Automatic Classification of Parameters and Cookies

Ali Reza Farid Amin¹, Gregor v. Bochmann¹, Guy-Vincent Jourdan¹, Iosif Viorel Onut²

¹ School of Information Technology and Engineering - University of Ottawa
² Security AppScan® Enterprise, IBM

Introduction

In an internet application, a set of parameters and cookies are exchanged between the client and the server. We classify these parameters and cookies into five different categories:

- **Session Identifiers**
- **Session Tokens**
- **User Identifiers**
- **User Settings**
- **Others**

The task of creating this classification manually is tedious and time consuming. We aim at automating this classification in order to create configuration files for security scanning systems such as IBM AppScan Enterprise.

Automatic detection of the user's authentication point can help identifying the types of parameters and cookies, since a number of parameters are only sent to the server after the user gets authenticated.

Motivation and Aim

**Motivation:**

- Classifying the types of parameters and cookies requires expert knowledge, and it is tedious to achieve manually.

**Goals:**

- Categorize the extracted parameters and cookies from users’ traces into Session identifiers, Session tokens, User identifiers, User Settings, and other types of parameters.
- Capture information on the users authentication point, and different parameters’ values and their behaviours.

Background

Server-side web applications generate unique session ids which are sent to the client through the cookies. This data is sent with every request from the client to the server. The server implements an associative array with its key as the session id and its value as some data of the client [1, 2].

The captured traffic of SSO-authentication-based websites were used to study browser relay messages to find OAuth authentication vulnerabilities. The requests communicated between ID provider and relay party were analyzed by labelling their request parameters syntactically and semantically [3, 4].

Methodology

The evaluation of classification has been done based on the website's configuration files. The green checkmark indicates the correct classification of parameter.

**Website Name:** ASE (IBM AppScan Enterprise)

**Session identifiers:**

- ASP.NET_SessionId
- JSESSIONIDSSO
- asc_access_token
- asc_session_id
- asc_access_token_secret

**User identifiers:**

- j_username

**Website Name:** RTC (Rational Team Concert)

**Session identifiers:**

- JSESSIONID
- JSESSIONID
- Etag

**User identifiers:**

- j_username

**Website settings:**

- X-com-ibm-team-foundation-auth-loop-avoidance,
- pageNum, JazzFormAuth, scope, hideAdmin hideGuest, proxyURL, hideArchivedUsers, net-jazz-ajax-cookie-rememberUserId, isLicenseSearch, hideUnassigned

Future Works

- Analysis of the first 50 popular websites which are ranked by 'Alexa.com'.
- Improve heuristics for detecting the type of parameters.
- Detection of additional authentication protocols for detecting the login point.

Acknowledgments

This work is supported in part by IBM and the Natural Science and Engineering Research Council of Canada.

DISCLAIMER

The views expressed in this poster are the sole responsibility of the authors and do not necessarily reflect those of the Center for Advanced Studies of IBM.