TP 3: XSS

Consignes générales :

- Un compte-rendu par binôme
- Justifiez vos réponses mais soyez concis.

Objectifs

Injection HTML

Pré-requis

VirtualBox, SQL

Introduction

Ce TP a pour objectif de vous permettre de réaliser une attaque de type XSS sur un site web existant. L'ensemble des manipulations proposées dans le cadre de ce TP ne doit être réalisé que dans un environnement personnel, virtuel de préférence.

NE LES UTILISEZ PAS POUR ATTAQUER DES SITES WEB NE VOUS APPARTENANT PAS !!

Maintenant reprenez vos deux VM, Kali Linux et Metasploitable2 et démarrez-les en mode pont.

- Kali Linux : root/toor
- Metasploitable2 : msfadmin/msfadmin

Activités

1. *Reflected* XSS

Ce formulaire est-il sensible à une attaque XSS? Reportez sur votre CR le lien modifié pour tester la possibilité d'exécuter l'attaque.

Ouvrez un nouvel onglet et collez le lien suivant dans la barre d'adresse en remplaçant meta2_IP par sa valeur :

http://meta2_IP/dvwa/vulnerabilities/xss_r/?name=%3Cb%3Evyda%3C/b%3E#

Que se produit-il ? Conclusion ?

Comment pouvez-vous afficher votre cookie de session ?

Quel est le danger lié à la récupération de ce type d'informations ?

Connectez-vous à Meta. Naviguez au répertoire /var/www/dvwa/vulnerabilities/xss_r/ et affichez le fichier low.php: comme prévu, vous pouvez constater qu'aucun filtrage n'a été mis en place sur les entrées utilisateur.

Comparez cette stratégie à celle mise en place dans le fichier medium.php

Revenez à l'interface web depuis Kali. Configurez le niveau de sécurité à medium: comment pouvez-vous passer outre la stratégie de sécurité medium?

Renseignez dans le CR la ligne entrée.

2. *Stored* XSS

Sélectionnez maintenant le thème « Stored XSS ». Dans la page présentée, entrez un commentaire et sauvegardez-le. Revenez sur la page: votre commentaire a-t-il été sauvegardé?

Enregistrer un autre commentaire dont le contenu sera:

```
<script>window.open('www.y.com','_blank')</script>
```

Que se passe-t-il? Combien d'utilisateurs de ce site seront impactés?

Créez un nouveau commentaire avec le contenu suivant :

```
<script>window.location="https://www.sfr.fr"</script>
```

Comment cette entrée peut-elle être exploitée pour du phishing ?

3. Defacing et redirection

Finalement, vous avez vent du fait que le fondateur de DVWA, en plus de ne pas déborder d'imagination sur ses paramètres de connexion, est un grand amateur d'huîtres. Etant vous-même membre de la Société Protectrice des Huîtres (SPH), comment pouvez-vous lui faire sentir votre désaccord ?

4. DOM XSS

Réalisez une recherche sur le DOM XSS et présentez-en le principe.

Indices

```
nmap -p1-65535 <ip_de_Meta> -O --osscan-guess
chmod 777 fichier
sudo /etc/init.d/apache2 start

telnet ip_meta
```