

**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)

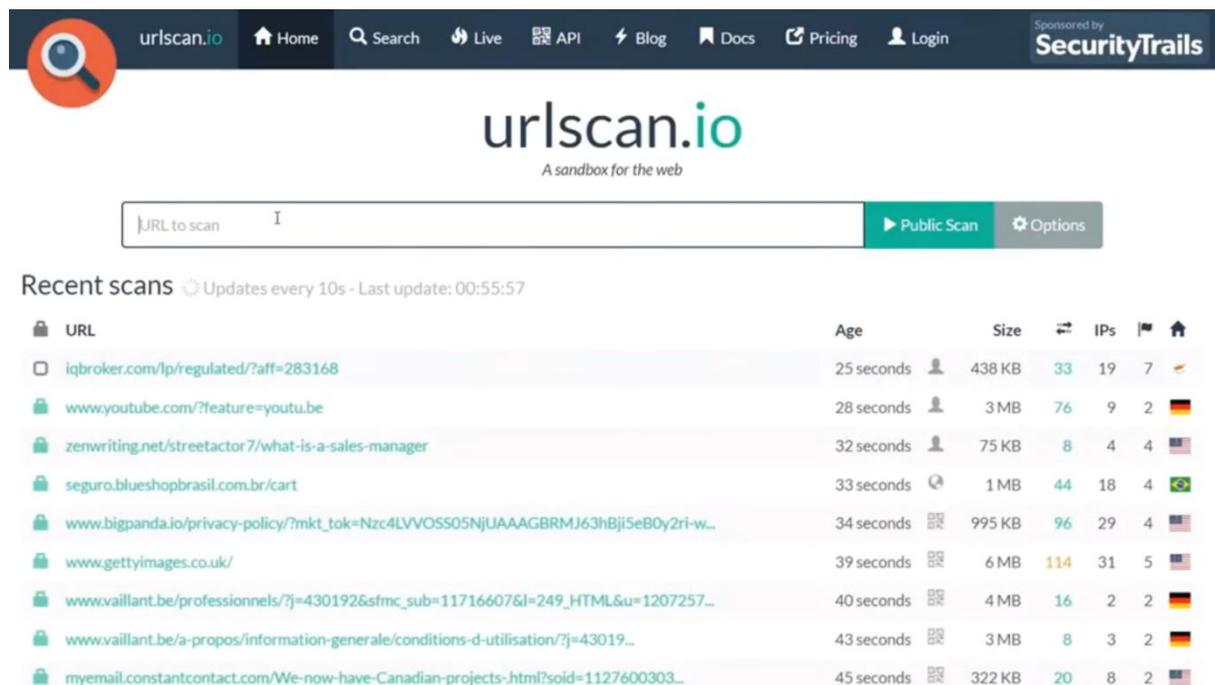
Tools: URL Scan io, BrightCloud, Browserling

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

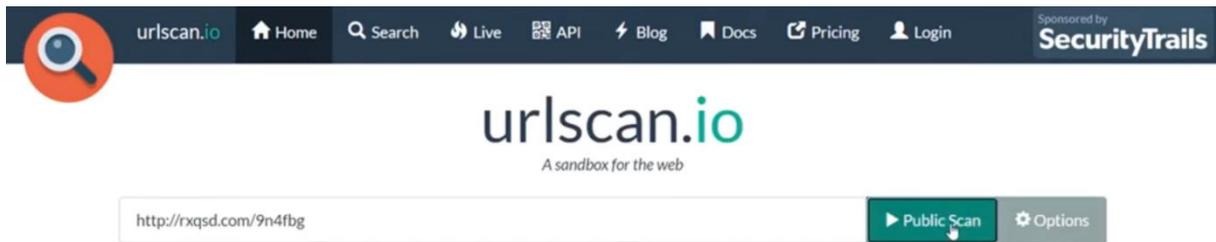
First, we need to check the URL behaviour using URLScan (<https://urlscan.io/>). Open the website.



The screenshot shows the urlscan.io website interface. At the top, there is a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. The main heading is "urlscan.io" with the tagline "A sandbox for the web". Below the heading is a search bar with the placeholder text "URL to scan" and a "Public Scan" button. A table titled "Recent scans" displays a list of scanned URLs with columns for URL, Age, Size, IPs, and a home icon. The table is updated every 10 seconds.

