Incident Report 12959: Intro: Burp Suite

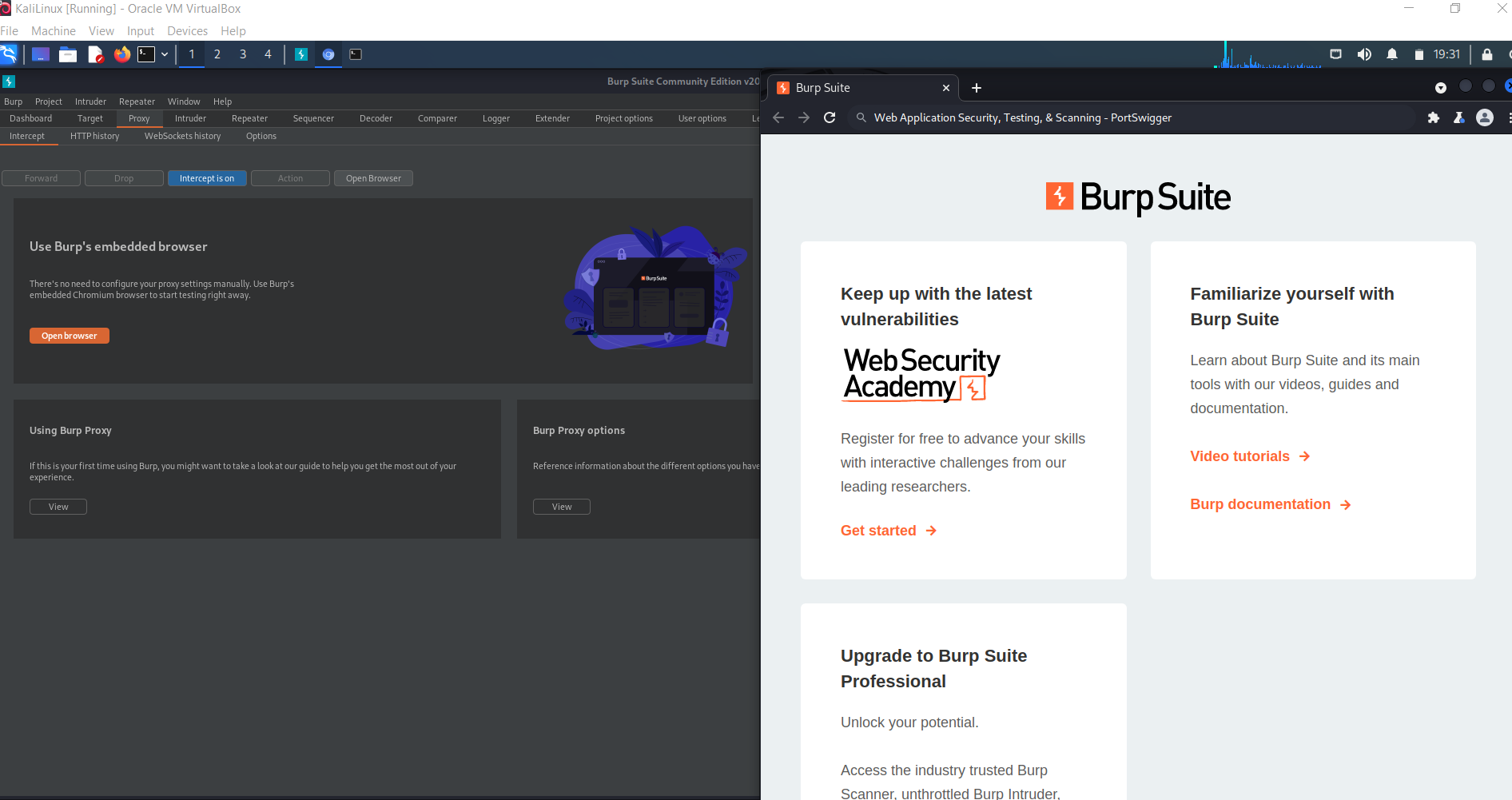
Date: 5-24-2022 (DS)

# Executive Summary:

I learned a few tips on how to navigate in Burp suite including:

* Intercepting Http requests and responses using the built in browser on Burp
* Using the repeater tab to send and resend individual requests by sending a URL to repeater or copy and pasting one in.
* How to use the scanner to scan websites for vulnerabilities by using many different configurations (including preset ones), and using audit and crawl to give visibility to vulnerabilities. You can also create reports on certain issues.
* How to use live tasks: (processing traffic and performing live actions on them) as a live audit from proxy or passive crawl
* Using projects to organize your work (temporary - nothing saved) (disk - all memory is saved in real time)
* Saving project options through the project menu through config files
* The Burp UI, like Dashboard (live tasks/scans), Target (Records all content and issues found in targeted URLs), Proxy (intercepts, view and modifies traffic between you and the server), Intruder (Automates custom attacks), Repeater (reissues an individual request that you can modify), Sequencer (runs statistical tests and tells you if data is random), decoder (encodes and decodes data in various formats) comparer does word or byte level comparisons between data), Extender (a customizer using your own or 3rd party app store) Project Options (a way to customize your project), and user options ( a way to configure Burp to the best way you like.) These are all found in the context menu by right clicking.
* Burp Infiltrator ( facilitates testing using burp scanner by modifying the target application so it can detect cases where its input is passed to potentially unsafe APIs.)
* Burp Clickbandit (proof of concept clickjacking attack)
* Collaborator payload generator
* Proxy interception rules, (have interceptor on, default requests are on, responses are default off, in options you can change your scopes and match types, or create your own rules. You can limit scope here but also in target tab.)
* Target Scope tells burp what you are working on by adding different URLs or excluding URLs.
* Testing Websockets in proxy/websockets history

**Results**

****

**Application Details:**

Application was installed successfully.

**Attack Narrative:**

No attack or defensive incidents yet. (Preparation)

**Conclusion:**

I learned a lot about Burp and how much of an extremely good tool it is to use for an analyst in cybersecurity. I still feel like I have a lot to learn with just what to look for but I hope the app will assist in making it easier.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_