Exploitation d'une plateforme d'apprentissage des vulnérabilités des applications web

Propriétés	Description
Intitulé long	Exploitation d'une plateforme d'apprentissage des vulnérabilités des applications web
Intitulé court	Sécurisation des applications web
Formation concernée	BTS Services Informatiques aux Organisations
Matière	SLAM4 : Réalisation et maintenance de composants logiciels.
Présentation	Ce Côté labo a pour objectif d'exploiter la plateforme d'apprentissage Mutillidae (OWASP) afin de se familiariser avec les principales vulnérabilités des applications web. Chaque activité couvre une problématique spécifique (SQLi, XSS, CSRF…) en référence au top 10 des vulnérabilités décrites par l'OWASP. Dans un premier temps, l'étudiant doit réaliser les attaques associées à chaque vulnérabilité. Dans un deuxième temps, l'objectif est d'analyser et de comprendre les codes sources des scripts présentés dans leur forme non sécurisée puis sécurisée en tant que contre-mesure. Cette première livraison comporte : • un document de présentation, • un document permettant de mettre en place l'environnement de test, • une première activité sur les injections, SQL notamment, et sa correction.
Notions	**Activités supports de l'acquisition des compétences** **D4.1 – Maintenance d'une solution applicative** • A4.2.1 Analyse et correction d'un dysfonctionnement, d'un problème de qualité de service ou de sécurité. **Savoir-faire** • Programmer un composant logiciel. • Adapter un composant logiciel. • Valider et documenter un composant logiciel. **Savoirs associés** • Techniques de sécurisation.
Prérequis	Commandes de base d'administration d'un système Linux, langages PHP et JavaScript.
Outils	Deux machines éventuellement virtualisées sont nécessaires avec Linux comme système d'exploitation. Site officiel : https://www.owasp.org
Mots-clés	OWASP, Mutillidae, BurpSuite, vulnérabilités, SQLi, XSS, IDOR.
Durée	Une heure pour les installations et une heure pour chaque activité.
Auteur(es)	Patrice DIGNAN, avec la relecture, les tests et les suggestions de Pierre François ROMEUF et de Yann BARROT.
Version	v 1.0
Date de publication	Décembre 2017

Table des matières

I Introduction

1 La sécurité des applications web

1.1 Les applications web sont partout

Aujourd'hui, les applications web sont partout. Elles sont utilisées quotidiennement dans nos activités personnelles ou professionnelles (réseaux sociaux, achats en lignes, démarches administratives…). Toute entreprise ou administration se doit d'avoir un site web. Ces applications facilitent les échanges et les transactions car elles sont accessibles de partout à l'aide d'un simple navigateur sur un smartphone ou un ordinateur de bureau.

Si au début des sites web, les aspects techniques et fonctionnels étaient suffisants, ce n'est plus du tout le cas aujourd'hui. L'actualité nous rappelle régulièrement que des entreprises voient leur site web attaqué. Les conséquences peuvent être lourdes (perte de données, baisse du chiffre d'affaire, effondrement de la réputation…). Avec comme enjeu, la survie de l'entreprise selon la gravité de l'attaque subie.

1.2 La sécurisation des applications web est indispensable

La sécurité des applications web est donc devenue un enjeu stratégique. Lors de son édition 2016, la société EY (http://www.ey.com/fr) a montré qu'une majorité des entreprises mondiales n'a pas de stratégie en matière de lutte contre les cybermenaces[1].

Au delà de l'aspect fonctionnel des outils de développement, il est indispensable pour tout développeur de savoir identifier les vulnérabilités potentielles et de prendre en compte les menaces en adaptant son développement à l'aide de bonnes pratiques. La phase de test ne doit pas se limiter au fonctionnement attendu du code mis en œuvre mais anticiper les utilisations malveillantes comme les injections de code SQL dans les formulaires.

Afin de mettre en place une veille stratégique sur la sécurisation des applications web, le groupe OWASP a développé une base de données qui recense la liste des incidents de sécurité recensés sur les applications web. Cette base nommée WASC-WHID (Web application Security Consortium - Web Hacking Database Project) permet de disposer de statistiques sur les failles de sécurité relevées sur les applications web. Les incidents sont déclarés et enregistrés afin d'alimenter une base de connaissance.

Le lien permettant d'accéder aux outils WHID est le suivant :

https://www.owasp.org/index.php/OWASP_WASC_Web_Hacking_Incidents_Database_Project.

