ACMate-Lite

Installation and Quick User Guide

SVV - 6 March 2016

Introduction

ACMate is a framework for testing and reverse-engineering access control (AC) policies. It is developed by the SVV Laboratory, SnT, University of Luxembourg.

Here we present ACMate-Lite - the reduced version of ACMate tool, with the basic functions for access control testing.

ACMate-Lite is a Java-based extension module for Burp Suite (https://portswigger.net/burp/) that can be loaded and run seamlessly with Burp Suite proxy and spider. ACMate-Lite provides hand-on testing functions to support the Web application developers to test the access control implemented in their web-based products.

ACMate-Lite contains the following key components:

- Mining input specification from logs
- Smartly generating AC requests using pairwise combination strategy
- Executing AC tests, taking into account contextual parameters

This document will walk you through the installation of the ACMate-Lite and show you how to quickly use with the help of an example.

Installation

Prerequisites

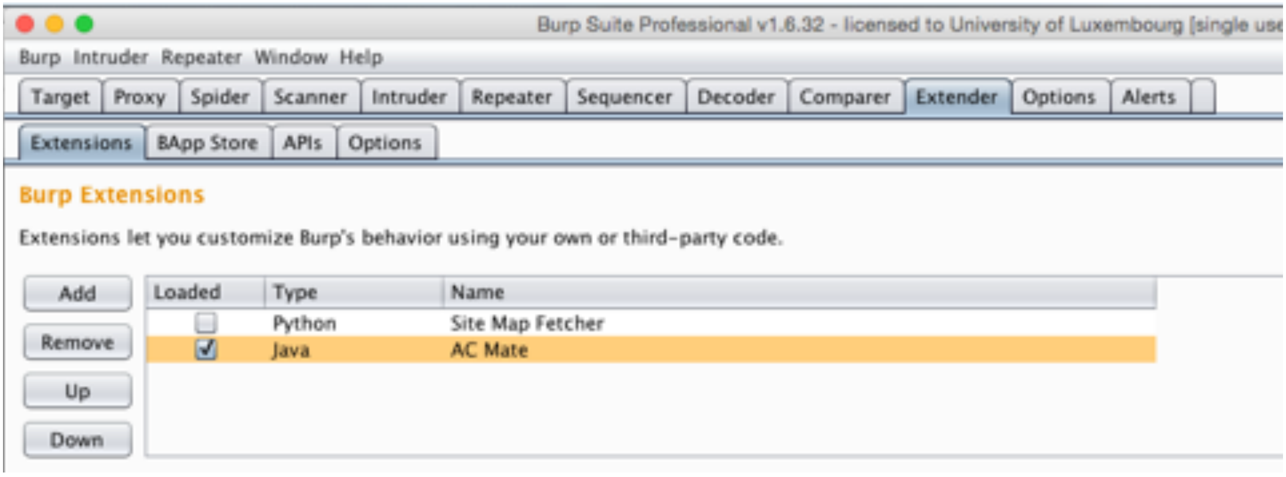
- Java (version 6 or later)
- BurpSuite Professional, version 1.6 or later, it is a security tool suite available here https://portswigger.net/burp/download.html

We use in this guide BurpSuite Professional version 1.6.30.

If this is the first time you use BurpSuite, it is recommended that you follow its user guide, especially these key features: Proxy, Target, and Spider.

