Das Scannen von Code wird von externen Tools übernommen. Zum aufrufen dieser Tools wird eine interne Version des Project Piper genutzt. Piper vereinfacht unterschiedlichste Schritte, die in einer Pipeline ausgeführt werden können – so zum Beispiel auch das aufrufen von eben solchen externen Scan Tools. Dafür gibt es in dem Bereich der Sicherheitsanalyse von Code eine Reihe von geeigneter Tools wie zum Beispiel Checkmarx oder Fortify, die unter anderem dem HANA & HANA Cloud Quality Engineering (HHCQE) Team genutzt werden. [**SASTTools**]

Solche Tools würden zum Beispiel ein Risikostelle wie in Abbildung **??** erkennen und als „Improper_Resource_Shutdown_or_Release“ einordnen. [**SecurityVulnerabilities**]

Damit wird von dem Scan eine Datei erzeugt, die enthält welche Risikostellen gefunden wurden. Zudem ist in solcher Datei meist eine Priorisierung, wie schwerwiegend die Risikostellen sind, enthalten.

Diese Datei stellt nun das Ergebnis des Scans da und liegt im JSON Format vor.

Außerdem besitzen externe Tools wie Checkmarx oft eine Weboberfläche, in der Details eines Scans mit den genauen Zeilen an Code, die Risikostellen sind, eingesehen werden können. In diesen Rahmen gibt es dann die Möglichkeit diese Risikostellen als unbedenklich zu markieren. Richtlinien beziehen sich oft darauf, wie viele von den Risikostellen als unbedenklich eingestuft werden müssen.