BurpSuite 101

Santiago

Disclaimer: This document is only for education purposes. Before assessing a web application, always ask for consent.

1 Setup

Practical examples in this documents can be done using the following setup:

- Ubuntu 20.04
- Burp Suite Community Edition[1]
- Docker[2]
- DVWA[3]

2 Introduction

BurpSuite is an application designed for web application security assessments.

BurpSuite is a framework because it includes multiple tools and because it allows users to create extensions. Among the tools that BurpSuite includes we can find:

- Proxy
- Repeater
- Decoder
- Comparer
- Sequencer
- Intruder
- Extender

2.1 BurpSuite Professional vs. Community Edition

BurpSuite Pro is a paid version of BurpSuite and includes multiple features:

- Saving projects
- Full Intruder
- Web scanner
- Search function
- Pro-exclusive extensions
- ...

However, BurpSuite Community Edition is enough to perform web security assessments. Also, some of the missing tools from the Pro version can be replaced with extensions and additional resources.

3 A little bit of Hypertext Transfer Protocol (HTTP)

HTTP[4] is a text-based protocol that generally runs on port TCP 80. Additionally HTTP is client-server based, meaning that clients send request to servers and servers send responses back to the client. Requests and responses are known as messages.

Requests are composed by:

- Request-Line: Method and resource. The most common methods are:
  - `GET`: obtains the resource from the server
  - `HEAD`: a GET method where the server does not return a body
  - `PUT`: uploads or update the resource at the server
  - `POST`: sends information to the server
  - `DELETE`: removes information from
- Message headers: different attributes that the message has. It includes:
- Message body: data sent to the

Responses are composed by:

- Status Code and Reason Phrase:
  - `200 OK`
  - `401 Unauthorized`

  - 404 Not Found
  - 500 Server Error

- Header Fields
- Body

For example, when a web browser (the client) wants to visualize a web page, it sends to a web sever a `GET` request whose header contains the location of the web page. The server, will send back a `200 OK` response to the client with body containing the web page that the browser then will render.

4 Using BurpSuite

4.1 Proxy

An HTTP proxy is an application that sits between the client and the server and might be able to see and modify HTTP messages.

In the case of BurpSuite Proxy is a tool that by default allows us to inspect and modify the content of HTTP requests before they are sent to the server.

Further, the proxy allows us to see the history of all the requests and its responses. Requests within the history view can be highlighted to facilitate their identification.

Finally, we can mention that modern browsers allow us to see the history of requests and responses; however, BurpSuite presents this information in a way that is more accessible for analysis.

4.1.1 Proxy Use Example

After starting DVWA[3] and starting BurpSuite with default settings, click on the tab called `Proxy`, then click on the button that says `Intercept is on` to turn interception, and then click on the button that says `Open Browser`.

An instance of chromium will open, type 127.0.0.1, fill the login form with `admin` as the username and `password` as the password. Finally, click on the `Login` button.

Go back to BurpSuite and under the `Proxy` tab, click on the `HTTP history` tab. Then, click on the different HTTP request, you will see the full requests and the responses from DVWA.

TIP: You can click on the request number to highlight the request with different colors.

4.2 Repeater

Repeater is a tool that allows us to:

- Re-send messages
- Modify and send messages
- Craft new messages and send them

Additionally, different requests can be named and organized in Repeater. Further modifications to request are being tracked by Repeater.

Just like with the Proxy, modern browsers present a similar functionality. But BurpSuite's Repeater enables the analyst to perform these activities in an easier way.

4.2.1 Repeater Use Example

While in DVWA, go to the tab `Command Injection`, then fill the field `Enter and IP address` with `127.0.0.1` and click the `Submit` button. You will see the output of a `ping` command.

Go back to the `Proxy` tab and select `HTTP History`. You will see a `POST` request for the Command Injection (`vulnerabilities/exec`), right-click on it and select `Send to Repeater`. The `Repeater` tab will change color.

Now go to the `Repeater` Tab, you will notice an item with a `Request` section filled and an empty `Response` section. If you click on the button `Send`, Burp will send that `POST` request to DVWA and we will get a response.

If you inspect the response, you will notice the output of the `ping` command as part of the body.

Now, go back to the `Request` section and, in the body of the request, change the field `ip` for `127.0.0.1; whoami`. After sending the new request, you will notice that the body of response includes the result of a `ping` command and the result of the command `whoami`.

4.3 Decoder

Decorder is a very simple tool that allows us to encode and decode data into different formats, including:

- Base64
- URL
- Hex
- Binary

- ...

Additionally, Decoder can produce hashes, for example:

- MD 2, MD4, and MD5
- SHA1, SHA2, and SHA3
- ...

