UQAC
Université du Québec
à Chicoutimi

6GEI186 - Architecture des ordinateurs

BONUS : Travail 4 – Trouver le Mot de passe Original du Programme

Remis à : Prof. Jérémy Bouchard

Par:

David Chalons – CHAD17070000

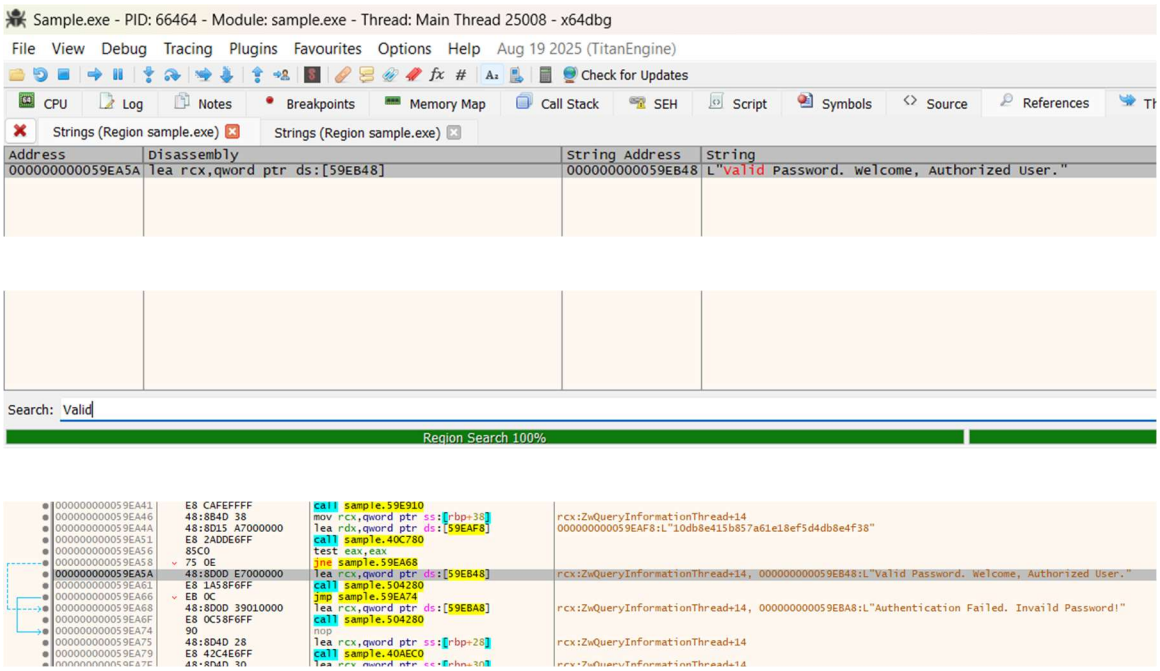
Mobina Shamsadini – SHAM1352060

Samara Boudreault – BOUS08610400

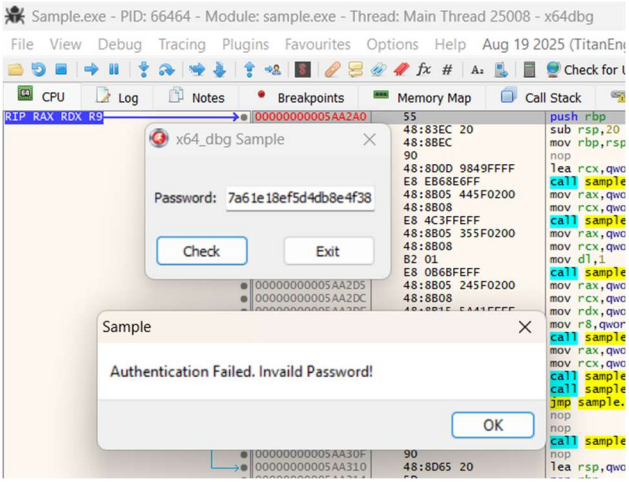
Bonus : Trouver le Mot de passe Original du Programme

Explication de la démarche utilisée

Premièrement, nous avons localisé l'endroit où se trouve le message de succès « Valid Password. Welcome, Authorized User. » à l'aide de l'option **Az** (recherche de chaînes de caractères) dans x64dbg.

