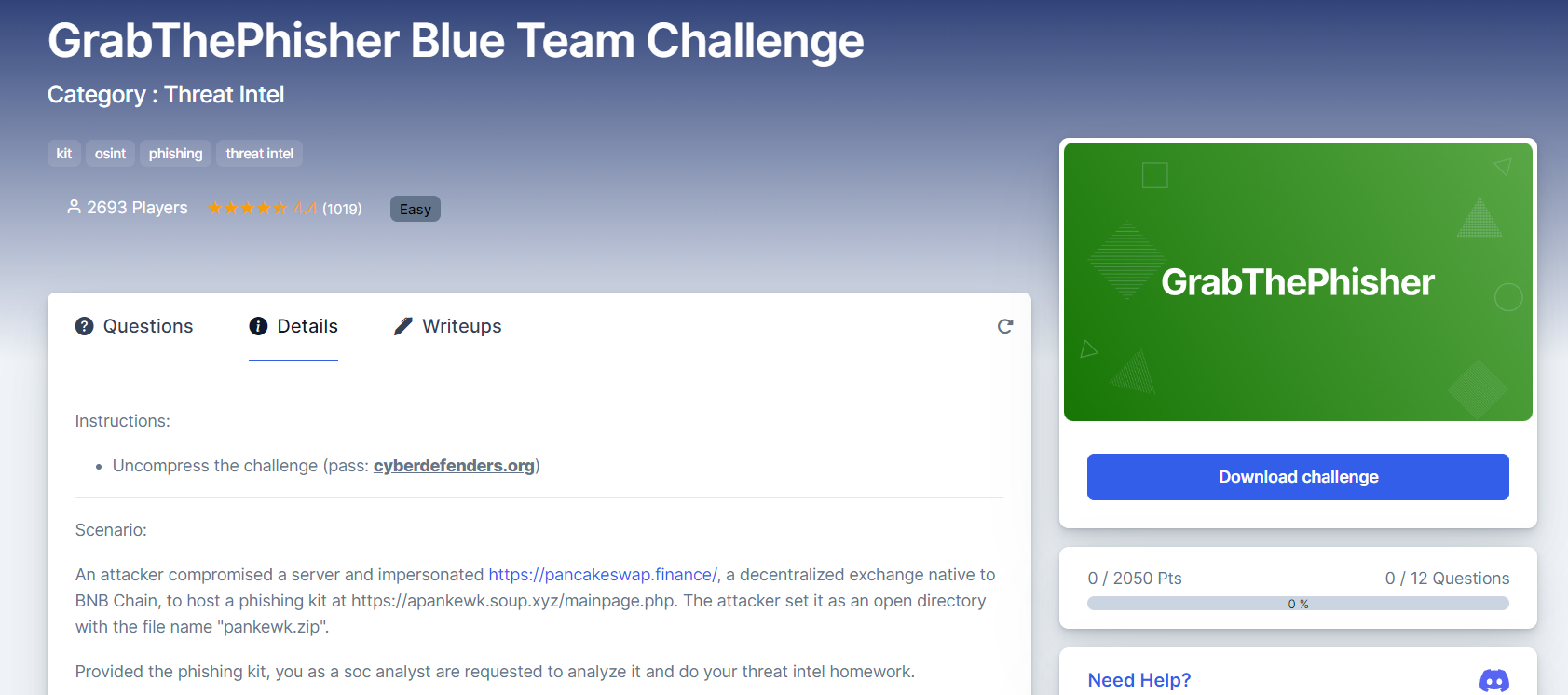
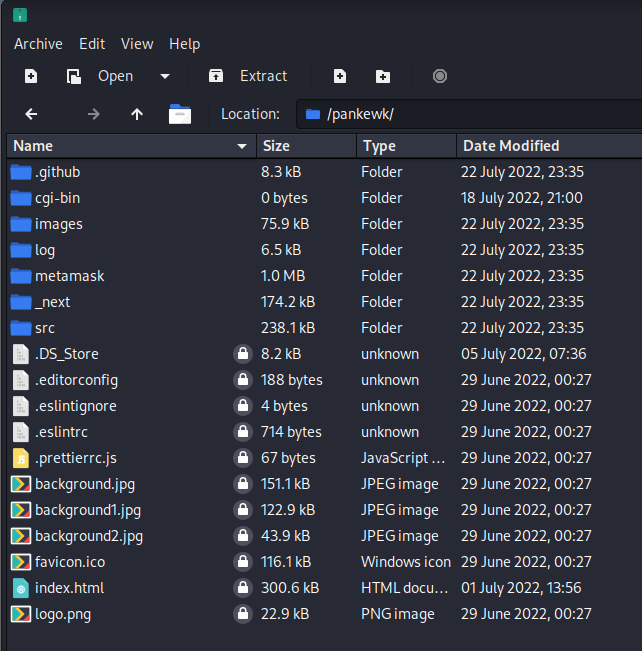
**GRABTHEPHİSHER**



