# ***Challenge Name :- Rainforest***

**Description:** Welcome to the Rainforest Challenge! Prepare to navigate through the dense foliage of the digital rainforest, where elusive secrets await. Your task is to explore the jungle and uncover the hidden flag.

**Level:** Hard

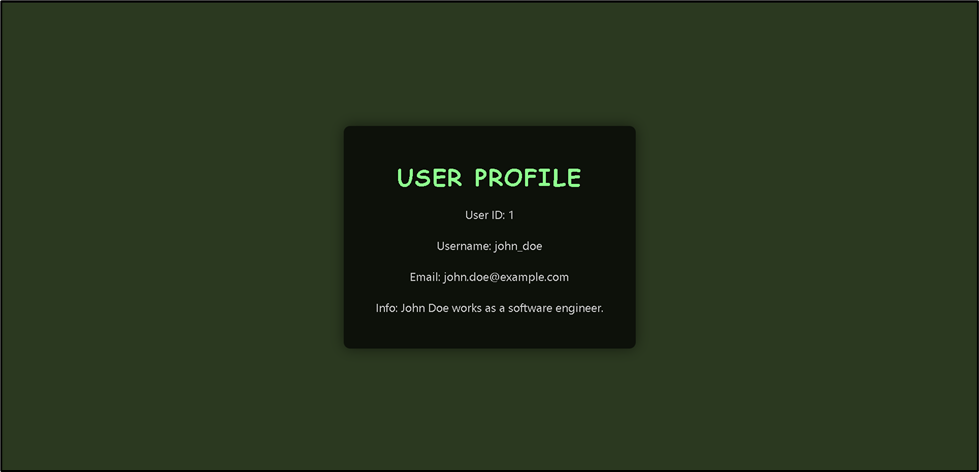
**Solution:**

In "Rainforest," exploit Insecure Direct Object References (IDOR) to decrypt hidden information and unveil the flag. Unravel the secret within the IDs. Start by exploring the main page, to get a feel for the environment.



Use trial and error to discover additional pages within the application. Try modifying the URLs by adding different parameters or values to see if it reveals new content.

[rain-forest/profile.php?userId=1](http://localhost/rain-forest/profile.php?userId=1)

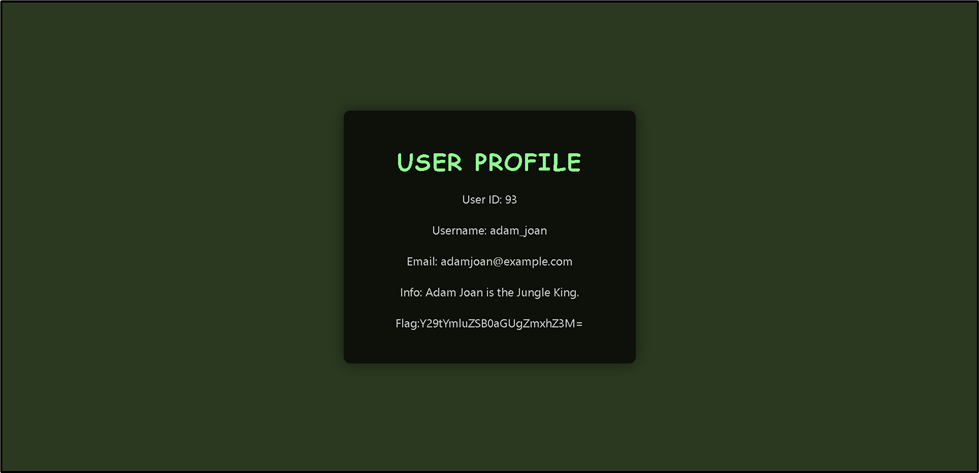


Once you discover the user profiles, begin exploring them one by one. Click on each profile to see what information is displayed and if any clues point to the flag.

