Authentication, Authorization, and Session Management in the HTTP Protocol

Klára Drhová | Supervisor: RNDr. Daniel Joščák, Ph.D.
Czech Technical University in Prague, Faculty of Information Technology

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

MOTIVATION

- **Internet** is a part of our lives and the **HTTP protocol** is one of the most common application protocols used in the Internet
- **Security** is a common topic in most companies
- Users and costumers are interested in what is happening with their data
- Consequences of a **cyber attack** on a vulnerable application may be serious and may lead to a damage to reputation
- It is thus important **to test web applications** regularly but also efficiently

BURP SUITE

- One of the **most popular web application testing tools used by security experts worldwide**
- It works with requests and responses (HTTP messages) between a browser/application and servers
- It offers an automated scanning tool, easy extensibility, and a number of options
- It automatically stores cookies and updates their values in requests
- It offers *macros* – sequences of one or more requests that are defined by a user and can be used for example for automatic login into the application
- *Match and Replace* feature can be used to automatically replace parts of requests and responses

- Burp Suite has several **drawbacks**
  - It is possible to maintain only one session (one set of cookies) at the same time
  - The *match and replace* functionality only works for messages going from browser to server and back – it is not possible to use it with automatic scanning or fuzzing requests

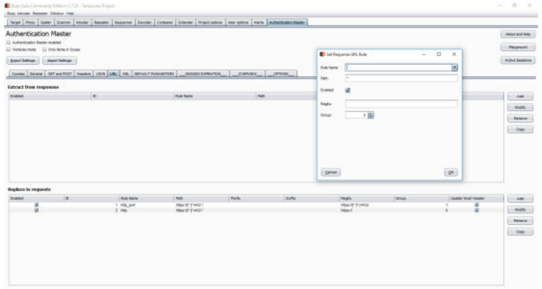
SOLUTION

- 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

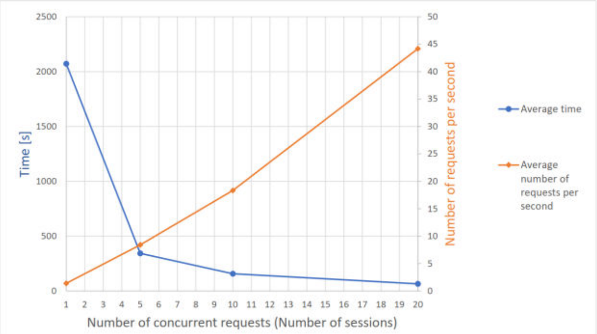
- Its general design enables much more than only the tasks described above – besides handling the mentioned tokens, it can be also used for handling **anti-CSRF tokens**, automatic **URL address modification**, etc.



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

RESULTS & CONCLUSION

- For some applications the testing can be **accelerated linearly** in the number of threads



- Great emphasis was placed on ease of use – **graphical user interface** with many components is used
- Most common **authentication schemes** are supported: Form-based, Basic, and Bearer authentication methods
- Settings of the extension can be exported to XML format and shared between testers
- We are not aware of any other available extension with such capabilities

FUTURE WORK

- We would like to **publish the source code** on the GitHub page and include the extension in the official Burp Suite store with extensions
- We would like to add support for **dynamic computation of tokens**
- Other additional features are also planned