

Debuggers are quintessential in software development, but they also play a pivotal role in cybersecurity. How do cybersecurity professionals utilize debuggers in their investigations, especially when dealing with advanced threats?

**Answer:** Cybersecurity professionals utilize debuggers to navigate through code, inspect memory, and trace the execution of programs. This functionality enables them to pinpoint vulnerabilities, comprehend the workings of malware, and uncover potential flaws in software systems. Debuggers play a crucial role in scrutinizing suspicious code, providing experts with valuable insights into the mechanisms of malicious programs.

Immunity Debugger is often brought up in the context of vulnerability research and malware analysis. What differentiates Immunity Debugger from other debugging tools, and how does it facilitate this kind of in-depth software inspection?

**Answer:** Immunity Debugger provides a user-friendly interface, making it accessible for security experts with varying levels of expertise. Its support for scripting is another notable feature, enabling users to automate repetitive tasks and customize their analysis processes. This scripting capability enhances efficiency in conducting in-depth software inspections.