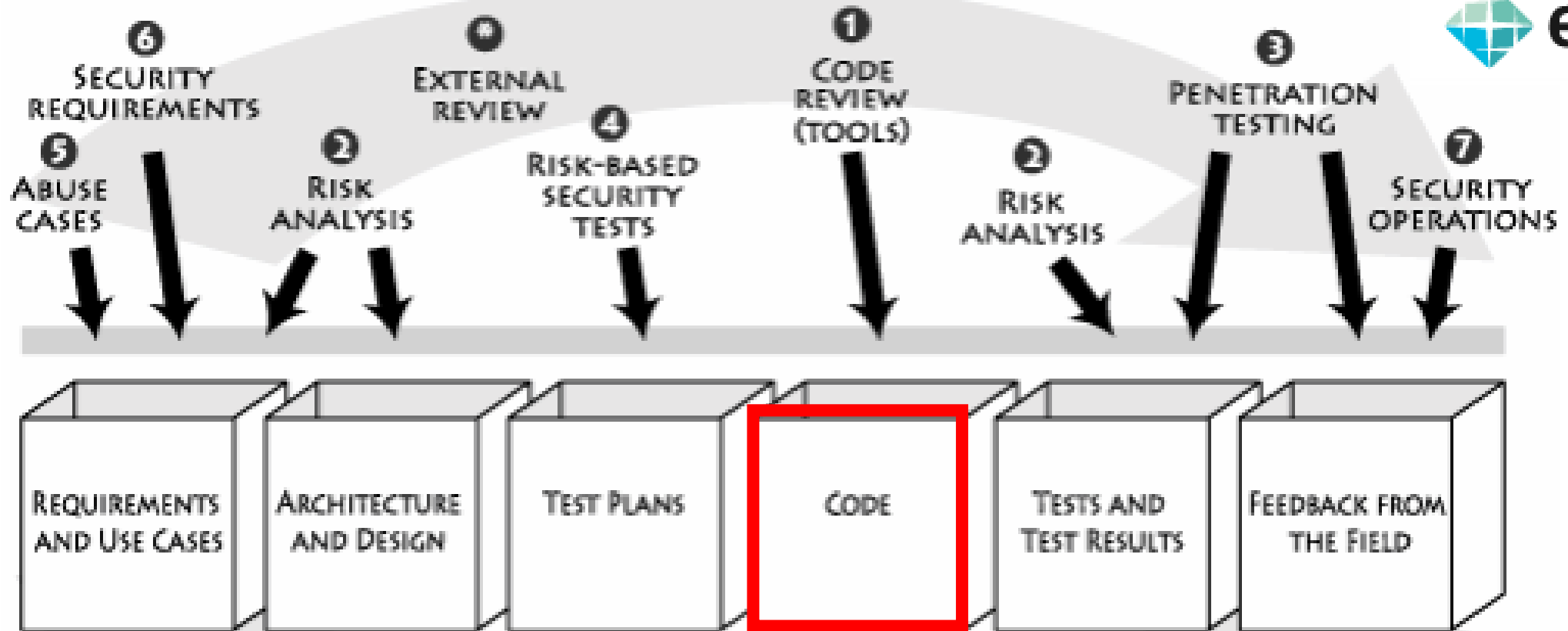


# Capítulo 4. Revisão de código com uma ferramenta

(Code Review with a Tool)

**Me. Marcelo Henrique dos Santos**

[www.marcelohsantos.com](http://www.marcelohsantos.com)



1. Revisão do código
2. Análise de risco arquitetônico
3. Teste de penetração
4. Testes de segurança baseados em risco
5. Casos de abuso
6. Requisitos de segurança
7. Operações de segurança

# O que é uma ferramenta de revisão de código?

A revisão de código é uma técnica de garantia de qualidade em que o autor de um código pede a outro desenvolvedor que o examine antes de se tornar parte da base de código.

# O que é uma ferramenta de revisão de código?

As ferramentas de revisão de código ajudam as equipes de desenvolvimento a trabalharem juntas no código e garantem a qualidade e a consistência do código.