URL	Age	Size	IPs	Home
iqbroker.com/lp/regulated/?aff=283168	25 seconds	438 KB	33 19 7	
www.youtube.com/?feature=youtu.be	28 seconds	3 MB	76 9 2	🇩🇪
zenwriting.net/streetactor7/what-is-a-sales-manager	32 seconds	75 KB	8 4 4	🇺🇸
seguro.blueshopbrasil.com.br/cart	33 seconds	1 MB	44 18 4	🇧🇷
www.bigpanda.io/privacy-policy/?mkt_tok=Nzc4LVVOSS05NjUAAAGBRMJ63hBji5eB0y2ri-w...	34 seconds	995 KB	96 29 4	🇺🇸
www.gettyimages.co.uk/	39 seconds	6 MB	114 31 5	🇺🇸
www.vaillant.be/professionnels/?j=430192&sfmc_sub=11716607&l=249_HTML&u=1207257...	40 seconds	4 MB	16 2 2	🇩🇪
www.vaillant.be/a-propos/information-generale/conditions-d-utilisation/?j=43019...	43 seconds	3 MB	8 3 2	🇩🇪
myemail.constantcontact.com/We-now-have-Canadian-projects-.html?soid=1127600303...	45 seconds	322 KB	20 8 2	🇺🇸

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

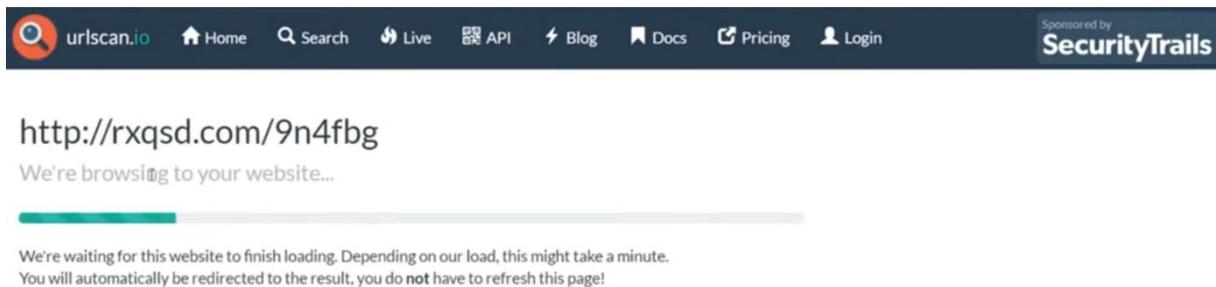


The screenshot shows the urlscan.io website interface. At the top, there is a navigation bar with the urlscan.io logo, a search icon, and links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A 'Sponsored by SecurityTrails' badge is also present. The main content area features the urlscan.io logo and the tagline 'A sandbox for the web'. Below this, there is a text input field containing the URL 'http://rxqsd.com/9n4fbg'. To the right of the input field are two buttons: 'Public Scan' and 'Options'.

Recent scans Updates every 10s - Last update: 00:56:07

URL	Age	Size	🌐	IPs	🏠
consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fuser%2Fvaillantb...	18 seconds	356 KB	25	6	2 🇩🇪
www.solarwinds.com/service-desk	23 seconds	2 MB	200	91	8 🇩🇪
thekeyrewards.com/tc/	23 seconds	428 KB	63	14	3 🇺🇸
ccmail.kofyksh.club/login	24 seconds	102 KB	12	1	1 🇨🇳
hvac-boston.org/	24 seconds	1 MB	60	4	3 🇨🇳
visitor.constantcontact.com/do?p=un&m=00114sO-QsMF7MDnBX6i0x00g%3D&ch=c560aa40-...	24 seconds	367 KB	10	6	3
get4click.ru/coupons/097c853f279b6bf87fed63e9083e2706f88bea210f156/	28 seconds	5 MB	162	15	4 🇷🇺
www.bigpanda.io/?mkt_tok=Nzc4LVVOSS05NjUAAAGBRMJ63vbF_Jb9uQ7rgVQzWEhoswdJFMBVTF...	30 seconds	2 MB	130	28	4 🇺🇸
iqbroker.com/lp/regulated/?aff=283168	34 seconds	438 KB	33	19	7 🇨🇳

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



The screenshot shows the urlscan.io website interface during a scan. The URL 'http://rxqsd.com/9n4fbg' is displayed at the top. Below the URL, there is a progress bar that is partially filled with green. A message below the progress bar reads: 'We're browsing to your website...'. At the bottom, there is a message: 'We're waiting for this website to finish loading. Depending on our load, this might take a minute. You will automatically be redirected to the result, you do not have to refresh this page!'.