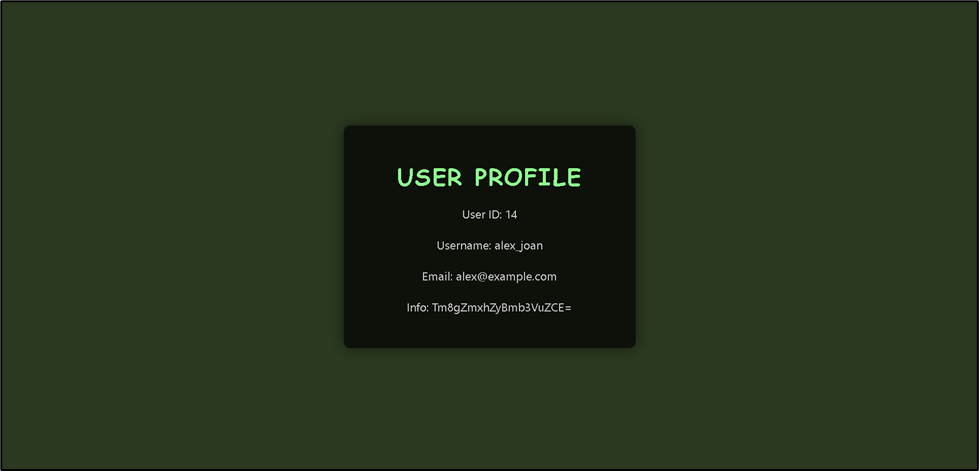
This challenge is very interesting as each user holds different information.



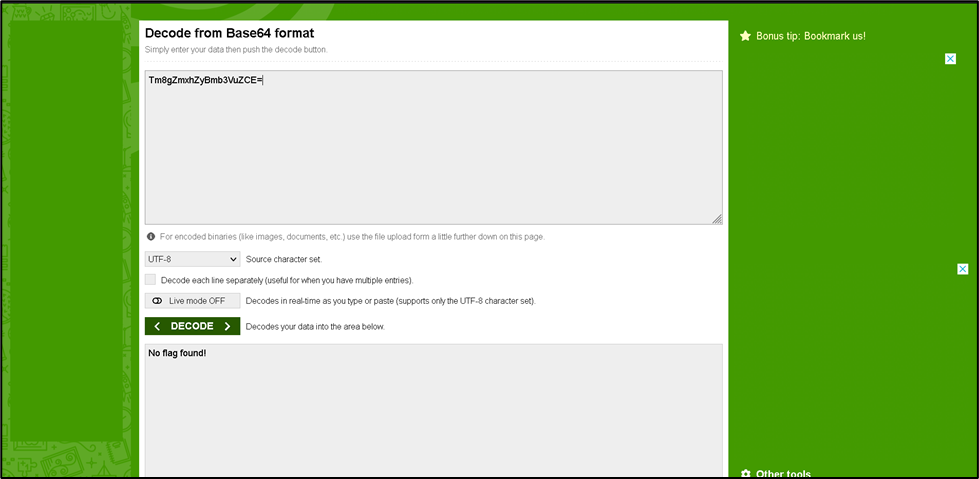
Given the large number of user profiles, it's important to approach your exploration systematically. Pay close attention to the information displayed on each profile page. Look for anything unusual or out of place that may indicate the presence of the flag.



Some users provide some specific information which is in encrypted format.



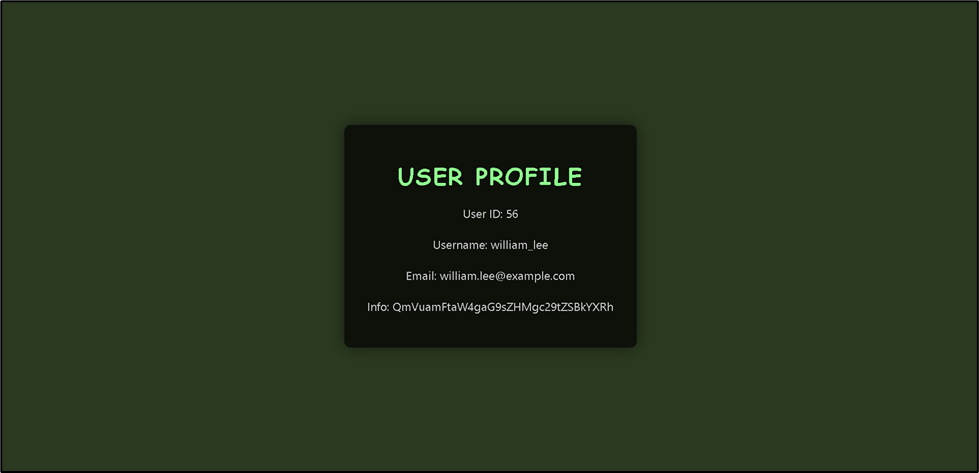
Exploring the rainforest can be challenging, but don't give up! Keep clicking through the profiles and examining the content until you find the flag. Decrypt to see what information is provided.