# O que é uma ferramenta de revisão de código?

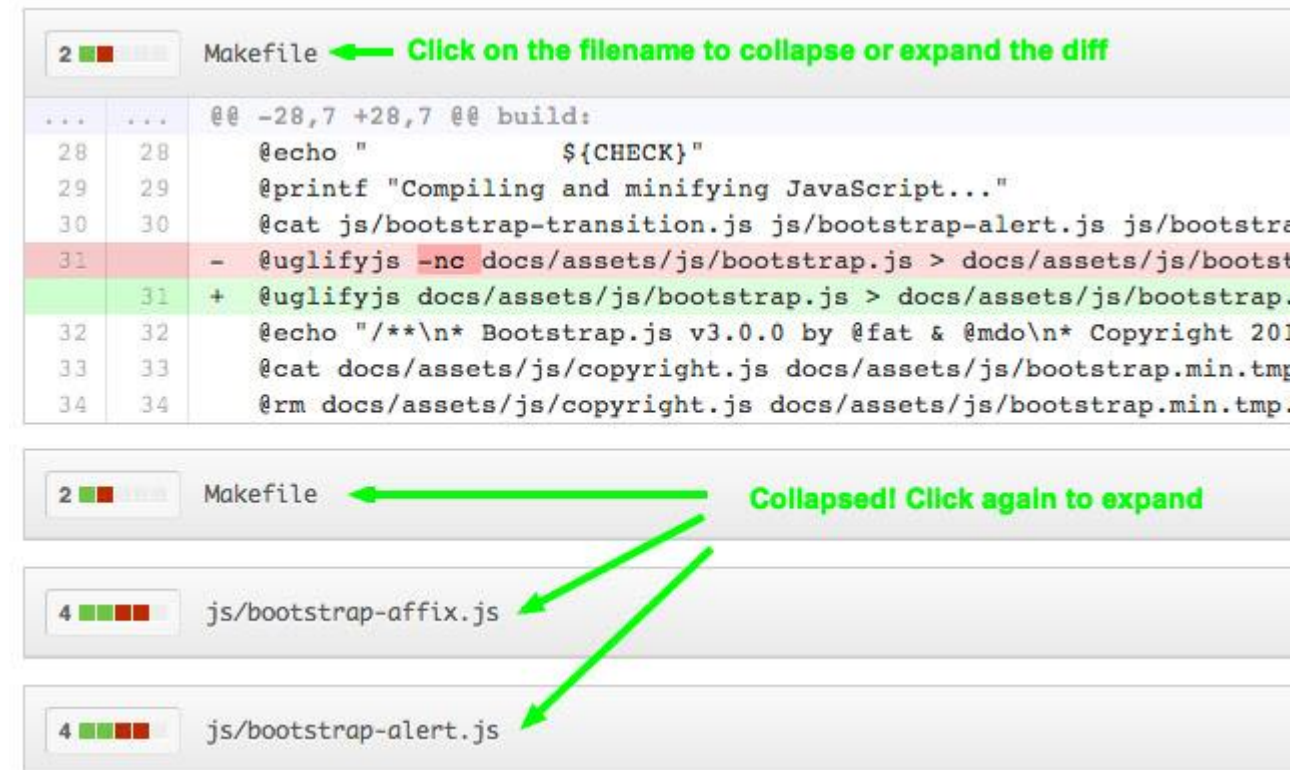
Essas ferramentas podem fornecer uma estrutura clara para as revisões, integrando-as em fluxos de trabalho de desenvolvimento maiores.

Elas também podem agilizar a comunicação entre as partes envolvidas, fornecendo um registro do processo e permitindo que os participantes acompanhem mais facilmente o que precisa ser feito.

# Ferramentas

## GitHub

No GitHub, as ferramentas de revisão de código são incorporadas às solicitações pull. Você pode solicitar revisões, propor alterações, acompanhar versões para melhorar a qualidade do seu código.



```
2 █ █ █ █ █ Makefile ← Click on the filename to collapse or expand the diff
...  ... @@ -28,7 +28,7 @@ build:
28 28  @echo "          ${CHECK}"
29 29  @printf "Compiling and minifying JavaScript..."
30 30  @cat js/bootstrap-transition.js js/bootstrap-alert.js js/bootstr
31 -  @uglifyjs -nc docs/assets/js/bootstrap.js > docs/assets/js/bootst
31 +  @uglifyjs docs/assets/js/bootstrap.js > docs/assets/js/bootstrap.
32 32  @echo "/*\n* Bootstrap.js v3.0.0 by @fat & @mdo\n* Copyright 201
33 33  @cat docs/assets/js/copyright.js docs/assets/js/bootstrap.min.tmp
34 34  @rm docs/assets/js/copyright.js docs/assets/js/bootstrap.min.tmp

2 █ █ █ █ █ Makefile ← Collapsed! Click again to expand
4 █ █ █ █ █ js/bootstrap-affix.js
4 █ █ █ █ █ js/bootstrap-alert.js
```


