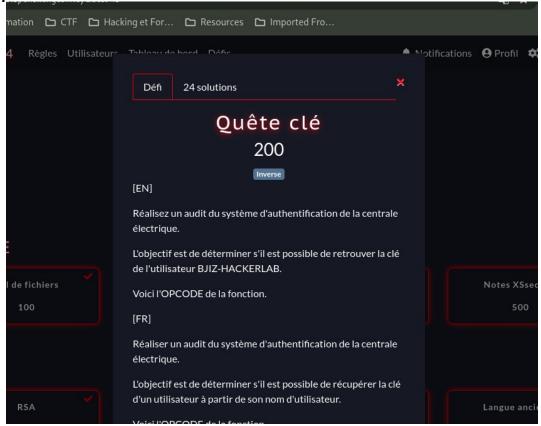
HackerLab 2024

Catégorie : Qualification Stages Challenge KeyQuest

Auteur:foundhack



Le système d'authentification décrit dans le code fonctionne de la manière suivante :

1. Initialisation et Définitions

• **Lignes 6-12:** Le code commence par définir une chaîne hint comme indice ou message d'information. Ensuite, il initialise la variable key à -9. Enfin, il crée trois fonctions (whippin5, whippin3, whippin4) en utilisant MAKE_FUNCTION. Ces fonctions seront utilisées pour des opérations spécifiques plus tard dans le script.

2. Définition des Fonctions

Fonction whippin5 (Lignes 13-15)

 Cette fonction utilise la bibliothèque md0 (probablement hashlib ou similaire) pour calculer un hachage SHA (sh) de l'entrée inpt.

Fonction whippin3 (Lignes 17-21)

 Cette fonction prépare une table de traduction (trans) pour effectuer une substitution de caractères basée sur des listes de lettres minuscules (lc), majuscules (uc), et chiffres (dc).
 Elle utilise cette table pour créer une fonction lambda qui traduit une chaîne de caractères en utilisant cette table.

Fonction whippin4 (Lignes 23-56)

Cette fonction prend deux arguments (a et b) et calcule b_etx, qui est utilisé comme un indice dans le traitement ultérieur. Elle génère une chaîne de bytes en utilisant un générateur (<genexpr>) qui effectue un XOR entre les caractères de a et b, puis encode le résultat.

3. Validation Principale (Lignes 25-92)

- **Lignes 25-44**: La validation principale commence en appelant les fonctions whippin5 et whippin4 avec les paramètres username et real_password.
 - whippin5(username, real_password) est utilisé pour générer une clé (y_key).
 - whippin4(a, b) est utilisé pour générer une chaîne de bytes (b'...').
- **Lignes 46-74 :** Si la clé générée (y_key) est égale à -9 et si username est 'BJIZ-HACKERLAB', un message de félicitations est affiché avec un drapeau construit.
- **Lignes 76-84**: Sinon, si username n'est pas 'BJIZ-HACKERLAB', un message est imprimé indiquant que la clé associée à cet utilisateur est le drapeau.
- Lignes 86-92 : En cas d'échec de la validation, un message d'erreur est imprimé.

4. Conclusion

Ce système d'authentification semble utiliser des techniques de hachage (avec whippin5), de substitution de caractères (avec whippin3), et de génération de bytes (avec whippin4) pour vérifier si un utilisateur spécifique (probablement 'BJIZ-HACKERLAB' dans ce cas) a le bon mot de passe ou clé. Si les conditions sont remplies, un drapeau ou un message de validation est affiché; sinon, un message d'erreur est affiché.

Avec l aide de chatgpt j ai ecrire un code pour déchriffée le message car moi je ne suis pas bon dans le domaine du rev

```
File Edit Selection Find View Goto Tools Project Preferences Help
       bb.py x voutu4t.py x v serveu.py x v rsa (2).py x v oRutput.txt x v ste.py x v keygenme-trial.py x v lab.py — hacl x v lab.py — Musique
       import hashlib
import string
       #·Fonction·pour·hasher·en·MD5
def hash_md5(input_str):
           return hashlib.md5(input str.encode()).hexdigest()
       def permute_chars(n):
    lc = string.ascii_lowercase
    uc = string.ascii_uppercase
    dc = string.digits
            trans = str.maketrans(
    lc + uc + dc,
    lc[n:] + lc[:n] + uc[n:] + uc[:n] + dc[n:] + dc[:n]
            return lambda s: s.translate(trans)
       # Fonction pour décrypter avec XOR
def xor_decrypt(a, b):
    b_extended = b * (len(a) // len(b) + 1)
    return ''.join(chr(ord(c) ^ ord(d)) for c, d in zip(a, b_extended))
       # Clé initiale de permutation initial_permutation = -9
       decryption_permutation = -initial_permutation
       # Données cryptées
donnees_cryptees = 'dpjLgviGRJJN1IUUFeKu1ls8'
       # Décryptage des données
donnees_reelles = permute_chars(decryption_permutation)(donnees_cryptees)
                                                                                                         kali@kali: ~/Musique
                                                                          ×
    -(kali⊗kali)-[~/Musique]
 __s python3 lab.py
Données décryptées : mysUperPASSW0RDD0nTd0ub7
Voici le Flag: HLB2024{b024de49126f7475451e90b383acefeb}
   —(kali⊛kali)-[~/Musique]
-$ [
```