HOW TO CHECK MALICIOUS/ PHISHING LINKS

How to check if the links/URLs are malicious/phishing or not?

Malicious URL: http://rxqsd.com/9n4fbg (URL Sample (link is dead), can use your own)

Tools: URL Scan io, BrightCloud, Browserling

We need to answer all the questions below:

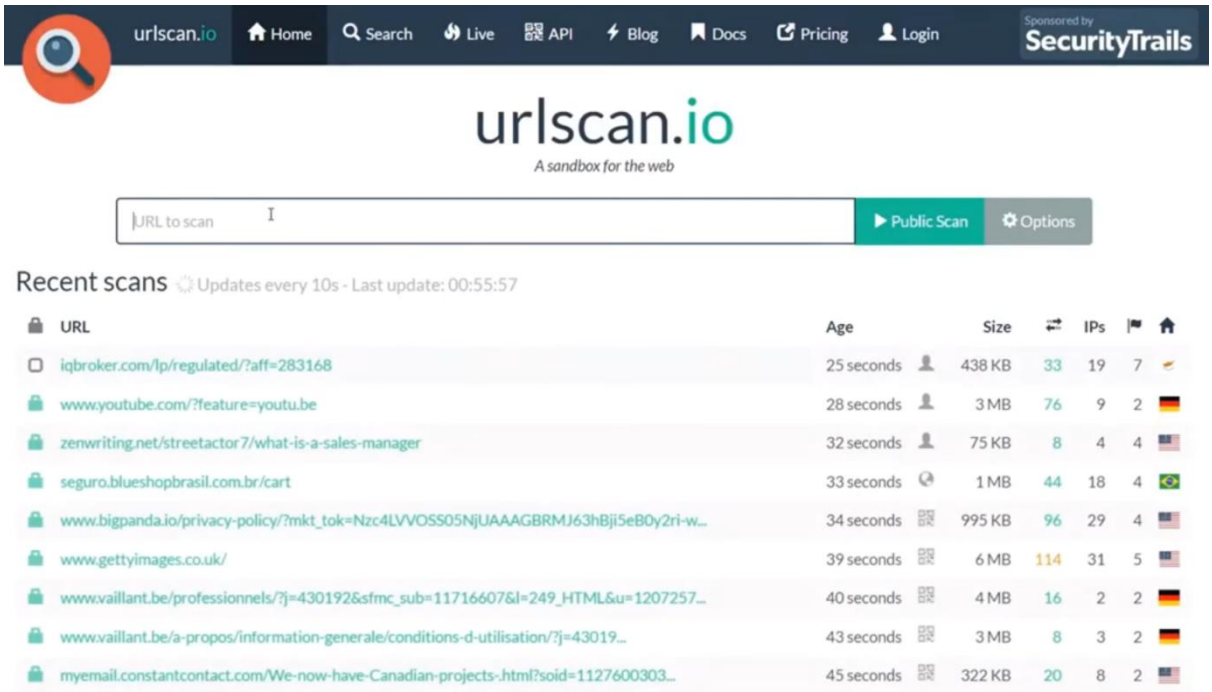
1. Check the URL behaviour using https://urlscan.io/
   Result:

2. Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php
   Result:

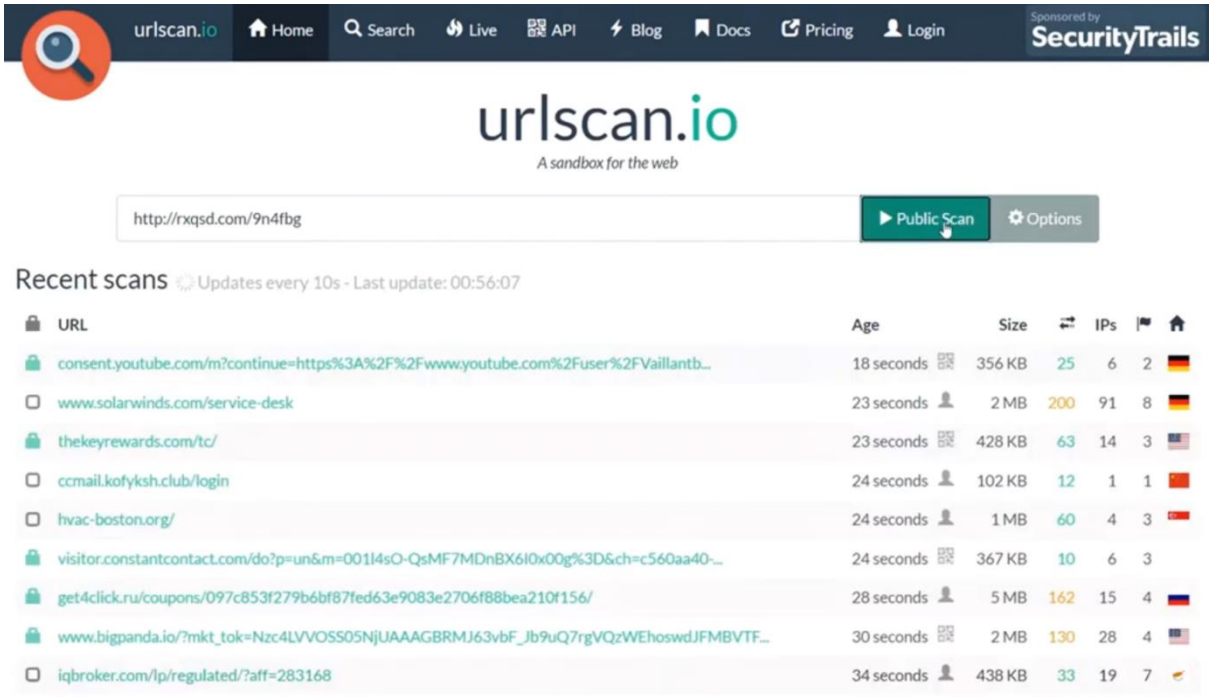
3. Interact with URL using virtual sandboxed browser from https://www.browserling.com/
   Result:

Investigation

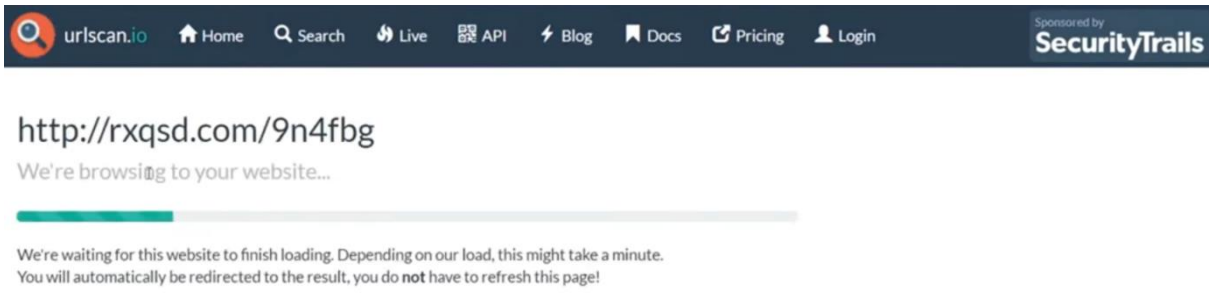
First, we need to check the URL behaviour using URLScan (https://urlscan.io/). Open the website.



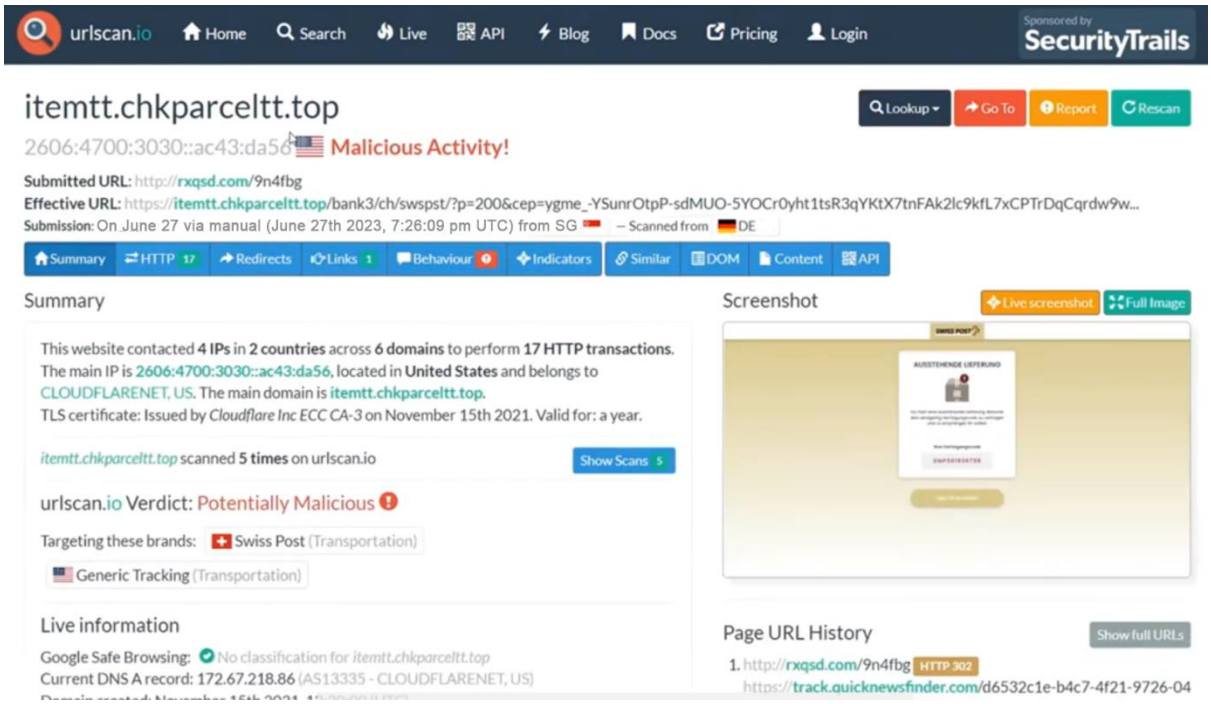
Then put the URL address that you want to check and click “Public Scan”.