# Ferramentas

## Add toString implementation #17

[Edit](#)[Open](#) maxjacobson wants to merge 1 commit into master from fix-git-tag-descriptions[Conversation](#) 0 [Commits](#) 1 [Files changed](#) 3

Changes from all commits ▾ Jump to... ▾ +20 -4

[Unified](#) [Split](#)[Review changes ▾](#)

20  src/main/java/com/github/koraktor/mavanagaiata/git/GitTagDescription.java | 88.24% cov | 8 [View](#) [Edit](#)

issues

```
@@ -67,9 +67,23 @@ public boolean isTagged() {
67 67      *
68 68      * @return The string representation of this description
69 69      */
70 - @Override
71 - public String toString() {
72 -     return "TODO: implement this method";
73 +
74 +     if (this.nextTag == null) {
75 +         return this.abbreviatedCommitId;
76 +     } else if (this.distance == 0) {
77 +         return this.nextTag.getName();
78 +     } else {
79 +         return this.nextTag.getName();
80 +     }
81 + }
```

▲ Method `toString` has a Cognitive Complexity of 7 (exceeds 5 allowed). Consider refactoring. ...

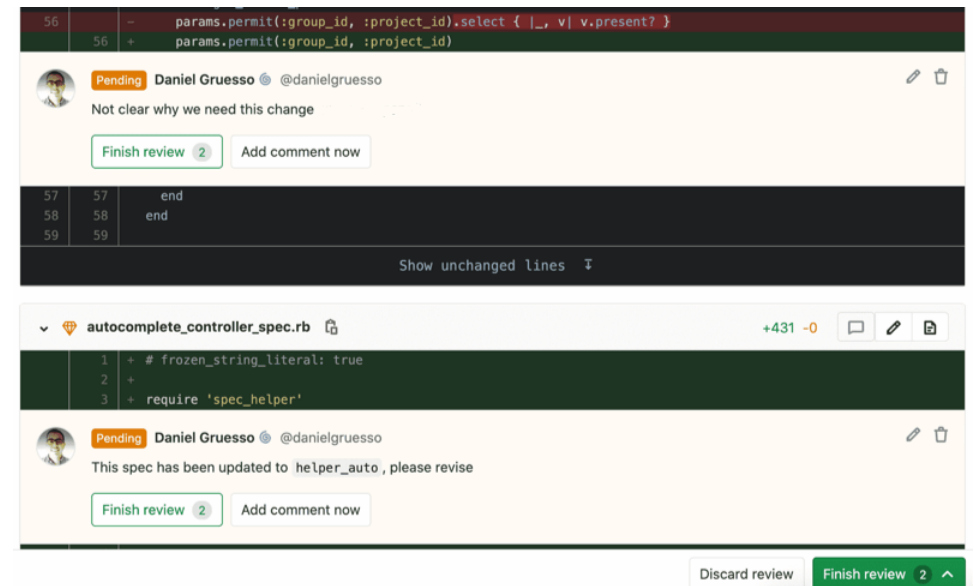
▲ '&&' should be on a new line. ...

# Ferramentas

## GitLab

O GitLab permite revisar código, discutir mudanças, compartilhar conhecimento e identificar defeitos no código entre equipes distribuídas por meio de revisão e comentários assíncronos.

O GitLab pode automatizar, rastrear e relatar revisões de código.