Loading ACMate-Lite

- Download ACMate-Lite from http://people.svv.lu/nguyen/public/ACMate-Lite-dir.zip
- Unpack the package to a directory — we call this dir acmate-dir from now on
- Launch BurpSuite
- Select Extender tab, Click Add to open Burp Extension Loader
- Follow the dialog to Select Java Type and Select file acmate-dir/ACMate-Lite.jar .
- Click Open to load ACMate-Lite


Burp Suite Professional v1.6.32 - licensed to University of Luxembourg [single use
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Extensions BApp Store APIs Options
Add
Remove
Up
Down

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

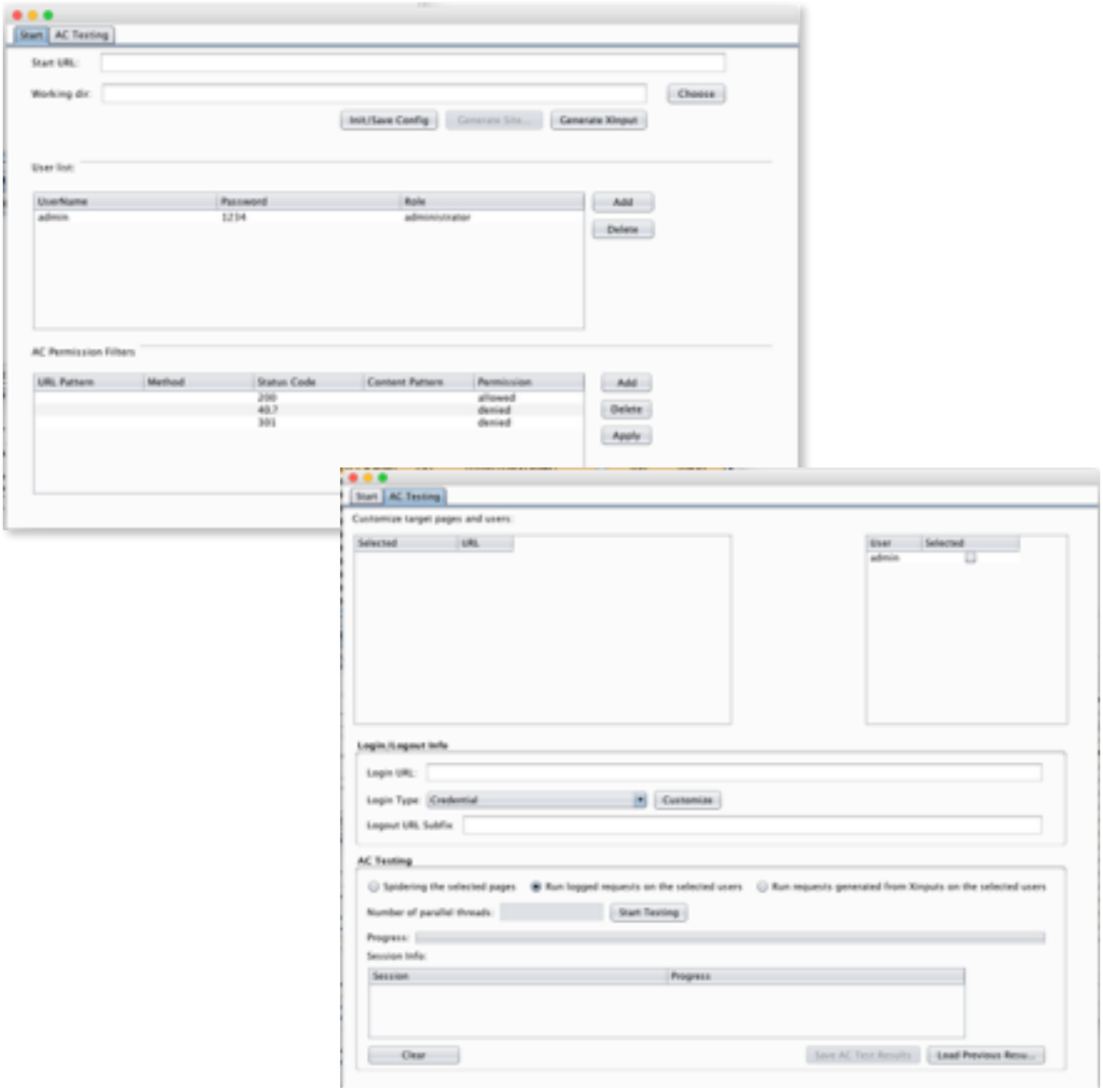
Loaded	Type	Name
□	Python	Site Map Fetcher
☑	Java	AC Mate

If there is no error and the ACMate-Lite is successfully loaded, you can close Load Burp Extension window and start using ACMate-Lite.