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

The screenshot displays the URLScan.io analysis for the domain `itemtt.chkparceltt.top`. The main heading is **Malicious Activity!**. The URLScan.io Verdict is **Potentially Malicious**. The analysis indicates that the website contacted 4 IPs in 2 countries across 6 domains to perform 17 HTTP transactions. The main IP is `2606:4700:3030::ac43:da56`, located in the United States and belonging to CLOUDFLARENET, US. The main domain is `itemtt.chkparceltt.top`. The TLS certificate is issued by Cloudflare Inc ECC CA-3 on November 15th 2021, valid for a year. The URLScan.io Verdict is **Potentially Malicious**. The analysis also shows that the website is targeting brands such as Swiss Post (Transportation) and Generic Tracking (Transportation). A screenshot of the website shows a notification for **AUSSTEHENDE LIEFERUNG** (Outstanding Delivery) from SWISS POST, with a tracking code `SWP001826759`.

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

This is a close-up view of the notification shown in the previous screenshot. It features the **SWISS POST** logo at the top. The main heading is **AUSSTEHENDE LIEFERUNG**. Below the heading is a box icon with a red exclamation mark. The text reads: "Du hast eine ausstehende Lieferung. Benutze den einzigartigen Verfolgungscode zu verfolgen und zu empfangen ihr Artikel." Below this text is a field for "Ihre Verfolgungscode" with the value `SWP001826759`. At the bottom of the notification is a button that says "Spüre Ihre Lieferung".

Now, we have an answer for Questions 1.

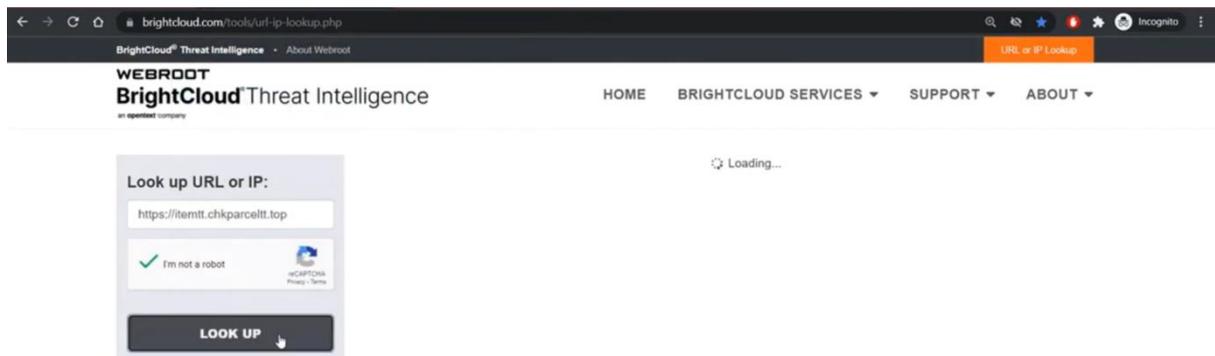
Check the URL behaviour using <https://urlscan.io/>

Result: Potential Malicious

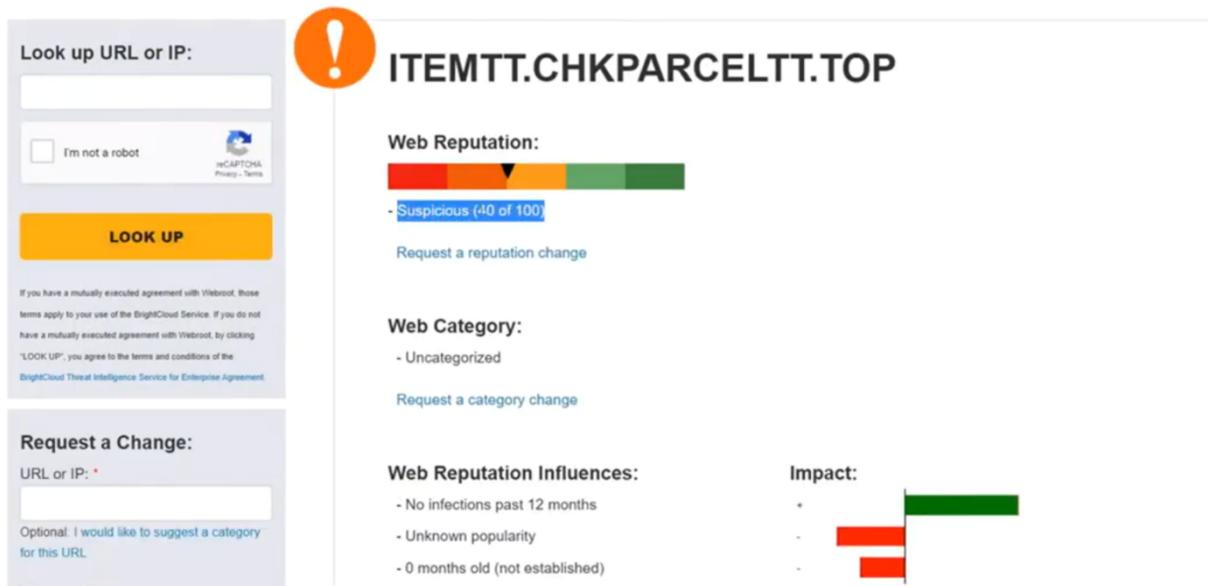
Next, we check the domain reputation using BrightCloud (<https://www.brightcloud.com/tools/url-ip-lookup.php>). Copy the “Effective URL” from the previous URL scan.