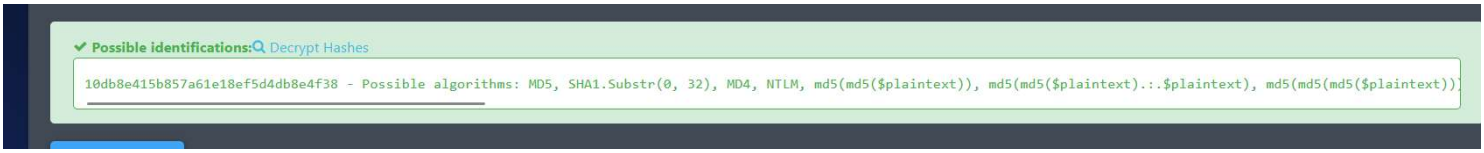


Par la suite, nous avons analysé les instructions qui gèrent la saisie du mot de passe et nous avons également remarqué une instruction *lea* qui charge dans *rdx* l'adresse d'une chaîne de caractères constants. Cette chaîne est ensuite utilisée dans un appel de fonction où elle est comparée avec la valeur de l'entrée utilisateur. Nous en avons conclu que la valeur pointée par *rdx* représentait la référence utilisée pour valider le mot de passe.

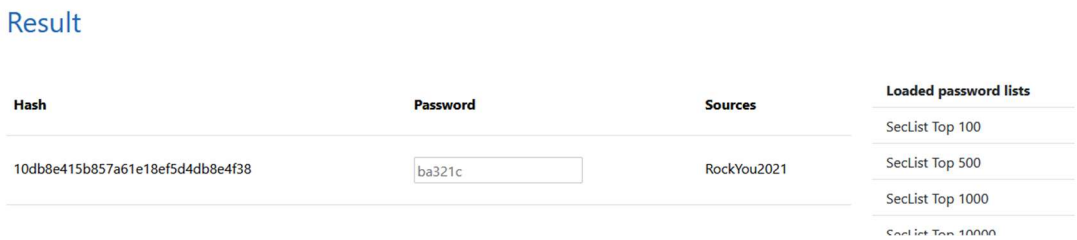


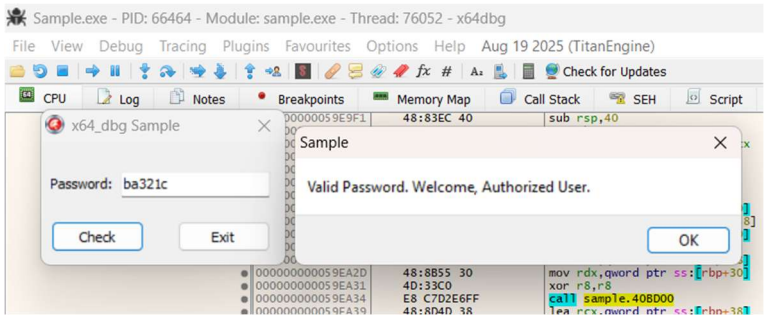
En observant cette chaîne, nous avons constaté qu'il s'agissait d'une suite de 32 caractères hexadécimaux. En la testant directement comme mot de passe, cela ne fonctionnait pas, ce qui confirmait qu'il ne s'agissait pas du mot de passe en clair, mais d'un hash.

Avec un site[1] pour détecter quel type d'encryptions c'était nous avons trouvé hash MD5.



Nous avons ensuite copié cette valeur de hachage et l'avons soumise au site *HashLookUp*[2], qui nous a retourné la chaîne de caractères suivants : « ba321c ». Enfin, après avoir essayé « ba321c » dans le programme original (non modifié), nous avons confirmé qu'il s'agissait bien du mot de passe correct.





[1] https://hashes.com/en/tools/hash_identifier
[2] https://binsec.tools/lookup/hash/