4.4 Comparer

Comparer is a tool that allows to compare two different requests or two different responses. Comparer highlights what has been modified, deleted, or added.

4.4.1 Comparer Use Example

While in the `Repeater` tab, you can right-click on the `Response` section of the last message, then select `Send to Comparer`. The `Comparer` tab will change color. Then, you can click on the back arrow next to the `Cancel` button at the top left, and send the older response to Comparer.

Now, go to the `Comparer` tab. By default, Comparer selects two different items to compare. Click on the button that says `Word` at the bottom right.

If you click on the checkbox that says `Sync views`, you can scroll down and find that som data has been modified and deleted.

4.5 Sequencer

Sequencer is a tool that analyzes the entropy of data. This is done by sending a response that sets session tokens. Then, Sequence sends multiple requests and compare the randomness of the different responses.

4.5.1 Sequence Use Example

In DWVA, go to the tab `Weak Session IDs`, and click on the button `Generate`. If you go back to the `Proxy` tab in BurpSuite, you will see that the responses to clicking that button generates a cookie called `dwvaSession` that has a sequential integer.

Right-click on the `Response` section and select `Send to Sequencer`. The `Sequencer` tab will change color.

Check the configuration for sequencer and notice that in the seciton `Token Location Within Response`, the field `Cookie` is set to `dwvaSession=`. Then click on the button `Start live capture`.

After the live capture is done, click on the button `Analyze now`. You will see a an empty graph. This empty graph means that the cookie value has no entropy and it is predictable.

Now, go back to DVWA, click on the `Logout` button, clear the browser's stored cookies, and refresh the page. Go back to BurpSuite and, in the `Proxy` tab send the latest response to sequencer.

In the `Sequencer` tab, you will see that the new response is selected and the settings have been pre-populated. Click on `Start live capture`.

Once the capture is completed, click on the button`Analyze now` and see how the results are different than the previous ones.

4.6 Intruder

Intruder is a tool that allows us to send multiple modified requests. These modifications are based on rules set by the analyst.

Intruder has different types of attacks[5]:

- Sniper: one single set of payloads. In this attack each position take turn in using the payloads. This is used for fuzzing attacks.
- Bettering ram: one single set of payloads. In this attack all the positions iterate through the payload list at the same time. This is used when one payloads is needed in multiple places in the request.
- Pitchfork: multiple payload sets. In this attack each position has a payload list and Burp iterates through the payloads in parallel.
- Cluster bomb: multiple payload sets. In this attack each position has a different payload and Intruder iterates through all positions and through all the payloads. This attack can be use to guess username/password combinations.

BurpSuite Community Edition does not include the full version of Intruder, as it lacks payload lists and as it is throttled.

In order to overcome the lack of payload lists, we can use SecLists[6] or PayloadsAllTheThings[7].

4.6.1 Intruder Use Example

Go back to DWVA, login, and click on the tab `SQL Injection`. If you type a number `1` in the field `User ID` and click on the button Submitt, you will get the information of user 1. You can repeat the same for user 2, user 3, and so on. This is a slow way to enumerate all the users in the system.

Go back to the Proxy tab and select the last request. Right-click on it and select Send to Intruder. The Intruder tab will change color.

Click on the Intruder tab, select the tab Positions, and click on the button that says Clear §. Then, in the request-line, select the integer number next to the parameter id, and finally click on the button that says Add §.

Move to the tab that says Payloads. Change the Payload type to Numbers. Then, in Payload Options [Numbers], set the following options:

- Type: sequential
- From: 0
- To: 20
- Step: 1

Finally, click on the button Start Attack at the top right of the screen.

After the attack is completed, sort the results by length and start analyzing the results. You will notice that the results that are 4770 Bytes correspond to IDs that do not exist.

4.7 Extender

Extender is a tool that allows to install external extensions to Burp. Some of these extensions are used to handle information, such as analyzing JSON Web Tokens (JWT); or to add specific attacks to BurpSuite, such as JSON Web Token Attacker.

Some of the extensions are only available to BurpSuite Professional.

Users can develop extensions for BurpSuite in Java and Python.

Before using an extension developed in Python, Jython[8] must be downloaded in the system running BurpSuite and then enabled in BurpSuite. Jython is a Java implementation of Python.

References

[1] https://portswigger.net/burp/documentation/desktop/getting-started/installing-burp

[2] https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04

[3] https://github.com/digininja/DVWA#docker-container

[4] https://datatracker.ietf.org/doc/html/rfc2616

[5] https://portswigger.net/burp/documentation/desktop/tools/intruder/positions

[6] https://github.com/danielmiessler/SecLists

[7] https://github.com/swisskyrepo/PayloadsAllTheThings

[8] https://www.jython.org/