



# School of Engineering

INIT Institut für angewandte  
Informationstechnologie

## Sichere Applikationen für den Studiengang

Die Anzahl der Applikationen für Projekt- und Bachelorarbeiten nehmen immer mehr zu. Da Security immer ein Thema ist, welches in Betracht gezogen werden muss, wird eine Zentrale Analyse benötigt, um den Wartungsumfang der einzelnen Projekte zu reduzieren. Das Ziel dieser Arbeit ist daher eine Pipeline, welche ausgewählte Punkte bezüglich der Sicherheit in einer Applikation prüft und einen Bericht generiert. Die zu prüfenden Punkte werden mittels eines Threat Modelings erhoben. Dabei werden Threat-Agents und Threats identifiziert und eine Risikoanalyse durchgeführt, um feststellen zu können, welche Punkte priorisiert werden müssen. Die Punkte, welche in einer Pipeline angesprochen werden können, lassen sich durch bestehende Analysetools wie OWASP ZAP oder Arachni abdecken.

Das Ergebnis sind Beispiel-Pipelines für SonarQube, OWASP Dependency Check, OWASP ZAP und Arachni, die bei Bedarf angestossen werden können.



Diplomierende  
Carl Lubojanski  
Leandro Meleti

Dozierende  
Patrick Feisthammel  
Stephan Neuhaus

The screenshot shows the Jenkins interface for a 'Dependency-Check' job. The main content is a 'Dependency-Check Results' page with a 'SEVERITY DISTRIBUTION' bar chart and a table of vulnerabilities. The table lists various packages and their associated CVEs, with severity levels ranging from 'Critical' to 'High'.

File Name	Vulnerability	Severity	Weakness
epj@2.7.4	<a href="#">CVE-1573412</a>	Critical	
<b>Description</b>			
The es_saka Embedded JavaScript templates package 3.1.6 for Node.js allows server-side template injection in settings via options(subfunctionName). This is passed as an extend option, and overwrites the outputFunctionName option with an arbitrary JS command (which is executed upon template compilation).			
eventsource@1.1.0	<a href="#">CVE-1373434</a>	Critical	
inquirer@3.0.1	<a href="#">CVE-1567120</a>	Critical	
minimist@1.2.5	<a href="#">CVE-1567342</a>	Critical	
url-parse@1.5.3	<a href="#">CVE-1567316</a>	Critical	
ansi-regex@0.0.7	<a href="#">CVE-2021-25424</a>	High	CWE-400
ansi-regex@0.0.7	<a href="#">CVE-1373006</a>	High	
ansi-regex@1.1.0	<a href="#">CVE-1373074</a>	High	
ansi-regex@5.0.0	<a href="#">CVE-1573275</a>	High	
async@2.6.2	<a href="#">CVE-2021-42138</a>	High	CWE-1321

Ausschnitt aus der Secure-Pipeline mit Fokus auf Dependency Issues.