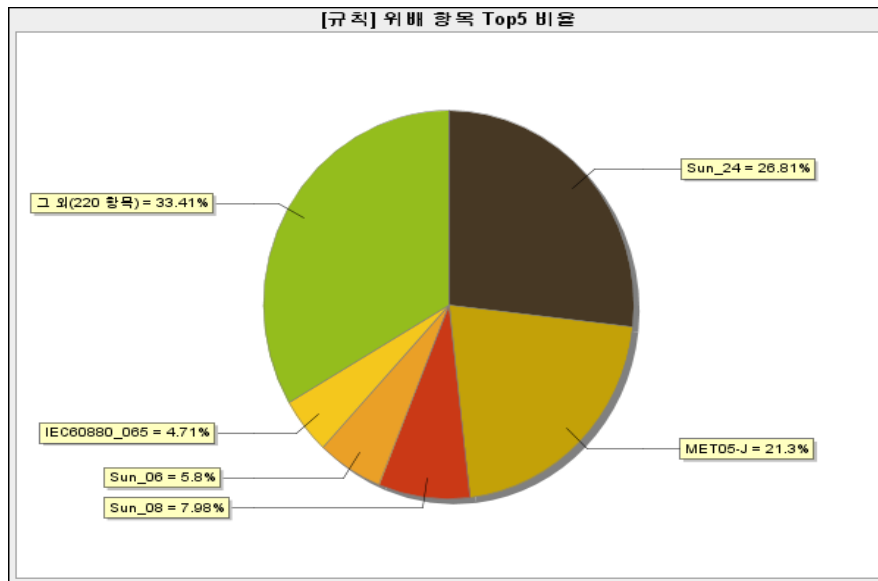
규칙 모음	규칙 수	위배 수	설명
Sun_Code_Conventions_for_Java	27	961	파일이름, 파일 구성, 들여쓰기, 주석, 선언, 문장, 이름 규칙, 프로그래밍 practice 등 Sun 에서 따르기를 권고하는 표준 코딩 가이드라인
CERT_Secure_Coding_Standard	99	440	Java Platform standard edition 6,7 에 대한 시큐어 프로그래밍을 위한 Rule 과 recommendation 제시
CODESCROLL_JAVA_RULES	72	136	일반적인 자바프로그램에서 지켜야 할 규칙과 권고들
IEC_60880	7	108	Nuclear Power Plants 의 안전성을 위한 표준
EGOV_Inspection_Standard	20	97	전자정부 표준 Inspection 규칙모음

Code Inspector 에서는 여러 규칙 모음을 제공함

다양한 규칙 모음을 선택하고 결과에서 심각도가 높은 것들을 뽑아 확인

1.2. Analysis Result

1.2.1. Overview



규칙	규칙 모음	위배 수	무시된 위배 수	규칙 설명
Sun_24	Sun_Code_Conventions_for_Java	467	0	숫자 상수 사용 금지
MET05-J	CERT_Secure_Coding_Standard	371	0	생성자에서 override 가능한 메서드를 호출하면 안 된다
Sun_08	Sun_Code_Conventions_for_Java	139	0	블록의 시작 부분에서만 선언 검사
Sun_06	Sun_Code_Conventions_for_Java	101	0	소스 라인 길이 검사
IEC60880_065	IEC_60880	82	0	if 가 있다면 else 가 반드시 있는 지 검사

1.2.2. Violations

- 필드의 이름(Name)이 규칙($^{\wedge}[a-z]([a-z][A-Z][0-9])^*$)에 맞지 않음.

```
121 :     private String Name;
```

[EGOV_26_VariableNamingConventions] 필드의 이름(Name)이 규칙($^{\wedge}[a-z]([a-z][A-Z][0-9])^*$)에 맞지 않음.

[Sun_20] 필드의 이름(Name)이 규칙($^{\wedge}[a-z]([a-z][A-Z][0-9])^*$)에 맞지 않음.