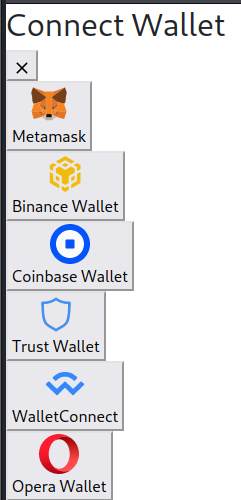
Bize bir zip klasörü veriliyor, bu klasör aşağıdaki dosyaları içeriyor. Bu dosyaları ayıklıyoruz.

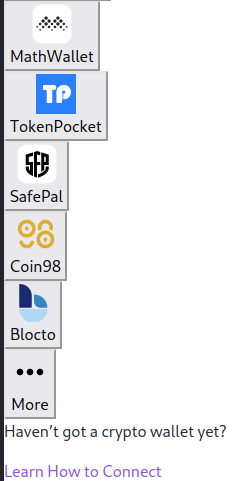


**SORU 1**

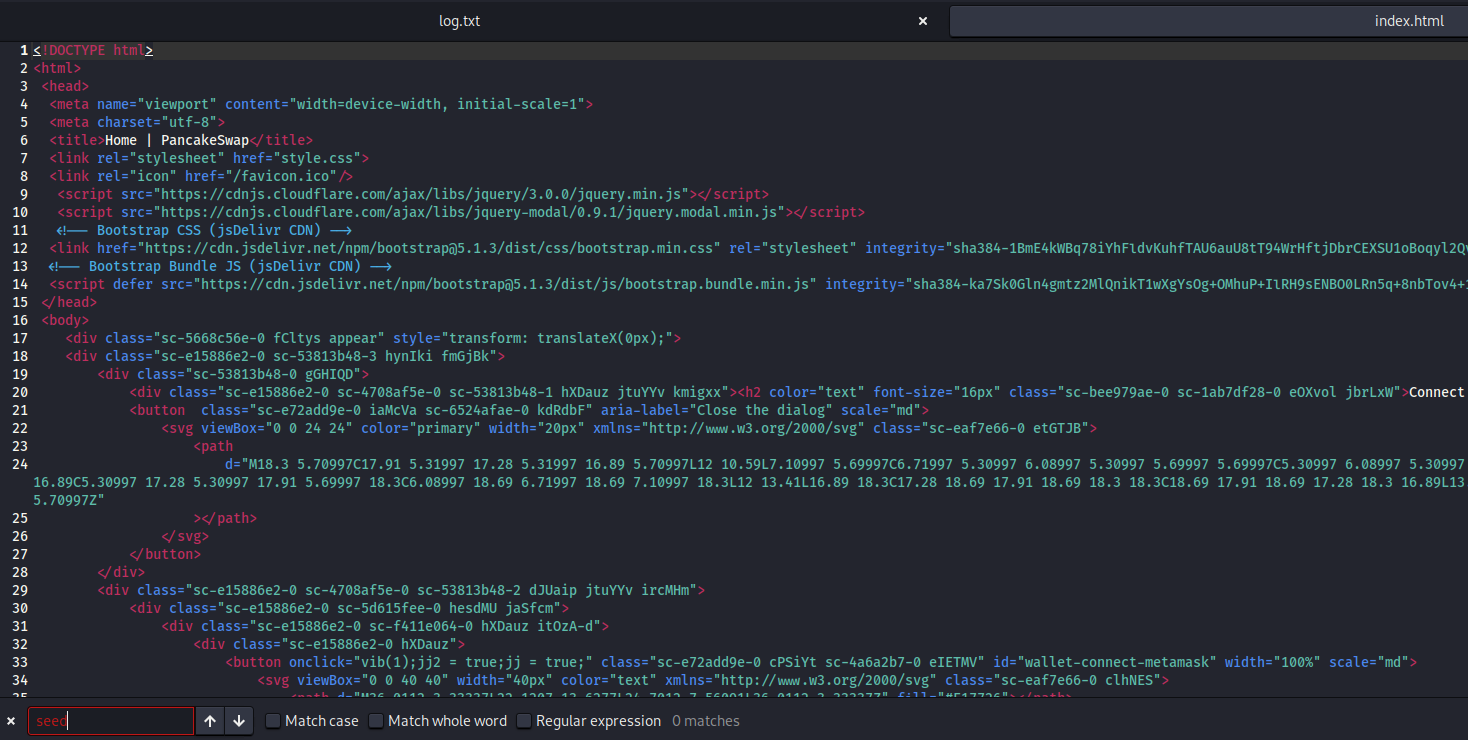
Which wallet is used for asking the seed phrase?

