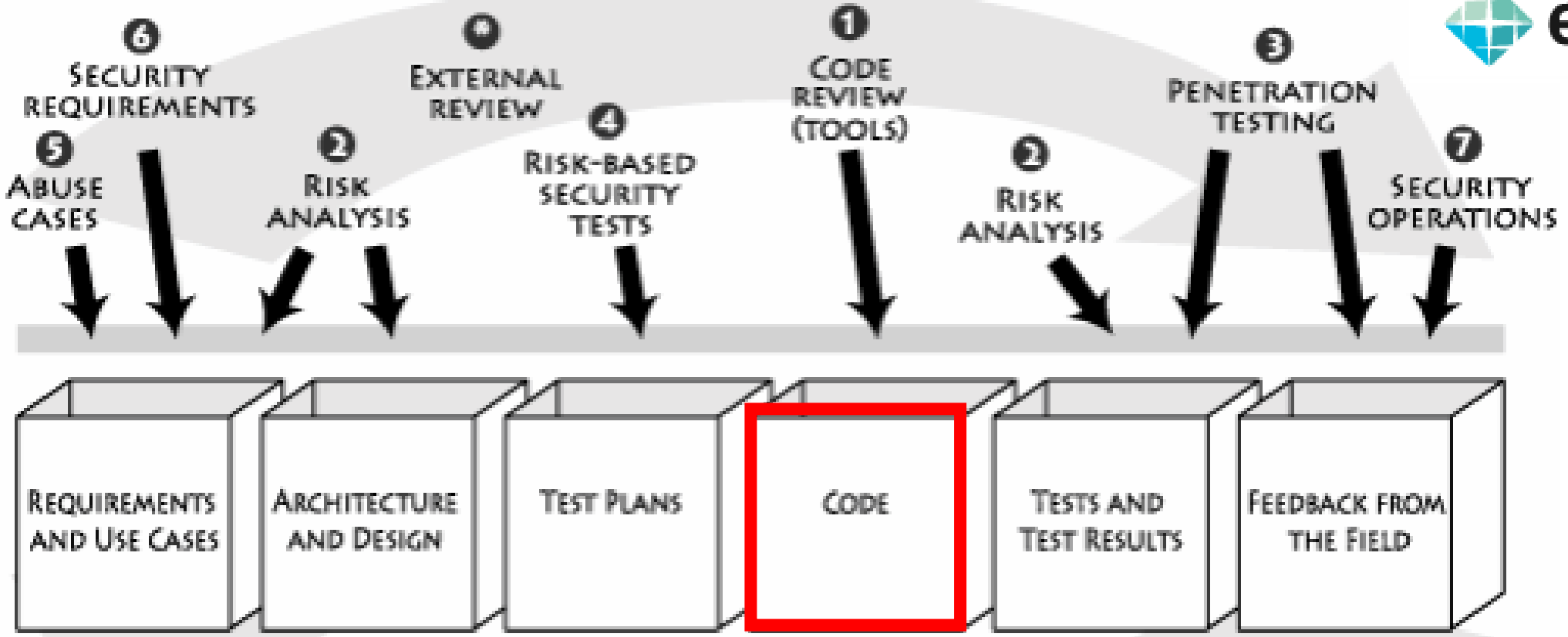
Capítulo 4. Revisão de código com uma ferramenta

(Code Review with a Tool)

Me. Marcelo Henrique dos Santos

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?