[Sun_05] 필드의 선언문이 메서드 선언문보다 코드상 뒤 쪽에 존재함

[EGOV_37_UnusedPrivateField] private 필드 Name 을 사용하지 않음

- 적절한 로그를 사용하지 않음. (println)가 사용됨.
(실제로 소스코드를 실행시켰을 때 콘솔에 log 가 남음 - 개발 완료 후 삭제 필요)

```
150 :         System.out.println(UserCount);
```

[EGOV_25_SystemPrintln] 메서드 (println)가 사용됨.

[ERR02-J] 적절한 로그를 사용하지 않음.

```
151 :         System.out.println(JackpotNum);
```

[EGOV_25_SystemPrintln] 메서드 (println)가 사용됨.

- Exception catch & printStackTrace 사용
(시스템 내부 데이터나 디버깅 관련 정보가 공개되면 공격의 빌미가 될 수 있다. 따라서 예외 발생 시 스택 정보를 출력하지 말아야 한다.)

```
16 :             } catch (Exception e) {
```

[ERR08-J] (Exception)을 catch함.

```
17 :                 e.printStackTrace();
```

[JAVA_44] 메서드 (printStackTrace)가 사용됨.

- identifier(frame)가 이미 필드로 선언되어 있어 hide 가 발생함

```
6 :     private static MainFrame frame;
```

```
7 :     public static void main(String[] args) {
```

[JAVA_72] 메서드의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음

```
8 :         // TODO Auto-generated method stub
```

```
9 :
```

```
10 :         try {
```

```
11 :             Main_controller main = new Main_controller();
```

```
12 :             MainFrame frame = main.getMainFrame();
```

[Sun_09] identifier(frame)가 이미 필드로 선언되어 있어 hide가 발생함

[Sun_23] 클래스 object를 이용하여 static 멤버에접근.

[JAVA_70] identifier(frame)가 이미 필드로 선언되어 있어 hide가 발생함

- 설명 주석 내용이 비어 있음. 의미 없는 주석 과다

```

8 : public class Manager {
    [JAVA_71] 클래스의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음
    [OBJ04-J] mutable 클래스가 신뢰할 수 없는 코드에 객체를 안전하게 전달하기 위한 복사 기능을 제공하지 않음.
9 :
10 :     /**
11 :      * Default constructor
12 :      */
13 :     public Manager(int id, int pw) {
    [JAVA_72] 메서드의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음
14 :         ManagerID=id;
15 :         ManagerPW=pw;
16 :     }
17 :
18 :     /**
19 :      *
20 :      */
21 :     private int ManagerID;
    [EGOV_26_VariableNamingConventions] 필드의 이름(ManagerID)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_20] 필드의 이름(ManagerID)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_05] 필드의 선언문이 메서드 선언문보다 코드상 뒤 쪽에 존재함
22 :
23 :     /**
24 :      *
25 :      */
26 :     private int ManagerPW;
    [EGOV_26_VariableNamingConventions] 필드의 이름(ManagerPW)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_20] 필드의 이름(ManagerPW)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_05] 필드의 선언문이 메서드 선언문보다 코드상 뒤 쪽에 존재함
27 :
28 :
29 :     /**
30 :      * @param inputID
31 :      * @return
32 :      */
33 :     public Boolean checkID(int inputID) {
    [JAVA_72] 메서드의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음

```

- public 메서드에서 private 필드 리턴 시 레퍼런스를 그대로 리턴함.
moneycount: private

```

32 :     public MoneyCount getATMcount() {
    [JAVA_72] 메서드의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음
33 :         return moneycount;
    [OBJ05-J] public 메서드에서 private 필드 리턴 시 레퍼런스를 그대로 리턴함.
34 :     }

```

- non-static 필드가 public으로 선언

```

132 :     public Set<Card> Have;
    [EGOV_26_VariableNamingConventions] 필드의 이름(Have)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_20] 필드의 이름(Have)이 규칙(^[a-z]([a-z]|[A-Z]|[0-9])*)에 맞지 않음.
    [Sun_05] 필드의 선언문이 메서드 선언문보다 코드상 뒤 쪽에 존재함
    [Sun_22] non-static 필드가 public으로 선언.

