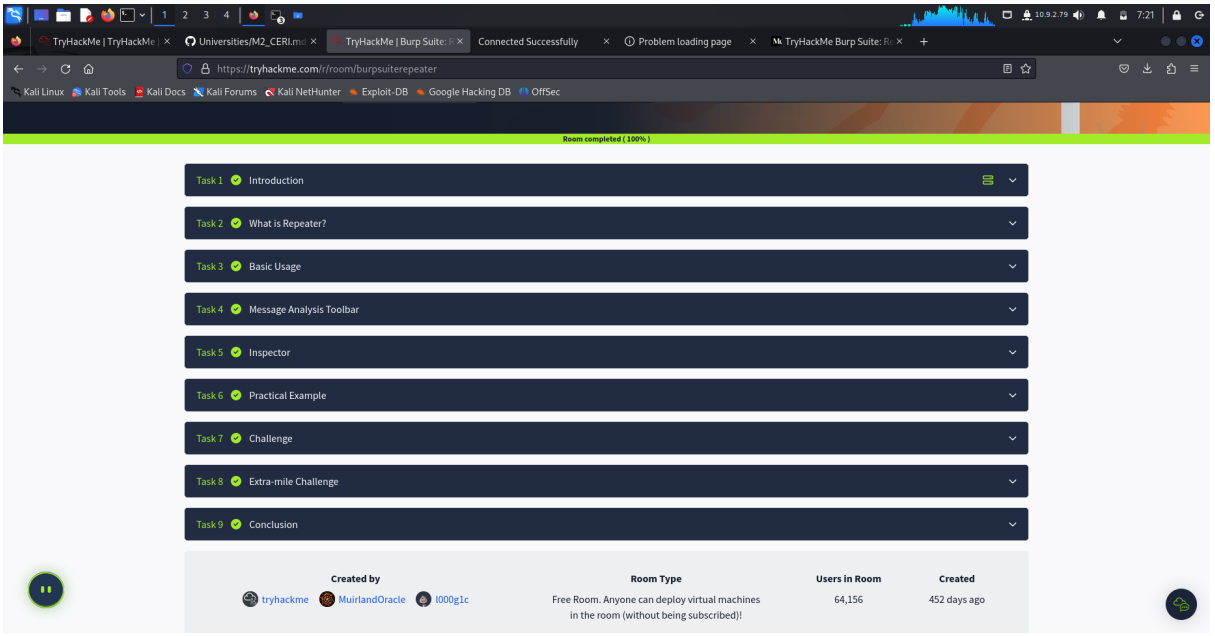
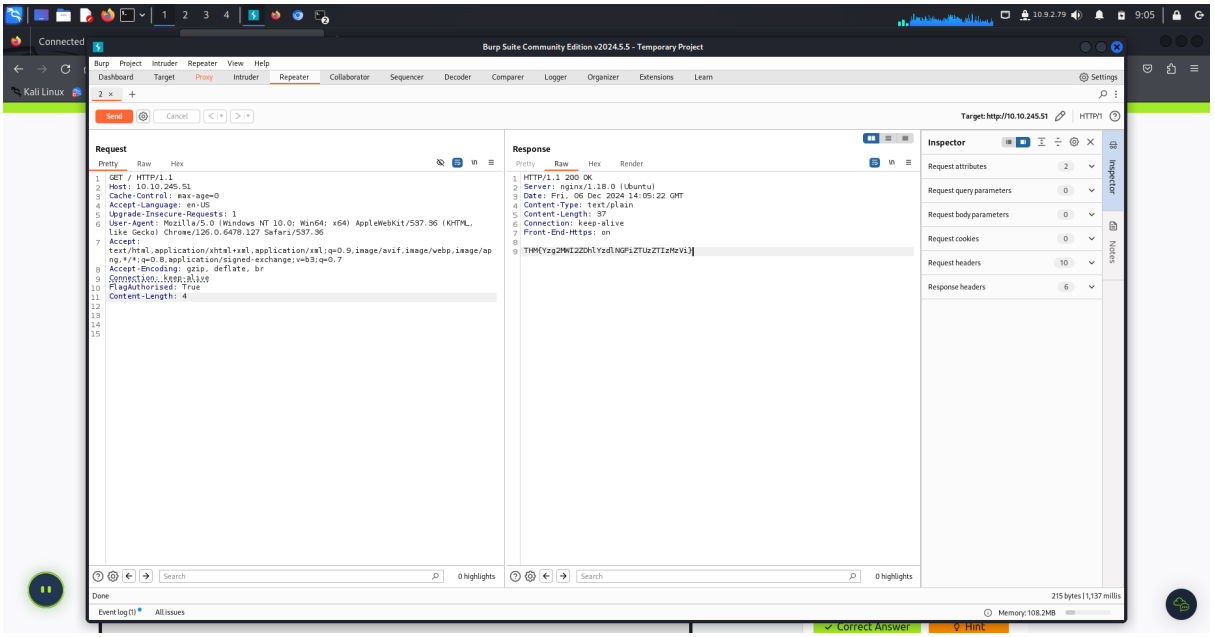
TD2 : burp

Room complété avec succès :

