If you build modern web applications using popular frameworks like **Next.js** or content management systems such as **WordPress**, you've probably heard about security headers like X-Frame-Options. But what exactly does the SAMEORIGIN directive mean? More importantly, how does understanding and implementing it protect your users and your site's reputation? In this article, we'll break down X-Frame-Options SAMEORIGIN in clear terms, explain why it's a critical aspect of **clickjacking protection**, and explore how securing your app integrates seamlessly into advanced workflows like multi-model AI orchestration and red teaming.

Table of Contents

What is X-Frame-Options and SAMEORIGIN?

X-Frame-Options is a **HTTP security header** designed to control whether a browser should allow a webpage to be embedded inside an