```

- 사용하지 않는 private 필드 존재
(TotalMoney, inputPW 등이 뒤에서 데이터를 저장하는 데에 쓰이긴 하나 활용되는 곳이 없음. 의미 없는 변수)

```
46 : private int TotalMoney;
```

[EGOV_26_VariableNamingConventions] 필드의 이름(TotalMoney)이 규칙(^[a-z]([a-z]|([A-Z]|([0-9]))*))에 맞지 않음.

[Sun_20] 필드의 이름(TotalMoney)이 규칙(^[a-z]([a-z]|([A-Z]|([0-9]))*))에 맞지 않음.

[Sun_05] 필드의 선언문이 메서드 선언문보다 코드상 뒤 쪽에 존재함

[EGOV_37_UnusedPrivateField] private 필드 TotalMoney 을 사용하지 않음

- switch 문은 두 개 이상의 case 를 가져야 함
이 경우 if 문을 사용할 것을 권장함

```
122     switch (inputMenu) {
123     case 5:
124         if(manager.checkID(input)) {
125             return true;
126         }
127         return false;
128
129     default:
130         for(int index=0; index<bank.size(); index++) {
131             int check=bank.get(index).searchID(input,1);
132             if(check==1) {
133                 currentbank=bank.get(index);
134                 return true;
135             }
136         }
137         break;
138     }
```

- 생성자 내에서 final 이나 private 이 아닌 메서드를 호출함
생성자 내에서 override 가능한 메서드를 호출해서는 안 됨

```
35 : public MainFrame() {
```

[JAVA_72] 메서드의 설명 주석이 없거나, 설명 주석 내용에 모든 태그가 포함되어있지 않음

[Sun_05] 생성자의 선언이 메서드 선언보다 코드상 뒤 쪽에 존재함

```
36 :
```

```
37 :         setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
```

[MET05-J] 생성자 내에서 final 이나 private 이 아닌 메서드를 호출함.

```
38 :         setBounds(100, 100, 540, 400);
```

[Sun_24] 숫자 상수를 사용함(for loop의 counter로 -1이나 0, 1을 사용하는 경우 제외)

[MET05-J] 생성자 내에서 final 이나 private 이 아닌 메서드를 호출함.

```
39 :         contentPane = new JPanel();
```

```
40 :         contentPane.setBorder(new EmptyBorder(5, 5, 5, 5));
```

[Sun_24] 숫자 상수를 사용함(for loop의 counter로 -1이나 0, 1을 사용하는 경우 제외)

```
41 :         setContentPane(contentPane);
```

[MET05-J] 생성자 내에서 final 이나 private 이 아닌 메서드를 호출함.

```
42 :         contentPane.setLayout(null);
```

