Tekoäly tietoturvatestauksissa

18.12.2025

Kyberturvallisuuden uhat kehittyvät nopeasti ja muuttuvat koko ajan yhä monimutkaisemmiksi. Perinteiset menetelmät tietoturvatestauksessa eivät välttämättä ole riittäviä vastaamaan kaikkiin haasteisiin, joita tekoälyn nopea kehitys tuo mukanaan.

Tekoälyn kehityksen myötä avautuu uusia mahdollisuuksia muun muassa hyökkäysten uhkasimulointiin ja tietoturvakoulutuksen tehostamiseen. Lisäksi tekoäly voi nopeuttaa tietoturvatestauksia ja parantaa niiden laatua. Tekoälyä voidaan siis käyttää hyödyksi myös tietoturvatestauksien apuna.

Perinteinen tietoturvatestaus keskittyy järjestelmien haavoittuvuuksien tunnistamiseen, todentamiseen ja raportointiin, jotta ne voidaan korjata. Keskeisiä testausmenetelmiä ovat haavoittuvuusskannaus sekä penetraatiotestaus.

Haavoittuvuusskannaus ja penetraatiotestaus

Haavoittuvuusskannauksessa käytetään automatisoituja työkaluja tunnettujen haavoittuvuuksien löytämiseen. Skannauksen tuloksia voidaan käyttää riskien arviointiin ja tarvittavien korjaustoimien suunnitteluun sekä korjausten priorisointiin. Penetraatiotestauksessa puolestaan simuloidaan oikeita hyökkäyksiä järjestelmiin. Tämän avulla voidaan paljastaa esimerkiksi järjestelmien teknisiä heikkouksia, konfiguraatiovirheitä sekä loogisia haavoittuvuuksia.

Penetraatiotestauksessa hyödynnetään automaattisia työkaluja, joista saatujen tulosten perusteella testausta voidaan edelleen mukauttaa ja tulosten perusteella käyttää erinäisiä työkaluja haavoittuvuuksien löytämiseen ja todentamiseen. Tietoturvatestauksen tarkoituksena on tunnistaa ja arvioida järjestelmien, sovellusten ja verkkojen haavoittuvuuksia, jotta niiden turvallisuutta voidaan parantaa ja suojata niitä mahdollisilta

hyökkäyksiltä.

Tekoäly voi tuoda merkittäviä etuja tietoturvatestaukseen. Se voi myös mahdollistaa monipuolisemman ja tasaisemman laadun tietoturvatestauksissa. Mahdollisia käyttökohteita ovat esimerkiksi simuloitujen hyökkäysten automatisointi, erilaisten hyökkäysskenaarioiden luominen ja testauksien suorittamisen avustaminen esimerkiksi tehtävälistojen avulla. Tekoäly voi myös analysoida testauksen tuloksia ja tarjota suosituksia niin uusien testien tekemiseksi kuin järjestelmien parantamiseksi.

On kuitenkin tärkeää huomioida, että nykyiset tekoälyratkaisut eivät välttämättä vielä ole niin kehittyneitä, että niiden tuloksiin voitaisiin täysin luottaa.

Tekoälyn hyödyntäminen testauksessa

Tämän opinnäytetyön tavoitteena oli tutkia tekoälyn soveltuvuutta hyökkäävän tietoturvatestauksen tueksi ja kehittää tekoälyä hyödyntävä lisäosa tietoturvatestauksessa käytettävään Burp Suite -ohjelmistoon. Lisäosan tarkoituksena on tuottaa tekoälyn tekemän analyysin perusteella tehtävälistoja tietoturvatestaajan käyttöön ja ohjaukseen. Taustalla on tarve automatisoida tietoturvatestauksessa käytettävää tehtävälistan luontia, jotta testaus olisi nopeampaa ja järjestelmällisempää. Tekoälyavusteinen testaus voi merkittävästi parantaa testauksen kattavuutta, tehokkuutta ja laatua tunnistamalla mahdollisia haavoittuvuuksia automaattisesti.

Työssä kehitettiin Burp Suite -ohjelmiston lisäosa käyttäen Python-ohjelmointikieltä ja llama.cpp-ohjelmistoa kielimallin suorittamiseen. Kehitystyö noudatti kevyttä iteratiivista ohjelmistokehitysprosessia, jossa lisäosaa paranneltiin vaiheittain ja sen toimivuutta testattiin jatkuvasti. Tekoälymalli muodosti annetuista verkkosivujen HTTP pyyntö ja vastausparien perusteella tehtävälistoja, joiden soveltuvuutta todelliseen testaukseen arvioitiin käsin. Tulosten analysoinnissa vertailtiin tekoälyn tuottamia tehtävälistoja manuaalisesti tunnistettuihin haavoittuvuuksiin, ja tämän perusteella pystyttiin arvioimaan tekoälyn tarkkuutta ja hyödyllisyyttä tähän käyttötarkoitukseen.

Tulosten perusteella voidaan todeta, että tekoälyn luomat tehtävälistat sisältävät joitain soveltuvia testitapauksia haavoittuvuuksien löytämiseksi. Kuitenkin niiden kattavuus jäi melko alhaiseksi. Tekoäly tarjosi silti hyödyllisiä lähtökohtia testausprosessin suorittamiseen.

Jatkokehityksenä havaittiin tarve parantaa sekä tekoälymallia että mallille annetun syötteen (prompt) tarkkuutta parempien testauslistojen luomiseksi. Tekoälymallin parantaminen voisi tarkoittaa esimerkiksi paremman suuren kielimallin valintaa, koulutusdatan laajentamista ja mallin hienosäätöä niin, että se sopii paremmin tehtäväänsä. Syötteen tarkentamisella tarkoitetaan mallille annettavien ohjeiden selkeyttämistä, yksityiskohtien lisäämistä ja tehtävän rajauksen täsmentämistä, jotta malli tuottaa paremmin tarpeisiin sopivia tuloksia.

Opinnäytetyön tulokset osoittivat, että tekoälyn hyödyntäminen hyökkäävässä tietoturvatestauksessa on lupaavaa, mutta sen täyden potentiaalin saavuttaminen edellyttää edelleen jatkokehitystä.

Opinnäytetyö on ladattavissa Theseuksessa: https://urn.fi/URN:NBN:fi:amk-2024120432749**Jarkko Vesiluoma**

Insinööri (ylempi AMK), Teknologiaosaamisen johtaminen
Principal Offensive Security Lead
Elisa Oyj

Juha Yli-Hemminki
FM, lehtori
Seinäjoen ammattikorkeakoulu

Kirjoittaja toimi Vesiluoman opinnäytetyön ohjaajana