

Øvelse 29 - Skanning for tredjeparts sårbarheder med Snyk CLI-værktøjet

Information

Formålet med denne øvelse er at vise, at der findes flere værktøjer til skanning for tredjeparts sårbarheder. I denne øvelse skal værktøjet Snyk anvendes.

Du skal anvende det samme projekt som i forrige øvelse.

Snyk er et populært sikkerhedsværktøj, som ikke blot scanner efter kendte sårbarheder i tredjepartsbiblioteker, men også kan give forslag til rettelser, overvåge afhængigheder over tid og integreres i CI/CD-pipelines for kontinuerlig sikkerhed.

Det er vigtigt at forstå, at scanning af sårbarheder kun er et led i en bredere strategi for sikker håndtering af tredjepartsafhængigheder.

Instruktioner

1. Du skal installere Windows package manageren `Chocolatey`. Følg guiden til installation [her](#).
 2. Brug `Chocolatey` til at installere `Snyk CLI`. Se guiden [her](#).
 3. Anvend kommandoen `snyk test` i projektmappen `Webgoat.NET` folder (Altså det skal eksekveres i `Webgoat.NET\Webgoat.NET`).
- Du vil blive bedt om at autentificer mod Snyk. Hvis du blot skriver `Snyk auth` bør du komme frem til autentificering, hvor du har mulighed for at anvende credentials fra andre kontoer, F.eks. Github.
4. Saml resultaterne med `dotnet vulnerability`.

▮ Bedste praksis for håndtering af tredjepartsafhængigheder

- Brug altid versionslåste afhængigheder (lock-filer) for at sikre reproducerbare builds.
- Scan jævnligt dit projekt for sårbarheder, helst automatiseret i CI/CD-pipelines.
- Prioriter opdateringer baseret på sårbarhedens alvorlighed og projektets risikoprofil.
- Hold øje med transitive afhængigheder, da de også kan indeholde sårbarheder.
- Integrér sikkerhedsvurdering som en naturlig del af softwareudviklingsprocessen.

□ Refleksionsspørgsmål

1. Hvordan kan brugen af flere værktøjer som Snyk og dotnet vulnerability forbedre jeres sikkerhedsindsats?
2. Hvilke udfordringer kan der være ved at holde tredjepartsbiblioteker opdaterede?
3. Hvordan kan automatisering i CI/CD-pipelines hjælpe med at forebygge sårbarheder?
(Hvis du endnu ikke er bekendt med CI/CD, så blier den introduceret senere i dette fag)

□ Kobling til relevante standarder og principper

Element i øvelsen	Relateret standard / princip	Kommentar
Sårbarhedsscanning	ISO/IEC 27002:2022, afsnit 8.8. (Styring af tekniske sårbarheder, særligt stykke d. og f.)	Anbefaler løbende scanning og håndtering af kendte sårbarheder i softwarekomponenter.
	OWASP Application Security Verification Standard (ASVS) Kontrol 15	Krav om håndtering af tredjepartskomponenter og kendte sårbarheder i applikationer.
	Secure by Design (Johnsson et al.)	Fremhæver vigtigheden af at kende og minimere risiko ved tredjepartssoftware.

□ *Proaktiv scanning og opdatering af tredjepartsbiblioteker er afgørende for at opretholde et sikkert softwaremiljø.*

Last update: 2025-10-30 12:07:19