Kravspecifikation

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

1 februari 2024

Version 0.1

Status

Granskad	NAMN	2024-xx-xx
Godkänd	NAMN	2024-xx-xx

1 februari 2024

Projektidentitet

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

Kund: Ola Angelsmark, Advenica AB
Tfn: 070-338 59 55
E-post: ola.angelsmark@advenica.com

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

Kursansvarig: Kristian Sandahl, Linköpings Universitet
Tfn: 013-28 19 57
E-post: kristian.sandahl@liu.se

Projektdeltagare

Namn	**Ansvar**	**E-post**	**Telefon**
Bacilika Glansholm	Arkitekt, Vice teamledare	bacgl188@student.liu.se	079-359 85 17
Edvin Gibro	Teamledare	edvgi966@student.liu.se	070-326 11 39
Erik Simonson	Konfigurationsansvarig	erisi409@student.liu.se	073-074 44 48
Jakob Söderström	Utvecklingsledare	jakso277@student.liu.se	072-548 23 18
Jessica Kjellin	Kvalitetssamordnare	jeskj559@student.liu.se	072-300 56 86
Max Randow	Dokumentansvarig	maxra518@student.liu.se	070-244 48 60
Simon Karlsson	Analysansvarig	simka157@student.liu.se	070-729 68 15
Viktor Holta	Testledare	vikho305@student.liu.se	070-019 95 19

INNEHÅLL

DOKUMENTHISTORIK

Version	Datum	Utförda ändringar	Utförda av	Granskad
0.1	2024-02-04	Första utkast	PUM14	

1 INLEDNING

Detta dokument är en kravspecifikation för produkten som skall utvecklas till kunden *Advenica AB* i kursen Kandidatprojekt i programvaruutveckling på Linköpings universitet. Projektgruppen som skall utveckla produkten heter PUM14 och produken som skall utvecklas heter *Open-Source Quality/Security Assessment*, förkortat *OSSQA*. Dokumentet dokumenterar samtliga krav under projektet: interna krav, kundkrav samt kurskrav. 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 preferenser.
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 utifall 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. Kravetskall genomföras om tid finns.

Krav	Version	Beskrivning	Prioritet
1	Original	Vad som skall göras.	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 är att förbättra säkerhetsstandarden inom *Free Open Source Software (FOSS)*-mjukvara. Det finns inget verktyg som i nuläget prioriterar säkerhetsrisker vid analys av en *SBOM*. Med hjälp av denna mjukvara kommer utvecklare lättare att kunna upptäcka och åtgärda säkerhetsrisker i deras projekt.

Målet med projektet är att utveckla ett verktyg som tar in en *SBOM* och analyserar den för att hitta säkerhetsrisker.

1.3 Användning

Produkten som utvecklas i projektet kommer att användas av mjukvaruutvecklare. Produkten kommer att användas för att söka igenom SBOM:s för att få reda på kvalitet samt säkerhet inom denna SBOM. Viss teknisk kompetens kan antas hos användarna av produkten.

1.4 Bakgrundsinformation

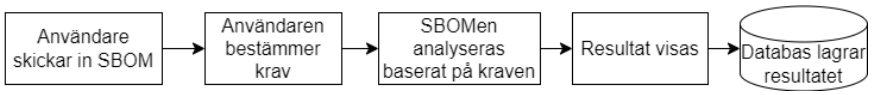
Projektet initieras som ett examensarbete för kursen "Kandidatprojekt i programvaruutveckling", utformad för att möta en beställning från en extern kund.