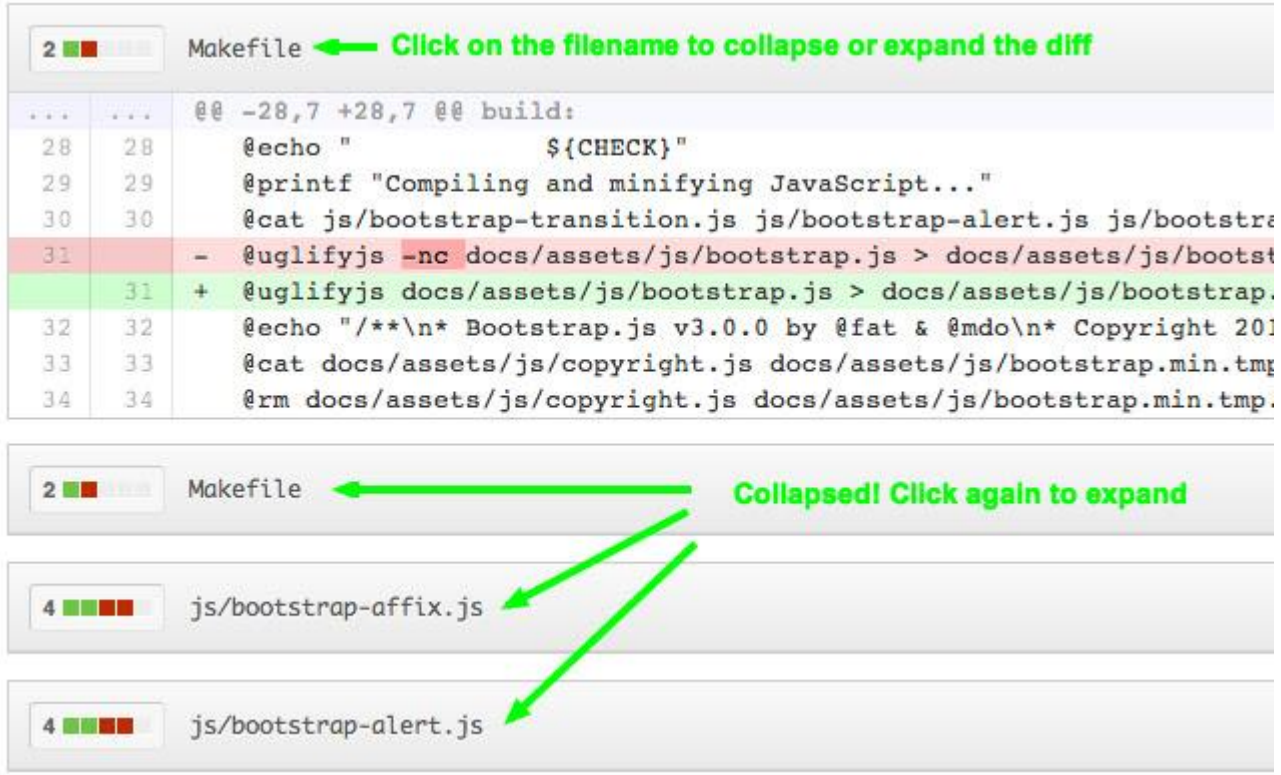
Essas ferramentas podem fornecer uma estrutura clara para as revisões, integrando-as em fluxos de trabalho de desenvolvimento maiores.

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.