ACMate-Lite GUIs

Current version of ACMate-Lite has two panels:

1. **Start**, where users, permission filters, and working directory can be configured
2. **AC Testing**, to run AC tests



UserName	Password	Role
admin	1234	administrator

URL Pattern	Method	Status Code	Content Pattern	Permission
		200		allowed
		403		denied
		301		denied

Selected	URL

User	Selected
admin	□

Login Type: Credential

○ Spidering the selected pages ● Run logged requests on the selected users ○ Run requests generated from Xinputs on the selected users

Session	Progress

A Quick use of ACMate-Lite with Example

In this part, we assume that you know how to use Burp Suite proxy and spider to capture the interaction between the target application with its end users and explore the application. With that asumption, we prepare an example to help you get a hand-on experience with ACMate-Lite quickly. The example is stored in the subdirectory called **itrust** located at **acmate-dir/itrust**, in which we put:

- a BurpSuite state file containing some initial access logs of the sample target application (we use iTrust - can be downloaded at http://agile.csc.ncsu.edu/iTrust/wiki/doku.php)
- configuration files containing information of users and permission filters

We will show you step-by-step how to use ACMate-Lite to launch the AC testing on the example application, including:

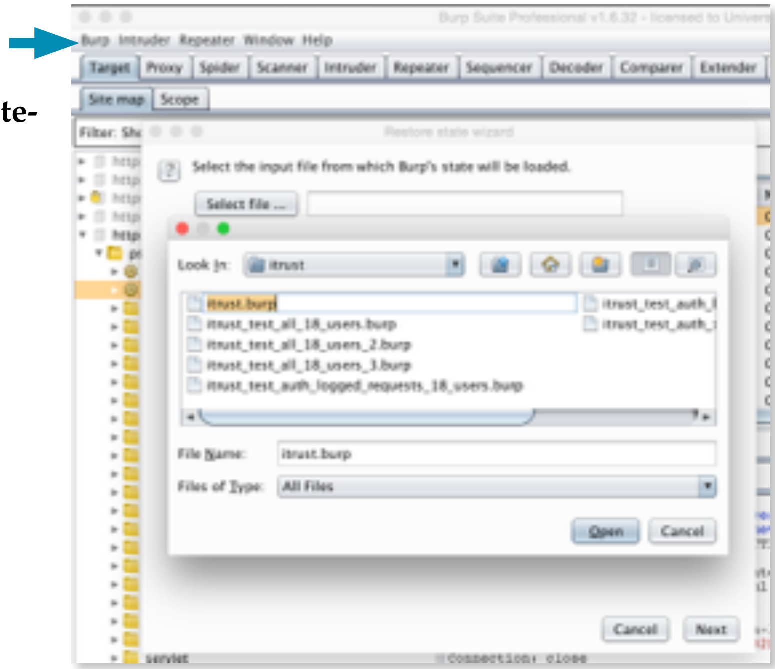
- Setting up the environment
- Launching tests
- Saving and inspecting test results

1. Setting Environment

In this step, we prepare for the AC testing. We will configure the testing environment, declare the users list, define the permission filter, and the xinput specification.

To load the captured state:

- Select menu Burp > Restore State
- Follow the dialog to open file **acmate-dir/itrust/iTrust-state**



Select the input file from which Burp's state will be loaded.