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).

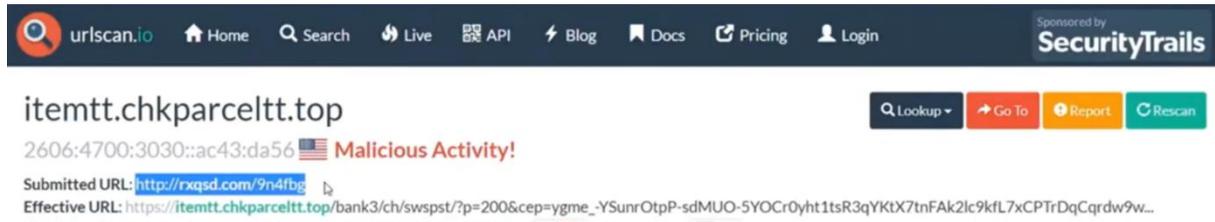


Now, we have an answer for Questions 2.

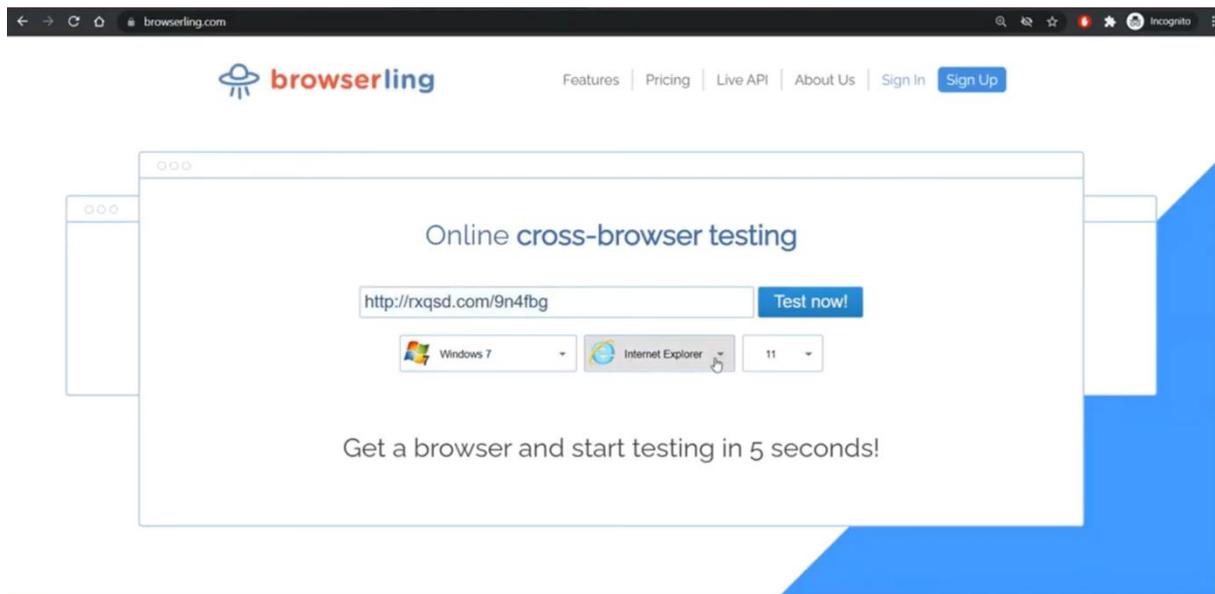
Check domain reputation using <https://www.brightcloud.com/tools/url-ip-lookup.php>

