|  |
| --- |
| Cyber Defenders |
| Grab The Phisher |
| Threat Intelligence |

|  |
| --- |
| Abdallah Chbaro  09/04/2023 |

Table des matières

[Scenario 2](#_Toc131953775)

[Write Up 2](#_Toc131953776)

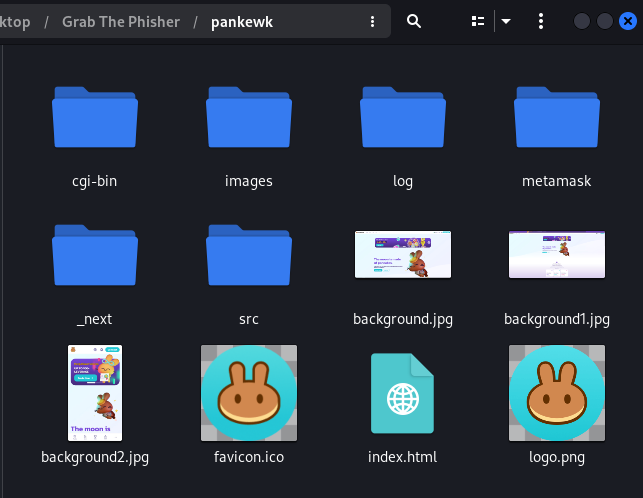
# Scenario

An attacker compromised a server and impersonated https://pancakeswap.finance/, a decentralized exchange native to BNB Chain, to host a phishing kit at https://apankewk.soup.xyz/mainpage.php. The attacker set it as an open directory with the file name "pankewk.zip".

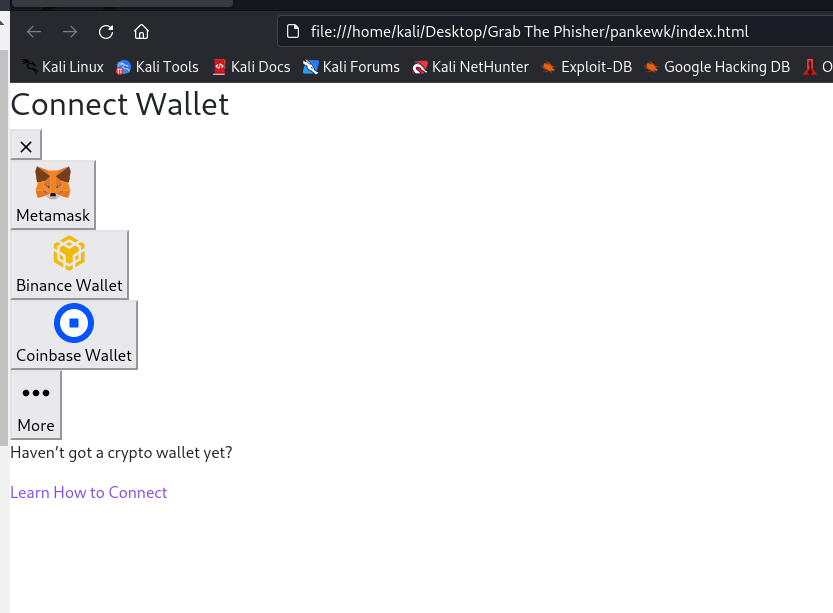
Provided the phishing kit, you are requested to analyze it and do your threat intel homework