1.5 Definitioner

- **SBOM** - Förkortning av *Software Bill of Materials*. En innehållsdeklaration för en mjukvara som definierar biblioteken som används.
- **CycloneDX** - En standard för hur en *SBOM* representeras.
- **SPDX** - En standard för hur en *SBOM* representeras.
- **FOSS** - Förkortning för *Free Open Source Software*. Detta innebär mjukvara som är gratis och tillgänglig för alla att läsa, utveckla och använda för eget bruk.
- **Sprint** - En kortare arbetsperiod som planeras detaljerat inom gruppen.
- **Kanban Board** - Digital tavla med korta beskrivningar av allt som vad som är kvar att göra under en sprint, allt som är pågående samt allt som är genomfört.
- **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 webbplatform för att lagra repos.
- **OpenSSF Scorecard** - Ett verktyg som analyserar Github repos utifrån förbestämda kriterier och get ett betyg mellan 0-10.

2 ÖVERSIKT AV SYSTEMET

Figur 1 visar en översiktlig beskrivning av produkten.



Figur 1: En översikt av systemet

2.1 Grov beskrivning av produkten

En produkt som tar emot en *SBOM*, söker igenom denna enligt användarens preferenser och ger tillbaka ett läsbart dokument till användaren med resultat av kvalitet och säkerhet utgående från ovan nämnda preferenser.

2.2 Beroenden till andra system

Det finns beroenden i projektet till följande system:

- CycloneDX
- OpenSSF Scorecard

2.3 Ingående delsystem

Följande delsystem ingår i det fullständiga systemet:

- Applikation
- Webbgränssnitt
- Databas

För mer information för varje delsystem se arkitekturdokumentet [1].

2.4 Avgränsningar

Delkapitel om de avgränsningar som finns i projektet.

2.4.1 *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.

2.4.2 *Tekniska avgränsningar*

Produkten utvecklas med öppen källkod och versionshanteras med hjälp av Git. Analysen av SBOMs utgår från *OpenSSF Scorecard*.

2.5 Designfilosofi

Designfilosofin för produkten är en produkt som är enkel och snabb att använda, som kan användas effektivt av utvecklare för att söka igenom SBOM och ger ett läsbart resultat i enlighet av användarens preferenser.

2.6 Generella krav

Generella krav över hela projektet.

Krav	Version	Beskrivning	Prioritet
1	Orginal	Projektarbetet skall ske i en iterativ utvecklingsmetod med sprints som är 2 veckor långa	1
2	Orginal	Det skall existera en Kanban Board internt i gruppen	1
3	Orginal	Programkod skall följa marknadsstandarder och vara kommenterad	1
4	Orginal	Programkod skall vara lättläst	1
5	Orginal	Programmet skall kunna ta emot en fil som innehåller en SBOM som argument	1
6	Orginal	Programmet skall kunna söka igenom en SBOM	1
7	Orginal	Samtliga gruppmedlemmar skall skriva under publiceringsgodkännande för kandidatrapport	1
8	Orginal	Gruppen skall visa på minst 1 försök till en processförbättring	1

3 APPLIKATION

Denna del kommer behandla krav för delsystemet **Applikationen**. Detta innebär krav på gränssnitt, design samt funktionella krav.

3.1 Gränssnitt

Gränssnittskrav för applikationen.

Krav	Version	Beskrivning	Prioritet
9	Orginal	Produkten skall vara lättanvänd och intuitiv	1
10	Orginal	Genom produktens gränssnitt skall man kunna sätta prioritet för resultat av analysen	2

3.2 Designkrav

Designkrav för applikationen.

Krav	Version	Beskrivning	Prioritet
11	Orginal	Programmet skall ha stöd för automatiserade arbetsflöden och integration med befintliga verktyg och tjänster	2

3.3 Funktionella krav

Funktionella krav för applikationen.

Krav	Version	Beskrivning	Prioritet
12	Orginal	Programmet skall kunna ta emot en SBOM i standardformat, exempelvis SPDX eller CycloneDX	1
13	Orginal	Programmet skall skapa ett resultat som är läsbart	1
14	Orginal	Programmets resultat skall kunna anpassas enligt prioritet från användaren	2
15	Orginal	Programmet skall söka igenom en SBOM enligt prioritet given från användaren	2

4 WEBBGRÄNSSNITT

Denna del kommer behandla krav för delsystemet **Webbgränssnitt**. Detta innebär krav på gränssnitt, design samt funktionella krav.