# Ferramentas

## GitLab

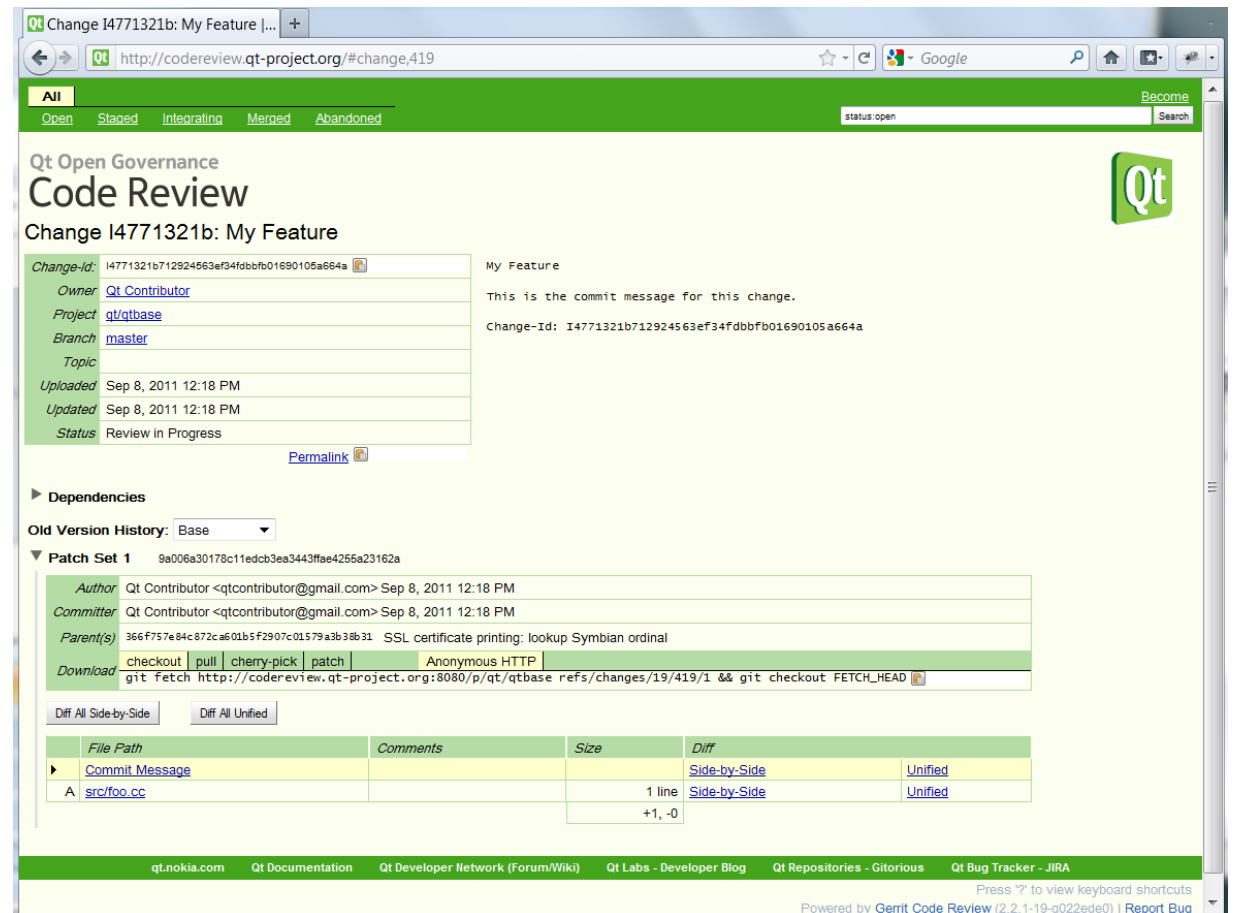
As revisões de solicitação de mesclagem permitem que os revisores de solicitação de mesclagem:

- enviem vários comentários de uma só vez,
- reduz o ruído de notificação para o autor da solicitação de mesclagem e permite um processo de revisão mais coeso e simplificado.

# Ferramentas

## Gerrit

Gerrit é uma ferramenta de código aberto para revisões de código baseadas na web, com servidores SSH e HTTP habilitados para Git.



The screenshot shows the Gerrit Code Review interface for a change titled "Change I4771321b: My Feature". The browser address bar shows the URL <http://codereview.qt-project.org/#change,419>. The page header includes "Qt Open Governance Code Review" and the Qt logo. The change details are as follows:

Change-Id:	I4771321b712924563ef34fdbbf01690105a664a	My Feature
Owner:	<a href="#">Qt Contributor</a>	This is the commit message for this change.
Project:	<a href="#">qt/qtbase</a>	Change-Id: I4771321b712924563ef34fdbbf01690105a664a
Branch:	<a href="#">master</a>	
Topic:		
Uploaded:	Sep 8, 2011 12:18 PM	
Updated:	Sep 8, 2011 12:18 PM	
Status:	Review in Progress	

Below the change details, there are sections for "Dependencies", "Old Version History" (set to Base), and "Patch Set 1" (9a006a30178c11edcb3ea3443fae4255a23162a). The patch set details include:

Author:	Qt Contributor <qtcontributor@gmail.com> Sep 8, 2011 12:18 PM
Committer:	Qt Contributor <qtcontributor@gmail.com> Sep 8, 2011 12:18 PM
Parent(s):	366f757e84c872ca601b5f2907c01579a3b38b31 SSL certificate printing: lookup Symbian ordinal
Download:	<a href="#">checkout</a>   <a href="#">pull</a>   <a href="#">cherry-pick</a>   <a href="#">patch</a>   <a href="#">Anonymous HTTP</a> git fetch <a href="http://codereview.qt-project.org:8080/p/qt/qtbase refs/changes/19/419/1">http://codereview.qt-project.org:8080/p/qt/qtbase refs/changes/19/419/1</a> && git checkout FETCH_HEAD