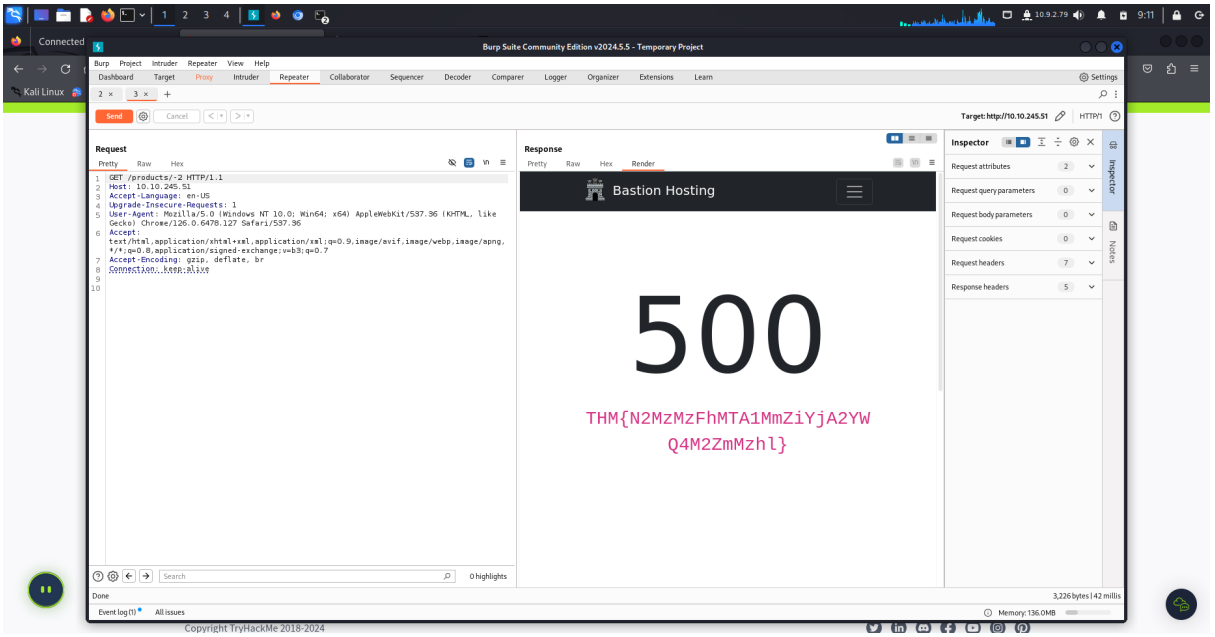


Explications des cas pratiques (récupération des flags)

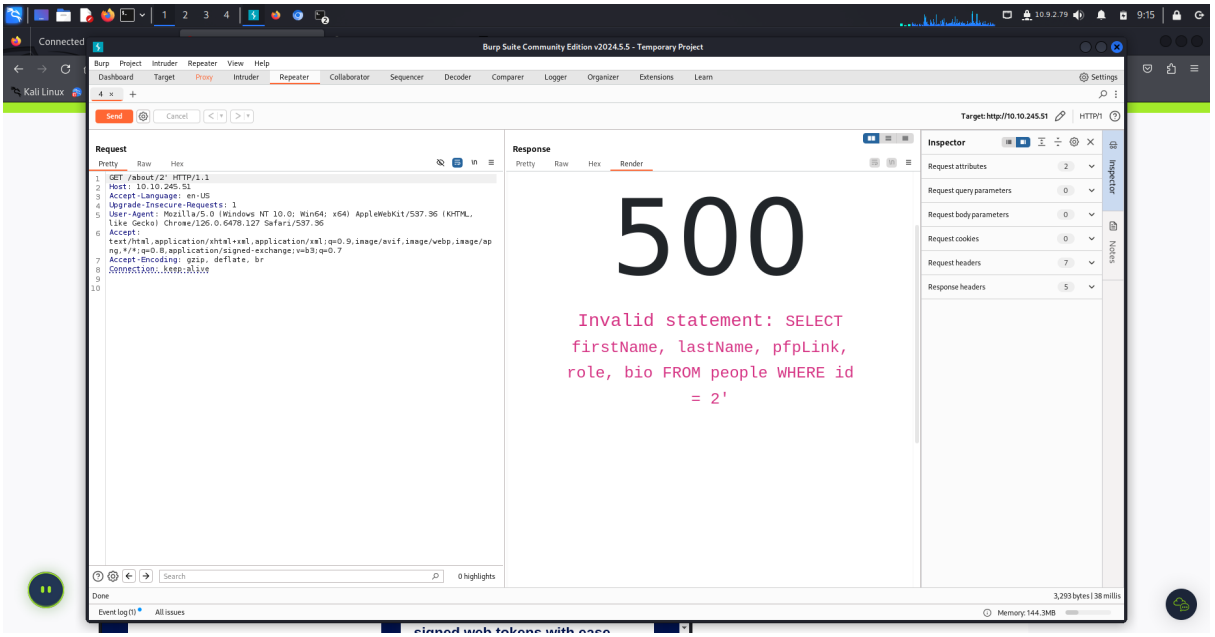
Pour récupérer le flag, on intercepte une requête HTTP avec Burp Suite, on la modifie dans **Repeater** en ajoutant un header personnalisé `FlagAuthorised: True`, puis on l'envoie au serveur. Si la requête est correcte, le flag est retourné dans la réponse.



Cette fois, on va essayer de reproduire une erreur 500 en lui donnant une un mauvaise endpoint (-2), voici le flag obtenu :



Pour le troisième flag, on va passer par de l’injection sql, on rajoute ‘ à la fin d’un endpoint comme mentionné sur tryhackme :



Voici le flag avec l'injection SQL :