Bouti-Mazouz Samy/Kapri Anish

Faille XSS

I. La faille XSS

L'attaque XSS, également appelée cross-site Scripting est une attaque qui consiste en le fait d'exploiter une faille du site afin de pouvoir injecter du code malveillant en HTML ou en JavaScript dans des variables qui sont mal protégées dans le script.

Cette attaque peut être réalisée de façon unitaire, c'est-à-dire que l'attaquant va l'exécuter une seule fois par l'envoi d'un formulaire ou bien stockée dans un fichier ou en base de données afin que celle-ci puisse être rejouée à chaque visite d'une page du site web.

II. XSSER

Afin de diagnostiquer le site web et repérer les différentes failles XSS, nous allons utiliser le logiciel XSSER sous Kali Linux qui permet de tester, exploiter et rapporter la plupart des combinaisons possibles de failles XSS sur un site web.

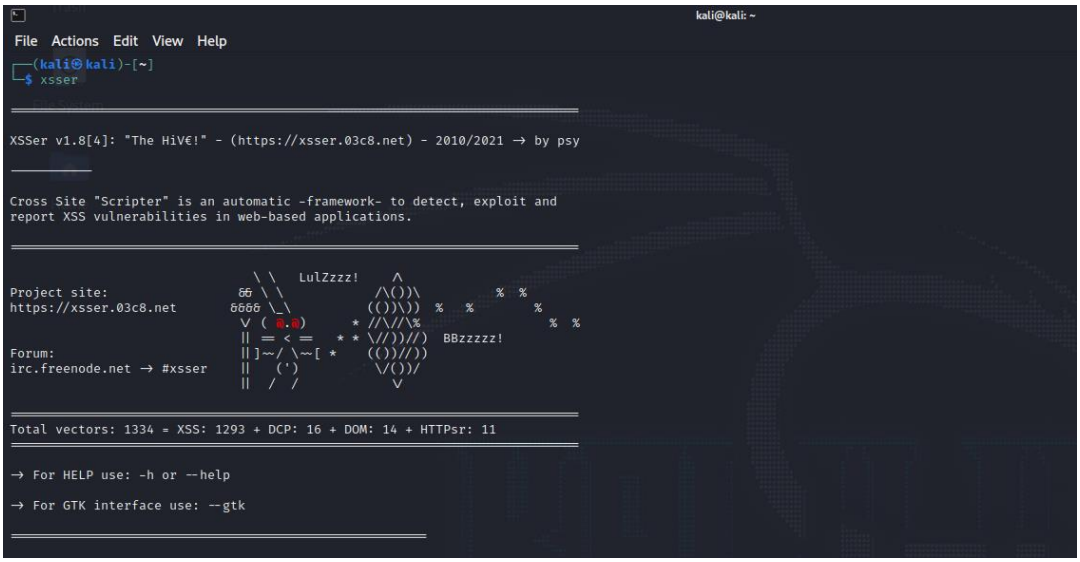
Pour ce faire, nous allons installer le logiciel XSSER en mettant à jour, dans un premier temps, la base de données APT de linux avec cette commande :

sudo apt-get update

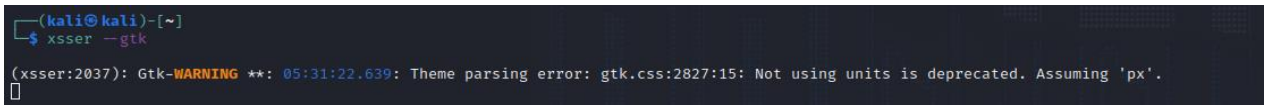
Puis dans un second temps, installer XSSER avec la commande suivante :

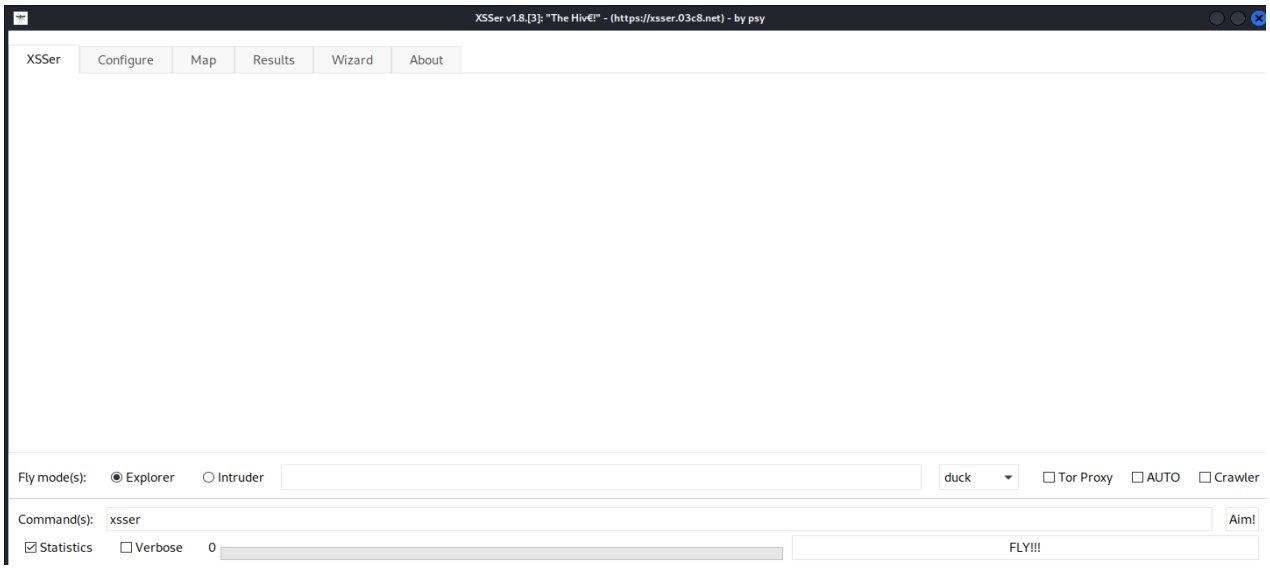
sudo apt-get -y install xsser

Nous pouvons maintenant utiliser XSSER en saisissant xsser comme commande dans le terminal



Mais pour davantage de simplicité, nous allons utiliser l'interface graphique XSSER avec la commande suivante : xsser --gtk





Pour les options à cocher, Intruder spécifie qu'il faut cibler la cible donnée juste à droite. Auto permet d'automatiser toute la procédure et crawler parcours les liens disponibles sur la page cible. Lors du clic sur le bouton « FLY !!! », XSSER procède au scan via une ligne de commande et délivre un rapport sur les failles trouvées ou non.

III. L'en-tête X-XSS-Protection

La mise en place d'une en-tête X-XSS-Protection constitue une protection contre les attaques de type Cross-Site Scripting. Cet en-tête peut être réalisée au niveau du site internet dans le fichier htaccess dans la section mod_headers

<IfModule mod_headers.c>

Header set X-XSS-Protection "1; mode=block"

</IfModule>

Ou dans les fichiers de configuration Apache, il suffit d'éditer ce fichier :

/etc/apache2/conf-available/security.conf

Et d'ajouter cette ligne de commande :

Header set X-XSS-Protection "1; mode=block"

Puis de redémarrer Apache pour que cela soit pris en compte :

systemctl restart apache2