Result: Suspicious

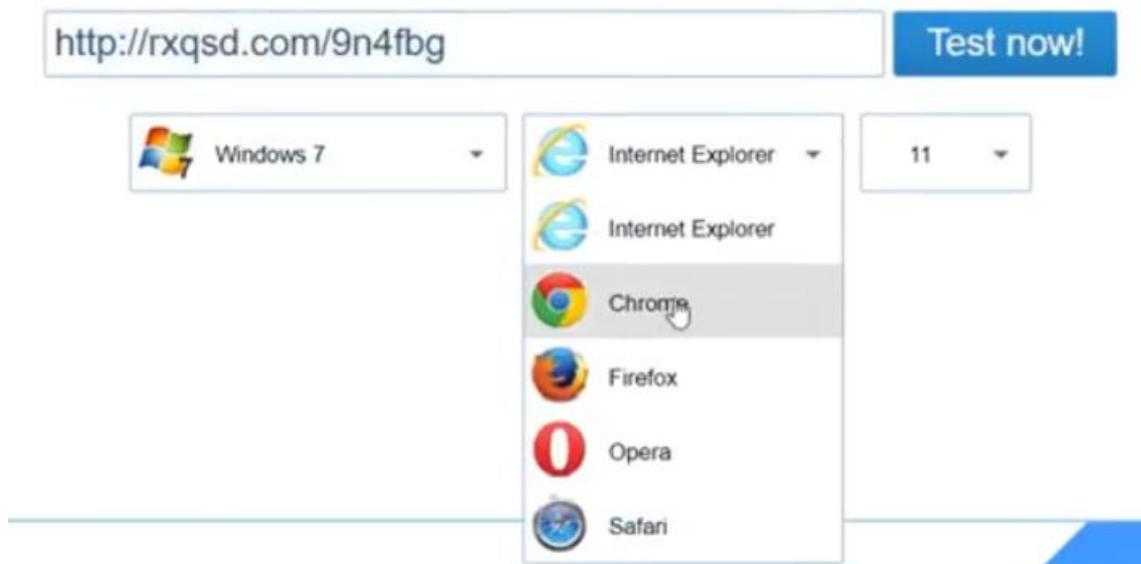
Finally, we interact with URL using Browserling (<https://www.browserling.com/>). This virtual sandboxed browser allows us to running web applications in isolated environments to prevent browser-based malware from spreading to the network. Copy the URL.



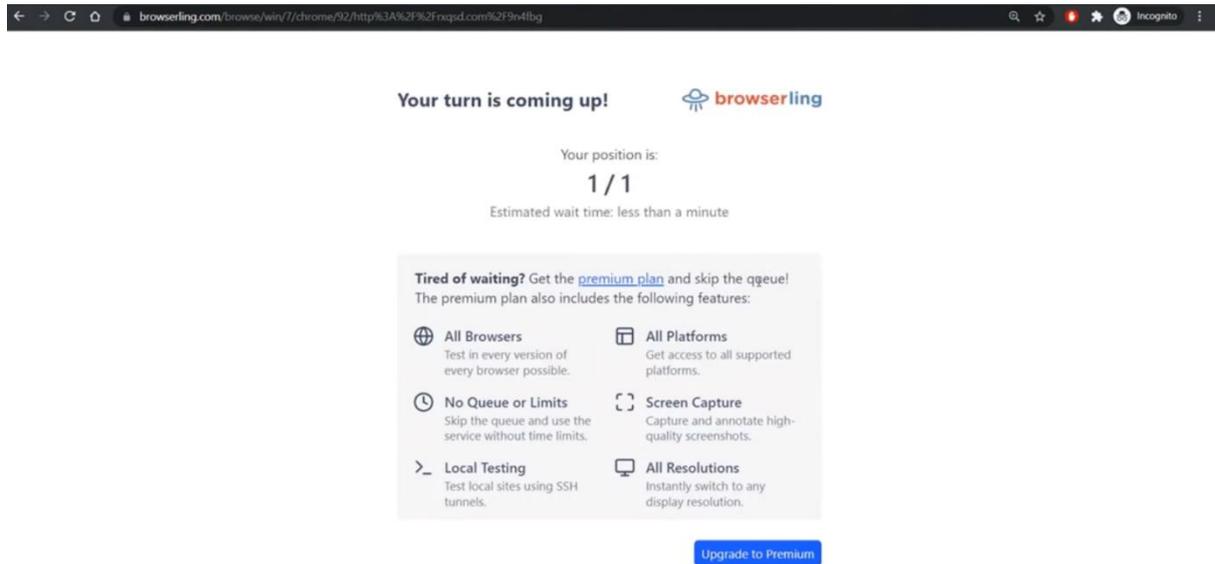
Then put the URL address that you want to check.



