


IA na sugestão de correção de vulnerabilidades de código © 2024 by Felipe Gabriel Moreira de Lima, Ricardo di Ricco Pinheiro, Mário Cordeiro Junior is licensed under [CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/)  CC BY-NC 4.0

Membros da equipe:

RA	Nome	Curso de cada membro (SISTEL, Eng. Mecatrônica, etc.)
2302020	Felipe Gabriel Moreira de Lima	SISTEL
2086913	Mário Cordeiro Junior	Sistemas de informação
2470420	Ricardo di Ricco Pinheiro	SISTEL

Título do projeto:

IA na sugestão de correção de vulnerabilidades de código

Descrição resumida do projeto (breve contexto, descrição do problema que se deseja resolver, objetivos, metodologia, resultados e conclusão – máximo 500 palavras)

No ano de 2020, a programação se popularizou devido ao aumento do trabalho remoto causado pela pandemia de COVID-19 e à crescente demanda por profissionais qualificados na área de desenvolvimento. Esse crescimento gerou uma nova preocupação: manter os códigos em locais públicos, como o GitHub, seguros e íntegros. Esses repositórios são populares, mas essa popularidade também atrai pessoas mal-intencionadas que disponibilizam códigos maliciosos e confusos, visando enganar novos programadores que ainda não sabem como identificar tais ameaças.

A inserção de código malicioso em repositórios públicos representa uma ameaça significativa à segurança dos projetos de software. Programadores inexperientes, ao reutilizarem códigos disponíveis na web sem uma devida análise, podem inadvertidamente incorporar vulnerabilidades em seus projetos, comprometendo a integridade e a segurança de seus sistemas. Diante desse desafio, nosso projeto de extensão surge como uma iniciativa educacional e preventiva voltada para novos programadores.

O principal objetivo do projeto é instruir novos programadores na análise de códigos disponíveis em plataformas como o GitHub, ajudando-os a identificar e evitar códigos maliciosos. O projeto é multidisciplinar, integrando conceitos de programação, segurança da informação e inteligência artificial (IA).

A metodologia inclui o desenvolvimento de um sistema baseado em IA que fornecerá informações relevantes sobre os códigos pesquisados, identificando a linguagem utilizada e oferecendo dicas de melhorias, além de alertar sobre bibliotecas e práticas recomendadas. Esse sistema também será capaz de detectar vulnerabilidades e códigos maliciosos, fornecendo feedback claro e objetivo aos usuários.

Os principais resultados esperados incluem a capacitação de novos programadores na identificação e mitigação de vulnerabilidades em códigos, o fortalecimento da segurança cibernética através da implementação de práticas seguras em projetos de software, e a promoção de uma cultura de segurança e responsabilidade entre desenvolvedores de software.

Pretendemos ajudar profissionais e estudantes iniciantes na área, promovendo a segurança e a integridade de seus projetos. A iniciativa não se limita a fornecer conhecimento técnico, mas também a fomentar uma cultura de segurança. Integrando programação, segurança da informação e inteligência artificial, estamos preparados para enfrentar os desafios emergentes e garantir um ambiente digital mais seguro e colaborativo para todos.

Resumo de cada reunião da equipe (incluir uma linha para cada dia que a equipe se reunir)

Reunião 1 (25/04/2024)

Atualização do tema, objetivo no interpretador do prompt

Reunião 2 (02/05/2024)

Análise e busca por códigos com má índole

Imagem de uma reunião da equipe (25/04/2024)



Imagem do dia apresentação do projeto em sala de aula

- Exemplos e script disponível no documento da apresentação.