At the bottom, there is a diff table showing the changes:

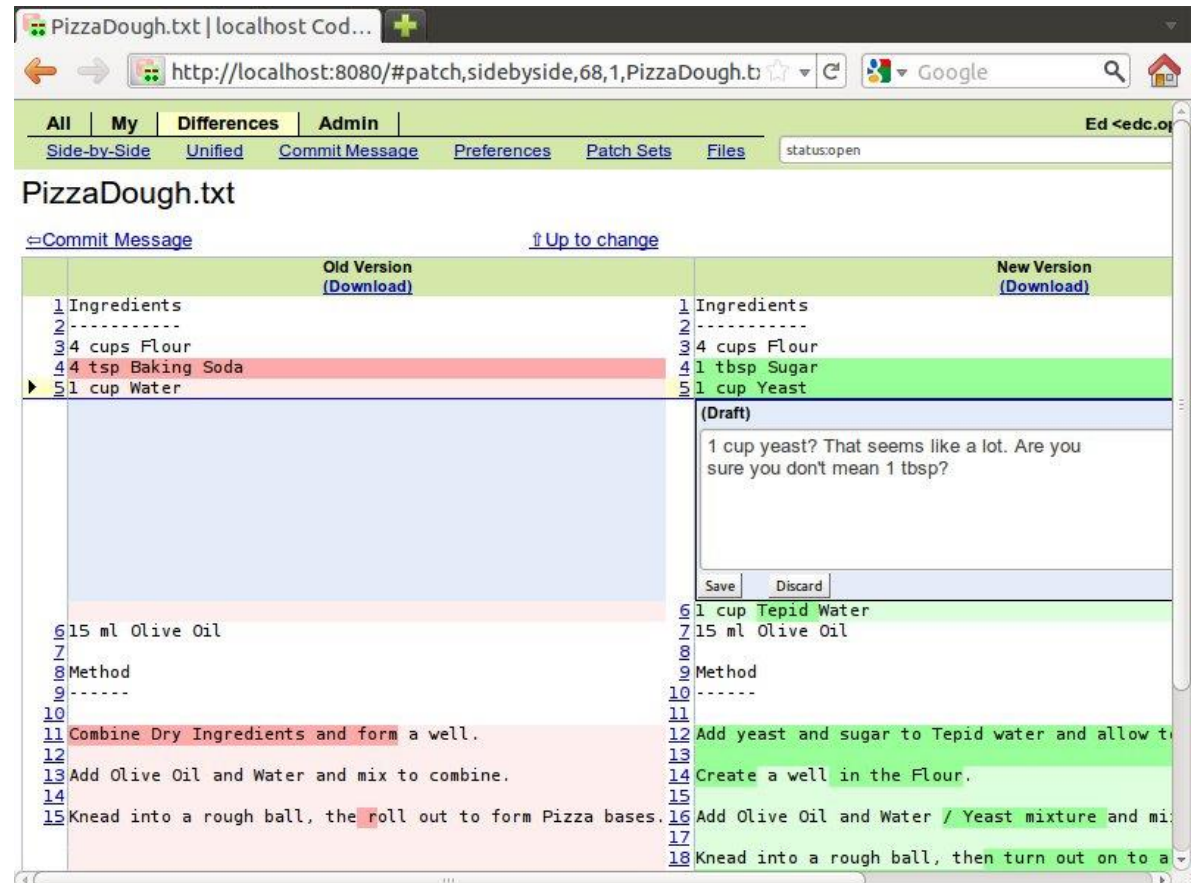
File Path	Comments	Size	Diff
<a href="#">Commit Message</a>			<a href="#">Side-by-Side</a>   <a href="#">Unified</a>
A <a href="#">src/foo.cc</a>		1 line	<a href="#">Side-by-Side</a>   <a href="#">Unified</a>
		+1, -0	

The footer of the page includes navigation links for [qt.nokia.com](#), [Qt Documentation](#), [Qt Developer Network \(Forum/Wiki\)](#), [Qt Labs - Developer Blog](#), [Qt Repositories - Gitorious](#), and [Qt Bug Tracker - JIRA](#). It also mentions "Powered by Gerrit Code Review (2.2.1-19-q022ede0) | Report Bug".

# Ferramentas

## Gerrit

O processo de revisão orientado a patches suporta o fluxo de trabalho típico de projetos de código aberto.