2 Les motifs des attaques

1 http://www.lemondeinformatique.fr/actualites/lire-55-des-entreprises-mondiales-n-identifient-pas-les-vulnerabilites-67146.html)

Les sites web peuvent être attaqués pour plusieurs raisons :

MOTIFS	EXPLICATIONS
Propagande	Certaines personnes peuvent attaquer un site pour des raisons politiques ou pour défendre une cause particulière (hacktivistes).
Distraction	Des personnes peuvent voir dans l'attaque de sites web une distraction ou un défi à relever.
Vol de données	Le vol de données lucratif, pour effectuer du chantage ou pour copier le savoir d'un concurrent sur un marché.
Machine zombie	Le serveur cible est utilisé dans un réseau destiné à faire des attaques distribuées par déni de service (DDOS), du stockage de fichiers illégaux, de l'envoi de spams …

II Présentation d'OWASP

1 La communauté OWASP

OWASP (Open Web Application Security project) est une communauté travaillant sur la sécurité des applications web. Elle a pour but de publier des recommandations de sécurisation des sites web et propose des outils permettant de tester la sécurité des applications web.

Site officiel : https://www.owasp.org/

2 Le top 10 d'OWASP

OWASP fournit une liste des risques de sécurité des applications web les plus courants. En 2017, OWASP a mis à jour son classement afin de sensibiliser les développeurs web aux risques encourus. Les 10 risques classés par ordre de dangerosité sont les suivants :

RISQUES		DÉFINITIONS	ACTIVITÉS
A1	INJECTION	Correspond au risque d'injection SQL (SQLi).	1
A2	BROKEN AUTHENTICATION AND SESSION MANAGEMENT	Correspond au risque de casser la gestion de l'authentification et de la session. Comprend notamment le vol de session (session hijacking) ou la récupération de mots de passe.	2
A3	CROSS SITE SCRIPTING (XSS)	Correspond au XSS soit l'injection de contenu dans une page, ce qui provoque des actions non désirées sur une page Web. Les failles XSS sont particulièrement répandues parmi les failles de sécurités Web.	3
A4	INSECURE DATA OBJECT REFERENCE (IDOR)	Correspond aux failles de sécurité des identifiants (ID) de données visualisées. Nécessite de mettre en place un contrôle d'accès aux données.	4
A5	SECURITY MISCONFIGURATION	Correspond aux failles de configuration liés aux serveurs Web, applications, base de données ou framework.	5
A6	SENSITIVE DATA EXPOSURE	Correspond aux failles de sécurité liées aux données sensibles comme les mots de passe, les numéros de carte de crédit ou encore les données personnelles et la nécessité de crypter ces données.	6
A7	MISSING FUNCTION LEVEL ACCESS CONTROL	Correspond aux failles de sécurité liées aux accès non souhaitables à une fonctionnalité.	7
A8	CROSS SITE REQUEST FORGERY	Correspond aux failles liées à l'exécution de requêtes à l'insu de l'utilisateur.	8
A9	USING COMPONENT WITH KNOWN VULNERABILITIES	Correspond aux failles liées à l'utilisation de composants tiers.	9
A10	UNVALIDATED REDIRECTS AND FORWARDS	Correspond aux faillies liées aux *redirect* et *forward* générique des applications.	10

III Démarche et organisation du côté labo

La découverte des vulnérabilités présentées dans le tableau précédent peut se faire de manière manuelle ou automatique.

Des scanners de vulnérabilités comme Nessus ou Vega permettent d'automatiser ces détections. Attention cependant, car ces outils laissent des traces dans les logs de l'administrateur du système cible. La plateforme utilisée dans ce côté labo étant intentionnellement vulnérable, ces outils ne seront pas présentés.

Les activités porteront donc sur la **détection manuelle** et **l'exploitation des vulnérabilités**. Elles permettront d'identifier des **bonnes pratiques** permettant d'obtenir un codage sécurisé.

Cette première production présente la plateforme de test des vulnérabilités puis étudie dans l'activité 1 la plus courante de toutes selon OWASP : l'injection SQL.

D'autres activités suivront selon le plan annoncé dans le tableau ci-dessus.

Piste d'exploitation pédagogique : cette production peut aussi être exploitée dans le cadre de PPE3-4 en SLAM. Il serait possible de partir d'une application faiblement sécurisée et de demander aux étudiants de renforcer sa sécurité en indiquant des objectifs précis.

IV Mise en garde juridique

Il convient de préciser que la loi interdit le fait d'accéder ou de se maintenir de manière frauduleuse dans un système de traitement automatisé de données (STAD) et que les organisations doivent garantir la confidentialité des données conservées.

Du point de vue de l'attaquant, on peut rappeler l'article de loi suivant :

L'article 323-1 du code pénal, lequel dispose que « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. »

Du point de vue des organisations, un minimum de précautions est nécessaire. La CNIL peut sanctionner les entreprises trop laxistes en la matière.

On peut citer les articles de loi suivant :

Article 34 de la loi du 6 janvier 1978 : Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.
Article 226-17 : Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Toutes les manipulations décrites sont réalisées uniquement sur la plateforme pédagogique présentée. Elles ne doivent en aucun cas être testées sur d'autres sites web.