Raamlepingu nr 2/39-26

lisa 1

TEHNILINE KIRJELDUS

Hanke eesmärgiks on tellija poolt tellitavate, olemasolevate ja valitud süsteemide turvalisuse testimine OWASP (Open Worldwide Application Security Project) ASVS (Application Security Verification Standard) versioon 5.0.0 (või juhul, kui sõlmitava raamlepingu kehtivuse perioodil peaks eksisteerima uuem versioon, siis uuemale) tasemetele 2 ja 3 ning MASVS (Mobile Application Security Verification Standard) versioon 2.1.0 (või juhul, kui sõlmitava raamlepingu kehtivuse perioodil peaks eksisteerima uuem versioon, siis uuemale).

Turvatestimise käigus tuleb metoodiliselt testida ja hinnata kõiki potentsiaalseid turvavigu (sealhulgas OWASP Top Ten) ning need tuleb testiraportis detailselt välja tuua koos võimalike lahenduste ja soovitustega, st leitud vigade puhul välja tuua võimalikud ohustsenaariumid.

Testimisel tuleb kontrollida, et testitavate süsteemide võimalike haavatavuste kaudu ei oleks võimalik juurde pääseda andmetele, mis asuvad väljaspool testitava rakenduse funktsionaalsust. Testimine hõlmab ka kasutajate horisontaalset ja vertikaalset õiguste ületamise turvatestimist.

Kõik testimised ja lähtekoodi kontrollid tuleb teostada ka käsitsi, sest testitavad süsteemid ei pruugi automaatsete vahenditega testimisel tõepäraseid tulemusi anda. Testimise lõppedes edastab täitja testitavate toodete/lahenduste testiraportid, krüpteerituna tellijale.
Turvatestimised viiakse läbi arendus- või testkeskkondades, kui ei ole kokku lepitud teisiti. Vajadusel luuakse tellija ja testija süsteemide vahele turvatud kanal süsteemidele ligipääsemiseks.

Testimise läbiviimiseks peab täitja esitama tellijale IP aadressid, millelt hakatakse turvateste läbi viima. Tellija avab ligipääsu vastavatelt IP aadressidelt testitavatele süsteemidele. Vajadusel teeb tellija ka vajalikud testkasutajad.
Lõppraport tuleb vormistada vastavalt OWASP ASVS/MASVS reeglitele.