PizzaDough.txt | localhost Cod... +

http://localhost:8080/#patch,sidebyside,68,1,PizzaDough.b

All My Differences Admin Ed <edc.oy

Side-by-Side Unified Commit Message Preferences Patch Sets Files status:open

PizzaDough.txt

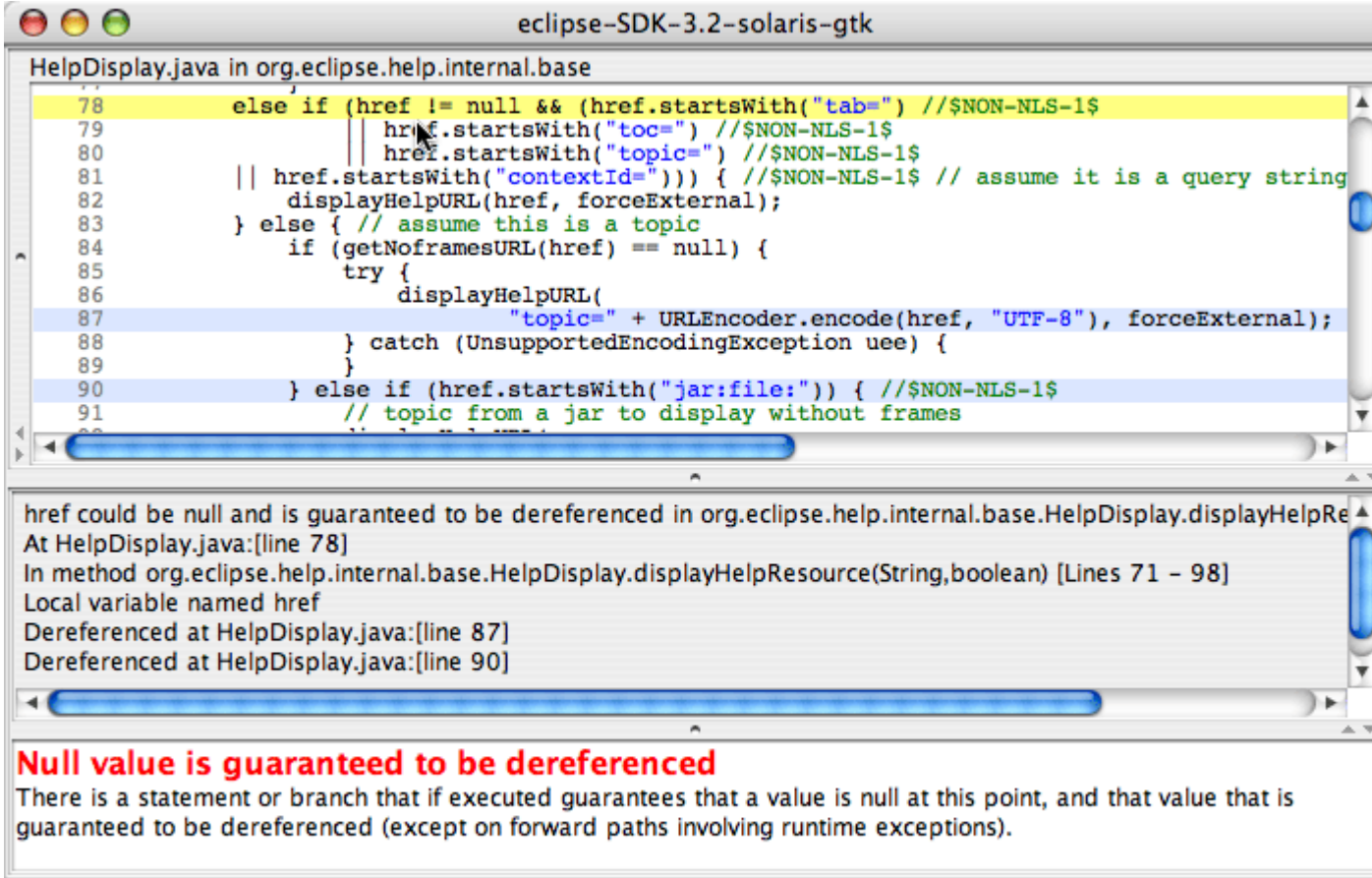
Commit Message Up to change

Old Version (Download)	New Version (Download)
1 Ingredients	1 Ingredients
2 -----	2 -----
3 4 cups Flour	3 4 cups Flour
4 4 tsp Baking Soda	4 1 tbsp Sugar
5 1 cup Water	5 1 cup Yeast
<b>(Draft)</b>	
1 cup yeast? That seems like a lot. Are you sure you don't mean 1 tbsp?	
Save Discard	
6 15 ml Olive Oil	6 1 cup Tepid Water
7	7 15 ml Olive Oil
8 Method	8 Method
9 -----	9 -----
10	10
11 Combine Dry Ingredients and form a well.	11 Add yeast and sugar to Tepid water and allow to
12	12
13 Add Olive Oil and Water and mix to combine.	13 Create a well in the Flour.
14	14
15 Knead into a rough ball, then roll out to form Pizza bases.	15 Add Olive Oil and Water / Yeast mixture and mi
16	16
17	17
18	18 Knead into a rough ball, then turn out on to a

