THE DEVELOPER'S CONFERENCE

Trilha – Java

Marcio Frayze David

Encontrando dependências desatualizada ou com com falhas de segurança em aplicações Java

Parte 1: Falhas de segurança

THE
DEVELOPER'S
CONFERENCE

Parte 1: Falhas de segurança

THE DEVELOPER'S CONFERENCE

- Alguma dependência do seu projeto contém falhas de segurança conhecidas?
- Como automatizar?

OWASP

THE DEVELOPER'S CONFERENCE

- *Open Web Application Security Project*
  - Organização sem fins lucrativos
  - Missão: tornar a segurança de software visível
  - Mais de 45.000 participantes ao redor do mundo

https://owasp.org

OWASP Dependency Check

THE DEVELOPER'S CONFERENCE

- Ferramenta para procurar dependências com falhas de segurança conhecidas
- Suporte oficial: **Java** e .NET
- Suporte experimental: Ruby, Node.js, Python e C/C++

OWASP Dependency Check - Java

THE DEVELOPER'S CONFERENCE

- **Linha de comando**
- Plugins
  - **Gradle**
  - Maven
  - Ant
  - Jenkins

OWASP Dependency Check - CLI

THE DEVELOPER'S CONFERENCE

- Passos:
  - Baixar e desempacotar a *dependency-check-cli*
  - Executar no terminal:
    - dependency-check.sh --project “Minha aplicação” --scan build
  - Resultado: *dependency-check-report.html*

VND: National Vulnerability Database

OWASP Dependency Check - CLI

THE DEVELOPER'S CONFERENCE

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
spring-boot-example-0.0.1-SNAPSHOT.jar: h2-1.4.197.jar	cpe:2.3:a:h2database:h2:1.4.197:*:*:*:*:*:*:*	pkg:maven/com.h2database/h2@1.4.197	HIGH	2	Highest	38
spring-boot-example-0.0.1-SNAPSHOT.jar: guava-20.0.jar	cpe:2.3:a:google:guava:20.0:*:*:*:*:*:*:*	pkg:maven/com.google.guava/guava@20.0	MEDIUM	1	Highest	23
spring-boot-example-0.0.1-SNAPSHOT.jar: spring-security-core-5.1.1.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_security:5.1.1:*:*:*:*:*:*:*	pkg:maven/org.springframework.security/spring-security-core@5.1.1.RELEASE	HIGH	2	Low	30
spring-boot-example-0.0.1-SNAPSHOT.jar: springfox-core-2.9.2.jar	cpe:2.3:a:gradle:gradle:2.9.2:*:*:*:*:*:*:*	pkg:maven/io.springfox/springfox-core@2.9.2	MEDIUM	1	Low	26
spring-boot-example-0.0.1-SNAPSHOT.jar: spring-boot-starter-security-2.1.0.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_boot:2.1.0:*:*:*:*:*:*:* cpe:2.3:a:pivotal_software:spring_security:2.1.0:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-security@2.1.0.RELEASE	HIGH	1	Low	25
spring-boot-example-0.0.1-SNAPSHOT.jar: jackson-databind-2.9.7.jar	cpe:2.3:a:fasterxml:jackson:2.9.7:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-databind:2.9.7:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.9.7	CRITICAL	4	Highest	40
spring-boot-example-0.0.1-SNAPSHOT.jar: tomcat-embed-core-9.0.12.jar	cpe:2.3:a:apache:tomcat:9.0.12:*:*:*:*:*:*:* cpe:2.3:a:apache_software_foundation:tomcat:9.0.12:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.12:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.12	HIGH	2	Highest	37

CVE: Common Vulnerabilities and Exposures

OWASP Dependency Check - Gradle

THE DEVELOPER'S CONFERENCE

```
buildscript {
    dependencies {
        classpath 'org.owasp:dependency-check-gradle:5.0.0-M2'
    }
    dependencyCheck {
        failBuildOnCVSS = 0
    }
}

apply plugin: 'org.owasp.dependencycheck'
```

Nova task:
./gradlew dependencyCheckAnalyze

CVSS: Common Vulnerability Scoring System

OWASP Dependency Check

THE DEVELOPER'S CONFERENCE

- Quando executar a task?
  - Integração contínua automatizada
    - Gitlab-ci
    - Jenkins
    - TeamCity
    - GoCD
  - Um dos últimos passos da *pipeline* (ou em paralelo)

Mais automatizado?