Now, here the information says ‘No flag found!’

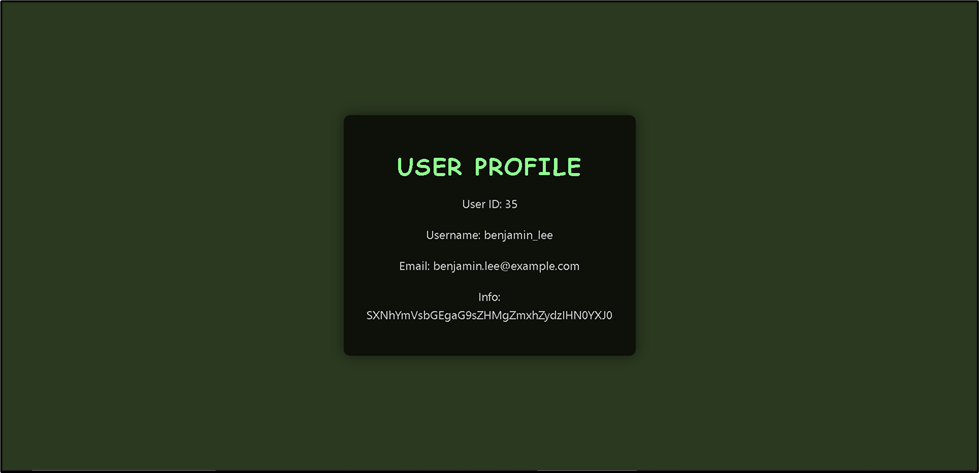
So here, the flag consists of two parts. Players must locate and decrypt the encrypted text to reveal the complete flag.

**User id – 56,**



The information says ‘Benjamin holds some data’ Now, player has to find out Benjamin