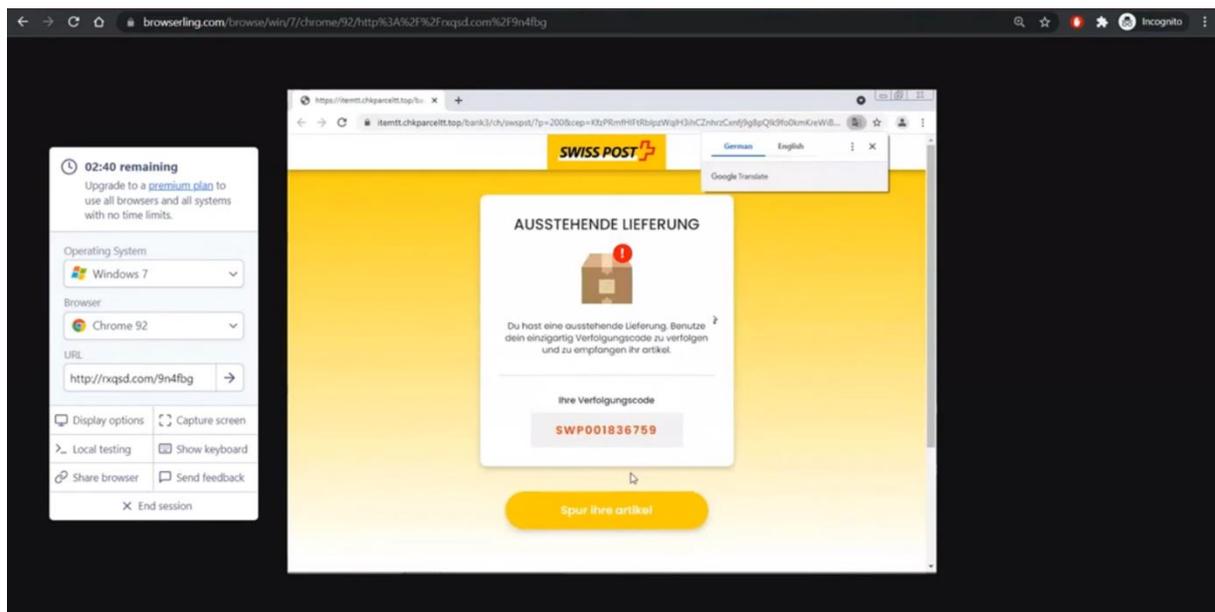
Choose the browser that you prefer and click "Test now!". For me, I like to use Chrome.



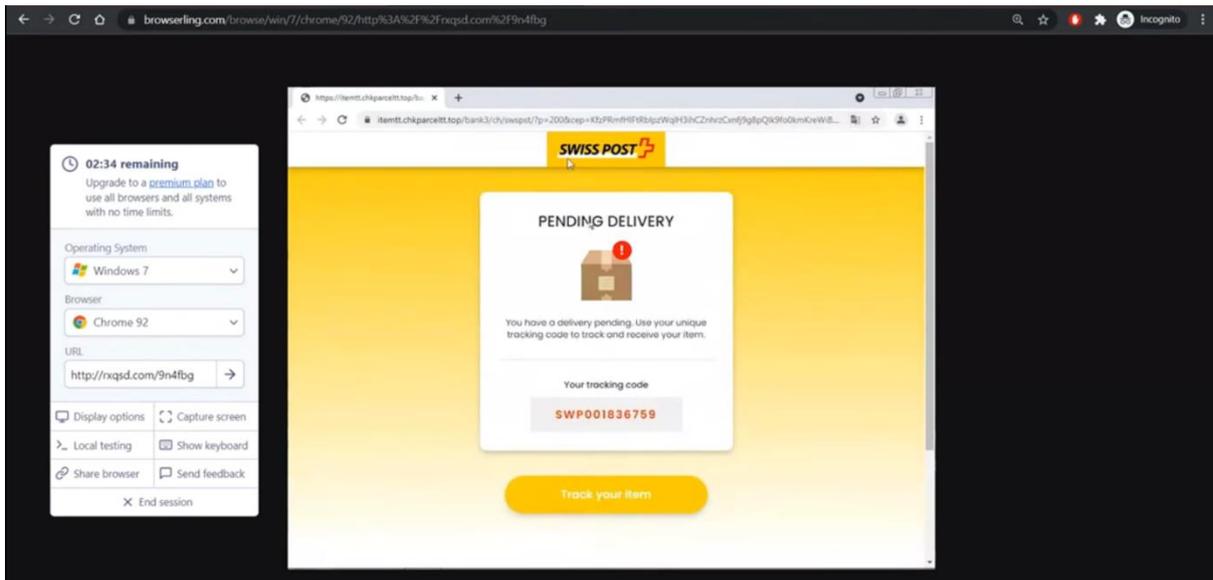
After clicking “Test now!”, you need to wait for a moment for the browser to establish the connection.