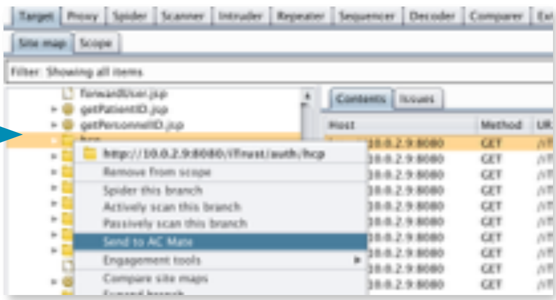
Look In: itrust

itrust.burp
itrust_test_all_18_users.burp
itrust_test_all_18_users_2.burp
itrust_test_all_18_users_3.burp
itrust_test_auth_logged_requests_18_users.burp
itrust_test_auth_
itrust_test_auth_

File Name: itrust.burp

Files of Type: All Files

Select the tab **Target** of Burp Suite, in the Site map view **Select a folder** (e.g., …) and choose “**Send to AC Mate**”

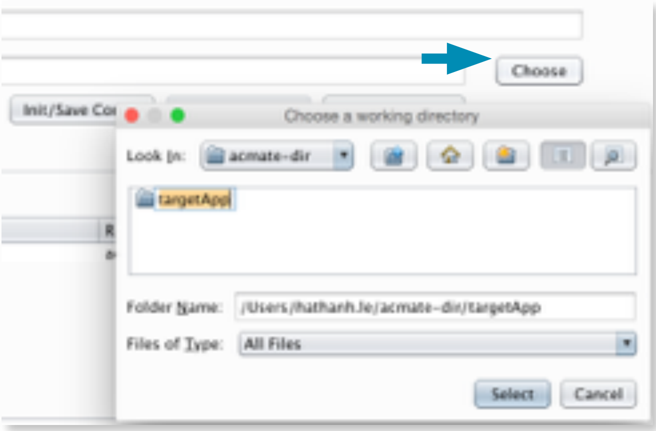


Switch to ACMate-Lite window. On the Start tab, you will see the link to the selected resource has been put into **Start URL**.

Step 1.1: Define a working directory and initialise the test configuration (tab Start)

Choose a working dir by “Choose” and then select the folder **acmate-dir/itrust**. You need to create a new folder (or use an existing one) to store all the files created during the test session.

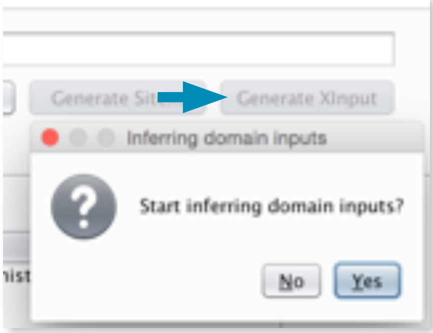
<u>Tip</u>: In Mac OS, you can choose the working folder by select a directory in Finder, drag and drop it into **Working dir:** text box.



Folder Name: /Users/hathanh.le/acmate-dir/targetApp

Click **Init/Save Config** to save the configuration and permission filters to the *config.xml* and *filters.xml* files accordingly in the working directory.

Click **Generate XInput** to scan the proxy log and generate the inputs specification, which is saved in the *xinput.xml* file in the working directory.

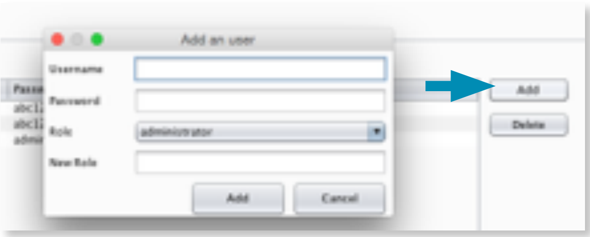


Start inferring domain inputs?

Step 1.2: Specify list of users credential used in the AC test

Here you will specify the list of authorised users' credential which are already created in the target application.

