



Breizh C@mp
Mix de technologies

DIY: Java Static Analysis

#sonarqube

Nicolas PERU - @benzonico
@sonarsource



Ego boost

- Java developer
- Developer @Sonarsource
 - Developer in language team
 - Lead of sonar java plugin
- Twitter / github : @benzonico
- Geneva Jug enthusiast



Static Analysis

Analyze code,

without executing it.



Code Quality

Continuous Inspection

sonarqube





Sonar Java Plugin

- Back Story





Challenge

Get the language.

```
import java.io.*;
import java.net.*;
import java.security.*;
import protection;

public class Client {
    public void sendAuthentication(String user, String password) throws IOException {
        OutputStream outStream = new DataOutputStream(out);
        long t1 = (new Date()).getTime();
        double q1 = Math.random();
        byte[] protected1 = Protection.mangle(q1, t1);
        long t2 = (new Date()).getTime();
        double q2 = Math.random();
        byte[] protected2 = Protection.mangle(q2, t2);
        out.writeUTF(user);
        out.writeInt(protected1.length);
        out.write(protected2);
        out.flush();
    }
}

public static void main(String[] args) {
    String host = args[0];
    int port = 7999;
    String user = "John";
    String password = "shh";
    Socket s = new Socket(host, port);
    Client client = new Client(s);
    client.sendAuthentication(user, password);
}
```

CHALLENGE ACCEPTED.





Lexical Analysis

Chez SonarSource il y a 31 employés mais

--	--	--	--	--	--	--

certains boivent plus de café que d'autres.



Syntactic Analysis

Chez SonarSource il y a 31 employés mais

certains boivent plus de café que d'autres.

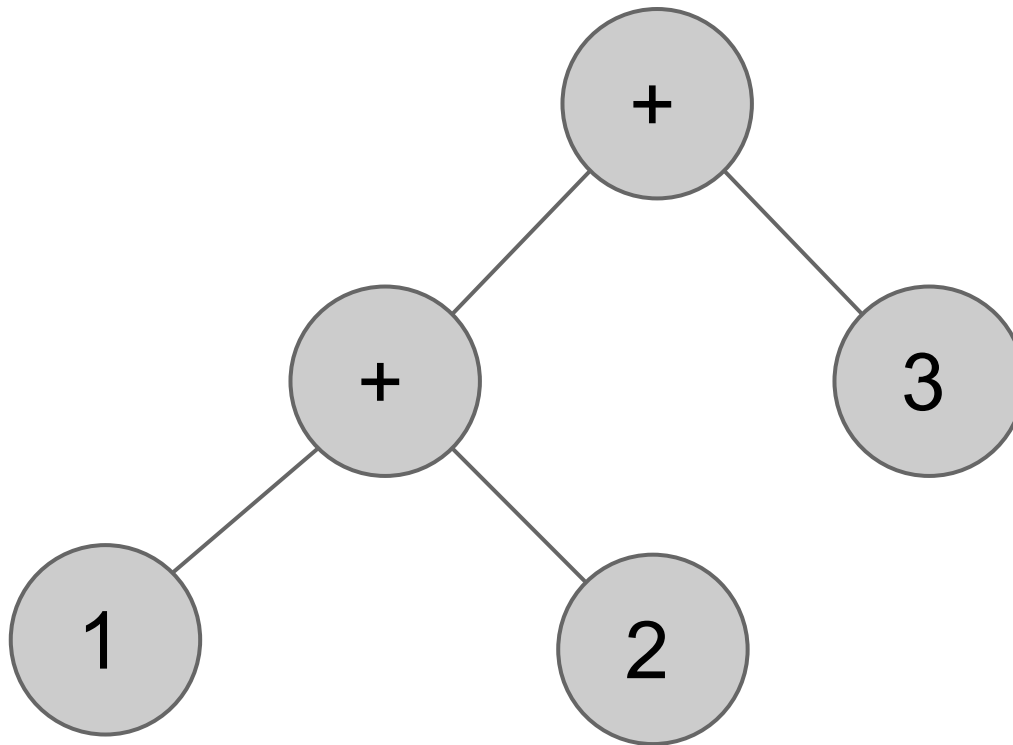
Sujets

Verbes



Syntax Tree

1 + 2 + 3





Java pop quizz !!

[]



[]) [] [] {



```
int[] foo(int a[]) [][] {  
    return null;  
}
```



```
int[] foo(int a[] ) [][] {  
    return null;  
}
```



```
int[ ][ ][ ] foo(int[ ] a){  
    return null;  
}
```



Semantic Analysis

Chez SonarSource il y a 31 **employés** mais
certains boivent plus de café que d'**autres**.



Java pop quizz !!

```
class Foo<T> {  
    class T {  
    }  
    T myField;  
}
```