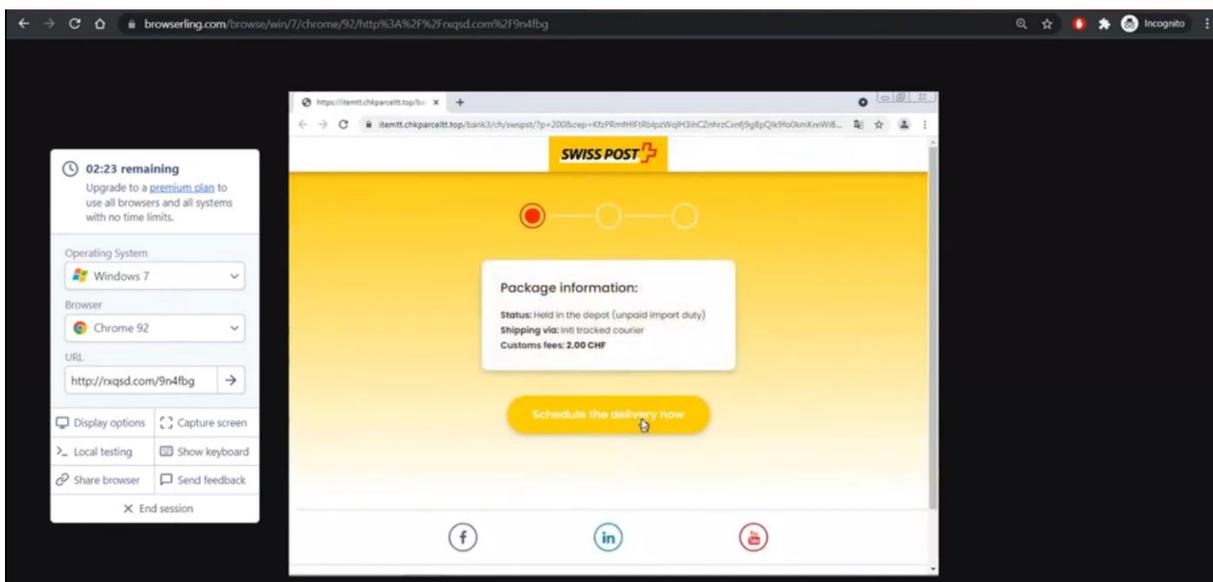
Now, we are in the isolated mode. Let's observe and analyse this website.



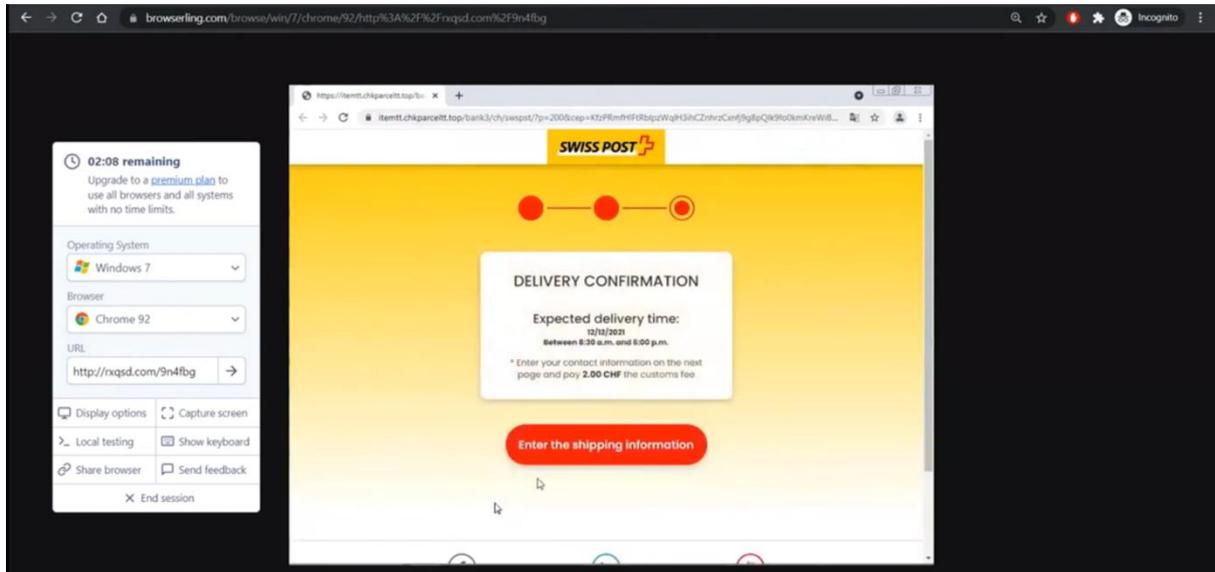
The content is in German language. Translate the website content to English to make sure we understand all the details.



