UFR
de **mathématique** et d'**informatique**
Université de Strasbourg

TP n° 4

Objectifs

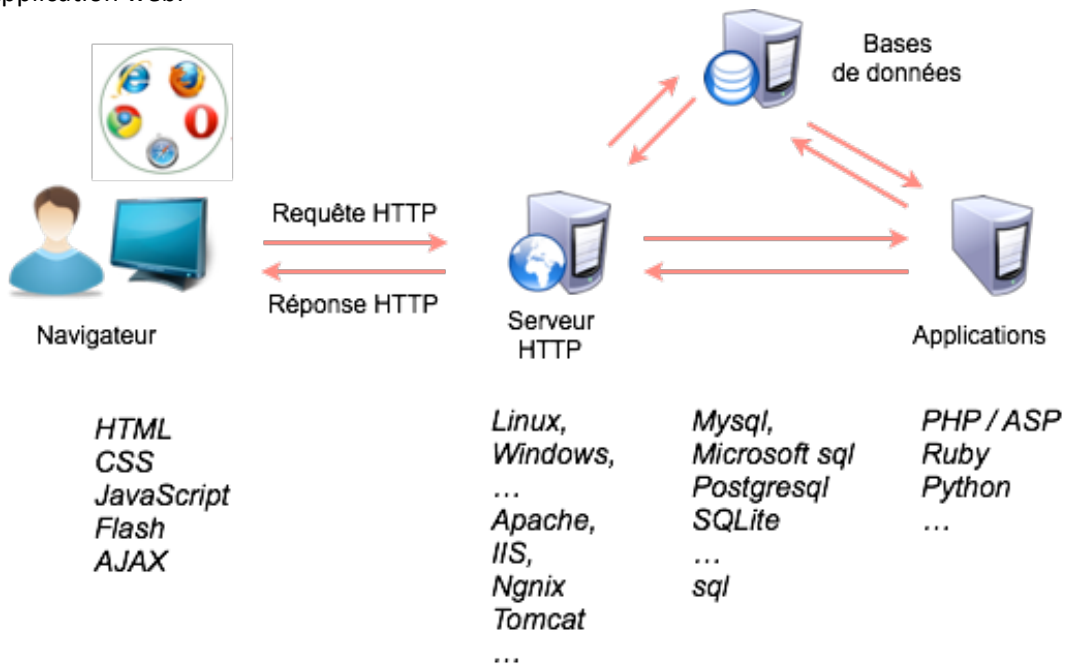
Comprendre et exploiter les principales vulnérabilités présentées par les services web dans le cadre d'un environnement de tests.

- Injection SQL ;
- Cross-Site Scripting (XSS) ;
- Falsification de requête intersites (CSRF) ;
- Violation de gestion d'authentification et de session.

1. Présentation

Les services web sont les éléments les plus vulnérables de nos systèmes d'information. Ils sont constitués de plusieurs éléments qui présentent chacun de nombreuses vulnérabilités :

- Navigateur côté client ;
- Communication client-serveur ;
- Serveur Web ;
- Base de données ;
- Application web.



Ces vulnérabilités sont connues du grand public essentiellement par le biais de deux organismes : le WASC (Web Application Security Consortium), et l'OWASP (Open Web Application Security Project).

Ces deux organismes assurent chacun à leur façon la promotion et la formation dans le domaine de la sécurité Web :

- Étude de vulnérabilités Web ;
- Production de référentiels de bonnes pratiques ;
- Développement d'outils de tests de pénétration ;
- Développement d'outils de sécurité.

Leur approche concernant l'étude des vulnérabilités diffère.

Le WASC tient à jour une base de vulnérabilités exhaustive ayant vocation de fournir des informations concernant toutes les vulnérabilités connues. Cette base est appréciée des professionnels du domaine.

L'OWASP propose une autre approche, plus orientée grand public. Celle–ci consiste à étudier les principales vulnérabilités Web du moment et à les vulgariser et les documenter de façon à faciliter leur compréhension par le plus grand nombre. Elle maintient ainsi à jour (publication tous les 3-4 ans) un document qui fait référence dans le domaine : l'OWASP Top Ten.

Ce document produit suite à une enquête menée auprès d'une large population d'entreprise du Net, compile les 10 principaux risques encourus par les services web durant les dernières années ayant précédées la publication des résultats de l'étude. Ce périmètre plus réduit (que celui traité par le WACS) permet de vulgariser et mettre à disposition du plus grand nombre une analyse/formation/aide sur les principales vulnérabilités Web.

Plusieurs laboratoires d'expérimentation ont vu le jour permettant ainsi de mettre en œuvre et étudier les vulnérabilités abordées par l'OWASP Top Ten.

Le présent TP propose d'utiliser un de ces laboratoires pour étudier ces vulnérabilités.

2. Plateforme de TP

La plateforme utilisée dans le cadre de ce TP est composé de deux machines virtuelles fonctionnant sur VirtualBox placées dans un même réseau (qualifié d'interne selon la terminologie VirtualBox).

- La première est un système Kali Linux (login/mdp : root/toor)

qui servira de plateforme d'attaque la seconde est un système Ubuntu spécialement vulnérable Metasploitable2 qui servira de cible aux attaques menées à partir du système Kali.

Plusieurs sites d'expérimentation sont disponibles dans cet environnement de tests :

- un site DVWA (Damn Vulnerable Web Application) en V1.0.7 disponible sur le système cible Metasploitable et accessible à partir du système Kali Linux à l'URL http://192.168.100.2/dvwa (login/mdp : admin/password)
- Un site Mutillidae (deliberately Vulnerable PHP Scripts of OWASP Top 10) disponible à l'URL http://192.168.100.2/mutillidae
- Un site DVWA en dernière version (V1.10) installé en local sur la machine Kali Linux disponible à l'URL http://127.0.0.1/dvwa (login/mdp : admin/password)

3. Travail à réaliser

En se basant sur les ressources ci-dessous, étudiez les risques de la dernière version de l'OWASP Top Ten.

https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf

Pour **trois** d'entre eux apportez une réponse aux points suivants :

a) Explication théorique de la vulnérabilité et du risque lié ;
b) Exemple théorique de mise en œuvre ;
c) Mesures de sécurité envisageables ;
d) Exemple pratique de mise en œuvre par le biais d'une des plateformes de tests.

Ressources

Sites Web vulnérables :

- http://192.168.100.2/dvwa
- http://192.168.100.2/mutillidae
- http://127.0.0.1/dvwa

OWASP Top Ten :

- https://www.owasp.org/index.php/Top_10-2017_Top_10

DVWA solutions :

- https://ogma-sec.fr/dvwa-brute-force-command-execution-solutions-protections/
- https://ogma-sec.fr/dvwa-csrf-file-inclusion-solutions-explications-protections/
- https://ogma-sec.fr/dvwa-sql-injection-solutions-protections/
- https://ogma-sec.fr/dvwa-solutions-protections-file-inclusion-xss/

Kali Linux :

- Différents outils de Pentest
- Metasploitable ;
- Webscarab ;
- Wfuzz ;
- Burp.

Rq : si vous désirez utiliser le lab local à la Kali (http://127.0.0.1/dvwa) pensez à lancer le service web (apache2) sur celle-ci ainsi que le SGBD (mysql).