We created an extension to Burp Suite that simplifies settings necessary for the security testing itself. It also brings new functionalities to Burp Suite that are lacked by its users. The extension allows users to handle authentication, authorization, and session tokens within cookies, URL addresses, headers, GET and POST parameters, JSON message bodies, XML message bodies and it is also possible to use regular expressions. This functionality is similar to match and replace but is much more complex and can be used with scanning, fuzzing, etc.

The extension automatically creates new sessions using macros and detects expired sessions. The extension can handle several sessions at the same time. Its general design enables much more than only the tasks described above – besides handling the mentioned tokens, it can be also used for handling anti-CSRF tokens, automatic URL address modification, etc.

* Based on requests for enhancements published on the official web site [https://support.portswigger.net/](https://support.portswigger.net/).