Tohum ifadesini sormak için hangi cüzdan kullanılır?

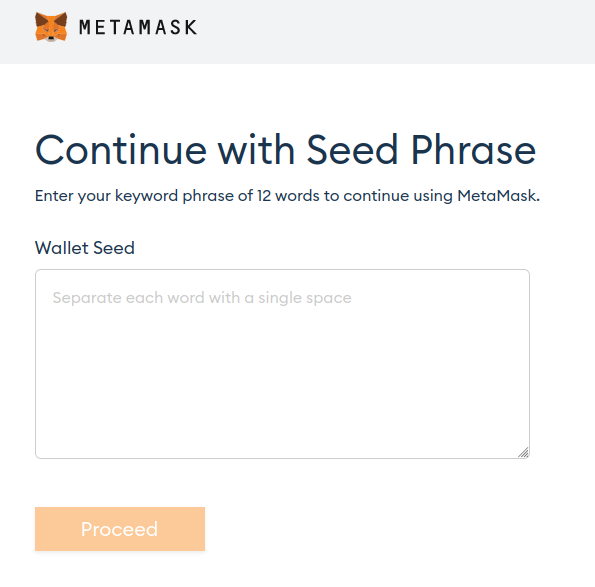




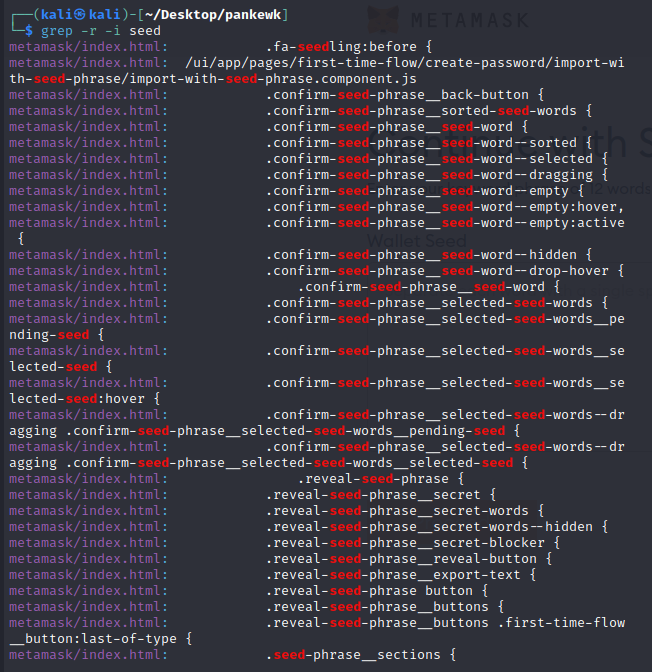
Cüzdanların hepsi yukarıda görüldüğü gibidir. Buraya index.html den eriştim. Daha sonra index.html’i txt formatında açtım seed içeren herhangi bir şey var mı bakmak için ama pek bir şey çıkmadı.



