

WU Hakamanu (Stegano)

Intitulé


La légende de Poena'iki est emplie de mystères. Nul ne sait exactement où sa mère s'est transformée en être magique. Le descendant d'un ancien tahu'a, qui possède un secret de famille, a bien voulu révéler le lieu mystique. Mais il tient à demeurer anonyme et nous a déclaré qu'il enverrait un message secret sur notre serveur Web.

Aide-nous à trouver ce lieu !

Le flag est de la forme OPENNC{xxxx}.

Solution

Préambule

Avec Google on trouve :	 <p>The screenshot shows a Google search interface. The search bar contains 'La légende de Poena'iki'. Below the search bar, there are tabs for 'Tous', 'Images', 'Vidéos', 'Actualités', 'Web', 'Livres', and 'Finance'. The 'Tous' tab is selected. The search results show a snippet from 'Destination Marquises' with the text: 'Poena'iki retourne auprès de son père à Puama'u, mais il est changé. Son expérience l'a rendu mature et il est maintenant en mesure de comprendre les mystères de la vie et de la mort. Il devient un guerrier puissant et respecté, mais il n'oublie jamais la danse de l'oiseau et l'histoire de sa mère.' Below the snippet, there is a link to 'Les légendes - TE HAAKAKAI - Destination Marquises'.</p>
-------------------------	---

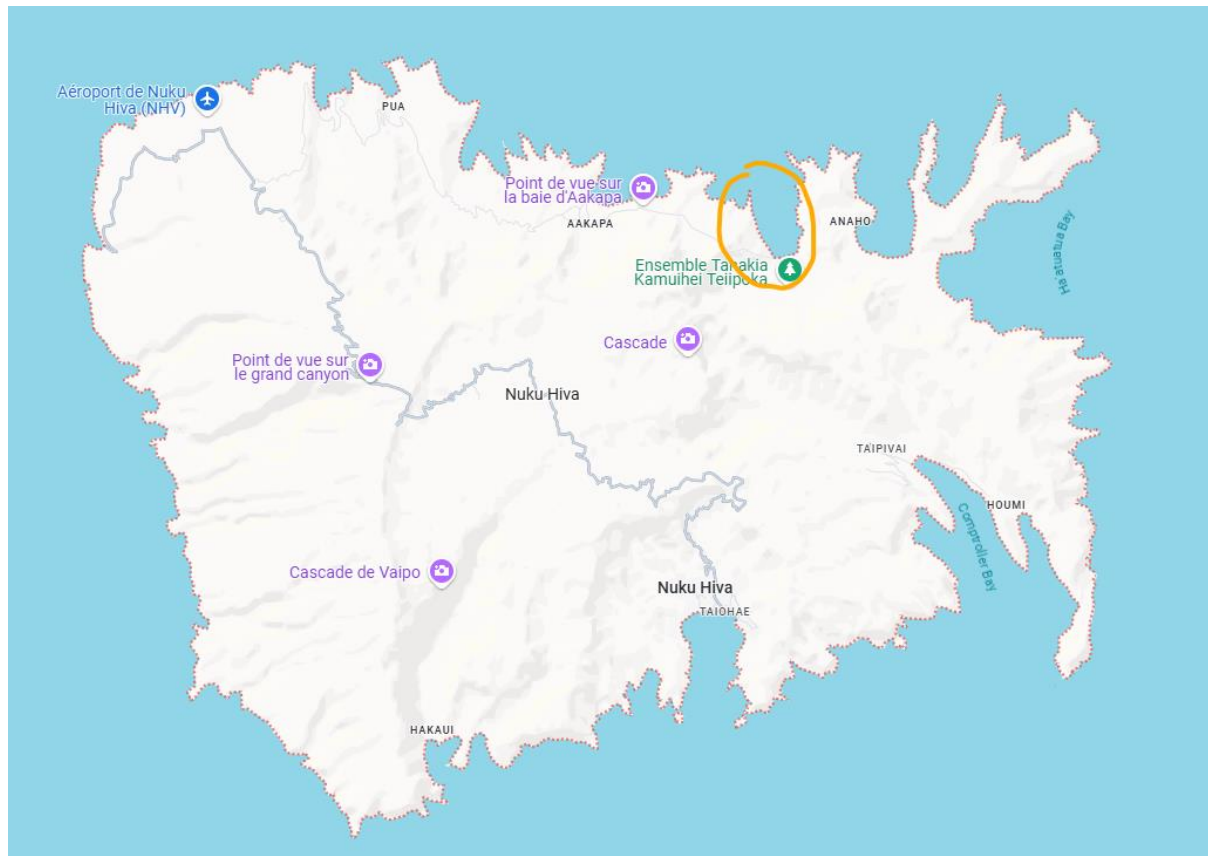
<https://destinationmarquises.com/les-legendes-te-haakakai#:~:text=Poena'iki%20retourne%20aupr%C3%A8s%20de,l'histoire%20de%20sa%20m%C3%A8re.>

La légende se passe aux Marquises, dans l'île de Nuku Hiva

Te Hakamanu signifie : la danse de l'oiseau

Dans le chall, il y a la phrase : **Nul ne sait exactement où sa mère s'est transformée en être magique.**

