Kravspecifikation

Edvin Gibro
Bacilika Glansholm
Viktor Holta
Simon Karlsson
Jessica Kjellin
Max Randow
Erik Simonson
Jakob Söderström

26 mars 2024

Version 2.0

Projektidentitet

Hemsida: https://github.com/OSSQA-PUM

Kund: Ola Angelsmark, Advenica AB
E-post: ola.angelsmark@advenica.com

Handledare: Eric Ekström, Linköpings Universitet
E-post: eric.ekstrom@liu.se

Kursansvarig: Kristian Sandahl, Linköpings Universitet
E-post: kristian.sandahl@liu.se

Projektdeltagare

Namn	**Ansvar**	**E-post**
Edvin Gibro	Teamledare	edvgi966@student.liu.se
Bacilika Glansholm	Arkitekt, Vice teamledare	bacgl188@student.liu.se
Viktor Holta	Testledare	vikho305@student.liu.se
Simon Karlsson	Analysansvarig	simka157@student.liu.se
Jessica Kjellin	Kvalitetssamordnare	jeskj559@student.liu.se
Max Randow	Dokumentansvarig	maxra518@student.liu.se
Erik Simonson	Konfigurationsansvarig	erisi409@student.liu.se
Jakob Söderström	Utvecklingsledare	jakso277@student.liu.se

INNEHÅLL

1 Inledning 1
1.1 Parter . . . 1
1.2 Syfte och mål . . . 1
1.3 Användning . . . 2
1.4 Bakgrundsinformation . . . 2
1.5 Definitioner . . . 2
2 Översikt av systemet 2
2.1 Användaren skickar in SBOM . . . 2
2.2 Användaren bestämmer krav . . . 3
2.3 SBOMen analyseras baserat på kraven . . . 3
2.4 Resultat visas . . . 3
2.5 Databas lagrar resultatet . . . 3
2.6 Beroenden till andra system . . . 3
2.7 Avgränsningar . . . 3
2.8 Leverans . . . 4
2.9 Designfilosofi . . . 4
3 Krav 4
3.1 Funktionella krav . . . 4
3.2 Icke-funktionella krav . . . 5
3.3 Kvalitetskrav . . . 5
3.4 Krav på koddokumentation . . . 6
3.5 Ekonomikrav . . . 6

DOKUMENTHISTORIK

Version	Datum	Utförda ändringar	Utförda av	Granskad
0.1	2024-02-04	Första utkast	SK, JK, MR, ES & JS	SK
0.2	2024-02-08	Krav tillkommit kring mätpunkter i kod	ES	SK
0.3	2024-02-15	Krav tillkommit kring användbarhet av program. Krav ändrats kring prestanda	SK	ES & EG
1.0	2024-02-28	Ändringar om struktur, förtydliganden och inledning har genomförts enligt feedback från handledare	SK	BG & VH
2.0	2024-02-28	Upprepade krav har tagits bort, och språkfel korrigerats	SK	

1 INLEDNING

Detta dokument är en kravspecifikation för projektgenomförande samt den produkt som skall utvecklas till kunden *Advenica AB* i kursen Kandidatprojekt i programvaruutveckling på Linköpings universitet. Projektgruppen som skall utveckla produkten heter PUM14 och produkten som skall utvecklas heter *Open-Source Security and Quality Assessment*, förkortat *OSSQA*. Dokumentet redogör för samtliga interna krav och kundkrav för produkten som utvecklas under projektet. Målet med projektet är att bygga ett program som tar emot en *Software Bill of Materials (SBOM)* från en fil som indata, där programmet därefter söker igenom denna och gör en analys utifrån användarens prioritet.

Kravbeskrivningarna är uppbyggda av tabeller som är skapade enligt följande modell:

- Kolumn 1 innehåller ett nummer som används för identifiering av kravet.
- Kolumn 2 beskriver om kravet är från originalversionen av dokumentet, eller om det är förändrat under projektet.
- Kolumn 3 innehåller en beskrivning av vad kravet innebär.
- Kolumn 4 beskriver prioritet på kravet, som är uppdelad på två nivåer; 1 och 2. Betydelsen av dessa prioriteringar är följande:
    1. Kravet måste genomföras.
    2. Kravet skall genomföras om tid finns.

Krav	Version	Beskrivning	Prioritet
1	Original	Beskrivning av kravet	1

Tabell 1: Exempel på kravbeskrivning.

1.1 Parter

De parter som är inkluderade i detta projekt är projektgrupp PUM14, handledare Eric Ekström, kursansvarig Kristian Sandahl, samt företaget Advenica AB som är kund till projektet.

1.2 Syfte och mål

Syftet med dokumentet är att dokumentera samtliga kundkrav och interna krav för projektet. Syftet är att tydligt redogöra för vad som behöver uppnås och mätas, samt att tydligt dokumentera för kund vad som kan förväntas av produkten.

