Hidden field exploit

Il s’agit d’exploiter des champs caché contenant des informations d’envoi de données

Exploration

Quand va sur la page pour se connecter un repère très vite un lien en cas d’oubli de mot de passe. Cette page ne contient qu’un simple bouton submit.

Offensive : 2 méthodes

Méthode 1 : avec burp suite

J’ai suivi le tutoriel https://portswigger.net/burp/documentation/desktop/getting-started/modifying-http-requests pour modifier les requêtes http avec le logiciel burp suite en ayant pour cible la page http://10.14.200.234/?page=recover
On repère une requête en particulier (cf requete_target.png) on l’envoie à un répétiteur pour pouvoir modifier le paramètre « mail » du corps de la requête (cf flag_get.png) une fois la requete modifiée envoyer on récupère le flag

Méthode 2 : avec firefox

On a inspecte la page http://192.168.1.16/?page=recover#, on inspecte le bouton submit et on voit qu'il y a un input cache avec le mail écrit en dur. Après le submit, on va dans l'onglet réseau on regarde la requête POST et on la modifie pour la renvoyer. on change le corps du message et on obtient le flag

Faille

Il y a qu’une adresse pour envoyer de requête pour recouvrer un mot de passe et celle-ci est écrit en clair dans le code de la page.

Mitigation

Plutôt que de faire une page avec un simple bouton subit, il faudrait un champ avec une adresse mail. Lors de l’envoie de la requête, on vérifie que le mail donné correspond à un compte enregistré et on envoie une page par mail pour récupérer le mot de passe.

Sources

- https://portswigger.net/burp/documentation/desktop/getting-started/modifying-http-requests