Brute force sign in

Le procédé consiste à lancer des requêtes avec différents username et/ou mot de passe de façon automatique jusqu'à ce qu'on trouve un couple solution.

On a constaté que quand on essayé de se connecter sur le site, le contenu des variables username et password était écrit en clair dans la barre d'adresse.

Exploration

Tim, nous a conseillé de faire un brute force avec un logiciel nommé hydra https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/ et d'autres amis nous ont parlé de kali https://www.kali.org/get-kali/#kali-virtual-machines

Quand on avait cherché le flag dans la barre « member search by id », on avait pu récupérer pas mal d'infos sur les différents membres enregistrés tels que first_name et last_name mais pas de username (http://10.13.200.240/?page=member&id=1+or+true+union+select+first_name%2C+last_name+from+users&Submit=Submit#) je suis donc partie sur ces infos comme indice pour le username et j'ai tenté de brute force avec hydra en utilisant rockyou.txt comme dictionnaire de mot de passe.
La ligne de commande pour brute force avec hydra ressemble à ça :

```
hydra -l two -P /usr/share/wordlists/rockyou.txt 10.13.200.240
http-get-form "/:?
page=signin&username=^USER^&password=^PASS^&Login=:Home"
```

^USER^ est la variable utilisée pour le username et renseignée par l'option -l
^PASS^ est la variable utilisée pour le password et renseignée par l'option -P (en majuscule c'est pour utiliser les éléments d'une liste).
Ce fut un echec.
On nous a alors conseillé de refouiller la DB et de regarder un « rang au dessus » pour voir toutes les basses et de faire un script de test pour le brute force.
Grace au site https://dev.mysql.com/doc/refman/5.7/en/information-schema-schemata-table.html « 1 or true union select schema_name, catalog_name from information_schema.schemata » donne un résultat intéressant (cf nameetcatalogfromschemata.png)
Face aux difficultés rencontrées pour inspecter le contenu des autres databases, je me lance dans l'écriture d'un script en bash pour faire le brute force.

Offensive

J'ai lancé mon script avec « admin » en tant que username et j'ai pu trouver un mot de passe correspondant ce qui m'a donné le flag.

Faille

Les requêtes se font directement via l'adresse avec l'écriture en clair du mot de passe et du username est une première faille. La choix du username pour le compte admin est une deuxième faille

Mitigation

Les requêtes ne devrait pas se faire via l'adresse mais via des post (par exemple) avec les mots de passes stocké chiffré. Choisir autre chose, de moins évident pour le username administrateur. Imposer des mots de passe mieux sécurisé (minuscule, majuscule, chiffre, caractère spécial et taille minimal). Imposer un délais entre plusieurs tentatives erronées

Sources

- https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/
- https://www.kali.org/get-kali/#kali-virtual-machines

- https://dev.mysql.com/doc/refman/5.7/en/information-schema-schemata-table.html
- https://medium.com/securebit/brute-forcing-using-custom-shell-scripts-abf73eaf9cda
- https://linuxhint.com/curl_bash_examples/
- https://debian-facile.org/doc:programmation:shells:script-bash-variables-arguments-parametres
- https://stackoverflow.com/questions/25877637/while-variable-is-not-equal-to-x-or-y-bash
- https://www.cyberciti.biz/faq/unix-howto-read-line-by-line-from-file/
- rockyou.txt https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiq8b3jp7j-AhUMif0HHVVYB5QQFnoECAgQAQ&url=https%3A%2F%2Fgithub.com%2Fbrannondorsey%2Fnaive-hashcat%2Freleases%2Fdownload%2Fdata%2Frockyou.txt&usg=AOvVaw3snAERl1mU6Ccr4WFEazBd