[MET05-J] 생성자 내에서 final 이나 private 이 아닌 메서드를 호출함.

```
43 :
```

- 함수는 최소의 exit point 를 가져야 함

```
59 public Boolean ATMBalanceUpdate(int inputMoney, int inputcount, int inputPOM) {
60     // TODO implement here
61     switch (inputMoney) {
62     case 50000:
63         if(inputPOM < 0) {
64             if(Count50000>=inputcount) {
65                 Count50000+=inputcount*inputPOM;
66                 return true;
67             }
68             else return false;
69         }
70         else {
71             Count50000+=inputcount*inputPOM;
72             return true;
73         }
74     case 10000:
75         if(inputPOM < 0) {
76             if(Count10000>=inputcount) {
77                 Count10000+=inputcount*inputPOM;
78                 return true;
79             }
80             else return false;
81         }
82         else {
83             Count10000+=inputcount*inputPOM;
84             return true;
85         }
86     case 5000:
87         if(inputPOM < 0) {
88             if(Count5000>=inputcount) {
89                 Count5000+=inputcount*inputPOM;
90                 return true;
91             }
92             else return false;
93         }
94         else {
95             Count5000+=inputcount*inputPOM;
96             return true;
97         }
98     case 1000:
99         if(inputPOM < 0) {
100             if(Count1000>=inputcount) {
101                 Count1000+=inputcount*inputPOM;
102                 return true;
103             }
104             else return false;
105         }
106         else {
107             Count1000+=inputcount*inputPOM;
108             return true;
109         }
110     default:
111         break;
112     }
113     return false;
114 }
115 }
```

2. SonarQube

2.1. URL

- http://106.10.40.194:9000/dashboard?id=Jackpot_ATM

2.2. Rules

- Plugins 설치: FindBugs, pmd
- Rule List

Sonar way 사용

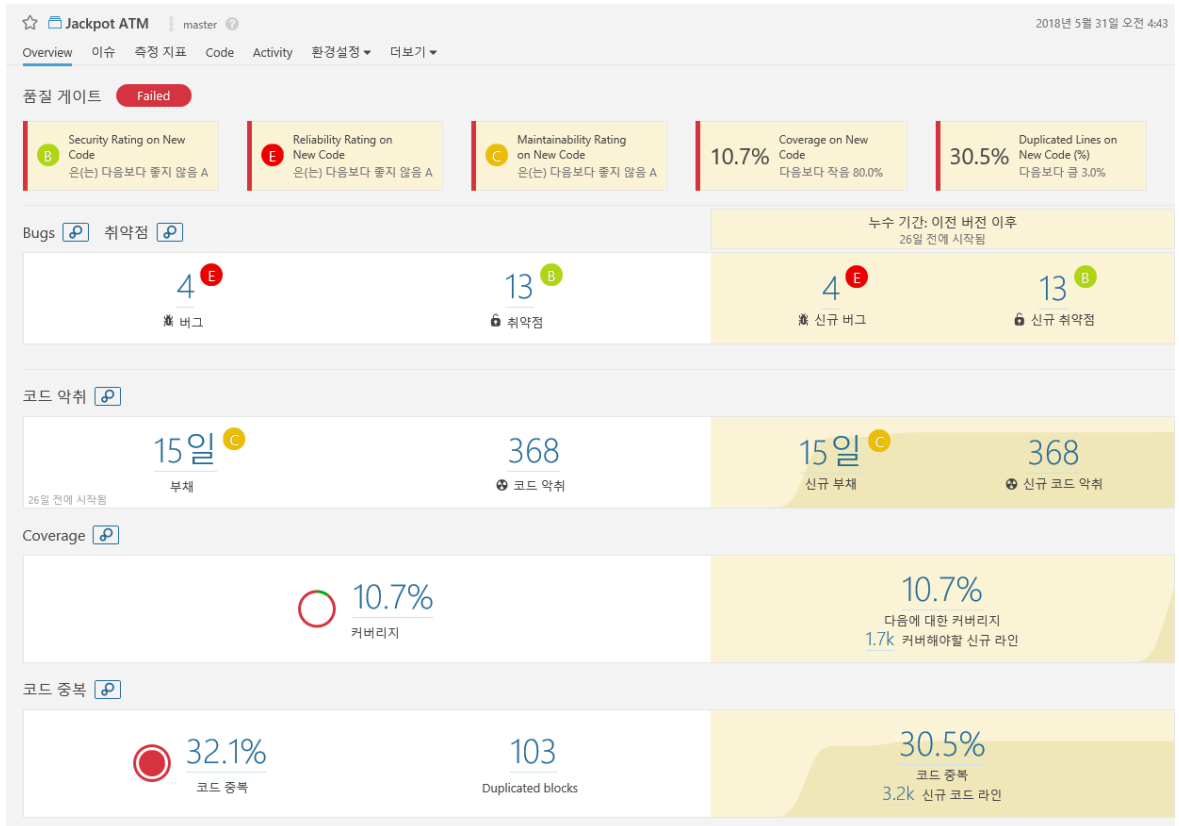
▼ 규칙	
Local variable and method parameter name	77
Track uses of "TODO" tags	49
Anonymous inner classes containing only one	31
Field names should comply with a naming conv	27
Sections of code should not be "commented o	23
String literals should not be duplicated	18
Class names should comply with a naming conv	16
Inheritance tree of classes should not be too	15
Method names should comply with a naming conv	13
Cognitive Complexity of methods should not	12
Throwable.printStackTrace(...) should not be	10
Unused local variables should be removed	10
Package names should comply with a naming conv	9
The diamond operator ("<>") should be used	8
Useless imports should be removed	7