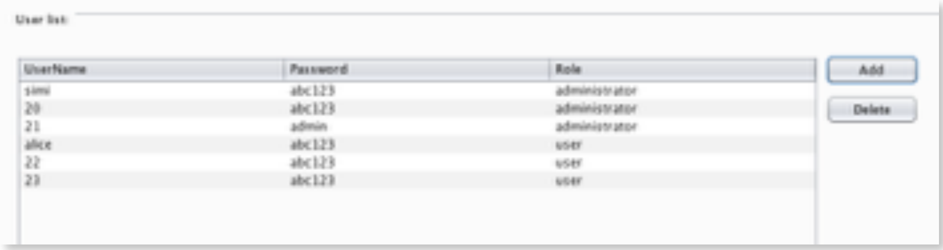
Click **Add** next to User list to open **Add an user** dialog box and enter user credential data includes username, password, user's role. The role can be selected from the exiting roles in the **Role** dropdown list. If the user role is not available in the roles list, type new role name into **New Role** text box and press **Enter** to confirm adding new role. The new role will be added into the role list. Finally, click **Add** to add user credential data into the current users list.



Role: administrator

Double click on the row of a user to modify that user data.

To delete a user account, you can select the user's record (row) from User list, and press **Delete** a user from the list.



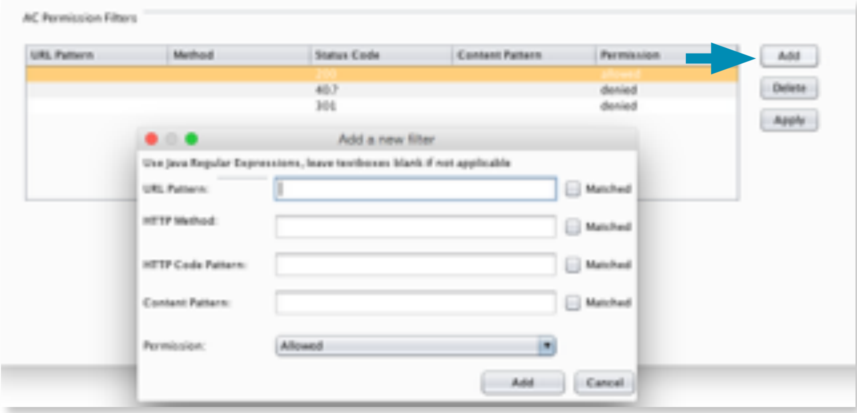
UserName	Password	Role
simi	abc123	administrator
20	abc123	administrator
21	admin	administrator
alice	abc123	user
22	abc123	user
23	abc123	user

Step 1.3: Define AC permission filters.xml

Now you define a set of filters that determine how the target application grants and denies permissions to the AC requests. By default, ACMate-Lite creates three common sense permission filters but you can always modify or delete them to fit your testing requirements.

Click button **Add** in AC Permission Filters area to add new permission filter.

The filter conditions are declared by the URL pattern, HTTP method, HTTP response code and response content. The ACMate-Lite will match the response with these filter conditions and conclude the permission (*allowed/ denided*) accordingly.



URL Pattern	Method	Status Code	Content Pattern	Permission
		200		allowed
		403		denied
		301		denied

Use Java Regular Expressions, leave textboxes blank if not applicable

URL Pattern: □ Matched

HTTP Method: □ Matched

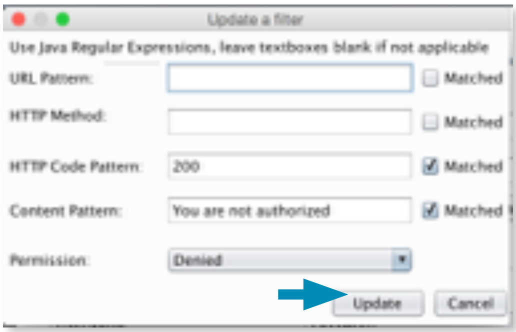
HTTP Code Pattern: □ Matched

Content Pattern: □ Matched

Permission: Allowed

Finally, click **Add** to save the new filter.

To modify a permission filter, double click the selected rule, change the filter conditions and press **Update**.



Update a filter

Use Java Regular Expressions, leave textboxes blank if not applicable

URL Pattern: ☐ Matched

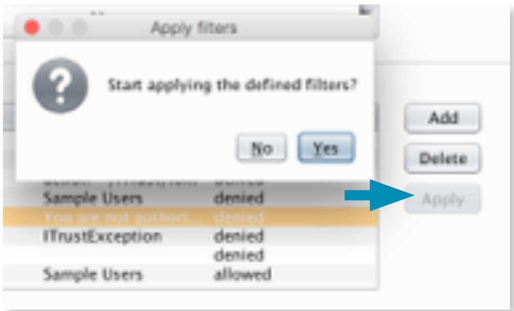
HTTP Method: ☐ Matched

HTTP Code Pattern: 200 ☑ Matched

Content Pattern: You are not authorized ☑ Matched

Permission: Denied

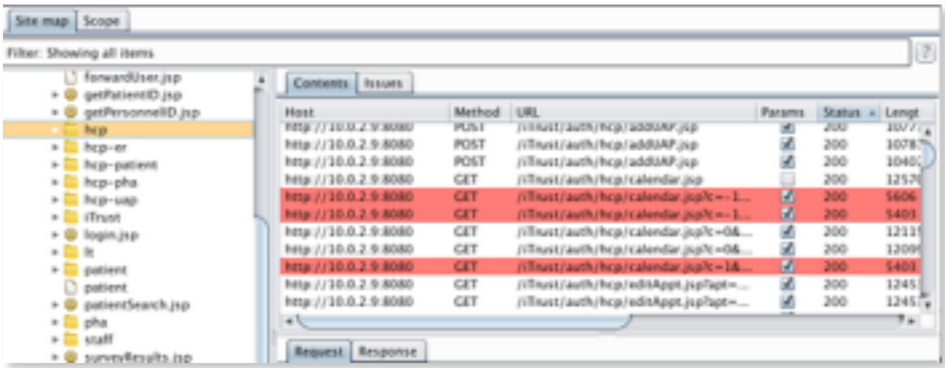
To preview the requests/responses if they match the defined AC permission filters, press **Apply**. In application site map, the request/response pair will be marked in Green if it matches an *"allowed"* filter rule, in Red for *"denied"* filter rule, and no color if it does not match any defined filter rules. Using this feature, you can quickly focus the classified requests/responses for further analysis (e.g., you may want to create new permission filter rules)



Apply filters

Start applying the defined filters?

Sample Users	denied
You are not authori...	denied
ITrustException	denied
	denied
Sample Users	allowed



Host	Method	URL	Params	Status	Lengt
http://10.0.2.9:8080	POST	/iTrust/auth/hcp/addUAP.jsp	☑	200	1077
http://10.0.2.9:8080	POST	/iTrust/auth/hcp/addUAP.jsp	☑	200	1078
http://10.0.2.9:8080	POST	/iTrust/auth/hcp/addUAP.jsp	☑	200	1040
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp	☐	200	1257
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp?c=-1...	☑	200	5606
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp?c=-1...	☑	200	5403
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp?c=0&...	☑	200	1211
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp?c=0&...	☑	200	1209
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/calendar.jsp?c=1&...	☑	200	5403
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/editAppt.jsp?apt=...	☑	200	1245
http://10.0.2.9:8080	GET	/iTrust/auth/hcp/editAppt.jsp?apt=...	☑	200	1245

IMPORTANT: Before going to next stage, you should save the users list and permission filters. Click **Init/Save Config** and press **Yes** to write the updated data into the *config.xml* and *filters.xml* file in the working directory.