Daha sonra dosyanın içinde gezinirken metamask klasörü içinde tekrar bir index.html ddosyayı gördüm. Açınca seed’i phrase etmek için metamask’ı kullandığını görüyorum.



Ben metamask klasörünü ve içindeki html dosyasını kurcalayarak buldum ama bulamasaydım pankewk içinde grep ile bir arama yaparak da tespit edebilirdim.



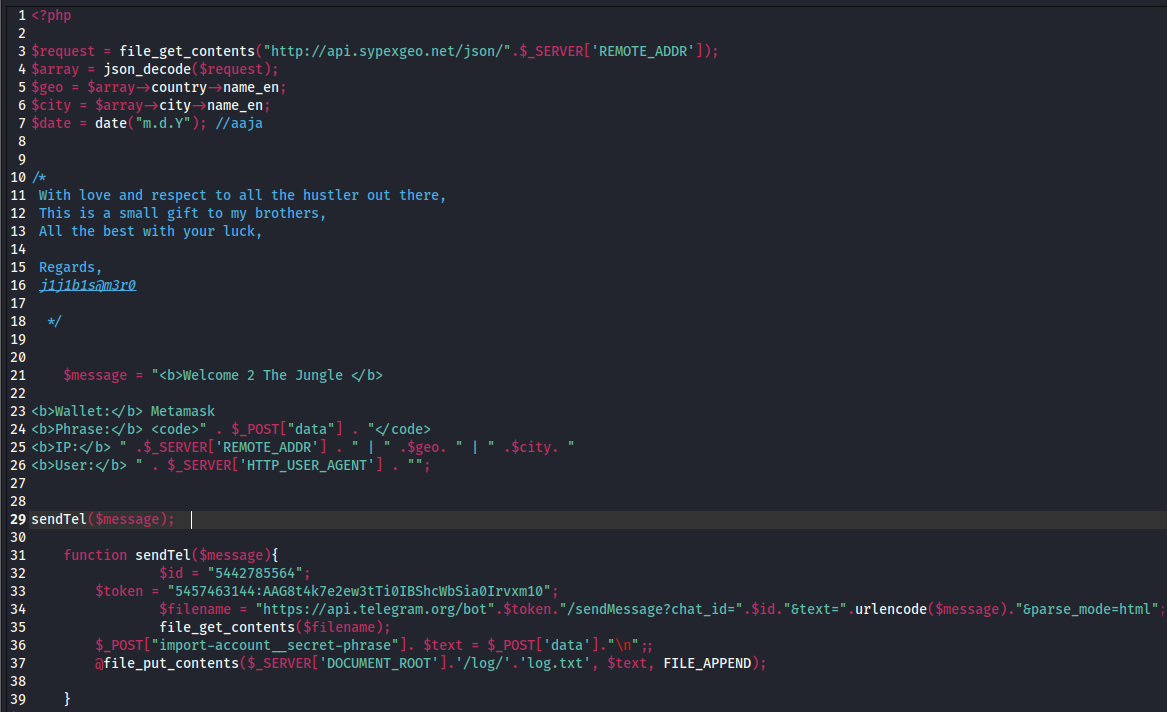
**CEVAP = Metamask**

**SORU 2**

What is the file name that has the code for the phishing kit?

Kimlik avı kitinin kodunu içeren dosya adı nedir?

Varsayım olarak da bunun yine metamask içerisinde bulunan metamask.php olduğunu düşünüyorum ama daha spesifik bir kanıta ihtiyacım var. Bu dosyayı inceliyorum.



Görüldüğü gibi 21. Satırdan başlayarak kullanıcı girişi alınıyor ve 29 dan sonraki satırlarda kullanıcıya gönderiliyor.

Aynı zamanda küçük bir not da bırakılmış yorum satırına diğer sorularda belki bize yardımcı olur o yüzden bunu da not alıyorum.

**CEVAP = Metamask.php**

**SORU 3**

In which language was the kit written?

Kit hangi dilde yazılmıştır?

