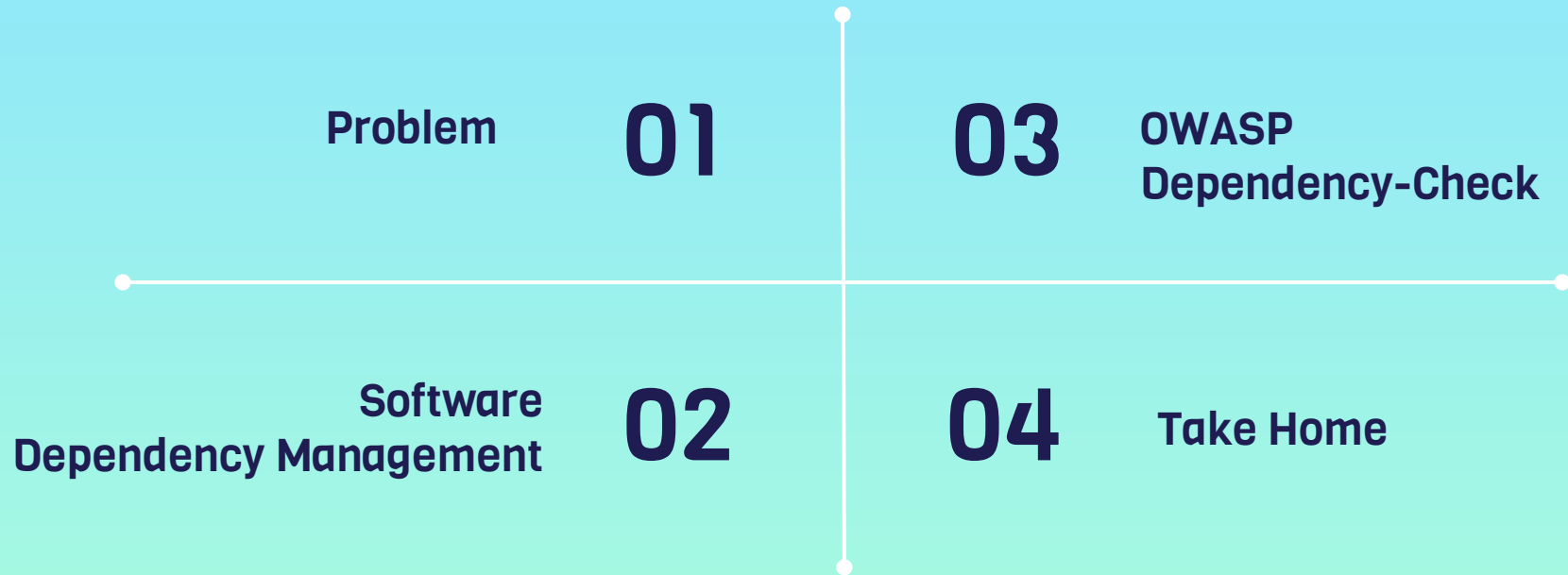




Third party Software Dependency Management with OWASP

Anna Nikolskaya
Carl Leijonberg

Go to www.menti.com and use the code **5996 5900**



Issues with Third Party Software Dependencies

- Widespread adoption of open-source components in commercial software
- Many open-source components contain known vulnerabilities
- OWASP Top Ten



Software Dependency Management

- Automate processes for managing open-source and third-party components
- Open-source software policies
- Dependency management





OWASP
DEPENDENCY-CHECK



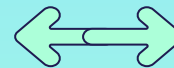
HOW IT WORKS



National Vulnerability
Database (NVD)



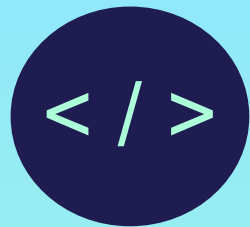
Common Vulnerabilities
and Exposures (CVE)



Common Platform
Enumeration (CPE)



Evidence



Your code



Open Source lib



Report (HTML, JSON, CSV, or XML)

Basic INSTALL with CLI

1

DOWNLOAD

```
brew install dependency-check
```

2

SCAN

```
/dependency-check.sh  
--project <myproject>  
--scan <3rd party lib>  
--out <reports path>
```

3

REPORT

A meme featuring Woody and Buzz Lightyear from the movie Toy Story. Buzz is in the foreground, looking excited and holding up three fingers. Woody is behind him, looking concerned. The background is a blurred indoor setting.