FindBugs 사용

Style - Dead store to local variable	9
l18n - Reliance on default encoding	6
Style - Write to static field from instance method	6
Performance - Unread field	3
Style - Switch statement found where default	2
Performance - Unused field	2
Style - Dead store to local variable that shadows	1
Malicious code - Field should be package private	1
Style - Dereference of the result of readLine()	1
Correctness - Nullcheck of value previously checked	1
Style - Unused public or protected field	1
Correctness - Unwritten field	1

2.3. Analysis Result

2.3.1. Overview



- SonarQube 에서 Coverage 확인

	Coverage	Uncovered lines	Uncovered conditions
Test/src/main/java/View/Main_controller.java	0.0%	12	-
Test/src/main/java/View/MainFrame.java	0.0%	1,187	382
Test/src/main/java/System/MoneyCount.java	9.8%	34	21
Test/src/main/java/System/System_Control.java	17.5%	131	90
Test/src/main/java/DataBase/Bank.java	47.8%	33	27
Test/src/main/java/User/Card.java	50.0%	4	3
Test/src/main/java/System/Timer.java	51.6%	37	7
Test/src/main/java/User/Account.java	52.4%	51	9
Test/src/main/java/DataBase/Manager.java	100%	0	0

- Jacoco Code Coverage Report 로 Coverage 확인

Element	Missed Instructions	Cov.	Missed Branches	Cov.	Missed	Cxty	Missed	Lines	Missed	Methods	Missed	Classes
View	7,377 of 8,229	0%	539 of 599	0%	273	273	1,199	1,199	82	82	47	47
System		28%		15%	89	105	202	281	18	27	0	3
User		54%		60%	13	26	55	110	4	11	0	2
DataBase		62%		43%	19	33	33	81	3	8	0	2
Total	7,377 of 8,229	10%	539 of 599	10%	394	437	1,489	1,671	107	128	47	54

- 참고) 모델링 팀이 작성한 JUnit Test 에 대한 Report

Test Summary

18 tests	0 failures	0 ignored	0.305s duration	100% successful

Packages **Classes**

Class	Tests	Failures	Ignored	Duration	Success rate
DataBase.BankTest	2	0	0	0.070s	100%
DataBase.ManagerTest	2	0	0	0.011s	100%
System.System_ControlTest	8	0	0	0.171s	100%
User.AccountTest	6	0	0	0.053s	100%

특정 중요 함수만 Unit Testing 하였음

2.3.2. Issues (Code Inspector와 중복 내용 생략)

- Local variable and method parameter names should comply with a naming convention

Test/src/main/java/System/System_Control.java

Rename this local variable to match the regular expression '[a-z][a-zA-Z0-9]*\$'. ... 8일 전 L264 convention

Code Smell Minor Open Administrator 2min effort 코멘트

Test/src/main/java/System/Timer.java

Rename this local variable to match the regular expression '[a-z][a-zA-Z0-9]*\$'. ... 8일 전 L148 convention