4.1 Funktionella krav

Här redovisas de funktionella kraven för webbgränssnittet.

Krav	Version	Beskrivning	Prioritet
16	Orginal	Användare skall kunna ladda upp SBOM-filer i format som stöds av applikationen	2
17	Orginal	Användare skall kunna initiera en analys av uppladdade SBOM-filer	2
18	Orginal	Användargränssnittet skall kunna presentera resultaten från en analyserad SBOM	2
19	Orginal	Användare ska kunna söka efter tidigare analyser och deras resultat	2

5 DATABAS

Denna del kommer behandla krav för delsystemet **Databas**. Detta innebär krav på gränssnitt, design samt funktionella krav.

5.1 Funktionella krav

Funktionella kraven för databasen som programmet kommer att använda.

Krav	Version	Beskrivning	Prioritet
20	Orginal	Databasen skall kunna lagra SBOM-filer samt de resultat och slutsatser som genereras av analysen	2
21	Orginal	Stödja effektiva sökningar baserade på kriterier som till exempel paketnamn	2
22	Orginal	Databasen skall kunna spara historiska analysresultat relaterade till projekt	2

6 PRESTANDAKRAV

Krav på produktens prestanda.

Krav	Version	Beskrivning	Prioritet
23	Orginal	Programmet skall gå att genomköras på under 5 minuter	1
24	Orginal	Programmet skall gå att genomköras på under 2 minuter	2

7 KRAV PÅ VIDAREUTVECKLING

Krav på produktens möjligheter till vidareutveckling

Krav	Version	Beskrivning	Prioritet
25	Orginal	Programmet skall ha kommenterad kod	1
26	Orginal	Programmet skall ha en dokumentation	1
27	Orginal	Programmet skall vara Open-Source	1

8 TILLFÖRLITLIGHET

Krav på produktens tillförlitlighet

Krav	Version	Beskrivning	Prioritet
28	Orginal	Produkten skall köras som produktbeskrivning antyder minst 90% av körningar	1
29	Orginal	Programmet skall klara av att ta in 25 unika SBOM:s samtidigt som programmet uppfyller den andra kraven	1
30	Orginal	Programmet skall klara av att ta in 100 unika SBOM:s samtidigt som programmet uppfyller den andra kraven	1

9 EKONOMI

Krav på projektets ekonomi.

Krav	Version	Beskrivning	Prioritet
31	Orginal	Varje gruppmedlem ska lägga ner 400 timmar ± 10% på projektarbetet	1

10 KRAV PÅ SÄKERHET

Under denna sektion står de säkerhetskrav som finns för programmet.

Krav	Version	Beskrivning	Prioritet
32	Orginal	Den SBOM:en som systemet använder som indata skall ej vara åtkomlig utanför systemet	1

11 LEVERANSKRAV OCH DELLEVERANSER

Krav på leveranser och delleveranser som inkluderas i projektet

Krav	Version	Beskrivning	Prioritet
33	Orginal	Sprint-demonstrering skall ske med Adnvenica AB via digitalt möte varje jämn vecka	1
34	Orginal	Slutleverans av produkt skall vara genomförd senast 8 maj	1
35	Orginal	Slutleverans skall genomföras genom att en release tag sätts på Git-repot	1
36	Orginal	Slutleverans skall redovisas med en presentation inför projektansvariga på Advenica AB	1

