mobb

AI and Security:

A hybrid approach

Fixing Security Issues: A task that requires precision

Fixing security issues is challenging and requires a deep understanding of not only the language and framework, but also the context in which the code is operating. It involves both technical comprehension and precise knowledge of how to make adjustments.

Vulnerability Remediation: AI's role in fixing code

AI should be given surgical and precise tasks. It's best to use AI when there is significant variance which requires many laborious hours.

GenAI is trained for addressing specific textual tasks right out of the box. While humans can achieve similar results, implementing algorithms to handle the multiple variances may take weeks or even months, compared to minutes.

What is Hybrid-AI?

Unlike competitive auto-remediation GenAI approaches, which have been shown to be unreliable and often produce erroneous and hallucinative results, Mobb's technology does not solely rely on AI. Mobb combines proprietary research and traditional semantic analysis with GenAI capabilities. This unique hybrid approach blends the rapid scalability of AI with the reliability and accuracy of deterministic algorithms. The result is code fixes that are precise, trustworthy, and free from code ownership concerns, thereby ensuring developer confidence.

What led us to using a Hybrid-AI approach?

We've tested numerous combinations to determine the optimal approach for combining LLMs. We've adapted the RAG framework to better suit our needs based on security best practices, research and testing.

What is the RAG framework?

RAG stands for Retrieval-Augmented Generation. It's a methodology that enhances the capabilities of generative models by combining them with a retrieval component. This approach allows the model to dynamically fetch and utilize external knowledge or data during the generation process.

RAG models effectively bridge the gap between the depth and specificity of retrieved information and the fluency and generativity of language models. This hybrid approach leverages the strengths of both retrieval-based and generative AI systems, enabling more accurate, informative, and context-aware outputs in a wide range of applications, from chatbots to research assistants.

How does Hybrid-AI address the following:

How does Hybrid-AI avoid hallucinations?

The Hybrid Fix represents a distinctly different approach that reduces the chance of generating hallucinations.

Instead of asking GenAI to write the entire fix, we leverage it to address specific surgical changes to the code.

We equip the model with RAG context, derived from our expertise as security experts and validated use cases. This assists Hybrid-AI in understanding precisely where and how to apply fixes.

How does Mobb determine confidence in our fixes?

During our research, every new fix is rigorously tested on a variety of samples to ensure its accuracy before it is made available to the public.

The generated code is tested to ensure it is both syntactically and semantically correct while validating that it fixes the reported findings. If additional steps are needed, those are highlighted to the user.

Leveraging AI Strengths

We use AI where it excels. Our focus is on the areas of string manipulation and understanding the location of functions and classes.

How does Mobb train their AI models?

We don't need to train the AI explicitly because the mentioned surgical tasks addressed by AI are general knowledge for the specific LLM we use. Meaning we will never need to use customers' data to train our LLM.

Our AI is trained in manipulating code, not fixing vulnerabilities.

How Do You Ensure These Fixes Work?

Our fixes are built on industry best practices, we source fixes from OWASP and other sources including language and frameworks documentation and as mentioned above, the accuracy of each new fix is rigorously tested before getting pushed to production.

How do we protect customers' IP and privacy?

Customer IP is not utilized for training data, and we do not retain customer IP. The data is never shared with third-parties (not even in an obfuscated or anonymized form) nor does it leave our environment.

Is This Approach to AI Reliable?

Our solution is deterministic and predictive since we leverage AI only for surgical time consuming tasks. This ensures that not only the code change actually fixes the vulnerability, but that for every instance of a given vulnerability, the users can expect to see the same fix generated, reducing the need to manually verify each fix.

Storing Customers' Code

We do not store customers' code in our database. We only cache the code for a short period of two weeks which allows your developers to interact with the fixes.

About Mobb

Mobb is the trusted, automatic vulnerability fixer that secures applications using deterministic algorithms and advanced AI to rectify coding flaws. This automated approach significantly reduces security backlogs and frees developers to focus on innovation and meeting business goals.