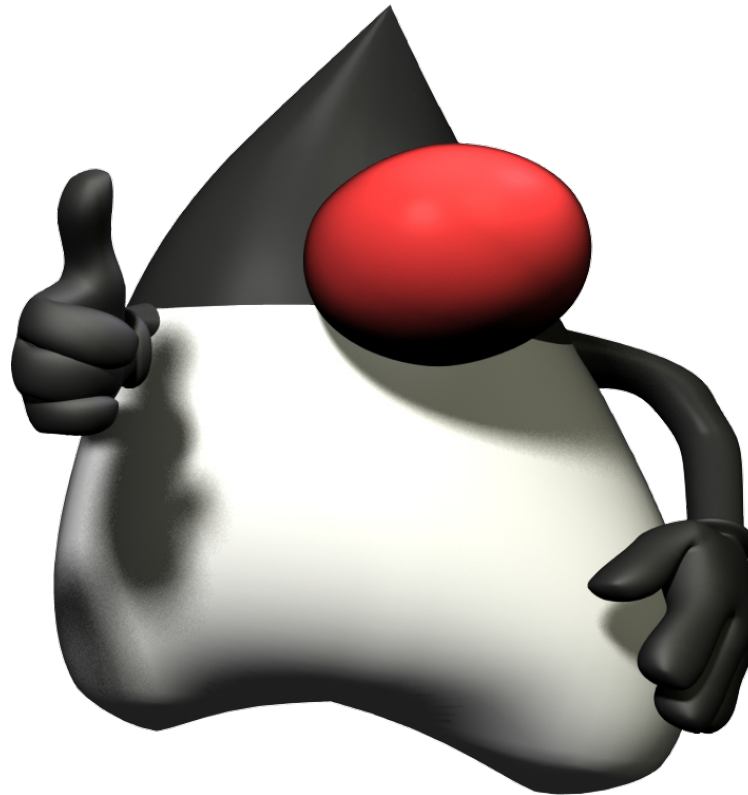
Java pop quizz !!

```
class Foo<T> {  
    class T {  
    }  
    T myField;  
}
```



How do you know that ?

JLS is your best friend



<http://docs.oracle.com/javase/specs/jls/se8/html/index.html>



Java pop quizz !!

```
interface F1 {  
}
```

```
interface F2 {  
}
```



Java pop quizz !!

```
class A<T extends F1 & F2>{  
    void fun(F1 f1){  
    void fun(T t){  
  
}
```



Java pop quizz !!

```
class A<T extends F2 & F1>{  
    void fun(F1 f1){  
    void fun(T t){  
  
}
```



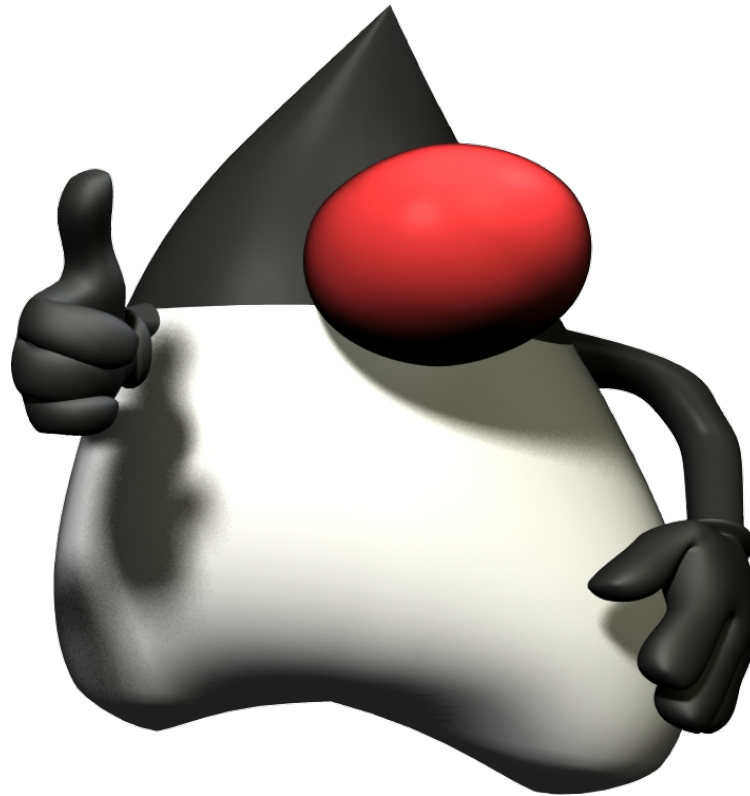
Java pop quizz !!

The erasure of a type variable is the erasure of its leftmost bound.



How do you know that ?

JLS is your best friend



<http://docs.oracle.com/javase/specs/jls/se8/html/index.html>



Sonar java plugin

SQUASHING



ALL THE BUGS!!

memegenerator.net



Incorrect logic

From... sonar-persitit... source code



```
for (int j = 0; j < 2 && index >= 0; j++) {  
    if (index < 0)
```

Change this condition so that it does not always evaluate to "false" ...

Bloquant Ouvert Non affecté Non planifié 15min debt

il y a 5 jours ▼ L4001

bug, cwe, misra

```
break;
```



Bad use of API

From OrientDB

```
l.ga... public boolean hasNext() {  
l.ga...     if (limit > 0 && resultCount >= limit)  
l.ga...         return false;  
  
l.ga...     if (lastTraversed == null)  
        // GET THE NEXT  
        lastTraversed = next();  
~~~~~
```

Refactor the implementation of this "Iterator.hasNext()" method to not call "Iterator.next()". ...

❗ Blocker ○ Open Not assigned Not planned 20min debt

```
enis... if (lastTraversed == null && !context.isEmpty())  
l.ga...     throw new IllegalStateException("Traverse ended abnormally");  
  
l.ga... if (!context.checkTimeout())  
        return false;  
  
l.ga... // BROWSE ALL THE RECORDS  
        return lastTraversed != null;  
}
```



Your turn now : Custom rules !





Let's Code !





Beyond semantic...

- Symbolic Execution :

Evgeny travaille chez SonarSource et il boit uniquement du café. Chez SonarSource il y a 31 employés mais certains boivent plus de café que d'autres.

Evgeny boit probablement plus de café que les autres employés.



Q & A