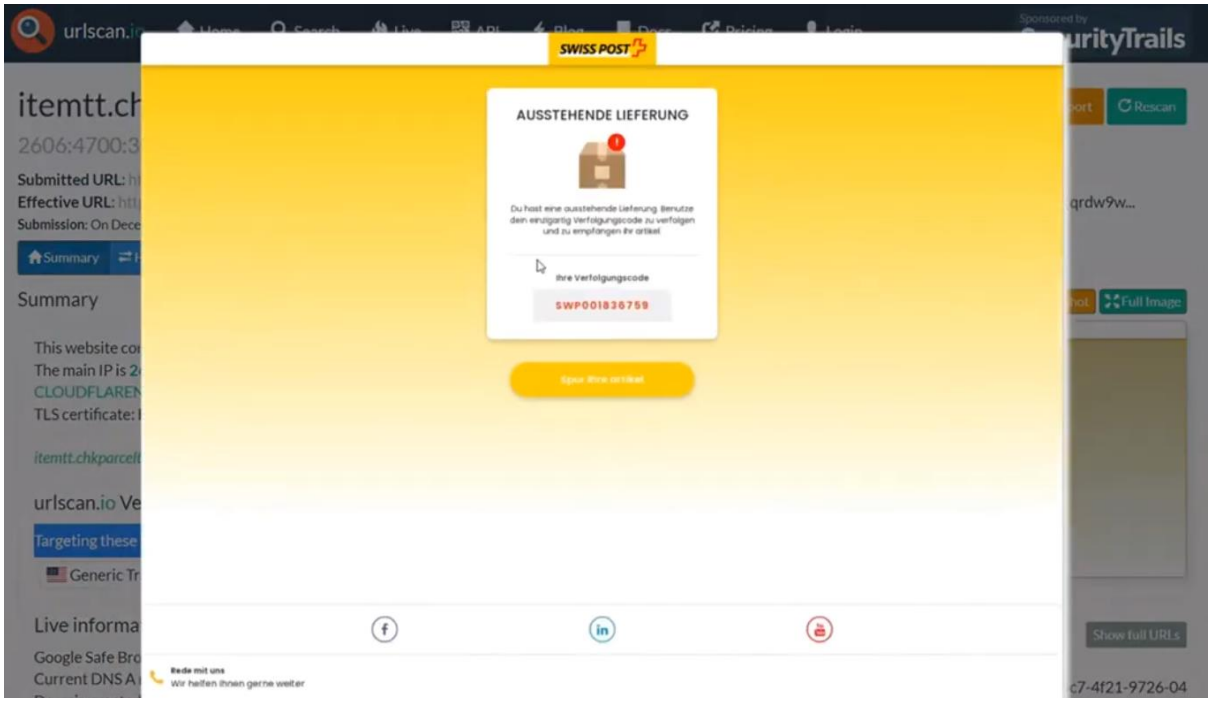
After you click the “Public Scan” it’s take some time to complete the scanning.



Now, we got the result. As we can see it stated this URL is “Malicious Activity!”. The URLScan io verdic this as potentially malicious.



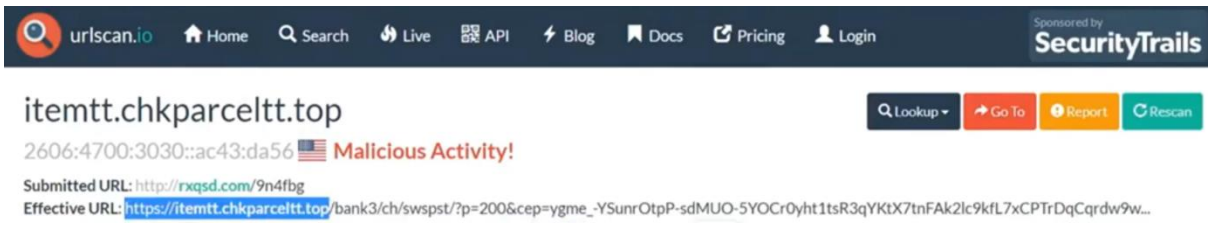
We also can see this URL targeting which brand. In this case, they are targeting Swiss Post (National postal service of Switzerland).



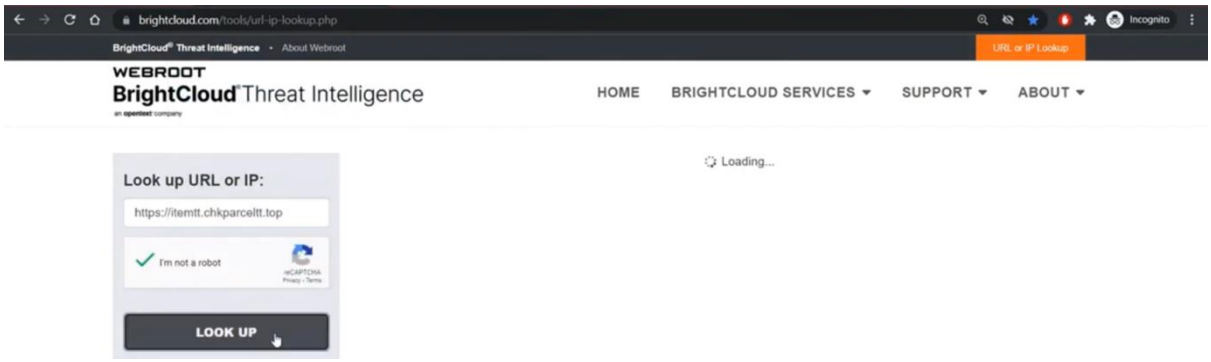
Now, we have an answer for Questions 1.