Code Smell Minor Open Administrator 2min effort 코멘트

Test/src/main/java/User/Account.java

Rename this local variable to match the regular expression '[a-z][a-zA-Z0-9]*\$'. ... 8일 전 L27 convention

Code Smell Minor Open Administrator 2min effort 코멘트

Rename this local variable to match the regular expression '[a-z][a-zA-Z0-9]*\$'. ... 8일 전 L28 convention

Code Smell Minor Open Administrator 2min effort 코멘트

- Track uses of "TODO" tags

```
public int searchID(int inputID, int choose) {
    // TODO implement here
}
```

Complete the task associated to this TODO comment. ... 8일 전 L56 cwe

Code Smell Info Open Administrator 코멘트

- String literals should not be duplicated

```
File f = new File("date.txt");
```

Define a constant instead of duplicating this literal "date.txt" 4 times. ... 8일 전 L33 design

Code Smell Critical Open Administrator 10min effort 코멘트

3. FindBugs

3.1. Rules

- 위의 SonarQube에서 확인한 FindBugs 규칙과 동일

3.2. Analysis Result

3.2.1. Overview

- Jenkins 에 plugin 설치 후 gradle 빌드로 자동 xml report 생성

FindBugs Result

Warnings Trend

All Warnings	New this build	Fixed Warnings
34	34	0

Summary

Total	High Priority	Normal Priority	Low Priority
34	0	0	34

Details

Package	Total	Distribution
DataBase	2	
System	8	
User	7	
View	17	
Total	34	

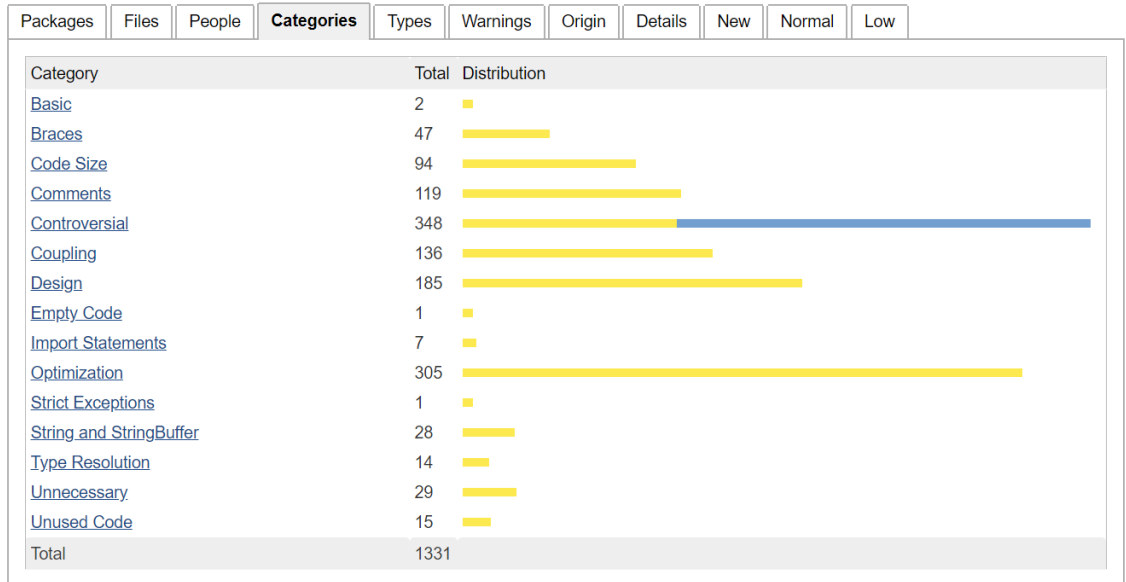
3.2.2. Warnings

File	Package	Priority	Rank	Type	Category
Bank.java-1	DataBase	Low	18	UUF_UNUSED_FIELD	PERFORMANCE
Bank.java-15	DataBase	Low	18	URF_UNREAD_FIELD	PERFORMANCE
System_Controller.java-1	System	Low	18	UUF_UNUSED_FIELD	PERFORMANCE
System_Controller.java-110	System	Low	15	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
System_Controller.java-190	System	Low	19	SF_SWITCH_NO_DEFAULT	STYLE
System_Controller.java-284	System	Low	19	SF_SWITCH_NO_DEFAULT	STYLE
System_Controller.java-339	System	Low	11	RCH_REDUNDANT_NULLCHECK_WOULD_HAVE_BEEN_A_NPE	CORRECTNESS
Times.java-38	System	Low	19	DM_DEFAULT_ENCODING	IN8N
Times.java-50	System	Low	19	DM_DEFAULT_ENCODING	IN8N