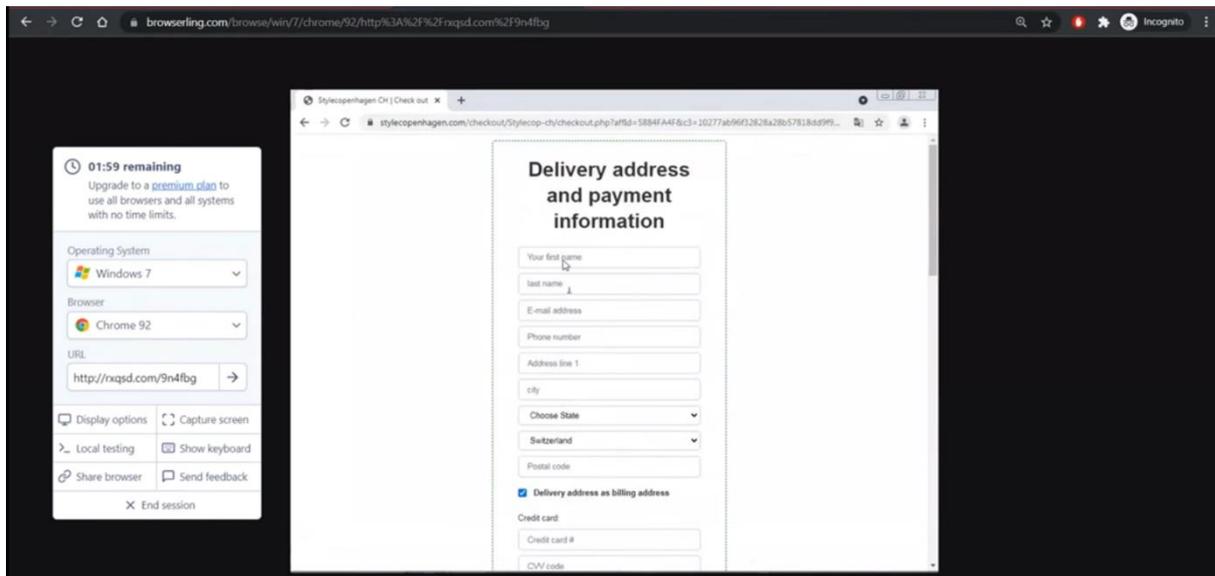
So, we want to observe what the threat actor trying to trick us with this website. First click the button "Track your item".



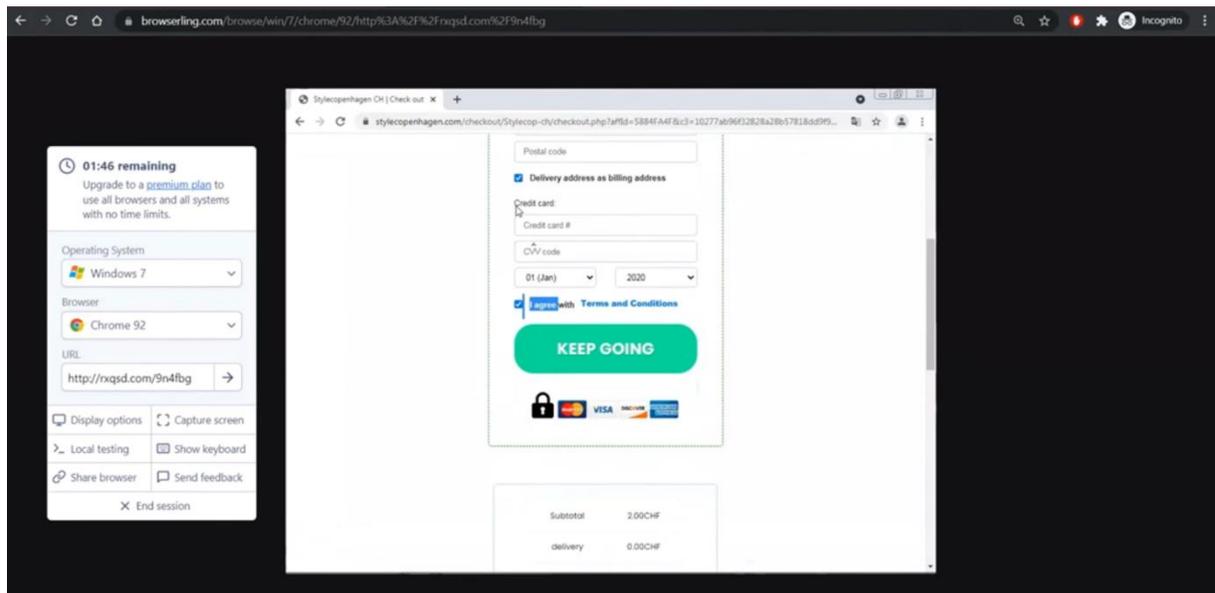
Next click “Enter shipping information”.



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.