Or dans le texte de la légende, il est évoqué : **Elle finit par arriver à Hatihe'u et apprend la capture de son fils**





Baie d'Hatiheu

Résolution technique

Dans le fichier de logs joint au chall, on voit qu'il s'agit de logs de connexion vers le serveur Web

<https://ctf.hackagou.nc>

En examinant, on observe des requêtes « bizarres », de la forme :

```
202.22.123.20 - - [30/Sep/2024:12:06:01 +0000] "POST /home HTTP/1.1" 200 512
"https://ctf.hackagou.nc/dashboard" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36"
"data%3D%7CDBMS_PIPE.RECEIVE_MESSAGE%28CHR%28118%29%2C15%29%7C%7C"
```

Avec <https://www.urldecoder.org/> on obtient quelque chose de beaucoup plus « human readable » :

```
data=|DBMS_PIPE.RECEIVE_MESSAGE(CHR(118),15)|
```

ce qui nous intéresse, c'est 118 car la fonction CHR est liée à la conversion ASCII de 118, ici vraisemblablement en décimal, vers le caractère suivant : « **V** »

En descendant dans l'ordre des requêtes, on trouve la suite de chiffres décimaux :

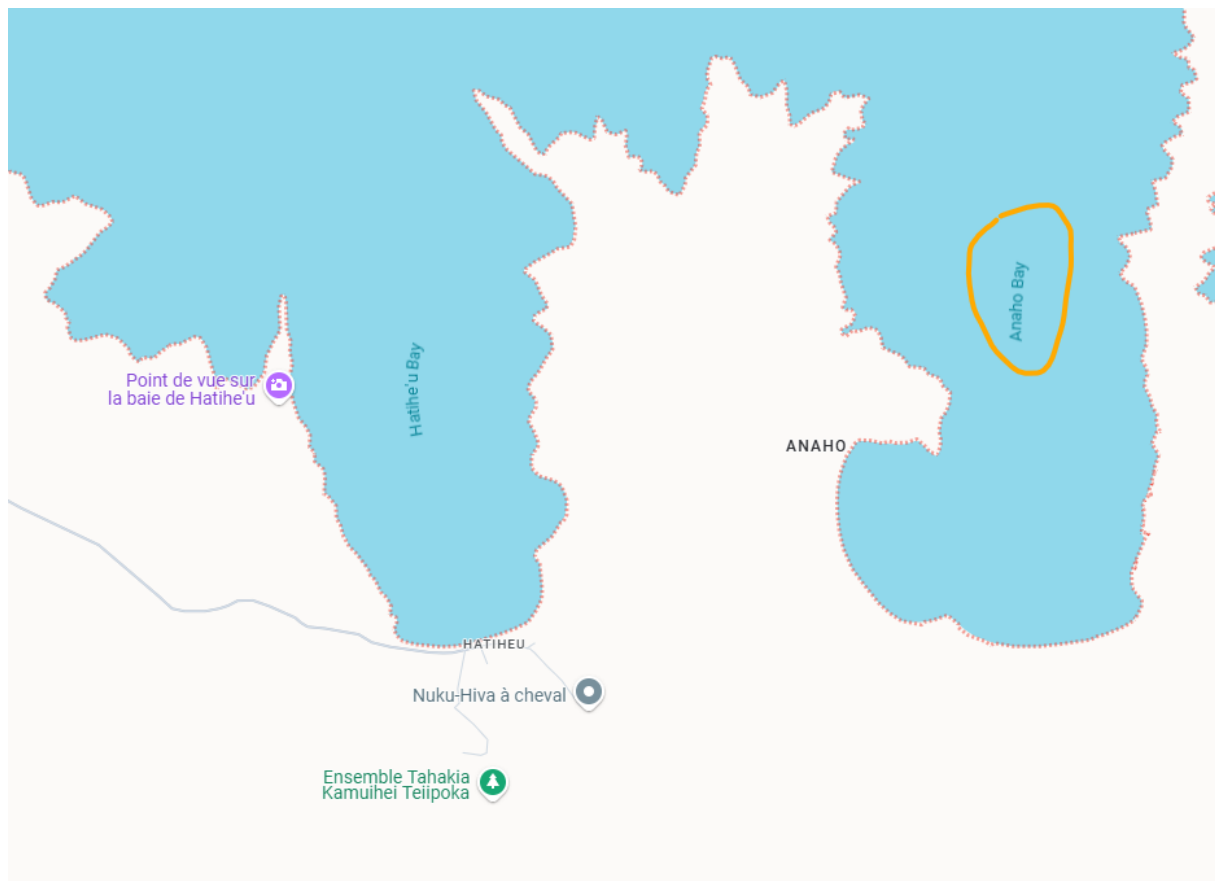
```
118 111 105 99 10532 108 101 32 102 108 97 103 32 58 32 79 80 69 78 78 67 123 65 110 97 104
48 125
```

Grâce à <https://www.dcode.fr/code-ascii> on trouve :



Flag : OPENNC{Anah0}

➔ Il se trouve que la baie d'Anaho jouxte la baie d'Hatiheu :



C'est un endroit merveilleux, j'ai eu l'occasion d'y passer quelques mois dans mon enfance (à l'âge de 11 ans).