R&D Intern: OWASP Dependency Check: add support for Go

While it is important to care about our own code, many vulnerabilities can arise from the usage of a vulnerable 3rd party library. Using libraries with a known vulnerability is in OWASP Top 10 list since 2013.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to extend OWASP Dependency Check to allow scanning Go libraries. This also includes research about relevant vulnerability sources for Go libraries.

OWASP Dependency Check is an open-source tool that allows developers to scan their application for knowingly vulnerable libraries. The tool can scan various libraries for various platforms like Java, .NET and JavaScript and many more. It uses primarily the National Vulnerability Database, but some scans can utilize another vulnerability database like NodeSecurity.io. OWASP Dependency Check is written in Java in quite a modular way, so we have already written some plugins.

While working as R&D Intern, there is a possibility to write a bachelor thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Přidaní podpory jazyka Go do nástroje OWASP Dependency Check

Při vývoji vlastního kódu je důležité dbát na jeho bezpečnost, ale zároveň je třeba pamatovat, že zranitelnost může způsobit i některé z knihoven třetích stran. Používání knihoven se známými zranitelnostmi je v seznamu OWASP Top 10 od roku 2013.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je rozšířit OWASP Dependency Check, aby uměl skenovat i knihovny v jazyce Go. Součástí je i průzkum toho, z jakých zdrojů (kromě NVD) lze čerpat informace o zranitelnostech těchto knihoven.

Díky open-source nástroji OWASP Dependency Check mohou vývojáři zkontrolovat svoji aplikaci a být upozornění na knihovny se známými zranitelnostmi. Tento nástroj umí oskenovat knihovny pro různé platformy – Java, .NET, JavaScript a další. Používá převážně databázi National Vulnerability Database, ale v některých případech umí využít i další databáze, jako například NodeSecurity.io. Nástroj OWASP Dependency Check je napsán v jazyce Java. Je dobře rozšiřitelný, takže už jsme pro něj napsali několik pluginů.

V rámci stáže je možné řešenou problematiku zpracovat jako bakalářskou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.

R&D Intern: OWASP Dependency Check: add support for C

While it is important to care about our own code, many vulnerabilities can arise from the usage of a vulnerable 3rd party library. Using libraries with a known vulnerability is in OWASP Top 10 list since 2013.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to extend OWASP Dependency Check to allow scanning C libraries. This also includes research about relevant vulnerability sources for C libraries.

OWASP Dependency Check is an open-source tool that allows developers to scan their application for knowingly vulnerable libraries. The tool can scan various libraries for various platforms like Java, .NET and JavaScript and many more. It uses primarily the National Vulnerability Database, but some scans can utilize another vulnerability database like NodeSecurity.io. OWASP Dependency Check is written in Java in quite a modular way, so we have already written some plugins.

While working as R&D Intern, there is a possibility to write a bachelor thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Přidaní podpory jazyka C do nástroje OWASP Dependency Check

Při vývoji vlastního kódu je důležité dbát na jeho bezpečnost, ale zároveň je třeba pamatovat, že zranitelnost může způsobit i některé z knihoven třetích stran. Používání knihoven se známými zranitelnostmi je v seznamu OWASP Top 10 od roku 2013.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je rozšířit OWASP Dependency Check, aby uměl skenovat i knihovny v jazyce C. Součástí je i průzkum toho, z jakých zdrojů (kromě NVD) lze čerpat informace o zranitelnostech těchto knihoven.

Díky open-source nástroji OWASP Dependency Check mohou vývojáři zkontrolovat svoji aplikaci a být upozornění na knihovny se známými zranitelnostmi. Tento nástroj umí oskenovat knihovny pro různé platformy – Java, .NET, JavaScript a další. Používá převážně databázi National Vulnerability Database, ale v některých případech umí využít i další databáze, jako například NodeSecurity.io. Nástroj OWASP Dependency Check je napsán v jazyce Java. Je dobře rozšiřitelný, takže už jsme pro něj napsali několik pluginů.

V rámci stáže je možné řešenou problematiku zpracovat jako bakalářskou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.

R&D Intern: OWASP Dependency Check: enhance support for JavaScript

While it is important to care about our own code, many vulnerabilities can arise from the usage of a vulnerable 3rd party library. Using libraries with a known vulnerability is in OWASP Top 10 list since 2013.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to improve OWASP Dependency Check to allow scanning of JavaScript libraries from WebJars (NPM, Bower, legacy WebJars) or NuGets. Plugin is preferred to a patch. This includes research about relevant vulnerability sources.

OWASP Dependency Check is an open-source tool that allows developers to scan their application for knowingly vulnerable libraries. The tool can scan various libraries for various platforms like Java, .NET and JavaScript and many more. It uses primarily the National Vulnerability Database, but some scans can utilize another vulnerability database like NodeSecurity.io. OWASP Dependency Check is written in Java in quite a modular way, so we have already written some plugins.

While working as R&D Intern, there is a possibility to write a bachelor thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Vylepšení podpory jazyka JavaScript v nástroji OWASP Dependency Check

Při vývoji vlastního kódu je důležité dbát na jeho bezpečnost, ale zároveň je třeba pamatovat, že zranitelnost může způsobit i některé z knihoven třetích stran. Používání knihoven se známými zranitelnostmi je v seznamu OWASP Top 10 od roku 2013.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je rozšířit OWASP Dependency Check, aby uměl skenovat i knihovny v jazyce JavaScript přidané přes WebJars (NPM, Bower, legacy WebJars) nebo NuGet. To zahrnuje i průzkum, z jakých zdrojů (kromě NVD) lze čerpat informace o zranitelnostech těchto knihoven.