Check the URL behaviour using https://urlscan.io/
Result: Potential Malicious

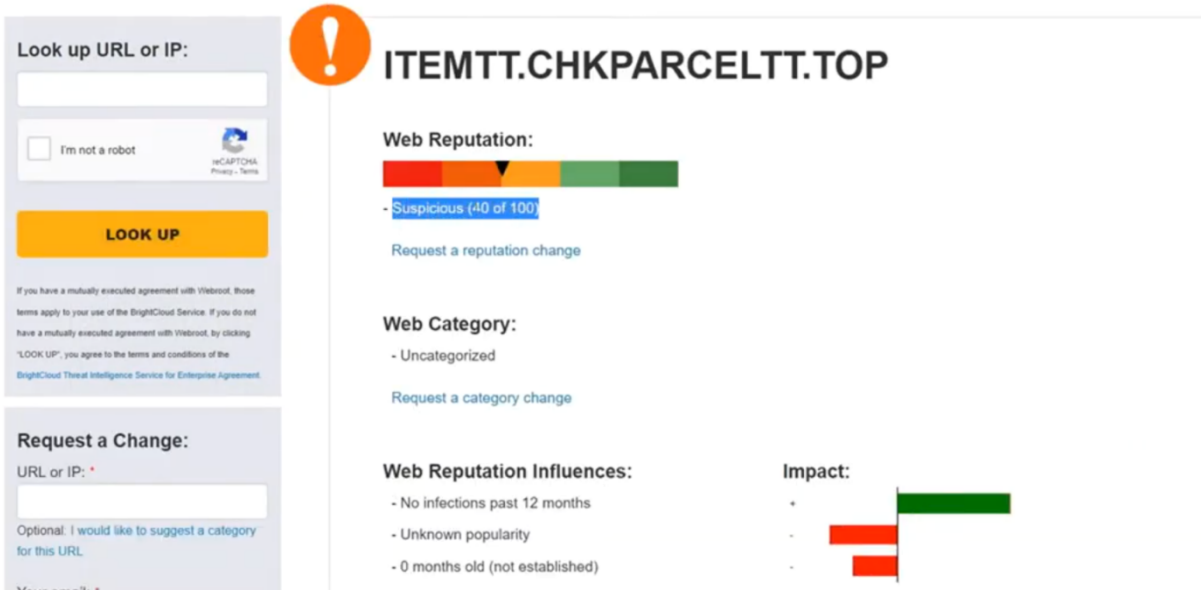
Next, we check the domain reputation using BrightCloud (https://www.brightcloud.com/tools/url-ip-lookup.php). Copy the “Effective URL” from the precious URL scan.



Then put the URL address that you want to check and click “LOOK UP”.



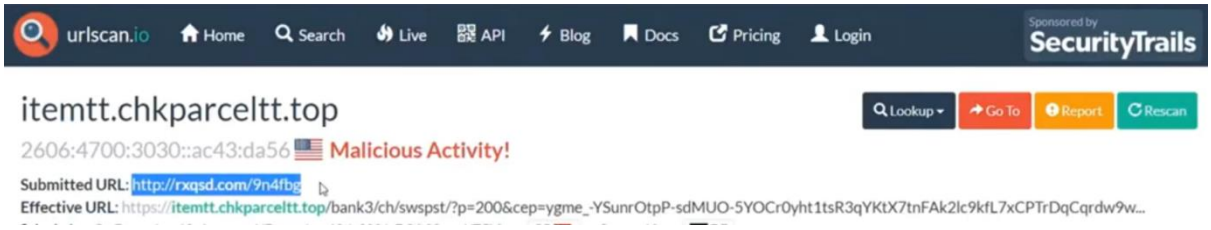
Now, we got the result. As we can see it stated that web reputation is suspicious (40 of 100).



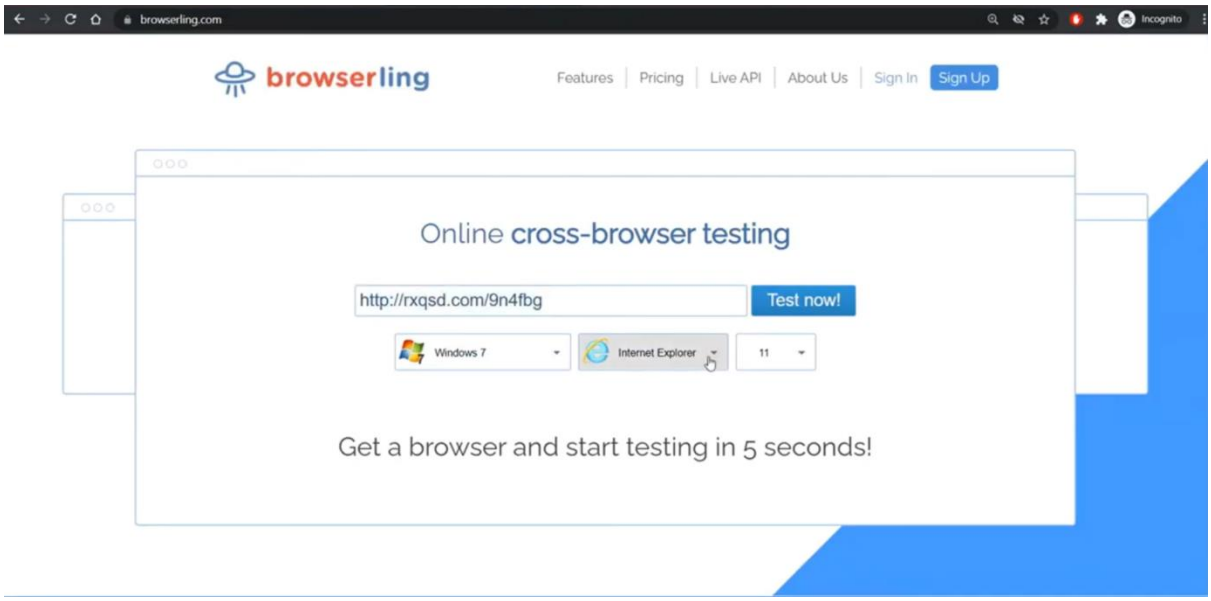
Now, we have an answer for Questions 2.

Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php
Result: Suspicious

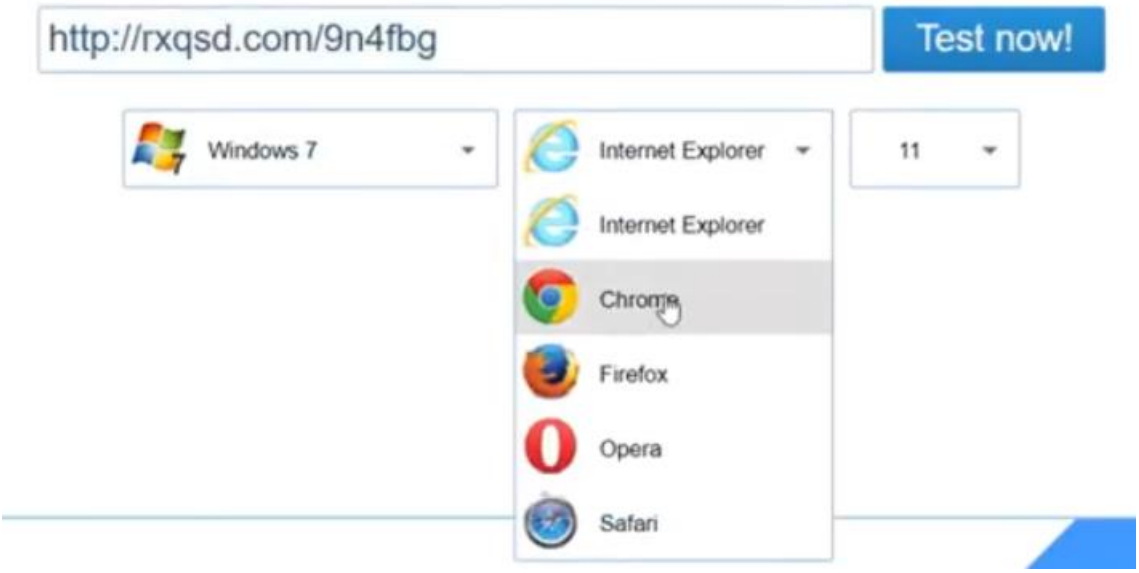
Finally, we interact with URL using Browserling (https://www.browserling.com/). This virtual sandboxed browser allows us to running web applications in isolated environments to prevent browser-based malware from spreading to the network. Copy the URL.



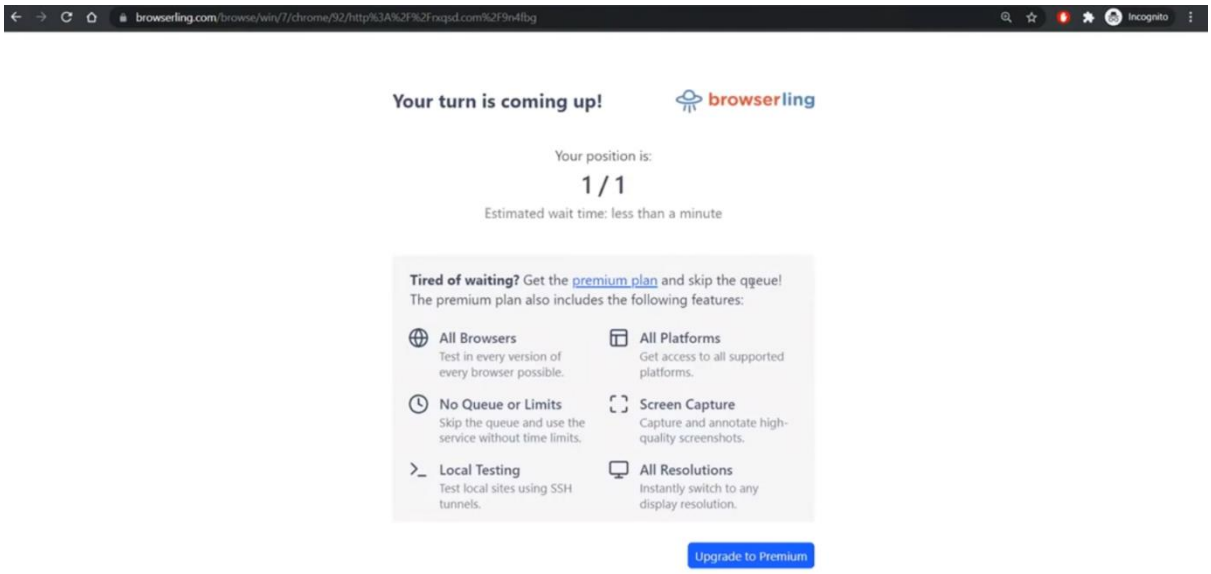
Then put the URL address that you want to check.