Times.java-85	System	Low	19	DM_DEFAULT_ENCODING	IN8N
Account.java-1	User	Low	17	UUF_UNUSED_PUBLIC_OR_PROTECTED_FIELD	STYLE
Account.java-22	User	Low	18	URF_UNREAD_FIELD	PERFORMANCE
Account.java-33	User	Low	19	DM_DEFAULT_ENCODING	IN8N
Account.java-38	User	Low	15	NP_DEREFERENCE_OF_READLINE_VALUE	STYLE
Account.java-45	User	Low	19	DM_DEFAULT_ENCODING	IN8N
Account.java-104	User	Low	18	URF_UNREAD_FIELD	PERFORMANCE
Account.java-203	User	Low	19	DM_DEFAULT_ENCODING	IN8N
MainFrame.java-1	View	Low	18	MS_PKGPROTECT	MALICIOUS_CODE
MainFrame.java-54	View	Low	17	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
MainFrame.java-68	View	Low	17	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
MainFrame.java-81	View	Low	17	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
MainFrame.java-94	View	Low	17	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
MainFrame.java-107	View	Low	17	ST_WRITE_TO_STATIC_FROM_INSTANCE_METHOD	STYLE
MainFrame.java-312	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-654	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-743	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-832	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-1011	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-1199	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-1265	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-1394	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
MainFrame.java-1490	View	Low	17	DLS_DEAD_LOCAL_STORE	STYLE
Main_controller.java-12	View	Low	11	DLS_DEAD_LOCAL_STORE_SHADOWS_FIELD	STYLE
Main_controller.java-23	View	Low	12	UWF_UNWRITTEN_FIELD	CORRECTNESS

4. Pmd

4.1. Rules

- Rule Sets



4.2. Analysis Result

4.2.1. Overview

- Jenkins 에 plugin 설치 후 gradle 빌드로 자동 xml report 생성

PMD Result

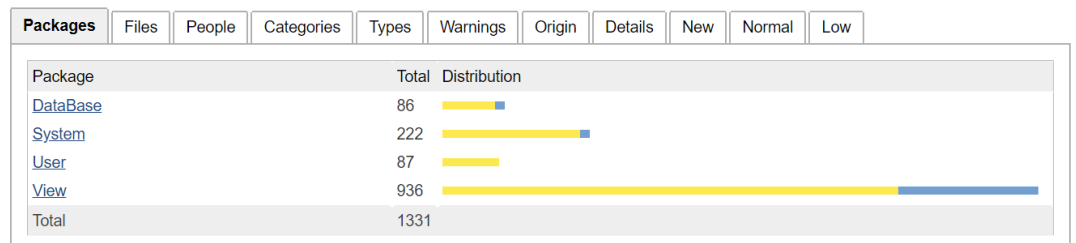
Warnings Trend

All Warnings	New Warnings	Fixed Warnings
1331	1331	0

Summary

Total	High Priority	Normal Priority	Low Priority
1331	0	1102	229

Details



4.2.2. Warnings Types

- 자세한 warning 내용은 지면 상 생략 (Jenkins 에서 report 참고 가능)