# Write Up

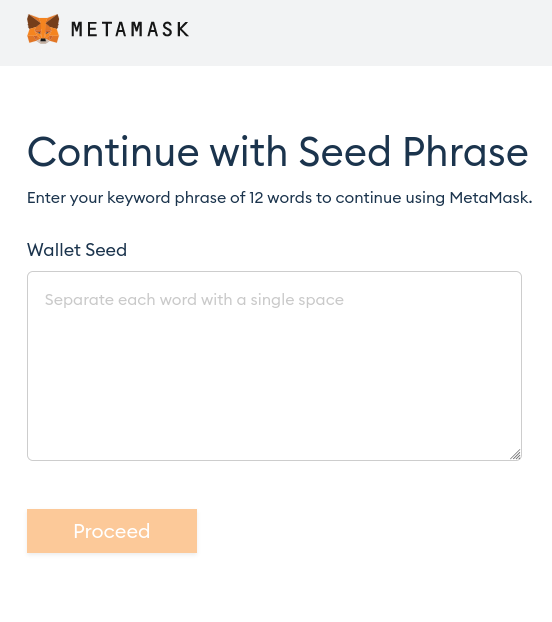
We are provided a zip file that contains the following:



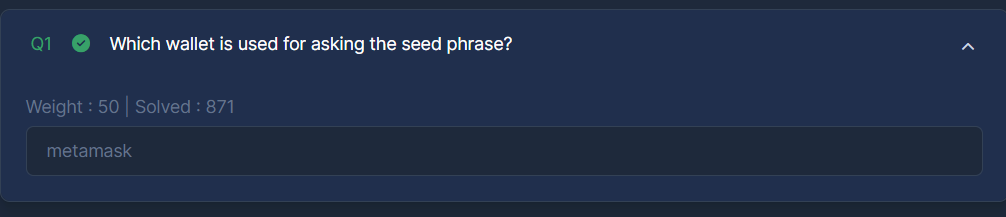
Opening index.html, we land on the following:



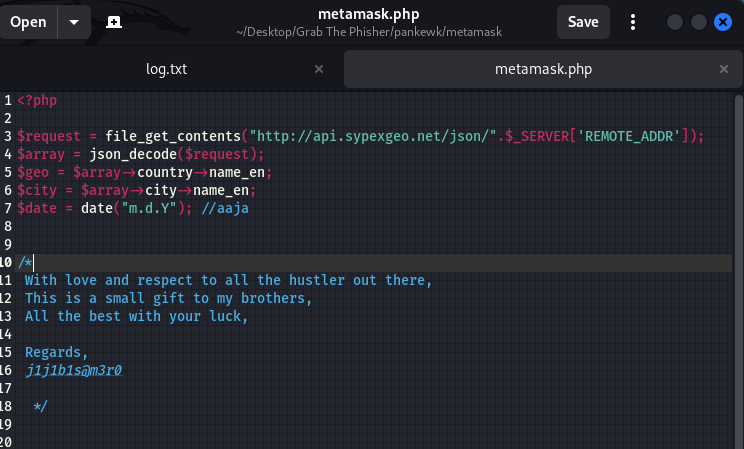
Opening the index.html of Metamask, found in the folder, we land on the following:



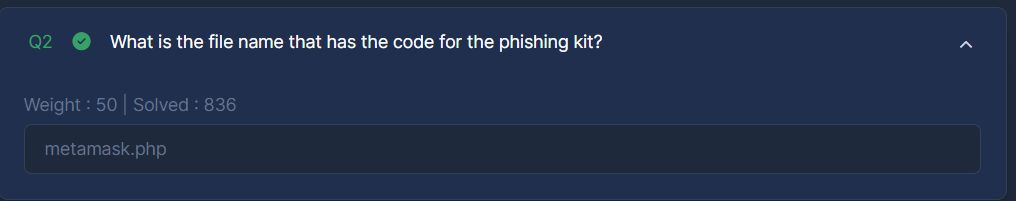
This is enough to answer the first question:



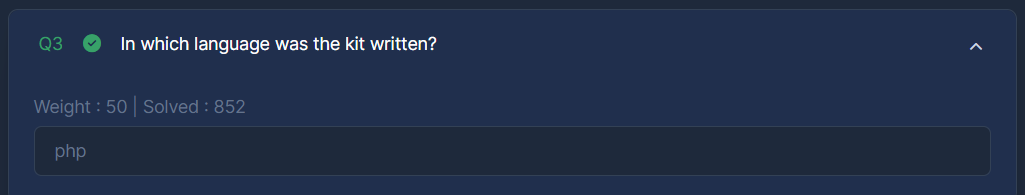
Looking at each file, we find a file called metamask.php that contains the code for the metamask:



This is enough to answer question 2:

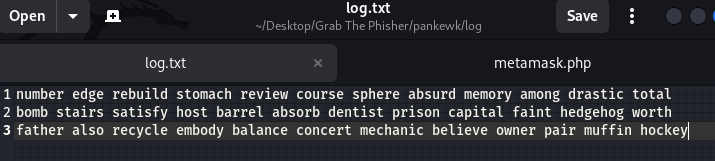


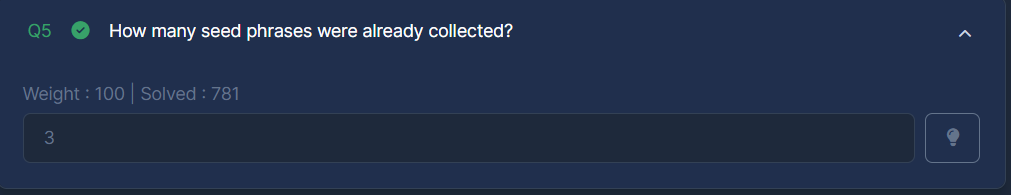
The third question asks about the language used to write the file. It is clear that it is written in php:



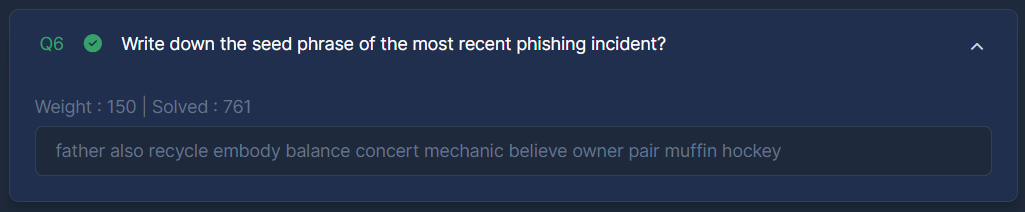
As for question 4, the service used is sypex geo, written in the PHP file.

The fifth question asks about the number of seeds collected. Looking through log.txt we can see 3 seeds collected:

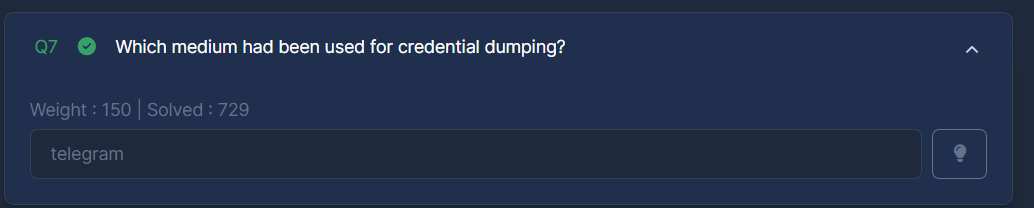




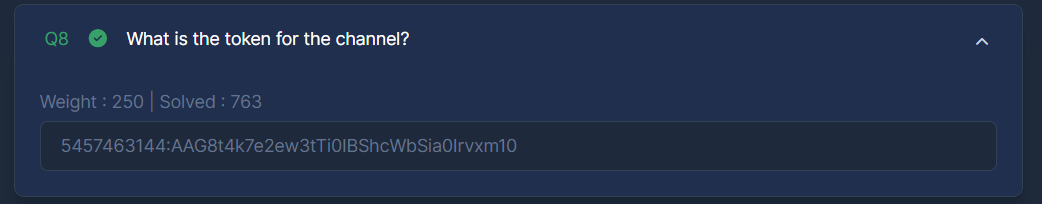
The next question asks about the most recent phishing incident. It is the last see in the document. We knew that it is the last seed, since the PHP file is using append functions, that will append the log.txt file.