12 DOKUMENTATION

Tabell 14 listar de dokument som skall produceras

Dokument	Syfte	Målgrupp	Format
Projektplan	Övergripande plan över hur projektet skall utföras.	Projektgrupp & Kursansvarig	PDF
Kravspecifikation	Beskrivning av kraven på produkten.	Kund & Kursansvarig	
Kvalitetsplan	Beskrivning av processer samt krav på utvärdering och förbättring.	Kursansvarig	PDF
Statusrapport	Redovisa status på projetket.	Kursansvarig	PDF
Systemanatomi	Övergripande visuell och ordagrann beskrivning av systemets uppbyggnad.	Projektgrupp & Kursansvarig	PDF
Arkitekturdokument	Översikt av systemets ariktektur.	Projektgrupp & Kursansvarig	PDF
Testplan	Översikt över vad som ska testat samt vilka typer av tester som skall utföras.	Kursansvarig	PDF
Testrapport	Sammanställning av testfall och deras resultat.	Kursansvarig	PDF
Utvärderingsdokument	Utvärdering av hur arbetet går.	Kursansvarig	PDF
Kandidatarbete	Rapport om projektet.	Kursansvarig	PDF
Tidrapport	Redovisning av arbetet som har gjorts varje vecka.	Handledare & Kursansvarig	Excel
Mötesprotokoll	Dokument som skrivs vid varje möte för att dokumentera beslutsamt vad som sägs på mötet	Projektgrupp	Docx
Sammanfattning av processrelaterade erfarenheter	Indivuduell rapport om processrelaterade erfarenheter från projektet.	Kursansvarig	PDF
Sammanfattning av tekniska erfarenheter	Indivuduell rapport om tekniska erfarenheter från projektet.	Kursansvarig	PDF

Tabell 14: Dokument som skall produceras

Krav	Version	Beskrivning	Prioritet
37	Orginal	Projektplan skall vara klar senast 2024-02-19	1
38	Orginal	Kravspecifikation skall vara klar senast 2024-02-19	1
39	Orginal	Kvalitetsplan skall vara klar senast 2024-02-19	1
40	Orginal	Statusrapport skall vara klar senast 2024-02-19	1
41	Orginal	Systemanatomi skall vara klar senast 2024-02-19	1
42	Orginal	Arkitekturdokument skall vara klar senast 2024-01-08	1
43	Orginal	Testplan skall vara klar senast 2024-03-08	1
44	Orginal	Utvärderingsdokument klar senast 2024-03-08	1
45	Orginal	Samtliga delkapitel förutom resultat, diskussion och slutsats i kandidatarbetet skall vara klart senast 2024-03-08	1
46	Orginal	Första utgåva av kandidatarbetet skall vara klart senast 2024-05-08	1
47	Orginal	Slutversion av kandidatarbetet skall vara klart senast 2024-05-23	1
48	Orginal	Tidrapport skall vara inlämnad senast kl. 13:00 varje måndag	1
49	Orginal	Mötesprotokoll skall föras på varje möte	1

13 UNDERHÅLLSBARHET

Denna sektion reogör för vilka underhållsbarhets krav som finns för programmet. Dessa krav kan ses i den nedanstående tabellen.

Krav	Version	Beskrivning	Prioritet
50	Orginal	Alla dokument som inehåller kod skall vara kommenterade	1
51	Orginal	Det skall finnas dokumentation som redogör för hur en användare kan interagera med systemet	1
52	Orginal	All kod skall vara skriven i ett välkänt och använt språk	1

14 MÖTESKRAV

Krav	Version	Beskrivning	Prioritet
53	Original	Varje gruppmedlem skall deltaga på minst 75% av handledarmöten	1
54	Original	Vid handledarmöten skall en majoritet av gruppen deltaga	1
55	Original	Mötesagenda skall skickas till handledare senast 24 h innan mötet	1
56	Original	Mötesagenda skall skickas till kund senast 24 h innan mötet	1

forts. på nästa sida

forts. från föregående sida			
Krav	Version	Beskrivning	Prioritet
57	Original	Mötessammanfattning eller mötesprotokoll skall skickas till kund senast 24 h efter mötet	1
58	Original	Kundmöte skall hållas minst en gång varje jämn vecka	1

REFERENSER

[1] PUM14, “Arkitekturdokument,” https://gitlab.liu.se/da-proj/microcomputer-project-laboratory-d/2023/g11/docs/-/blob/main/ban_och_tavlingsspecifikation_1.1.pdf?ref_type=heads, 2024.