**User Id – 35 (Benjamin)**

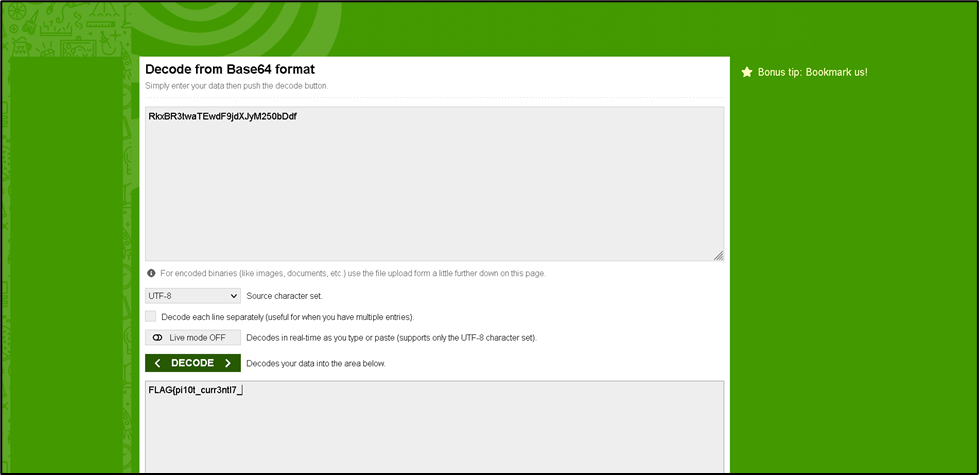


Info: Isabella holds flag's start

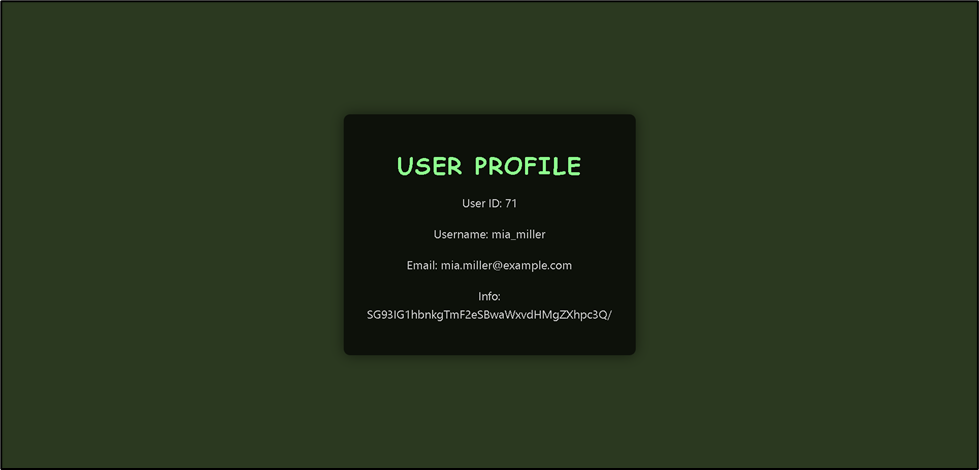
**User Id – 62**



So, Isabella holds the flag's start. Let’s decrypt the message.



Similarly, different users do have a way to the 2nd part of the flag.

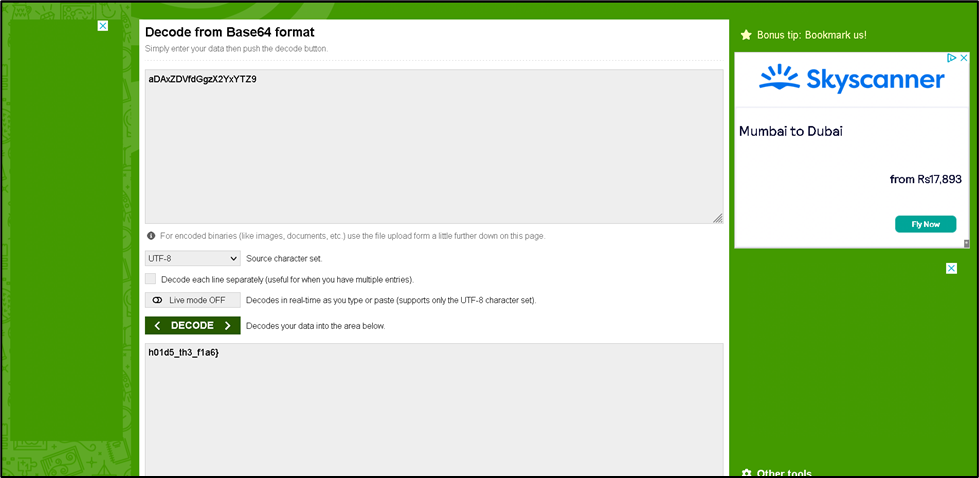


Info: How many navy pilots exist?

So let’s assume the 2nd part of the flag might be with a pilot and let’s find out how many pilots there are.

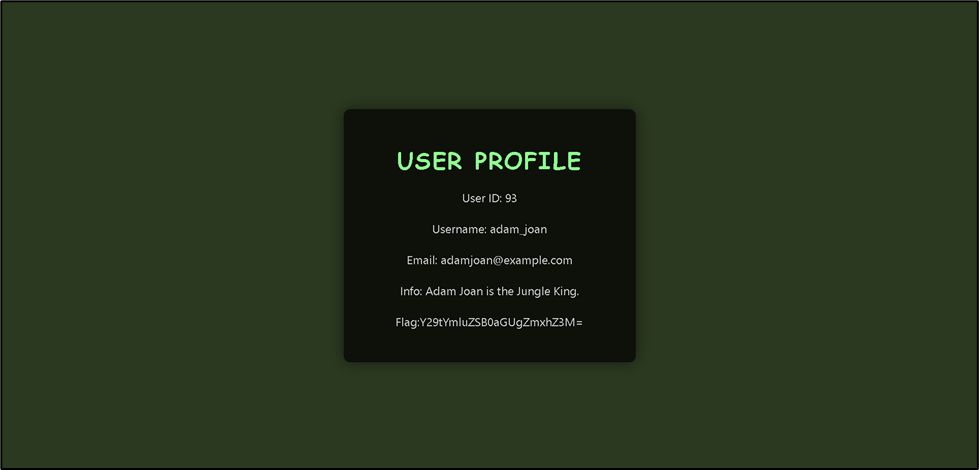
**User Id - 29**

Now. Let’s decrypt the message.



And here we found the 2nd part of the flag.

**User Id – 93**



Info – combine the flags

After combining:

**FLAG{pi10t\_curr3ntl7\_h01d5\_th3\_f1a6}**

Once you believe you've found the flag, take a moment to validate your discovery. Congratulations!

This page is intentionally left blank