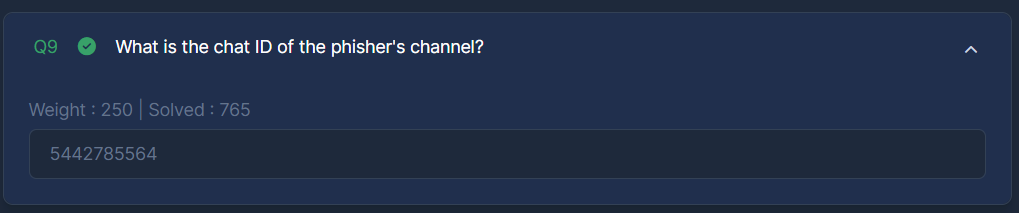
Next, they ask about the channel used for credential dumping. Looking at the PHP file, we can see it is Telegram:



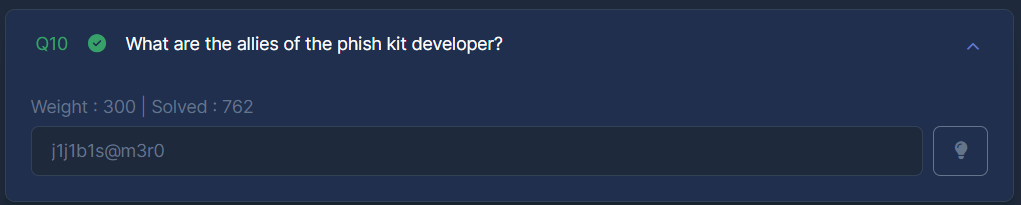
In the next question, they ask about the Telegram token used, which we can see in the PHP file:



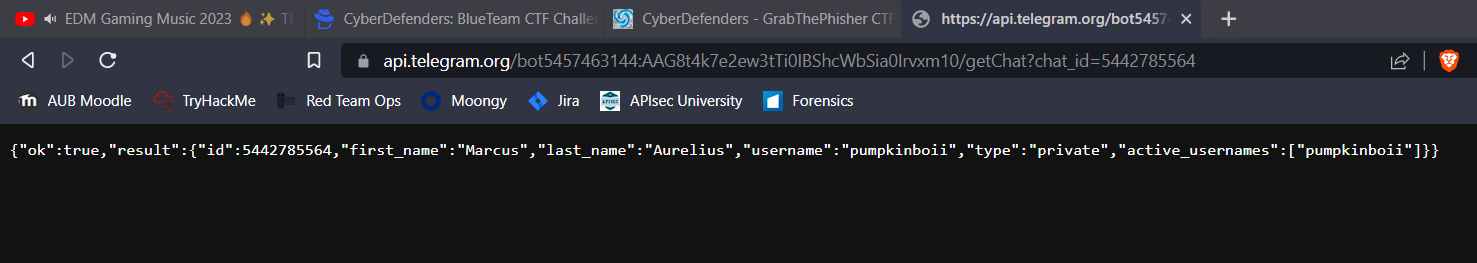
They ask next about the ChatID, which is also present in the PHP file:



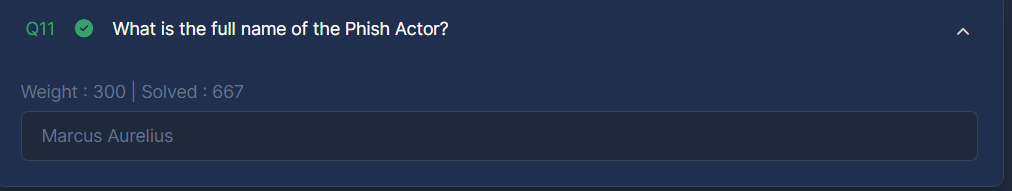
Next, they ask about the allies of the developer, which are also present in the PHP file:



Accessing the API with the required information as shown below:



We get the name of the phish actor:



We get also its username:

