TP : Étude de la faille XSS

DUREE 4H

EPISEN - ITS
Université Paris-Est Créteil

Faille XSS

1. Objectifs pédagogiques :

Sécurisé un système d'information est sans conteste une tâche ardue et il est inenvisageable de penser en faire le tour en une série de TP. Cette série de TP est donc conçue comme une série de challenges qui répondent, chacun, à un objectif différent. Le but espéré est de vous pousser à la réflexion et à approfondir les sujets étudiés.

L'étude de ces failles informatiques est uniquement à but pédagogique et ne vise pas à pousser à l'illégalité. L'objectif pédagogique de cette activité est de sensibiliser les étudiants aux vulnérabilités des failles informatiques les plus classiques.

2. Prérequis :

Avant de commencer le TP nous recommandons fortement de lire et comprendre le cours relatif à la vulnérabilité étudiée. En plus de comprendre le fonctionnement de la faille, ses risques et ses enjeux ceci vous permettra d'acquérir de la facilité dans la réalisation du TP.
Après la réalisation de ce TP, nous vous encourageons à tester vos connaissances via le QCM présent sur la plateforme.

3. TP :

a) Préparation des machines virtuelles

Pour ce premier TP, nous partirons sur une machine cible dont certaines vulnérabilités ont été volontairement exposées que nous appellerons Machine Victime. Vous prendrez une machine de type badstore que vous trouverez à la fin.

Cette machine a pour objectif de vous aider à comprendre comment certaines vulnérabilités Web que peuvent exploiter des pirates éventuels afin que puissiez mettre en place et tester des politiques palliatives.
Télécharger et créer une machine virtuelle configurée en accès par pont sur votre hyperviseur préféré. Supposant, pour la suite du TP que la machine en question a pour adresse X.X.X.X

On suppose que la machine attaquante est une machine Debian/Ubuntu qui est également configurée en accès par pont. Vous pouvez retrouver un lien permettant de télécharger cette VM en fin de TP.

b) Mise en place de la faille XSS

La commande netstat permet d'identifier les ports ouverts et les services en écoute sur une machine Linux.

1- A quoi correspondent les options tunap de la commande netstat.

2- Quels sont les ports ouverts ?

Un attaquant, à moins d'avoir un accès distant à la machine, ne peut accéder au résultat de la commande que vous venez de saisir. Il peut, néanmoins, arriver au même constat en effectuant un scan réseau. L'outil nmap est très utile pour cela. Il s'agit d'un outil multi-plateforme qui dispose d'une GUI installable séparément.

Installer l'outil nmap

apt install nmap

3- A quoi correspondent les options PE, PA, PR, PO de la commande nmap.

4- Donner la commande complète qui vous a permis d'identifier les ports ouverts.

4. Approfondir la réflexion :

Si vous êtes arrivé jusque-là c'est que vous avez la confirmation que la machine cible héberge un serveur WEB. L'outil skipfish développé par Mickal Zalewski et co (Google) est un formidable outil pour identifier les vulnérabilités web.

5- Après la lecture de la page github du projet : *https://github.com/spinkham/skipfish*, citer 2 autres outils semblables à Skipfish*

6- Expliquer le fonctionnement de Skipfish

7- Le manuel de badstore peut être téléchargé sur le lien suivant : *https://www.cs.umd.edu/class/fall2012/cmsc498L/materials/BadStore_net_v1_2Manual.pdf*,
Vous pouvez également utiliser les informations issues de ce site : *https://medium.com/@0x0FFB347/badstore-1-2-3-walkthrough-vulnhub-7816f3001333*

En vous basant sur le résultat de Skipfish, je vous propose de vous amuser en exploitant sur une faille assez simple à exploiter, « Le cross-site scripting (abrégé XSS) ». Il s'agit d'une faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs web visitant la page.

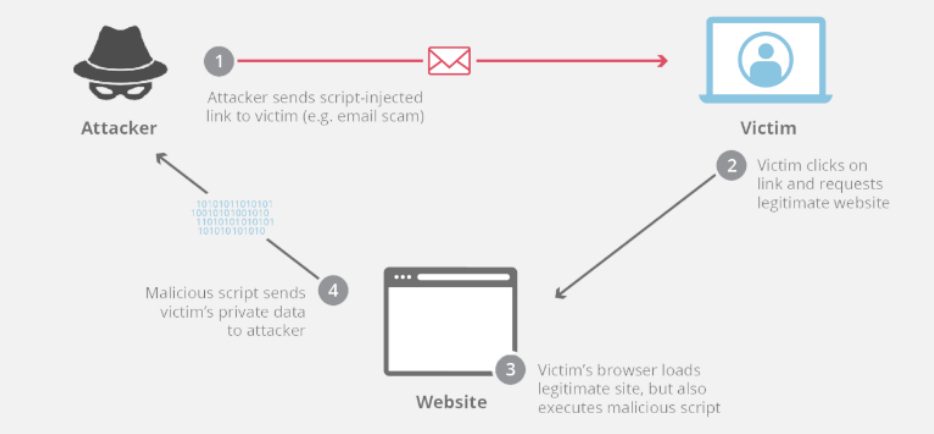

Figure 1 : Source : cloudflare

L’exploitation de cette faille consiste dans Injection de code de script dans un site Web exécuté dans le navigateur de la victime comme s'il faisait partie du code original.

Le logiciel client fait confiance au code. Le code donne accès à :

- Des données sensibles
- Des cookies de session
- La possibilité de détourner une session
- ...

• Q1 : Trouver (ou changer) le mdp de l’utilisateur ’admin ‘

• Q2 : BadStore Guestbook

Créer un guestbook comme suit :

<script> alert(“boooom”); </script>
Stored XSS = Persistent XSS

• Q3 : Analyzer le Cookie