Díky open-source nástroji OWASP Dependency Check mohou vývojáři zkontrolovat svoji aplikaci a být upozornění na knihovny se známými zranitelnostmi. Tento nástroj umí oskenovat knihovny pro různé platformy – Java, .NET, JavaScript a další. Používá převážně databázi National Vulnerability Database, ale v některých případech umí využít i další databáze, jako například NodeSecurity.io. Nástroj OWASP Dependency Check je napsán v jazyce Java. Je dobře rozšiřitelný, takže už jsme pro něj napsali několik pluginů.

V rámci stáže je možné řešenou problematiku zpracovat jako bakalářskou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.

R&D Intern: Unused code detection

Legacy code often contains unused parts that further complicate software maintenance. This also skews results from static analysis tools since identified issues might be present in code parts which are never executed.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to research and compare static and dynamic approaches for detection of unused code. Provide tooling and methodology to identify chunks of code that can be safely removed without an impact on functionality. Focus on Java and .NET platforms, high degree of automation is preferred.

While working as R&D Intern, there is a possibility to write a thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Detekce nepoužívaného kódu

Údržbu software mohou komplikovat starší části kódu, které často obsahují nepoužívané oblasti. Kvůli nim také dochází ke zkreslení výsledků nástrojů pro statickou analýzu, protože identifikované problémy se mohou nacházet v částech kódu, které se nikdy nespouštějí.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je výzkum a srovnání statických i dynamických přístupů pro detekci nepoužívaného kódu. Výstupem je poskytnutí nástroje a postupů pro identifikaci oblastí v kódu, které mohou být bezpečně odstraněny bez ovlivnění funkcionality. Při výzkumu jsou preferovány platformy Java a .NET a vysoký stupeň automatizace.

V rámci stáže je možné řešenou problematiku zpracovat jako bakalářskou nebo diplomovou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.

R&D Intern: Automatic API extraction from traffic analysis

To utilize dynamic analysis testing methods such as fuzzing all entry points into the application need to be identified first. Automatically extracted definition of application interfaces could be used to check consistency with documentation and as an input for other automatic tools.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to research and implement a method to extract API definitions from traffic analysis (e.g., captured analysis from Wireshark on a network where YSoft SafeQ is run for some time). The extracted API should be output in appropriate format including identified data types.

While working as R&D Intern, there is a possibility to write a bachelor thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Automatická extrakce API ze síťové komunikace

Pro využití testovacích metod dynamické analýzy jako je fuzzing je nutné nejprve identifikovat všechny vstupní body do aplikace. Automatická extrakce definic aplikačních rozhraní je používána ke kontrole konzistence s dokumentací a jako vstup pro další automatické nástroje.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je výzkum a implementace metody extrakce definic API z analýzy síťového provozu (např. analýza zaznamenaná programem Wireshark na síti, kde bylo provozováno řešení YSoft SafeQ). Výstupy extrahovaného API jsou zpracovávány ve vhodném formátu a obsahují identifikované datové typy.

V rámci stáže je možné řešenou problematiku zpracovat jako bakalářskou nebo diplomovou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.

R&D Intern: Dynamic security analysis of web application

Automatic dynamic security analysis is an efficient way to find web vulnerabilities with low false positives rate.

We are currently seeking a new colleague to join the Y Soft Product Security team as R&D Intern. Your task in this role is to select and work with tools that can crawl a specified web interface and perform active scanning for application-level vulnerabilities such as SQL injection and XSS (passive scan for detection of presence of security headers etc. is a bonus). The solution must support scanning of AJAX-based application with authentication and CSRF protection as used by YSoft SafeQ web interfaces. Regular analysis must be setup in Y Soft's CI environment and have flexible configuration to support suppression of false positives and be usable for security regression testing. It can be continuation of previous research (using tools such as OWASP ZAP) or a new approach (consider utilization of frameworks such as BDD Security or OWTF).

While working as R&D Intern, there is a possibility to write a thesis in this field. This internship is paid and has a form of DPP/DPČ contract.

R&D Intern: Dynamická bezpečnostní analýza webových aplikací

Automatická dynamická analýza bezpečnosti je efektivní způsob pro hledání webových zranitelností s nízkým podílem falešných detekcí.

Do Product Security teamu hledáme nové kolegy na pozici R&D Intern. Hlavní náplní této role je práce s nástroji, které dovedou prozkoumat aplikaci přes webové rozhraní a aktivně hledat aplikační zranitelnosti jako SQL injekce nebo XSS (pasivní kontrola přítomnosti bezpečnostních HTTP hlaviček apod. je bonus). Navrhovaná řešení musí podporovat skenování AJAXových aplikací i po autentizací a s ochranou před CSRF, tak jak jsou používány webovým rozhraním produktu YSoft SafeQ. Analýza probíhá pravidelně v prostředí CI firmy Y Soft a jsou na ni kladeny požadavky dostatečné konfigurovatelnosti pro potlačování falešných detekcí a použitelná pro regresní testování bezpečnosti. V rámci této stáže je možné navázat na předcházející výzkum (s použitím nástrojů jako OWASP ZAP) nebo zvolit nový přístup.

V rámci stáže je možné řešenou problematiku zpracovat jako diplomovou práci. Tato stáž je placená a je uskutečněna formou DPP/DPČ.