Artifact Sanitization

When writing your reports, it's of critical importance that you sanitize any URLs or IP Addresses in a process known as *defanging* ("make something harmless").

But why?

Imagine, that you've given a post incident report to a colleague which contains information about a recent compromise you've been investigating. One of the unsanitized URLs inside of this report was found within a PowerShell script, which downloads and automatically executes a malicious payload. If your colleague accidentally clicks on that link, then there's a chance that it will open up within their web browser, download, and potentially execute compromising a system within your organization.

To overcome this, we can perform defanging of URLs and IP address. The rules for doing this are simple:

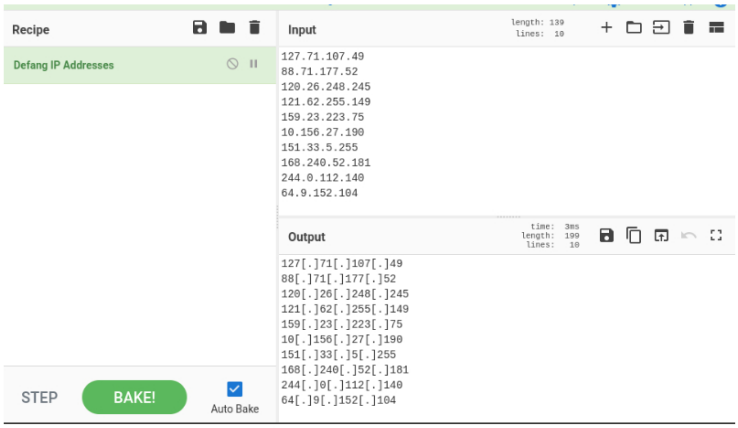
- Surround the "." within URLs and IP addresses with a "**[]**" to become "**[.]**".
- Change the "**tt**" to "**xx**" within the **http** of URLs to become "**hxxp**".

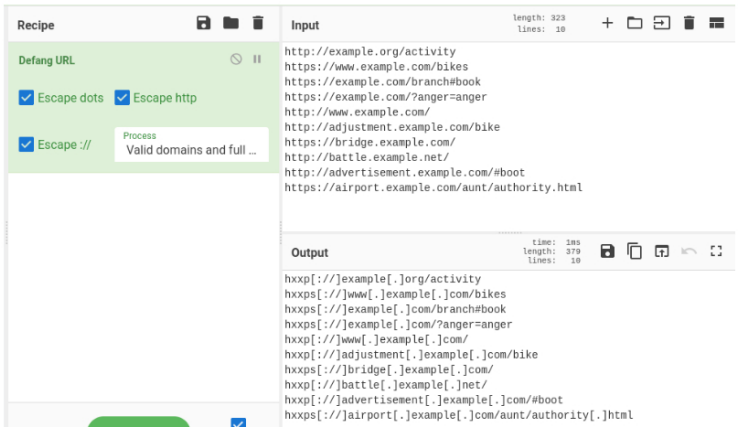
For example:

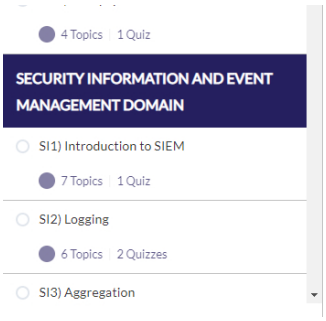
8.8.8.8 *becomes* **8[.]8[.]8[.]8**

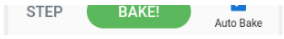
http://hello.example.com *becomes* **hxxp[://]hello[.]example[.]com**

Doing this for a batch of URLs and IP addresses can be a little tedious. Luckily, this can be "automated" using CyberChef's ***Defang IP Addresses*** and ***Defang URL*** operations:









Previous Topic
Mark Complete
Next Topic
Back to Lesson