**Web Cache poisoning assignment**

**Prerequisites:**

* Kali Linux /Windows /Mac machine with Burp suite installed

**Steps to perform attack**

1. Open the following link in any browser initially and remember the random number for testing purpose <https://9676190a.poison.digi.ninja:2443/basic.php> Graphical user interface, text, application, email

   Description automatically generated
2. Open Burp suite with default settings and go to proxy tab Graphical user interface, text

   Description automatically generated
3. Click on **open browser** and open the same link (make sure **intercept is on** before you open the link here)
4. While the link loads observe and click on the **forward button** in the intercept tab.
5. Move to HTTP history tab and check the **Request/Response. Graphical user interface, text, application, email

   Description automatically generated**
6. Right-click on the Request and send it to Repeater
7. Click send in Repeater and Observe the Age param in the response.
8. Observe similarities between the Key-Value-pairs of both request and response. (here we can notice **Host: f41a3b7a.poison.digi.ninja:2443** URL is used on the response for an image ) Graphical user interface, text, application, email

   Description automatically generated
9. Install param miner from **BApp Store** located at Extender tab. Graphical user interface

   Description automatically generated
10. Comeback to Repeater and right-click on request and choose from extensions->param miner-> Guess headers.
11. Send multiple requests for param-miner to mine the similar pram value (here: f41a3b7a.poison.digi.ninja) and choose one such identified header to inject the malicious script to perform attack. Graphical user interface, text, application, email

    Description automatically generated
12. Insert the malicious script and send to see the response. Graphical user interface, text, email

    Description automatically generated
13. After successfully finishing the above steps if you try it in any browser in your machine you should see below message. Graphical user interface, text, application

    Description automatically generated

Submission Files:

1. Screenshot of the Result [Ref: step 13]
2. Screenshot of the param miner [Ref: step 11].
3. After successful attack save Request and Response into txt files.