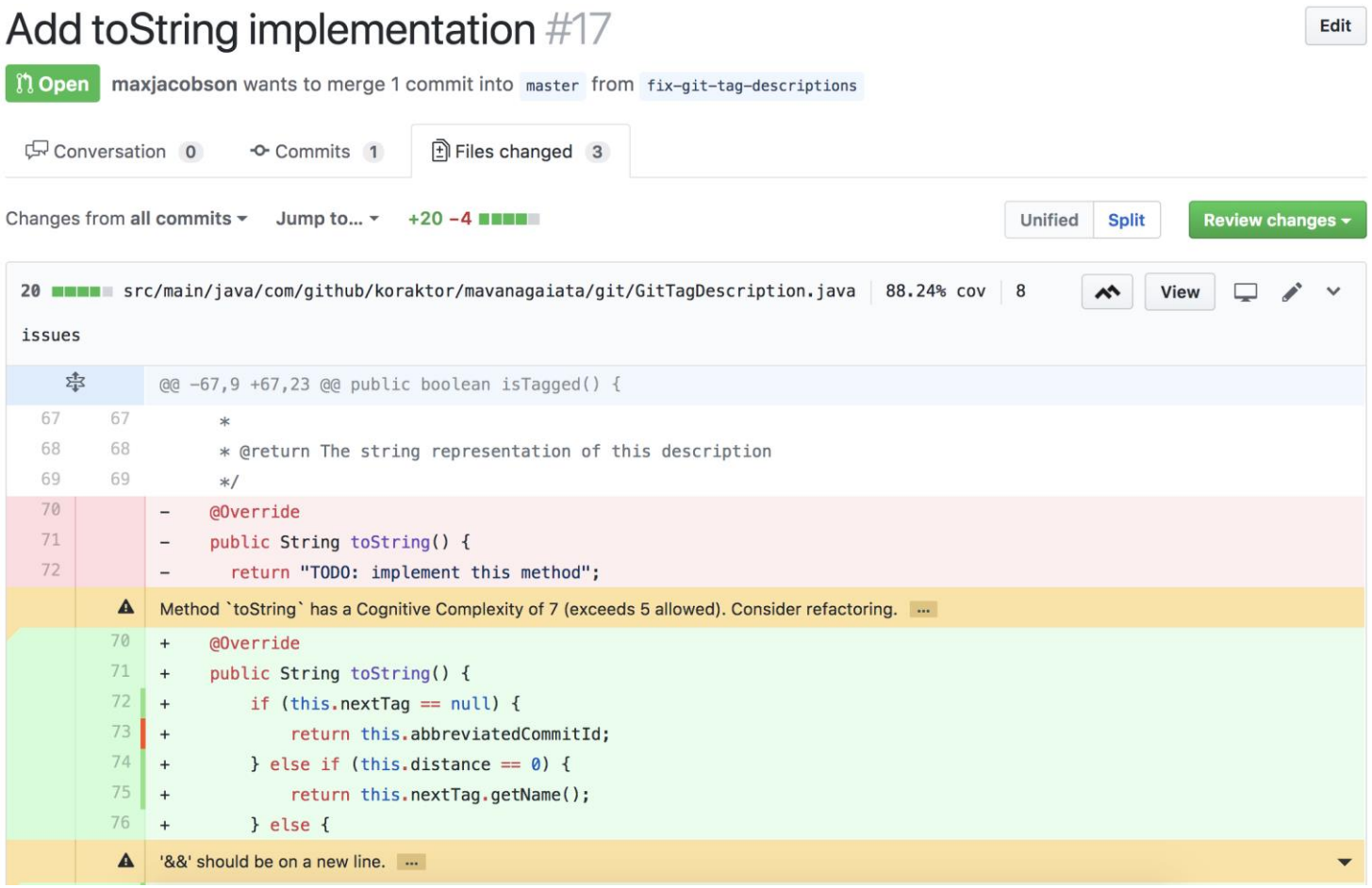
Ferramentas

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.



