DESTAQUES – ELIXIR

Matheus Moreira Sorrentino
Pontifícia Universidade Católica de Minas Gerais - PUC Minas

Primeiramente, destaca-se a importância da metodologia utilizada, tendo em vista que a utilização da própria ferramenta de busca e classificação do Github para selecionar os repositórios referentes à linguagem que o trabalho de pesquisa foi direcionado (Elixir) foi uma estratégia muito eficiente, já que selecionará os repositórios mais populares da plataforma, ou seja, os que são mais relevantes e utilizados pelos usuários. Apesar dos autores terem restringido a pesquisa apenas a 25 repositórios, foi possível realizar análises importantes.

Ademais, a utilização do processo de codificação fechada foi outra estratégia muito eficiente empregada pelos autores, no qual dois avaliadores determinam, individualmente, se cada um dos commits coletados são relacionados à segurança, fazendo uso de palavras-chave para seletar ainda mais os repositórios, buscando, nesse momento, aproximar-se ainda mais da questão da pesquisa, que se refere à vulnerabilidade e segurança.

Entretanto, somente com essas duas estratégias, haveria a chance de obter-se dados falso positivos, ou seja, que se enquadram em todas as validações anteriores, porém, não tratam problemas de vulnerabilidade no código ou não são relacionados à segurança. Este problema foi solucionado utilizando duas etapas, na primeira, o avaliador determina que um commit está relacionado à segurança se a mensagem do commit indicar que uma ação foi tomada para resolver um problema de segurança para o software correspondente. O avaliador determina que uma mensagem de commit estará relacionada a uma vulnerabilidade se algum dos seguintes pilares de segurança for violado: confidencialidade, integridade ou disponibilidade. E na última etapa, é utilizado o Kappa de Cohen para calcular a concordância entre os avaliadores, afim de eliminar possíveis conflitos de avaliação de commit.

REFERÊNCIAS

BOSE, Dibyendu Brinto; COTTRELL, Kaitlyn; RAHMAN, Akond. **Vision for a secure Elixir ecosystem: an empirical study of vulnerabilities in Elixir programs**. Proceedings of the 2022 ACM Southeast Conference (ACM SE '22). Nova Iorque, NY, EUA: Association for Computing Machinery, v. 2, p. 215-218, abr. 2022.