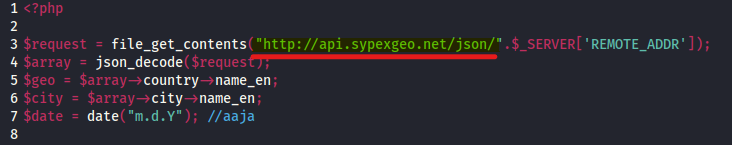
**CEVAP = Php**

**SORU 4**

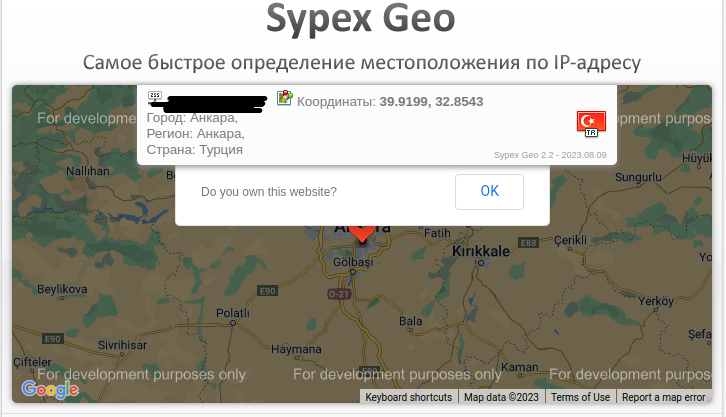
What service does the kit use to retrieve the victim's machine information?

Kit kurbanın makine bilgilerini almak için hangi hizmeti kullanıyor?

Bu hırsızlığı yine aynı kit üzerinden yaptığını düşünüyorum ve php dosyasını daha detaylı inceliyorum.



İncelemem sonucunda bu api ile ülke ve şehir bilgilerini çektiğini görüyorum. Bununla ilgili biraz araştırma yaptığımda ip bilgilerini çektiğini de görüyorum.



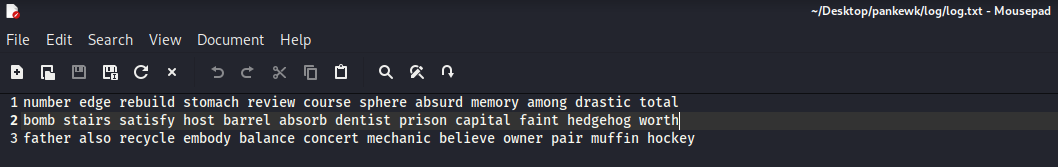
**CEVAP = Sypex Geo**

**SORU 5**

How many seed phrases were already collected?

Şuanlık kaç tane tohum cümlesi toplandı ?

Bunu log dosyalarına bakarak bulacağımı düşünüyorum. Ön incelemelerimden hatırladığım kadarıyla log dosyası elimizde mevcut. Yazdığı php kodunda bilgileri bir telegram botuna yönlendiriyordu aynı zamanda log kaydı tuttuğunu düşünüyorum.



Log dosyası içinde 3 satır mevcut. Bu satırlar seed phrase etmek için metamask cüzdanına girilecek 12 kelimelik anahtarlar, böylelikle cevabımız 3.

**CEVAP = 3**

**SORU 6**

Write down the seed phrase of the most recent phishing incident?

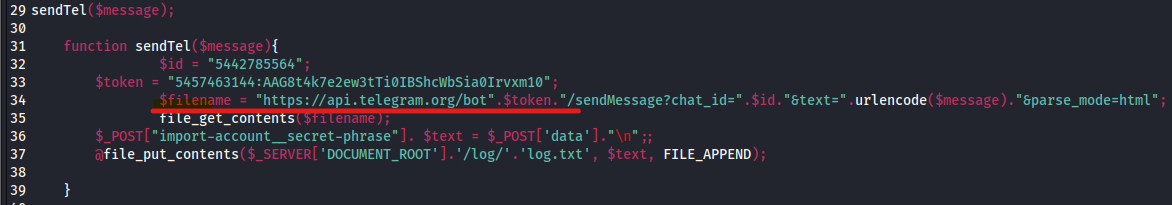
En son kimlik avı olayının temel ifadesini yazın? Diye çevirildi anladığım kadarıyla log dosyasında yer alan son key’i soruyor. Bu denemem olumlu sonuçlanıyor.

**CEVAP = father also recycle embody balance concert mechanic believe owner pair muffin hockey**

**SORU 7**

Which medium had been used for credential dumping?

