uOttawa

SOFTWARE SECURITY RESEARCH GROUP

In Collaboration With IBM

Automatic Classification of Parameters and Cookies

Ali Reza Farid Amin[1], Gregor v. Bochmann[1] , Guy-Vincent Jourdan[1], Iosif Viorel Onut[2]

[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.

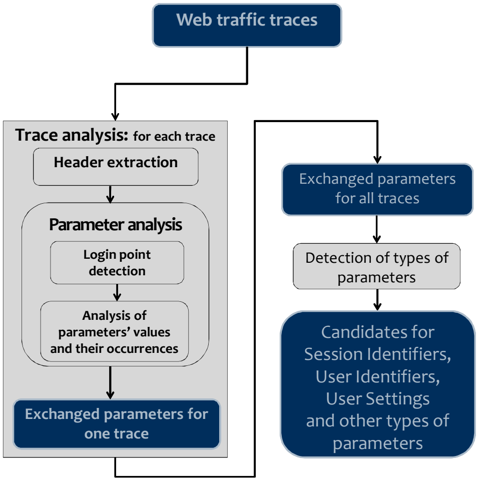
Background

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].

1. Ihm, Sunghwan, and Vivek S. Pai. "Towards understanding modern web traffic."*Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011.
2. Breton, Bergeron, et al.A Reference Framework for the Automated Exploration of Web Applications. 19th International Conference on Engineering of Complex Computer Systems(2014)
3. Wang, Rui, Shuo Chen, and XiaoFeng Wang. "Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services." *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012.
4. Bai, Guangdong, et al. "AUTHSCAN: Automatic Extraction of Web Authentication Protocols from Implementations." *NDSS*. 2013.

Methodology



Web traffic traces

Trace analysis: for each trace

Header extraction

Parameter analysis

Login point detection

Analysis of parameters' values and their occurrences

Exchanged parameters for one trace

Exchanged parameters for all traces

Detection of types of parameters

Candidates for Session Identifiers, User Identifiers, User Settings and other types of parameters

Functionality of Configuration Detection Tool

- ✓ **Detection of the login point:**

  To detect the login point and also to attempt detecting the type of OAUTH authentication, if any.

- ✓ **Analysis of parameter values and their occurrences:**

  The behaviour of parameters after login point in each trace is analyzed. Two important factors of this study are the number of times that a parameter value has changed and the number of appearances of a parameter with the same value during consecutive requests.

- ✓ **Detection of type of parameters:**

  To identify the types of the parameters by comparing traces.

  - ✓ ***Session Identifiers:***

    Complex values that are set at some point in the trace and do not change afterwards, and have different values in all traces.

  - ✓ ***Session Tokens:***

    Values that are set at some point, remain constant over a period of time, and have different values in all traces.

  - ✓ ***User Identifiers:***

    Complex values that are set at some point and do not change afterwards, and have different values for different users but same values for the same user.

  - ✓ ***User Settings:***

    Values that are set once the user is identified and do not change afterwards. Can be the same across traces.

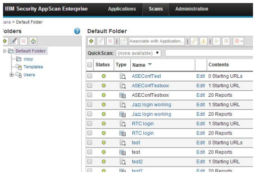
Experiments

Below is the result of the classification experiment on two websites. 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



cans > Default Folder

olders

Default Folder

copy

Templates

Users

Default Folder

Associate with Application...

QuickScan: (none available)

Status	Type	Name		Contents
●		ASEConfTest	Edit	0 Starting URLs
●		ASEConfTestxxx	Edit	1 Starting URL
●		ASEConfTestxxx	Edit	20 Reports
●		Jazz login working	Edit	1 Starting URL
●		Jazz login working	Edit	20 Reports
●		RTC login	Edit	1 Starting URL
●		RTC login	Edit	20 Reports
●		test	Edit	0 Starting URLs
●		test	Edit	20 Reports
●		test2	Edit	1 Starting URL
●		test2	Edit	20 Reports

User identifiers:

j_username

User settings:

SliderX, SliderIsHidden, instance, featureKey, redirectPath, tempToken,net-jazz-ajax-cookie-rememberUserId, oauth_callback, JazzFormAuth, include _proxyURL, locale, exception_occurred, exception_details, t, SliderX, SliderIsHidden

Website Name: RTC (Rational Team Concert)

Session identifiers:

- ✓ JSESSIONIDSSO
- ✓ JSESSIONID
- ✗ Etag

The Jazz Team Server at ssrgworker02.site.uottawa.ca in Jazz requires a user ID and password:

User ID: ADMIN

Password: •••••

□ Remember my User ID

Log In

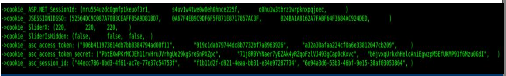
Licensed Material - Property of IBM Corp. © Copyright IBM Corp. and its licensors 2008, 2013. All Rights Reserved. IBM, the IBM logo, Jazz, and Rational are trademarks of IBM Corporation, in the United States, other countries and regions, or both. Built on Eclipse is a trademark of Eclipse Foundation, Inc. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates in the United States, other countries and regions, or both.

User identifiers:

j_username

User settings:

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



```
->cookie_ ASP.NET_SessionId: (mru554uzdc0gmfp1keuof3r1,       s4uv1w4twe0w0eh0hnce225f,      o0hu1w3tbrz1wrpknxpqjoec,      )
->cookie_ JSESSIONIDSSO: (52564DC9C087A70B3CEAFF85A9D81BD7,    0A67F4EB9C9DF6F5FB71E8717857AC3F,      B24BA1A8162A7FABF64F3684AC924DED,      )
->cookie_ SliderX: (220,      220,    220,    )
->cookie_ SliderIsHidden: (false,      false,  false,  )
->cookie_ asc_access_token: ("906b411973614db7bb8384794ad08f11",      "919c1dab79744dc8b7732bf7a8963926",     "a32a30afaa224cf0a6e33812047cb209",     )
->cookie_ asc_access_token_secret: ("PbtBXwPKrMCJEh11rvHruJVrhgUe29kgSreSnPXZpc",      "71j8R9YYNaer7yEZAk4yRZqoFzlVJ493gCap0cKxvc",   "bHjvxqUrkxhHelcAniEgwzpM5EfUKMP91f6Mzu0GdI",   )
->cookie_ asc_session_id: ("44ecc786-0bd3-4f61-ac7e-77e37c54753f",    "f1b11d2f-d921-4eaa-bb31-e34e97287734", "6e94a3d6-53b3-46bf-9e15-38af03053864", )
```

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.