# Ferramentas

## FindBugs™

FindBugs é uma ferramenta de código aberto usada para realizar análises estáticas em código Java.



The screenshot shows the Eclipse IDE window titled "eclipse-SDK-3.2-solaris-gtk". The editor displays the source code for `HelpDisplay.java` in the package `org.eclipse.help.internal.base`. Lines 78-91 are highlighted in yellow, showing an `else if` block where `href` is dereferenced. A FindBugs warning is displayed below the code, indicating a null value is guaranteed to be dereferenced. The warning text is as follows:

```
href could be null and is guaranteed to be dereferenced in org.eclipse.help.internal.base.HelpDisplay.displayHelpResource
At HelpDisplay.java:[line 78]
In method org.eclipse.help.internal.base.HelpDisplay.displayHelpResource(String,boolean) [Lines 71 - 98]
Local variable named href
Dereferenced at HelpDisplay.java:[line 87]
Dereferenced at HelpDisplay.java:[line 90]
```

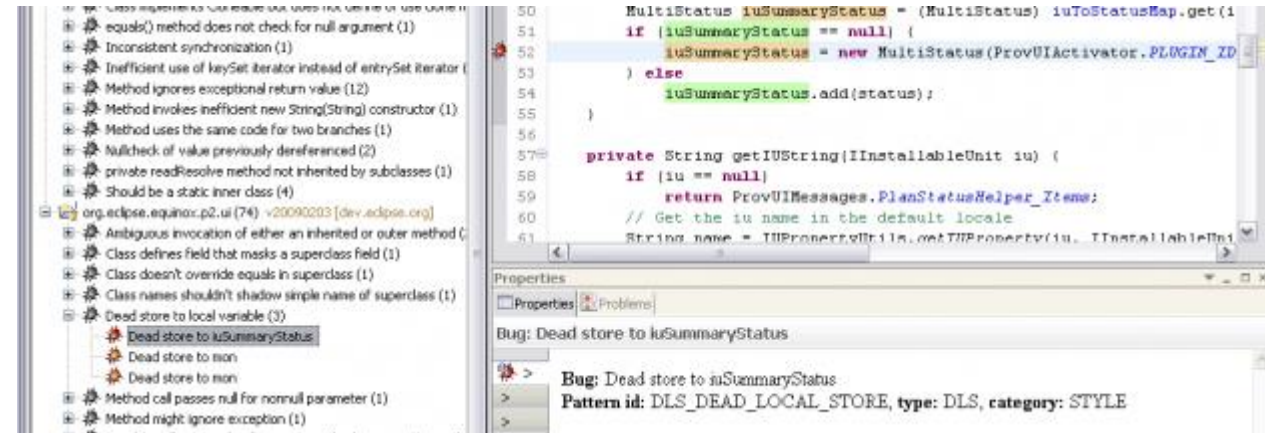
**Null value is guaranteed to be dereferenced**  
There is a statement or branch that if executed guarantees that a value is null at this point, and that value that is guaranteed to be dereferenced (except on forward paths involving runtime exceptions).

<http://findbugs.sourceforge.net/>

# Ferramentas

## FindBugs™

Ele verifica o código de bytes para o chamado *padrão de bug* para encontrar defeitos e/ou código suspeito.



The screenshot displays the FindBugs tool interface. On the left, a list of detected bugs is shown, including:

- equals() method does not check for null argument (1)
- Inconsistent synchronization (1)
- Inefficient use of keySet iterator instead of entrySet iterator (1)
- Method ignores exceptional return value (12)
- Method invokes inefficient new String(String) constructor (1)
- Method uses the same code for two branches (1)
- Nullcheck of value previously dereferenced (2)
- private readResolve method not inherited by subclasses (1)
- Should be a static inner class (4)
- org.eclipse.equinox.p2.ui (74) - v20090203 [dev.eclipse.org]
- Ambiguous invocation of either an inherited or outer method (1)
- Class defines field that masks a superclass field (1)
- Class doesn't override equals in superclass (1)
- Class names shouldn't shadow simple name of superclass (1)
- Dead store to local variable (3)
- Dead store to iuSummaryStatus
- Dead store to mon
- Dead store to mon
- Method call passes null for nonnull parameter (1)
- Method might ignore exception (1)

