Given the diverse capabilities of tools like ZAP, Burp Suite, and Nikto, can you delineate the distinct scenarios or types of web applications where you would opt for one platform over the others?

Answer: Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP). ZAP is designed specifically for testing web applications and is both flexible and extensible. Burp Suite is an integrated platform and graphical tool for performing security testing of web applications, it supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Nikto is an Open-Source software written in Perl language that is used to scan a webserver for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers. It can also fingerprint servers using favicon.ico files present in the server. It is not designed to be a particularly stealth tool rather than it is designed to be fast and time-efficient to achieve the task in very little time. Because of this, a web admin can easily detect that its server is being scanned by looking into the log files. It can also show some items that do not have a security problem but are info only which shows how to take full use of it to secure the webserver more properly.