Kimlik avından elde edilen bilgilerin nerede tutulduğunu soruyor ben bunu daha önceden tespit etmiştim. Php dosyasında elde edilen bilgilerin Telegram botuna göderildiğini görmüştüm.



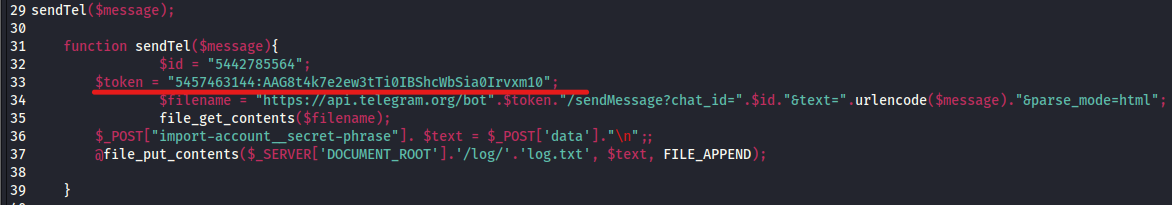
**CEVAP = Telegram**

**SORU 8**

What is the token for the channel?

Kanal için belirteç nedir?

Burada verilerin gönderileceği kanalın token bilgisini soruyor. Yine php kodundan bu token bilgisine erişebiliyoruz.

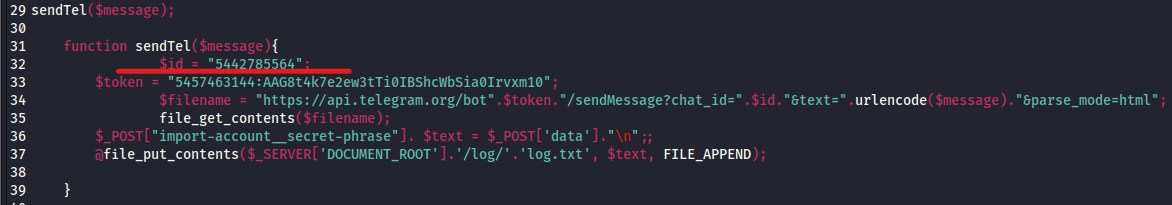


**CEVAP = 5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10**

**SORU 9**

What is the chat ID of the phisher's channel?

Burada da yine sohbet id’sini soruyor. Aynı şekilde php kodunda sohbet id’si yer alıyor.



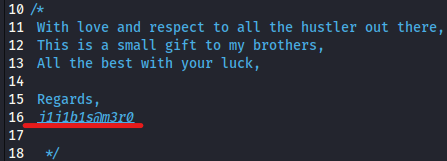
**CEVAP = 5442785564**

**SORU 10**

What are the allies of the phish kit developer?

Kimlik avı kiti geliştiricisinin müttefikleri nelerdir?

Bu soruyu görünce aklıma direkt php kodundaki yorum satırı geliyor.