Ferramentas

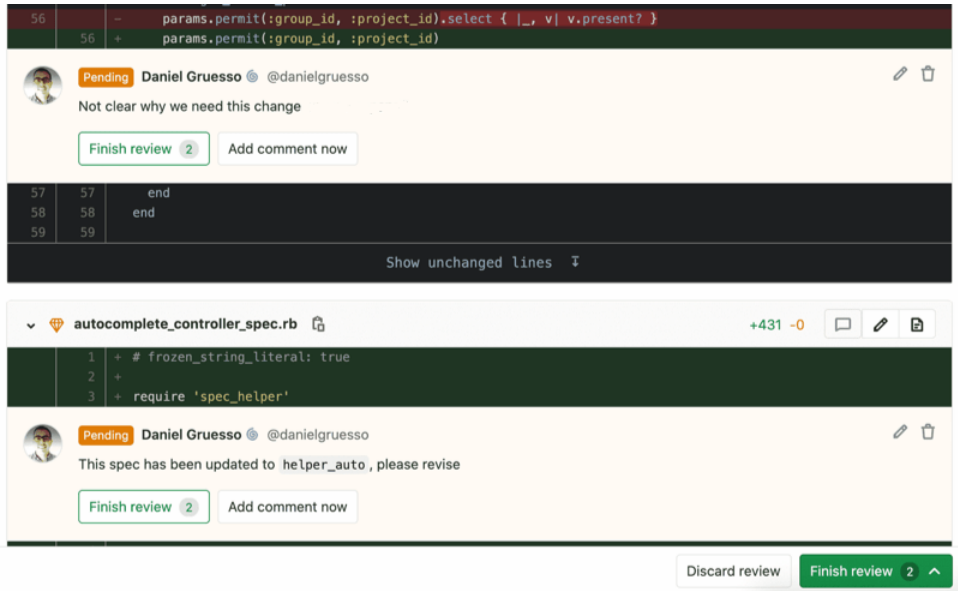


Ferramentas

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

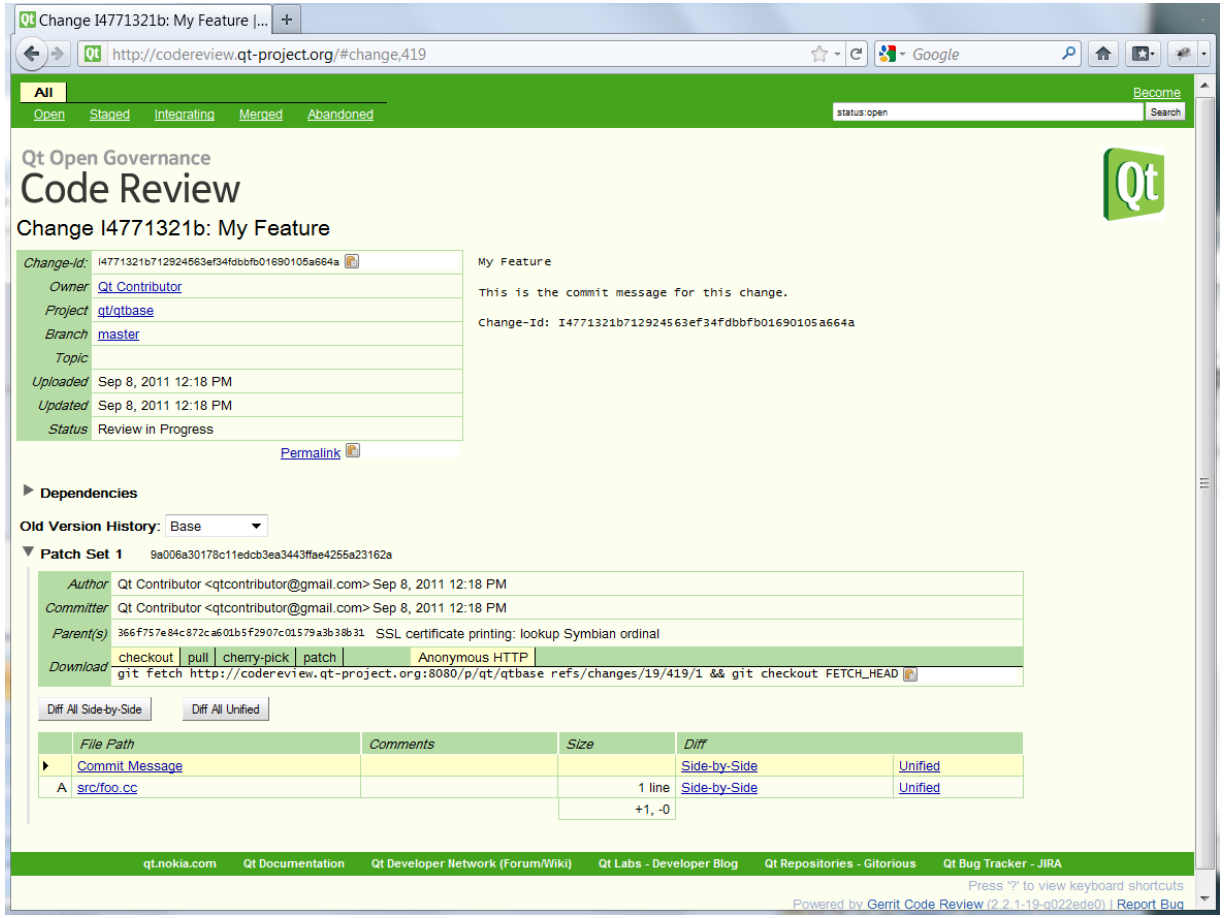
As revisões de solicitação de mesclagem permitem que os revisores de solicitação de mesclagem:

- 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

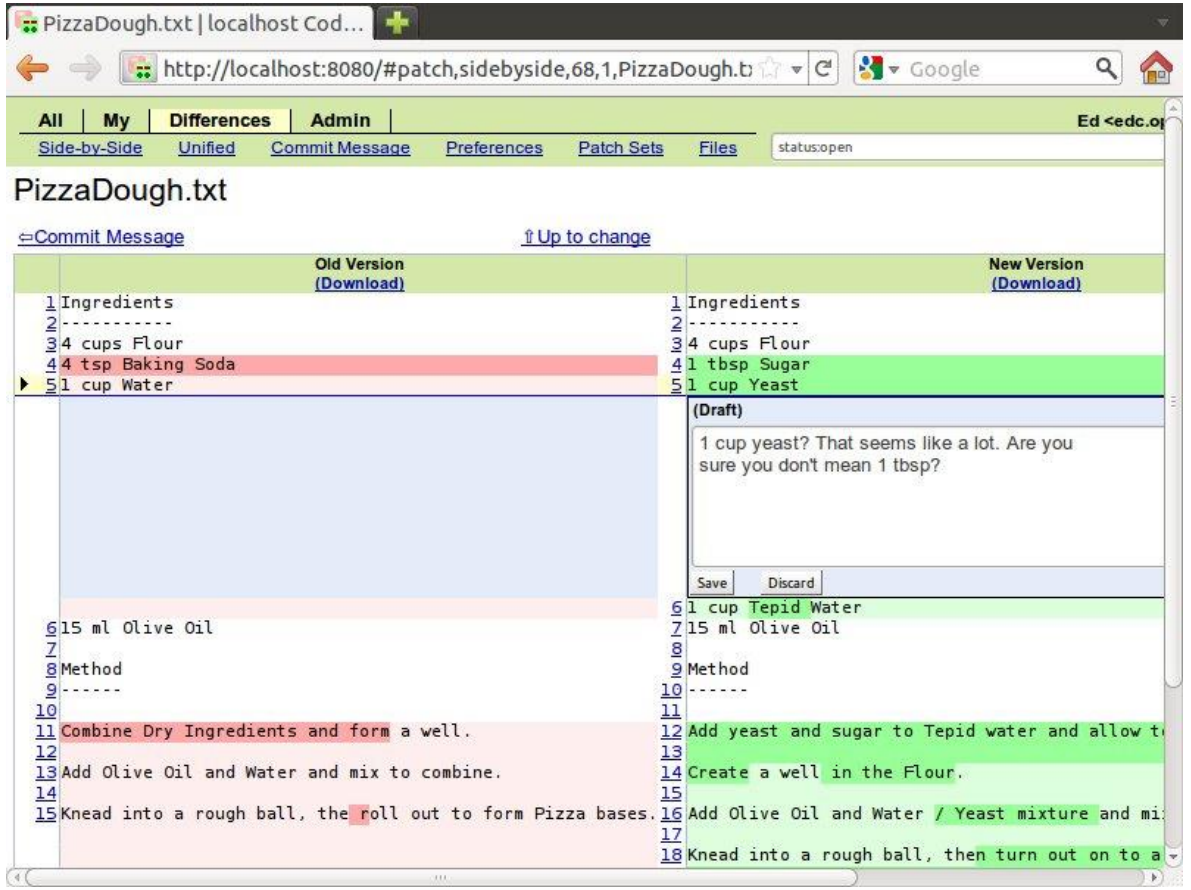
Gerrit é uma ferramenta de código aberto para revisões de código baseadas na web, com servidores SSH e HTTP habilitados para Git.