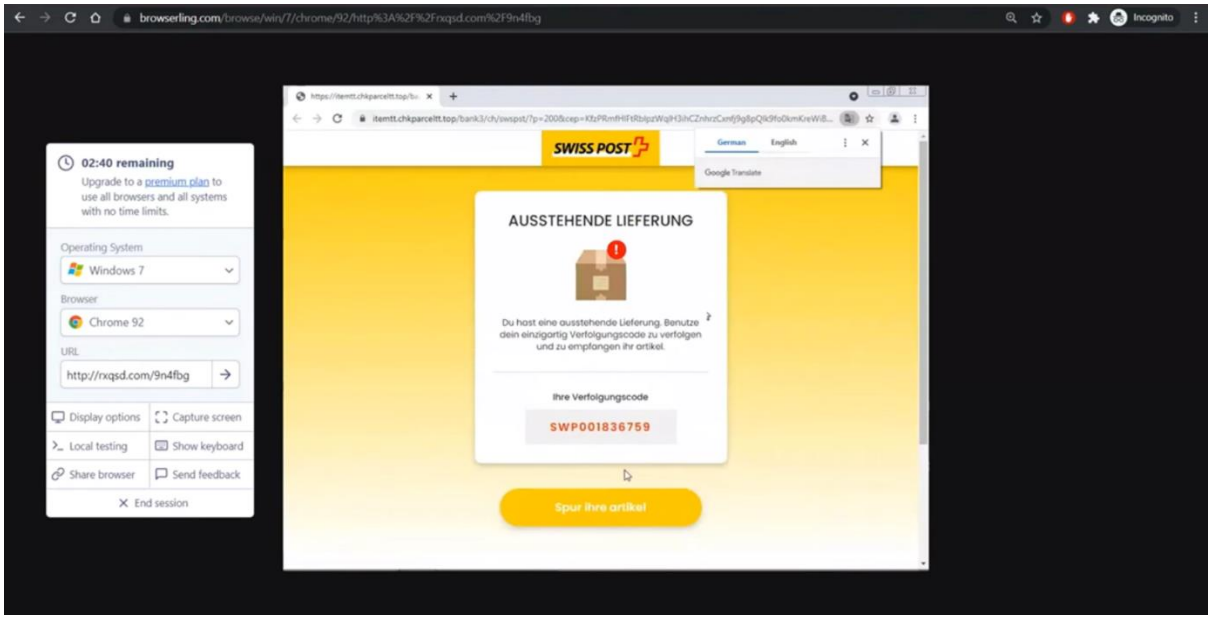
Choose the browser that you prefer and click “Test now!”. For me, I like to use Chrome.



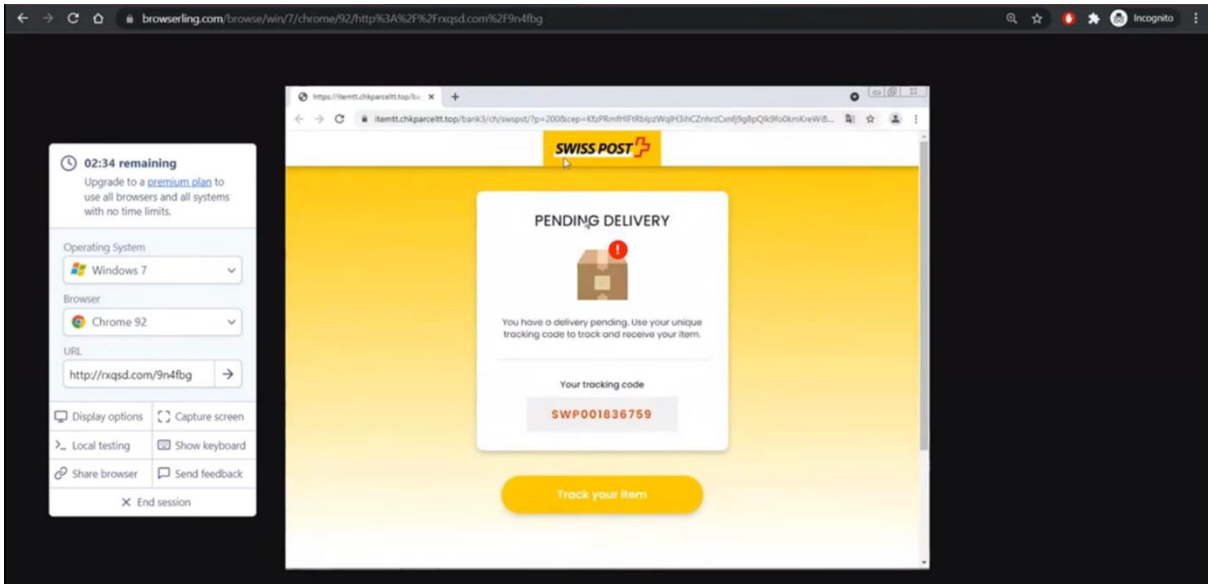
After clicking “Test now!”, you need to wait for a moment for the browser to establish the connection.