Alerta de segurança no Github

THE DEVELOPER'S CONFERENCE

Linguagens suportadas	Formato recomendado	Formatos suportados
Java	**pom.xml**	**pom.xml**
JavaScript	package-lock.json	package-lock.json, package.json
.NET	.csproj, .vbproj, .nuspec	.csproj, .vbproj, .nuspec
Python	requirements.txt, pipfile.lock	requirements.txt, pipfile.lock
Ruby	Gemfile.lock	Gemfile.lock,Gemfile, *.gemspec

Alerta de segurança no Github

THE DEVELOPER'S CONFERENCE

37 commits | 1 branch | 0 releases | 1 contributor

We found potential security vulnerabilities in your dependencies.

Only the owner of this repository can see this message.

Manage your notification settings or learn more about vulnerability alerts.

See security alerts

Branch: master | New pull request | Create new file | Upload files | Find File | Clone or download

mfdavid Depreciando — Latest commit `a59f760` on 5 Nov 2018

images	Otimizando imagens	a year ago
segunda.tech.elm	Adicionando uma versao bem inicial em Elm	a year ago
src	Adicionando episodio sobre conceitos basicos da POO	a year ago
test	Alterando para teste passar mas teste ainda sem muita utilidade	2 years ago
.eslintrc.json	Primeira versao	2 years ago
.firebaserc	Primeira versao	2 years ago
.gitignore	Primeira versao	2 years ago

Alerta de segurança no Github

THE DEVELOPER'S CONFERENCE

10 Open ✓ 0 Closed — Sort

extend opened on 7 Feb by GitHub • package-lock.json	low severity
request opened on 9 Nov 2018 by GitHub • package-lock.json	moderate severity
cryptiles opened on 5 Nov 2018 by GitHub • package-lock.json	high severity
lodash opened on 5 Nov 2018 by GitHub • package-lock.json	moderate severity
randomatic opened on 8 Oct 2018 by GitHub • package-lock.json	low severity
minimatch opened on 8 Oct 2018 by GitHub • package-lock.json	high severity
hawk opened on 31 Jul 2018 by GitHub • package-lock.json	moderate severity
tough-cookie opened on 24 Jul 2018 by GitHub • package-lock.json	high severity

Parte 2: Dependências desatualizadas

THE DEVELOPER'S CONFERENCE

Parte 2: Dependências desatualizadas

THE DEVELOPER'S CONFERENCE

- Alguma dependência do seu projeto está muito desatualizada?
- Como automatizar?

Gradle versions plugin

THE DEVELOPER'S CONFERENCE

```
plugins {
  id 'com.github.ben-manes.versions' version '0.21.0'
}
```

Nova task:
./gradlew dependencyUpdates

Gradle versions plugin

THE DEVELOPER'S CONFERENCE

```
------------------------------------------------------------
: Project Dependency Updates (report to plain text file)
------------------------------------------------------------

The following dependencies are using the latest milestone version:
 - com.github.ben-manes.versions:com.github.ben-manes.versions.gradle.plugin:0.21.0
 - com.sun.xml.bind:jaxb-core:2.3.0.1
 - io.springfox:springfox-swagger-ui:2.9.2
 - io.springfox:springfox-swagger2:2.9.2
```

Gradle versions plugin

THE DEVELOPER'S CONFERENCE

The following dependencies have later milestone versions:
 - com.h2database:h2 [1.4.197 -> 1.4.199]
     http://www.h2database.com
 - com.sun.xml.bind:jaxb-impl [2.3.1 -> 2.4.0-b180830.0438]
     http://jaxb.java.net
 - io.micrometer:micrometer-core [1.1.0 -> 1.1.4]
     https://github.com/micrometer-metrics/micrometer
 - javax.xml.bind:jaxb-api [2.3.1 -> 2.4.0-b180830.0359]
     https://github.com/javaee/jaxb-spec
 - org.asciidoctor.jvm.convert:org.asciidoctor.jvm.convert.gradle.plugin [2.0.0-alpha.3 -> 2.1.0]

Gradle versions plugin

THE DEVELOPER'S CONFERENCE

Gradle release-candidate updates:
 - Gradle: [4.10.2 -> 5.4]

Generated report file build/dependencyUpdates/report.txt

Quando atualizar?

THE DEVELOPER'S CONFERENCE

Quando atualizar?

THE DEVELOPER'S CONFERENCE

- Atualize *frameworks* agressivamente e bibliotecas pasivamente
- Não deixe um *framework* ficar defasado em mais de 2 versões *major*

Livro: *Building Evolutionary Architectures*

Quando atualizar?

THE DEVELOPER'S CONFERENCE

- Dependência diretas
  - Sem quebras no código e nos testes automatizados: atualize sempre
  - Com quebras: planeje para próxima sprint
- Dependências transitivas
  - Apenas em casos extremos

THE DEVELOPER'S CONFERENCE

Trilha – Java

Marcio Frayze David

Encontrando dependências desatualizada ou com com falhas de segurança em aplicações Java

https://segunda.tech

mfdavid@gmail.com

github.com/mfdavid

@marcio.frayze