Ferramentas

Gerrit

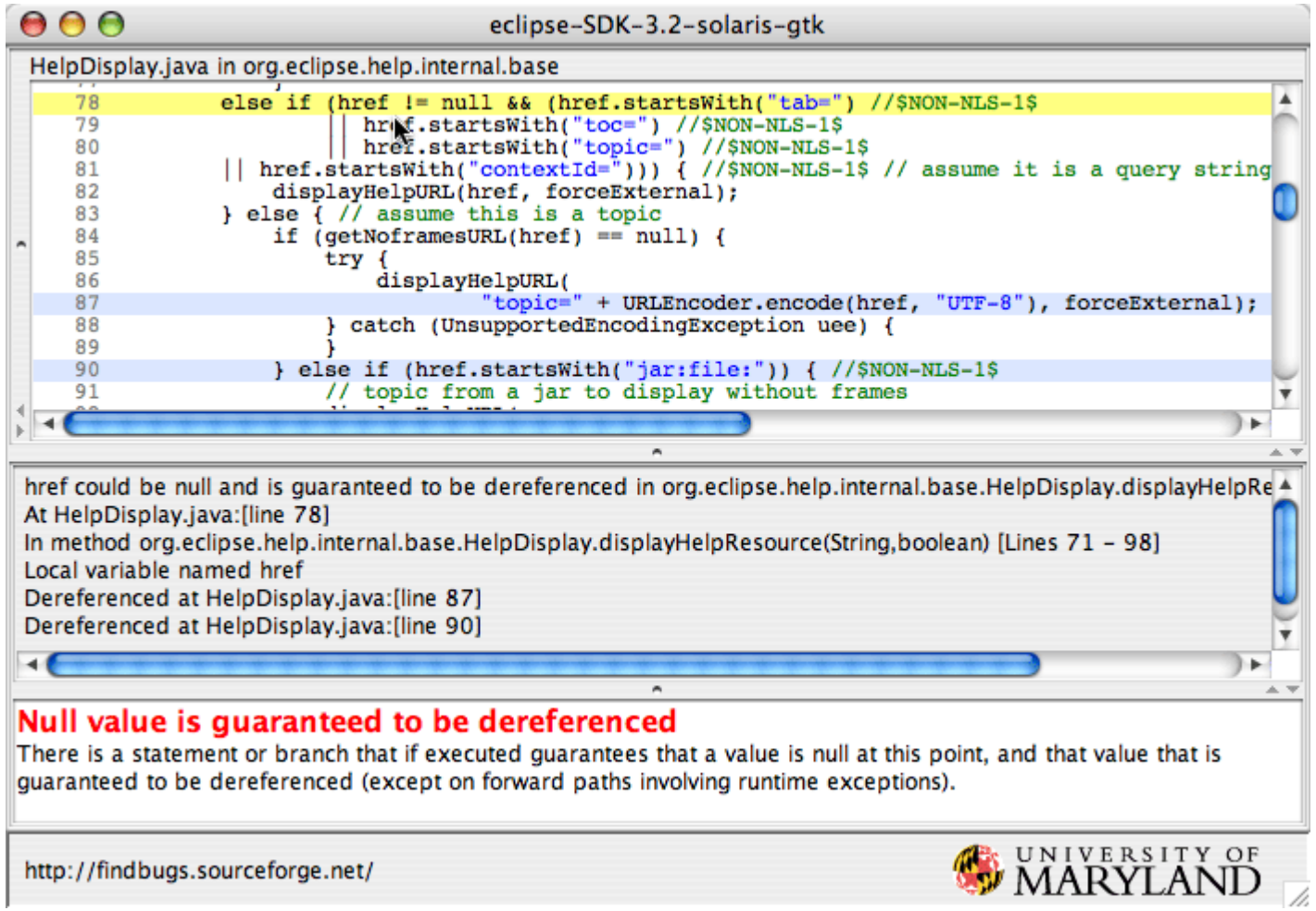
O processo de revisão orientado a patches suporta o fluxo de trabalho típico de projetos de código aberto.



Ferramentas

FindBugs™

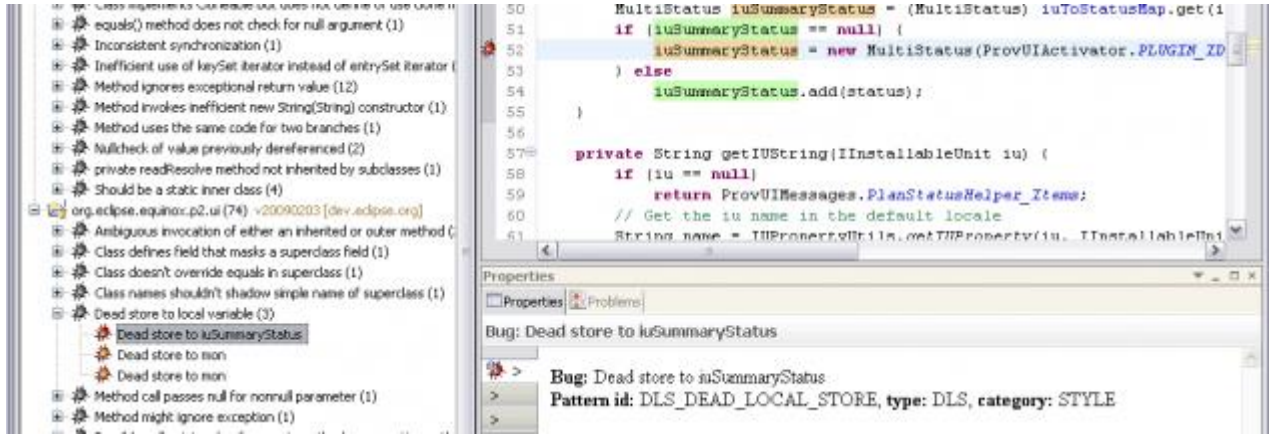
FindBugs é uma ferramenta de código aberto usada para realizar análises estáticas em código Java.



Ferramentas

FindBugs™

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



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.