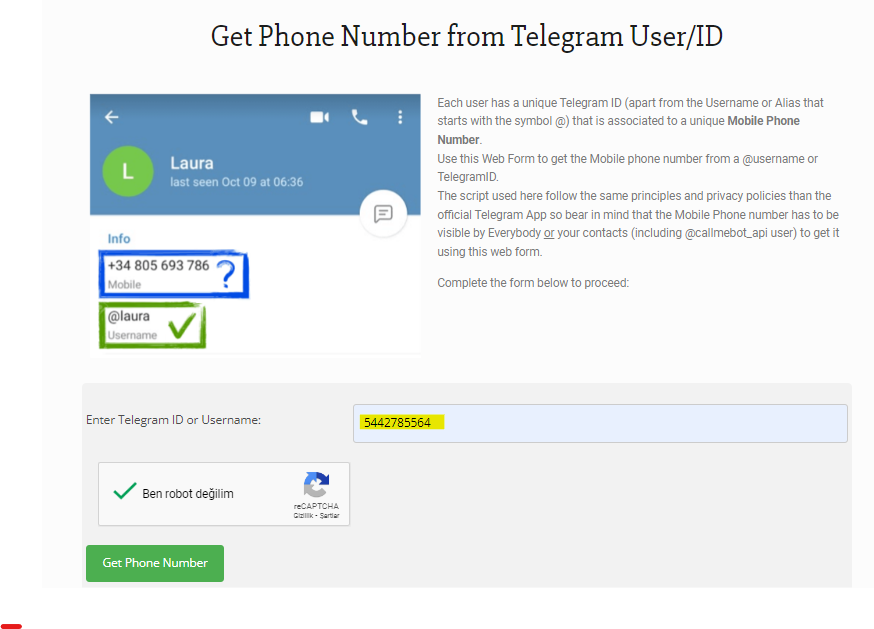
**CEVAP = j1j1b1s@m3r0**

**SORU 11**

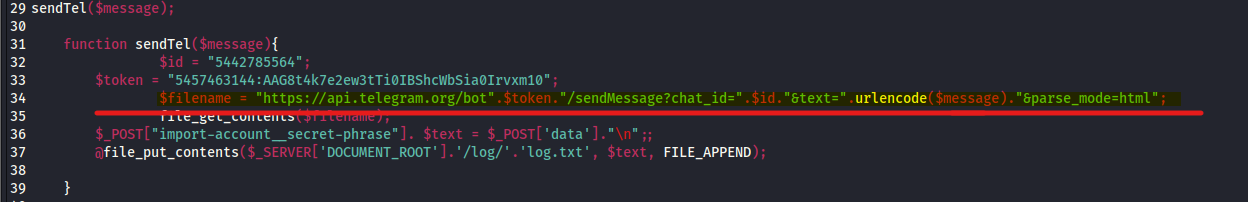
What is the full name of the Phish Actor?

Phish Actor'ın tam adı nedir?

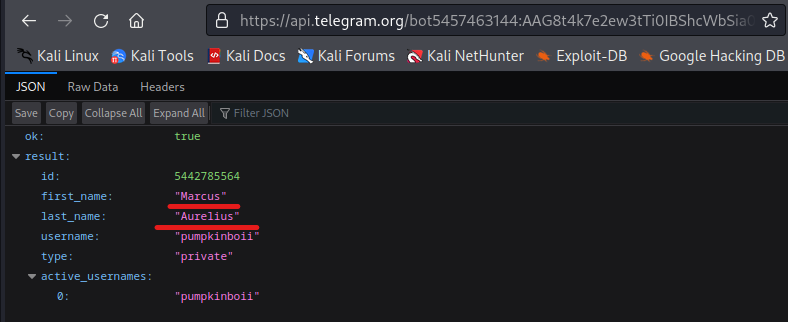
Yukarıda eriştiğim bilgilerle tam adına erişmeye çalışacağım. Telegram id’si ile bişeylere erişebileceğimi düşünüp biraz osint yapmaya çalışıyorum. Telefon numarasıyla kullanıcı adı bulan sitelerde falan bakınıyorum ama bir şeyler çıkaramadım.



Daha sonra aklıma php içindeki api’ye yaptığı istek geliyor. Buna benzer bir istek oluşturursam benden istenilen bilgilere erişeceğimi düşünüyorum.



https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getchat?chat\_id=5442785564

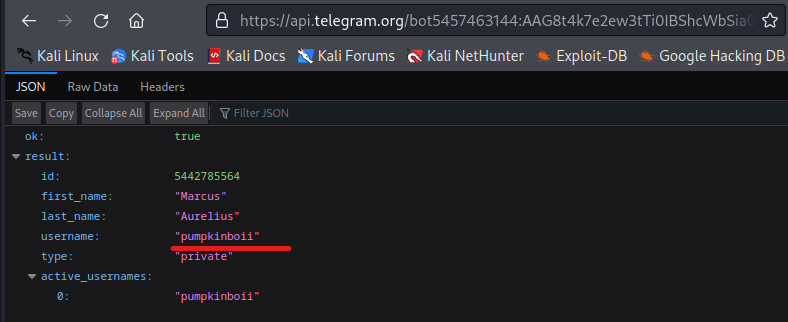


**CEVAP = Marcus Aurelius**

**SORU 12**

What is the username of the Phish Actor?

Yaptığımız istekle ad ve soyadının yanında kullanıcı adını da bulmuştuk.

****

**CEVAP = pumpkinboii**