Prerequisites

Burp Setup

1. Download Burp Community Edition (Link) if you don't have Burp. If you have professional edition - great
2. Install ATOR Plugin by going to Extensions -> BAppStore -> Authentication Token Obtain and Replace -> Click on Install
3. Also Install JWT Editor by going to Extensions -> BAppStore -> JWT Editor -> Click on Install

Proxy & Browser Setup

1. Open Burp
2. Go to Proxy -> Intercept -> Open Browser
3. You should see a chromium plugin open up

Demo Config using ATOR

Complex auth setup

Background

1. Go to Juiceshop (Link)
2. Create a user (Link)
3. Go back to Burp & Click on Proxy -> Intercept
4. Login to Juiceshop (Send the request to repeater). Right click and send to repeater
5. Purchase a juice by entering address, payment and checkout (Don't enter any valid data please)
6. Go to saved payment instruments (Link) & send the request to repeater

ATOR Setup

1. Go to repeater, you should have 2 requests (Login & saved payment instruments)
2. Remove one letter from the bearer token (notice that it is there on both the header and the cookie) on the saved payment instruments request
3. You should see a 401 in the response code.
4. Right click & send both requests to ATOR Plugin
5. Configure the error condition

Step by step process is show in the video.

Useful Links:

Hosted Juiceshop: Link
Burp community edition: Link
ATOR Configuration: Link Video

Demo using Akto

This demo is focused on the blackbox testing mode where we provide the api inventory to Akto. For ease of use, we have hosted Akto - you can self host on your laptop (docker container).

Setup of Akto

1. Setup account on Akto dashboard (Link)
2. Credentials are here: **username:** test_user@akto.io **password:** test1234 P@ssw0rd!
3. Create a collection:
   Observe -> API Inventory -> Create new collections (format: yourname-burp)
4. Download the Akto burp plugin (Link)
5. Unzip the Jar file
6. Open Burp -> Extensions -> Installed -> Add (Java JAR) and select the downloaded jar file
7. This will add a new tab called “akto” in the Burp toolbar (this means Akto plugin is successfully added).
8. Click on “Akto” and then click on “options”. Change the value of “export collection name” from “burp” to the name of the collection you created earlier. (i.e. yourname_burp)
9. Click on the Open Browser in Proxy tab and start browsing the website you want to analyze.
10. Akto will automatically send your Burp history to the collection you created in Akto Dashboard

Video for setup. (link)

Exercises to be done

1. Identify apis with sensitive parameters
   a. Click on the collection you just created
   b. There should be a checkbox for sensitive parameters
   c. This will give you all the apis with sensitive parameters (Note: Custom regexes can be added)

2. Run a test on a targeted api
    a. Go to the feedback form (Link)
    b. Add your feedback
    c. Check if the api is exported Burp -> Akto -> View Logs -> Check if API is present there (https://juiceshop.akto.io/api/Feedbacks/)
    d. Now go to the Akto Portal -> Observe -> API Inventory -> Click on your collection
    e. Search for the API -> Click on Endpoint -> Enter feedback in the search bar -> Check the feedback api
    f. Click on Run test on the top right
    g. Now click on Testing -> Your Collection Name
    h. This will tell you the vulnerabilities identified

    Repeat Exercise 2 with functionality below:
    - https://juiceshop.akto.io/#/search?q=egg
    - Provide product review by clicking on a product & writing a review