Challenge 1 Web Server http open redirect.

En lisant l’énoncé, j’ai cru que je devais juste changer le lien des boutons par on autre site.

J’ai donc remplacé tout le lien pour <https://google.com> mais ça ne fonctionnait pas.

Pour mieux comprendre le challenge, j’ai donc cherché le titre « open redirect ».

J’ai donc compris comment se composait un lien web de redirection : le site et les paramètres, leurs mauvaises utilisations peut créer des vulnérabilités (diriger vers un site avec virus).

Revenons au problème, j’ai copier les paramètres sur google et on me donne comme site correspondant facebook par décryptage des paramètres (MD5).

Alors pour changer le lien complet du button, il faut donc changer les deux parties du lien.

La première sera <https://guillaume.com>, et pour les paramètres je suis allé sur un site pour le hash MD5 afin de faire correspondre les paramètres au site guillaume.com.

On finit avec : (qu’on remplace dans le html).

<https://guillaume.com&amp;h=0d971f0b58dbace59e01ae2679fa6bad>

Second challenge; Cryptanalyse Encodage ASCII

Pour trouver le mdp je dois décoder cette ligne.

Cette ligne de données est encodé, cela veut dire qu’elle n’est pas en ASCII, j’ai donc copier la ligne dans un convertisseur ASCII, en ayant le résultat en outpout, j’ai cru que le mdp à rentrer était un mdp sous forme de texte.

En me rendant compte que ce n’était pas le cas j’ai juste copier le code sous forme ASCII est ce fut le bon mot de passe.

Voici le résultat: 2ac376481ae546cd689d5b91275d324e