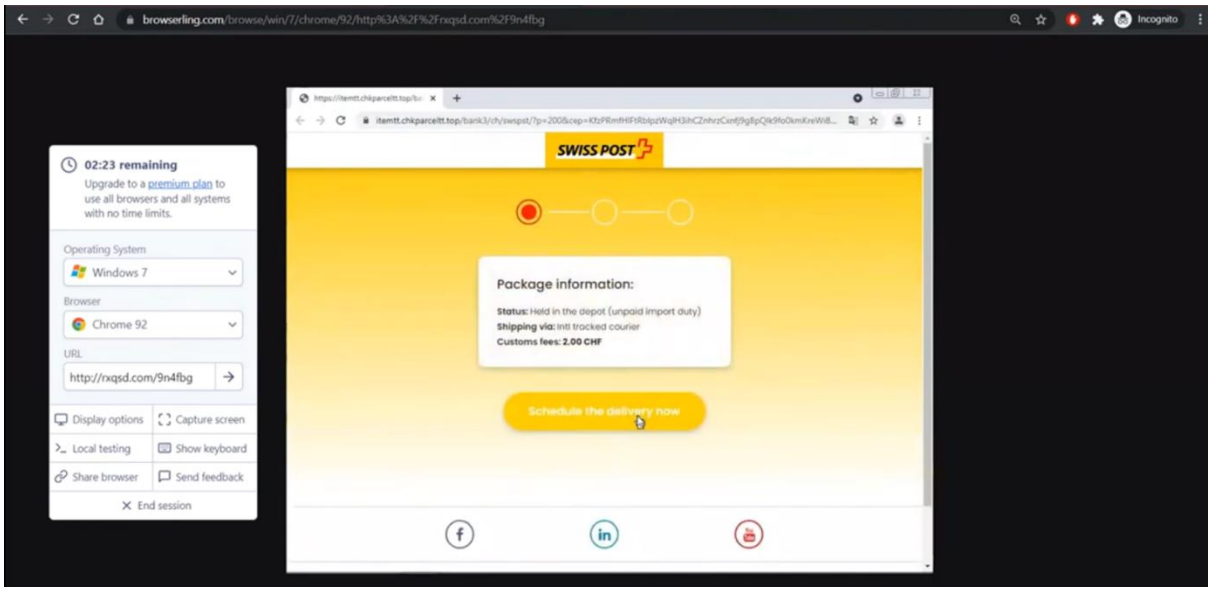
Now, we are in the isolated mode. Let’s observed and analyse this website.



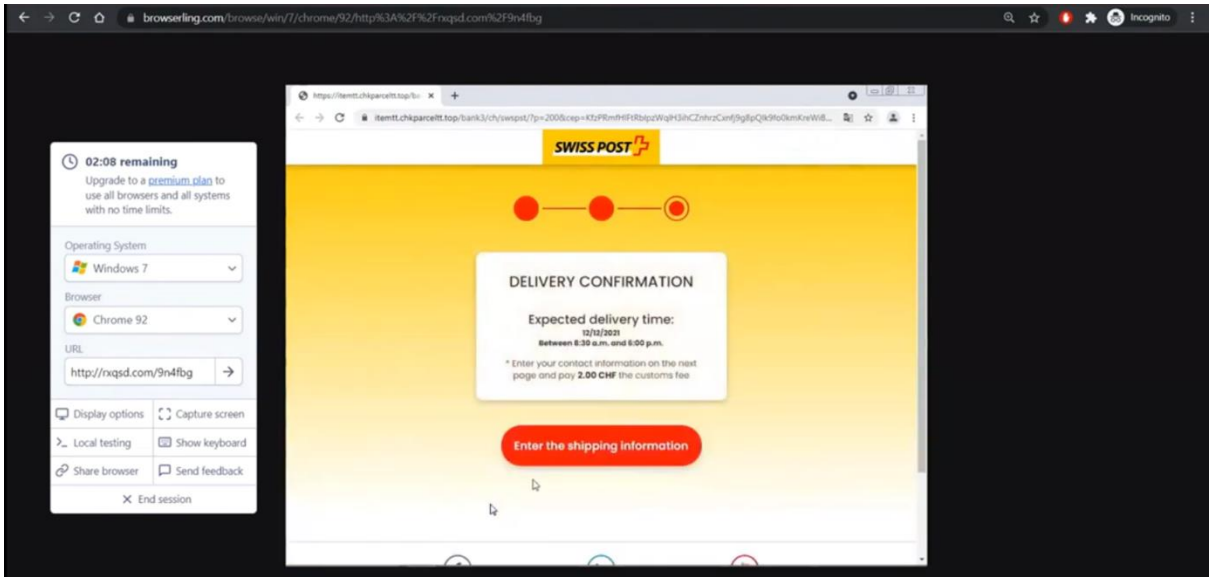
The content is in German language. Translate the website content to English to make sure we understand all the details.