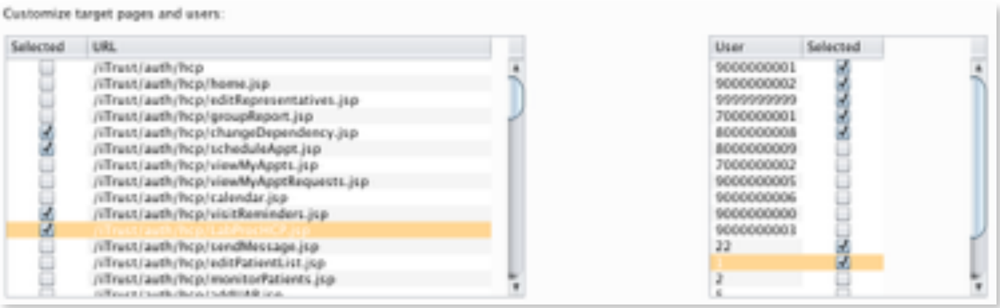
TIP: If you want to restore or reuse the settings in an old test, simply open the test's working directory in ACMate-Lite. ACMate-Lite will read and load the saved configuration, value domain Xinput, users list and defined permission filter rules for your new AC test project. It is recommended that you create a different working directory and save these settings for the new test. If you don’t provide new working directory, the files created in the new test will overwrite the existing files of the old test and you will loose the old test’s result.

2. Lauching Tests

In this stage, you will run the AC tests. Based on the settings in the previous stages, you select the target resources and set of users’ credential used in the test. You also need to define the Login/Logout schema for the target application. ACMate-Lite test engine will send test requests to the target application and analyse the received responses and determine access permission based on the defined filters.

Step 2.1: Select the target resources and set of users’ credential for AC test

You can select a subset of target resources (pages) and users’ credential for the AC test. ACMate-Lite test engine will only generate and send test requests to the selected target resources in the working session of selected users.



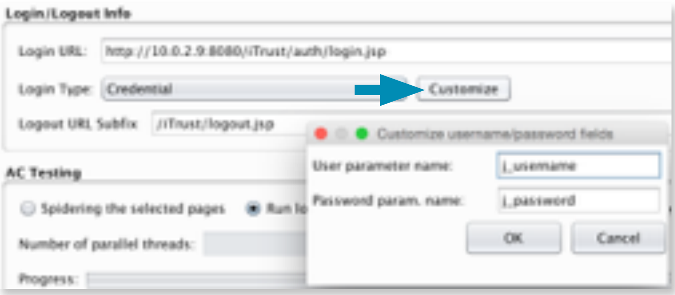
Customize target pages and users:

Selected	URL
□	/iTrust/auth/hcp
□	/iTrust/auth/hcp/home.jsp
□	/iTrust/auth/hcp/editRepresentatives.jsp
□	/iTrust/auth/hcp/groupReport.jsp
☑	/iTrust/auth/hcp/changeDependency.jsp
☑	/iTrust/auth/hcp/scheduleAppt.jsp
□	/iTrust/auth/hcp/viewMyAppts.jsp
□	/iTrust/auth/hcp/viewMyApptRequests.jsp
□	/iTrust/auth/hcp/calendar.jsp
☑	/iTrust/auth/hcp/visitReminders.jsp
☑	/iTrust/auth/hcp/LabProcHCP.jsp
□	/iTrust/auth/hcp/sendMessage.jsp
□	/iTrust/auth/hcp/editPatientList.jsp
□	/iTrust/auth/hcp/monitorPatients.jsp

User	Selected
9000000001	☑
9000000002	☑
9999999999	☑
7000000001	☑
8000000008	☑
8000000009	□
7000000002	□
9000000005	□
9000000006	□
9000000000	□
9000000003	□
22	☑
1	☑
2	□

Step 2.2: Specify the Login/Logout schema

In order to successfully log in the target application during the test, you must specify the *link* to the application’s login page, the *username input field* and *password input field*. In **Login Type**, select *Credential* and press button **Customize**. In the opened “Customize username/password fields” dialog, enter the user parameter name and password parameter name. For example, in the case of iTrust, you must enter *j_username* and *j_password* as shown in the picture.