Plugins, plugins

EVEERRYWHERE



Gradle



Jenkins

Maven™

sbt

REFLECTION

NVD update



TAKE HOME

? Secure environment

? Secure products

! Dependency
vulnerability analyzer

STAY SAFE!

Anna Nikolskaya
Carl Leijonberg

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by **Stories**



Useful resources

OWASP DEPENDENCY CHECK

<https://owasp.org/www-project-dependency-check/>

NATIONAL VULNERABILITY DATABASE

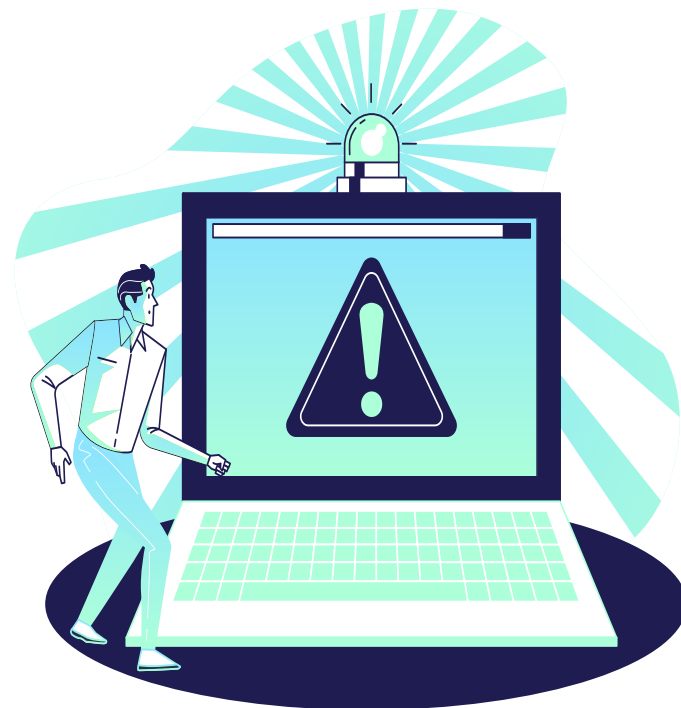
<https://nvd.nist.gov/vuln/full-listing>

OWASP DEPENDENCY CHECK IN JENKINS PIPELINE

<https://technology.amis.nl/continuous-delivery/jenkins-pipeline-sonarqube-and-the-owasp-dependency-check/>

DEPENDENCY MANAGEMENT CHEAT SHEET

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerable_Dependency_Management_Cheat_Sheet.html




Starting the scan example

```
tharindu@tharindu-pc:~/ProgramFiles/dependency-check/bin$ ./dependency-check.sh  
  --project "myproject" --scan /home/tharindu/dependencies/mydependencies --out /  
home/tharindu/dependencies/reports  
[INFO] Checking for updates  
[INFO] Skipping NVD check since last check was within 4 hours.  
[INFO] Check for updates complete (2080 ms)  
[INFO] Analysis Started  
[INFO] Creating the CPE Index  
[INFO] CPE Index Created (1588 ms)  
[INFO] Analysis Complete (6625 ms)  
tharindu@tharindu-pc:~/ProgramFiles/dependency-check/bin$
```

Report example

file:///home/tharindu/dependencies/reports/dependency-check-report.html



DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

Project: myproject ← Project Name

Scan Information ([show all](#)):

- dependency-check version: 1.4.3
- Report Generated On: Oct 5, 2016 at 07:46:19 IST
- Dependencies Scanned: 2 (2 unique) ← Number of 3rd party libraries scanned
- Vulnerable Dependencies: 1 ← Number of 3rd party libraries with known vulnerabilities
- Vulnerabilities Found: 3 ← Total number of known vulnerabilities identified
- Vulnerabilities Suppressed: 0
- ...

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-httpclient-3.1.jar	cpe:/a:apache:commons-httpclient:3.1	commons-httpclient:commons-httpclient:3.1	Medium	3	LOW	20

Dependencies

commons-httpclient-3.1.jar

Description: The HttpClient component supports the client-side of RFC 1945 (HTTP/1.0) and RFC 2616 (HTTP/1.1), several related specifications (RFC 2109 (Cookies), RFC 2617 (HTTP Authentication)), etc.

License:

Apache License: <http://www.apache.org/licenses/LICENSE-2.0>

File Path: /home/tharindu/dependencies/mydependencies/commons-httpclient-3.1.jar

MD5: 8ad8c9229ef2d59ab9f59f7050e846a5

SHA1: 964cd74171f427720480efdec40a7c7f6e58426a

Evidence