Dengan *stress testing* diharapkan dapat memenuhi informasi mengenai kebutuhan jumlah pengguna ideal yang dapat mengakses perangkat lunak secara bersamaan, pengujian ini mencakup pengukuran terhadap kecepatan perangkat lunak mengakses permintaan pengguna, skala maksimum pengguna yang dapat mengakses secara bersamaan, stabilitas perangkat lunak dibawah tekanan berbagai permintaan pengguna. Kinerja perangkat lunak yang buruk, cenderung akan mendapatkan reputasi buruk dan gagal memenuhi kepuasan pengguna.

Tujuan dilakukannya pengujian dengan metode security testing diharapkan dapat menemukan celah atau kelemahan sistem dari sisi keamanannya agar nantinya tidak akan terjadi pelanggaran privasi bagi pengguna dan kebocoran data-data sensitif yang terdapat di dalam sistem, sehingga akan berakibat pada pencorengan reputasi *owner* dari aplikasi.

Begitu juga dengan *UI testing* diharapkan interaksi antar halaman telah berjalan susuai dengan fungsinya, misalnya seperti adanya tombol-tombol fungsinya telah sesuai jika difungsikan akan menuju pada halaman yang dimaksudkan,

Pengujian kinerja maupun pengujian keamanan diharapkan dapat dilakukan oleh setiap pengembang perangkat lunak, agar perangkat lunak dapat digunakan dengan nyaman oleh pengguna, karena beberapa hambatan bisa muncul bukan hanya dari perangkat lunak, tetapi dari perangkat keras yang digunakan, baik dari sisi pengguna atau penyedia perangkat lunak. Maka dari itu, pengujian kinerja maupun pengujian keamanan sangat penting dilakukan terhadap suatu perangkat lunak.

Perangkat lunak yang dapat digunakan untuk pengujian fungsional ini yang akan dipakai seperti *JMeter* untuk menguji *perfomance testing* dan *OWASP ZAP* untuk menguji *security testing* yang dapat digunakan di berbagai platform. Keduanya bersifat *open source* dan merupakan perangkat lunak yang sangat populer untuk melakukan pengujian fungsionalitas suatu aplikasi.