Login/Logout Info

Login URL: http://10.0.2.9:8080/iTrust/auth/login.jsp

Login Type: Credential

Logout URL Subfix: /iTrust/logout.jsp

AC Testing

○ Spidering the selected pages ● Run lo

Number of parallel threads:

Progress:

Customize username/password fields

User parameter name: j_username

Password param. name: j_password

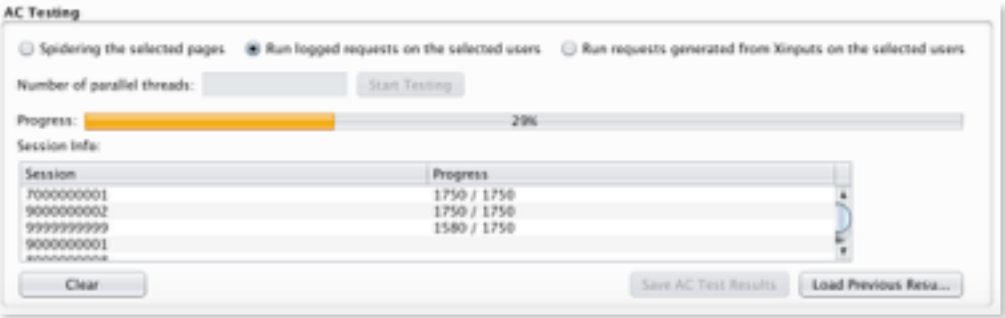
The logout procedure requires the logout URL. As the full URL to the application is already specified in the Login URL, you only need to enter the Logout URL Subfix.

Step 2.3: Run AC test

There are three AC testing modes:

- **Spidering the selected pages**: ACMate-Lite test engine calls Burp Suite spider to crawl the target application. The crawling starts from the selected pages onward.
- **Run with existing requests on all users**: ACMate-Lite test engine tests the requests previously captured to the selected target resources for the selected users.
- **Run with existing requests and Xinputs on all users**: ACMate-Lite generates the test requests using Xinputs combinatorial testing-based specification. Then the generated test requests are used to test the selected target resources for the selected users.

Once a testing mode is selected, click **Start Testing** to start the ACMate-Lite test engine. The progress bar shows how much work of the test has been done while the Session Info lists the current running session. ACMate-Lite also shows the number of threads running in parallel.



AC Testing

○ Spidering the selected pages ● Run logged requests on the selected users ○ Run requests generated from Xinputs on the selected users

Number of parallel threads:

Progress: 29%

Session Info:

Session	Progress
7000000001	1750 / 1750
9000000002	1750 / 1750
9999999999	1580 / 1750
9000000001	

3. Saving and Inspecting Test Results

Once testing sessions are finished, you can **Save AC Test Results** to export AC testing results to output XML file for inspection.

Test results are stored following this XML structure:

```
<Sessions>
  <Session>
    <ACTest>
      <Request>
      </Request>
      <AccessResponse permissionColor="green"> </AccessResponse>
    </ACTest>
  </Session>
  <Session>
  </Session>
</Sessions>
```

The colour is interpreted as follows:

- green: allowed

- red: denied
- orange: cannot classified based on the defined filters

ACMate-Lite Configurations

Please notice that ACMate-Lite has been pre-configured so that the AC tests are executed with following settings:

- Use BurpSuite callback HTTP only
- Follow server redirections
- No group requests to a web page based on their set of parameters
- Remove the ending forward slash from URL, this makes URL/folder/ equals URL/folder

You may need to consider these settings when running the AC tests for the target applications.

This is all you need for ACMate-Lite. You can get the extension at the link provided.

If you have questions or comments about the tool, please send a message to hathanh.le@uni.lu