Målet är att dokumentet ska kunna användas av projektgrupp PUM14 samt kund Advenica AB för att utläsa de krav som finns på produkten som skapas under projektet. Målet är att det tydligt ska kunna läsas ut vad som kan förväntas av produkten och vad som måste prioriteras av projektgruppen.

1.3 Användning

Dokumentet kommer att användas för granskning av huruvida produkten nått minsta godkända produkt. Detta kommer genomföras genom att funktionalitet av produkten jämförs med de krav som finns dokumenterade i detta dokument.

1.4 Bakgrundsinformation

Projektet initieras som ett examensarbete för kursen "Kandidatprojekt i programvaruutveckling", utformad för att möta en beställning från en extern kund.

1.5 Definitioner

I nedanstående lista presenteras ett antal viktiga definitioner som kommer att användas i detta dokument.

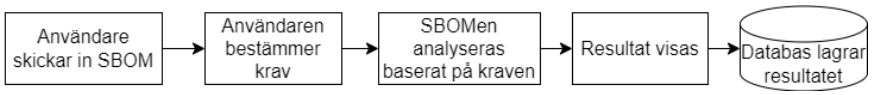
- **SBOM –** Förkortning av *Software Bill of Materials*. En innehållsdeklaration för en mjukvara som definierar samtliga programbibliotek som används.
- **CycloneDX –** En standard för hur en SBOM representeras.
- **Sprint –** En kortare arbetsperiod på två veckor som planeras detaljerat inom gruppen.
- **Git –** Versionshanteringsverktyg. Används för att enkelt kunna hantera ett projekt.
- **Repo –** Från engelskans *repository*. Ett Git-repo är en katalog eller lagringsenhet där alla filer, historik och konfiguration för ett projekt sparas.
- **GitHub –** En webbplattform för att lagra *repos*.
- **OpenSSF Scorecard –** Ett verktyg som analyserar *GitHub* – repos utifrån 5 förbestämda kriterier och get ett betyg mellan 0-10 på hur säkra dessa är. 0 innebär enorma brister, medan 10 är att brister saknas.
- **SUS –** Förkortning av System Usability Score. SUS är en etablerad enkät inom mjukvaruindustrin för att mäta användbarhet av ett system.
- **Förväntad utdata –** Beräknas genom en sammanfattning av några SBOM-exempel där vi separat beräknar den utdata som bör utkomma från analysen.

2 ÖVERSIKT AV SYSTEMET

Figur 1 visar en översiktlig beskrivning av produkten. I detta kapitel kommer samtliga block i figuren redovisas och förklaras mer detaljerat.

2.1 Användaren skickar in SBOM

Första blocket i *figur 1* representerar användarens första steg i programmet. Användaren skickar en *SBOM* som indata i programmet.



Figur 1: En översikt av systemet

2.2 Användaren bestämmer krav

Andra blocket i *figur 1* representerar det som sker efter att programmet tagit emot en SBOM. Programmet ger användaren möjligheten att prioritera de fem olika kategorierna som mäts av OpenSSF Scorecards; *code vulnerabilities, maintenance, continuous testing, source risk assessment* samt *build risk assessment*, på en skala mellan 0–10. Prioritet 0 representerar att programmet skall inte inkludera kategorin i resultatberäkningen, prioritet 10 representerar att resultatet räknas med full prioritet i resultatet. De olika prioriteterna påverkar resultatet i relation till varandra.

2.3 SBOMen analyseras baserat på kraven

Tredje blocket i *figur 1* representerar att programmet analyserar den SBOM som skickats som indata i programmet med hjälp av OpenSSF Scorecards och med den prioritet som användaren angett.

2.4 Resultat visas

Fjärde blocket i *figur 1* representerar att resultatet presenteras för användaren.

2.5 Databas lagrar resultatet

Femte blocket i *figur 1* representerar att resultatet som redovisades för användaren i block 4 sparas i en databas. Denna databas samtalar med programmet, och om samma SBOM, med ändringar, anges som input, så analyseras enbart de delarna som har ändrats, övrigt presenteras enligt data som hämtas ifrån databasen.

2.6 Beroenden till andra system

Det finns beroenden i projektet till följande system:

- CycloneDX
- OpenSSF Scorecard

För mer detaljerad information om beroendena till andra system, se *Arkitektplan [1]*

2.7 Avgränsningar

Detta delkapitel tar upp de avgränsningar som finns i projektet. Detta innefattar avgränsning angående hur mycket tid som finns att tillgå för projektets genomförande samt relevanta tekniska avgränsningar.

2.7.1 *Tid*

Den avgränsning som finns inom projektet är att vardera gruppmedlem enbart har 400 timmar arbete att lägga ner under hela projektet. Detta inkluderar föreläsningar, informationsintag, möten, dokumentskrivning samt programmering av produkt.

2.8 Leverans

Leveransen inkluderar tre separate delar:

- Release tag sätts på Git-*repot* i *GitHub* som innehåller källkoden för produkten OSSQA
- Produkten presenteras för Advenica AB av projektgrupp PUM14 med hjälp av Microsoft-programmet Powerpoint.
- En dokumentation som beskriver hur en användare kan interagera med systemet levereras till Advenica AB.