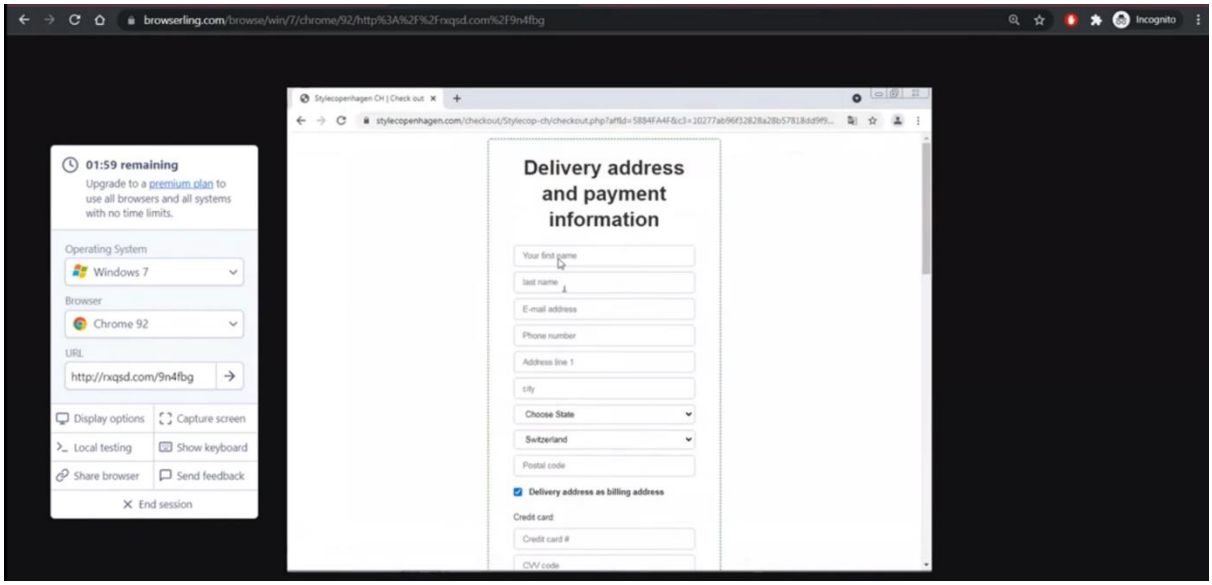
So, we want to observe what the threat actor trying to trick us with this website. First click the button “Track your item”.



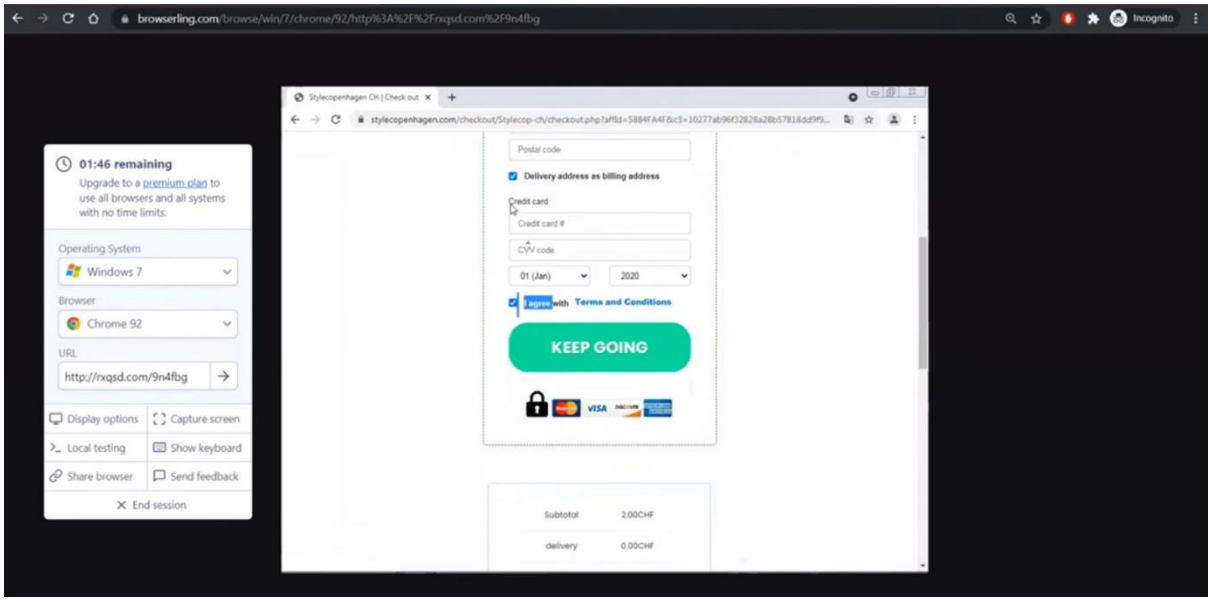
Next click “Enter shipping information”.



Finally, we are on the page that we need to fill all the details. From here we know this is phishing.



They also ask for our credit card details. This is red flag.



Now, we have an answer for Question 3

Interact with URL using virtual sandboxed browser from https://www.browserling.com/
Result: Phishing URL to harvest credit card info and personal data | Phishing link

So, we already have answered all the questions:

1. Check the URL behaviour using https://urlscan.io/
   Result: Potential Malicious

2. Check domain reputation using https://www.brightcloud.com/tools/url-ip-lookup.php
   Result: Suspicious

3. Interact with URL using virtual sandboxed browser from https://www.browserling.com/
   Result: Phishing URL to harvest credit card info and personal data | Phishing link

   Now, we can conclude that links/URLs are malicious. The threat actor used the phishing method to harvest credit card info and personal data.