On the right, a code snippet is shown with a bug highlighted:

```
50     MultiStatus iuSummaryStatus = (MultiStatus) iuToStatusMap.get(iuSummaryStatusId);
51     if (iuSummaryStatus == null) {
52         iuSummaryStatus = new MultiStatus(ProvUIActivator.PLUGIN_ID, iuSummaryStatusId);
53     } else {
54         iuSummaryStatus.add(status);
55     }
56
57     private String getIUString(IInstallableUnit iu) {
58         if (iu == null)
59             return ProvUIMessages.PlainStatusHelper_Items;
60         // Get the iu name in the default locale
61         String name = IUPropertyUtils.getDefaultProperty(iu, IInstallableUnit
```

The Properties window at the bottom shows the bug details:

Bug: Dead store to iuSummaryStatus

> Bug: Dead store to iuSummaryStatus

> Pattern id: DLS\_DEAD\_LOCAL\_STORE, type: DLS, category: STYLE

# Ferramentas

## FindBugs™

Embora Findbugs precise dos arquivos de classe compilados, não é necessário executar o código para a análise. É também uma excelente motivação para melhorar as habilidades das equipes de desenvolvimento para escrever um código melhor.

# AVALIAÇÃO

Leia o trecho da matéria “**Uber Claims No Sensitive Data Exposed in Latest Breach... But There's More to This**”, disponível no seguinte site:  
<https://thehackernews.com/2022/09/uber-claims-no-sensitive-data-exposed.html> para responder as questões a seguir.

# AVALIAÇÃO

A Uber, em uma atualização, disse que "não há evidências" de que as informações privadas dos usuários tenham sido comprometidas em uma violação de seus sistemas internos de computadores.

A empresa também disse que colocou de volta online todas as ferramentas de software internas que derrubou anteriormente como precaução.



# AVALIAÇÃO

Não está claro se o incidente resultou no roubo de qualquer outra informação ou por quanto tempo o intruso estava dentro da rede da Uber.

A Uber não forneceu mais detalhes sobre como o incidente aconteceu além de dizer que seus esforços de investigação e resposta estão em andamento.

# AVALIAÇÃO

A violação supostamente envolveu um hacker solitário, um adolescente de 18 anos, enganando um funcionário do Uber para fornecer acesso à conta por engenharia social para que a vítima aceitasse um prompt de autenticação multifator (MFA) que permitia ao invasor registrar seu próprio dispositivo.

# AVALIAÇÃO

Ao obter uma posição inicial, o invasor encontrou um compartilhamento de rede interno que continha scripts do **PowerShell** com credenciais de administrador privilegiadas, concedendo acesso a outros sistemas críticos, incluindo **AWS** e **Google Cloud Platform**.

O ataque direcionado ao Uber, bem como a recente série de incidentes contra a Cisco, ilustra como a engenharia social continua a ser um espinho persistente na carne para as organizações.

# AValiação

Ele também mostra que tudo o que é necessário para que uma violação ocorra é que um funcionário compartilhe suas credenciais de login, provando que a autenticação baseada em senha é um elo fraco na segurança da conta.

Episódios como esses também são prova de que os códigos de senha de uso único – normalmente gerados por meio de aplicativos autenticadores ou enviados como mensagens SMS – são inadequados para proteger os bloqueios de 2FA.

# AVALIAÇÃO

Uma maneira de combater essas ameaças é o uso de chaves de segurança físicas, que descarta as senhas em favor de um dispositivo de hardware externo que lida com a autenticação.

# Pergunta

O desenvolvimento de software seguro deve ser uma prioridade nos dias de hoje. Em uma era de ataques cibernéticos que podem afetar qualquer pessoa (indivíduos, empresas e governos) os riscos espreitam em todos os lugares. A partir desse contexto:

- 1 - Relacione e explique de que forma podemos proteger nossos sistemas (de forma ampla e geral).
- 2 – Aponte quais práticas poderiam ser adotadas para evitar o problema enfrentado pela empresa de transporte (UBER).

# Referências bibliográficas

VERBINA, E. **Best Code Review Tools for 2022 – Survey Results.** 2021. Disponível em: <https://blog.jetbrains.com/space/2021/12/15/best-code-review-tools/>. Acesso em: 20 Set. 2022.