Leveransen sker till kund Advenica AB senast 8 maj 2024. Ovanstående delar skall ske under leveranstillfället.

2.9 Designfilosofi

Designfilosofin för produkten är en produkt som är enkel och snabb att använda. Produkten kan användas effektivt av utvecklare för att söka igenom SBOMs och ger ett läsbart resultat i enlighet med användarens prioritet.

3 KRAV

I detta kapitel kommer samtliga krav att dokumenteras. Det inkluderar funktionella krav, icke-funktionella krav, kvalitetskrav, krav på koddokumentation samt ekonomikrav.

3.1 Funktionella krav

Detta delkapitel dokumenterar krav över funktionaliteten för produkten *OSSQA*. Detta innebär krav på hur produkten fungerar, och vad den kan göra.

Krav	Version	Beskrivning	Prioritet
1	Original	Programmet skall kunna ta emot en SBOM i standardformatet *CycloneDX*	1
2	Original	Programmet skall tillåta användare att initiera en analys av uppladdade SBOM:s	2
3	Original	Programmet skall tillåta användare att söka efter tidigare analyser och deras resultat	2

forts. på nästa sida

forts. från föregående sida			
Krav	Version	Beskrivning	Prioritet
4	Original	Användargränssnittet skall kunna presentera resultaten från en analyserad SBOM	1
5	Original	Databasen skall kunna lagra SBOMs samt de resultat och slutsatser som genereras av analysen	2
6	Original	Databasen skall stödja effektiva sökningar baserade på kriterierna paketnamn och URL	2
7	Original	Databasen skall kunna spara historiska analysresultat relaterade till beroenden i en SBOM	2
8	Original	Webbgränssnittet skall kunna ta emot en fil som innehåller en SBOM i standardformatet CycloneDX som argument	2
9	Original	Webbgränssnittet skall kunna presentera resultaten från en analyserad SBOM	2
10	Original	Webbgränssnittet skall tillåta användaren att söka efter tidigare analyser och deras resultat	2

3.2 Icke-funktionella krav

Detta delkapitel dokumenterar krav som är icke-funktionella för produkten *OSSQA*. Detta innefattar krav runtom systemet. Vad som tillåts, hur produkten skall fungera och hur projektarbetet skall genomföras.

Krav	Version	Beskrivning	Prioritet
11	Original	Programmet skall ha integrerade automatiserade tester i GitHub	1
12	Original	Programmet skall inte tillåta att en analyserad SBOM är åtkomlig utanför systemet	1
13	Original	*Sprint*-demonstrering skall ske med Advenica AB via digitalt möte varje jämn vecka, med undantag vecka 12 med anledning av tentamensperiod	1
14	Original	Slutleverans av produkt skall vara genomförd senast 8 maj enligt **2.8 Leverans**	1
15	Original	Det skall finnas dokumentation som redogör för hur en användare kan interagera med systemet	1

3.3 Kvalitetskrav

Detta delkapitel dokumenterar de mätbara krav som finns över kvaliteten för produkten *OSSQA*.

Krav	Version	Beskrivning	Prioritet
16	Original	Programmet skall klara att ge *förväntad utdata* vid 90% av testkörningar	1
17	Original	Programmets tester skall omfatta 60% funktionstäckning enligt pytest_func_cov [2]	1
18	Original	Programmet skall ha 75 poäng enligt *SUS* [3]	1
19	Original	Programmet skall ge färdigt resultat på en SBOM på 200 beroenden på under 5 timmar	1

3.4 Krav på koddokumentation

Detta delkapitel dokumenterar krav som finns i dokumentationen av kod för programmering av produkten *OSSQA*. Detta innefattar hur utvecklarna inom projektgruppen skall dokumentera den kod som skrivs för produkten.

Krav	Version	Beskrivning	Prioritet
20	Original	Programmets kod skall skrivas och vara kommenterad enligt PEP 8	1

3.5 Ekonomikrav

Detta delkapitel dokumneterar de krav som finns på ekonomi för att bygga produkten *OSSQA*. Detta innefattar den budget som finns att tillgå inom projektet, och vad som förväntas minimalt.

Krav	Version	Beskrivning	Prioritet
21	Original	Varje gruppmedlem ska lägga ner 400 timmar på projektarbetet	1

REFERENSER

[1] PUM14. ”Arkitektplan”, Hämtad: 2024-02-28. [Online].

[2] Radu Ghitescu. ”pytest-func-cov 0.2.3.” The Python Package Index, Hämtad: 2024-02-28. [Online]. Tillgänglig: https://pypi.org/project/pytest-func-cov/.

[3] J. R. Lewis, “The system usability scale: past, present, and future,” *International Journal of Human–Computer Interaction*, vol. 34, no. 7, pp. 577–590, 2018.