Compte Rendu de la conférence OWASP AppSec NYC 2008.

La conférence annuelle de l'OWASP s'est déroulée du 22 au 25 Septembre à New York à l'hôtel Park Central de New York, à 2mn de Central Park. Elle a réuni plus de 1000 participants, majoritairement des nord américains (plus des deux tiers). Un seul français était présent !

Tout le contenu est disponible sur le site web de l'OWASP dédié aux conférences : http://www.owasp.tv

La conférence a adopté les mêmes principes que les conférences Blackhat, à savoir : 2 jours de formations (Trainings) puis 2 jours de conférences.

Les formations proposées cette année étaient au nombre de 8 ; l'attaque et la défense des applications web étaient abordées avec un accent sur les méthodes de défense et de sécurisation.

Premier Jour des conférences

Après ces deux jours de formations, les conférences ont débuté dans une ambiance assez électrique, parce que deux présentations étaient particulièrement attendues :

- tout d'abord beaucoup spéculaient sur ce que serait l'annonce de l'ISC2 (http://www.isc2.org),
- et surtout tout le monde se demandait si la présentation de Robert (RSnake) Hansen et Jeremiah Grossman sur le « clickjacking » aurait lieu, du fait des pressions exercées par différents éditeurs.

Nous conservons encore quelques minutes le suspense et vous laissons découvrir la réponse à ces questions dans la suite de ce compte-rendu.

Keynote et CTF

Jeff Williams, Chair of OWASP, a introduit la conférence en présentant l'état du projet OWASP ; l'utilisation des finances, les projets sponsorisés, les guides publiés. Il a aussi largement encouragé chacun à devenir des « builders » et non pas des « breakers » dans le cycle de la sécurité applicative. Il a expliqué enfin que l'OWASP allait mettre de plus en plus l'accent sur l'éducation, la sensibilisation, la production de documents « aidant » à sécuriser le code.

La première journée a aussi été l'occasion de lancer le premier challenge "Capture The Flag Web" (CTF) des conférences OWASP avec pour le gagnant une prime de 2000 Dollars.

La présentation du Homeland & Security :

La branche CyberSecurity du Département de la défense intérieur américain (Homeland and security) a effectué une présentation du programme SwA (Software Assurance) déployé en interne. Le DHS a présenté son approche d'assurance logicielle dans le processus des achats, qui permet d'après eux de pouvoir disposer d'un niveau de sécurité plus poussé lors de l'intégration de progiciel. Leur démarche est venue d'un constat sur le fait qu'il existe peu de programmes éducatifs sur la bonne façon de coder, et de sécuriser des progiciels. En prenant ce principe, ils ont effectué une démarche consistant à demander lors des achats une assurance (via des tests bien définis, des revues de codes, ...) à leurs fournisseurs. Les informations seront bientôt en ligne sur leur site Web.

BotNet HTTP

Cette présentation s'est intéressée à l'étude du phénomène des BotNets HTTP. Si ce type de botnet semble devenir de plus en plus "populaire" (et prendre le pas sur les traditionnels Botnets IRC), l'étude présentée montre aussi que nous ne sommes qu'aux balbutiements des problèmes autour de ces programmes malveillants. Les premières générations sont en effet très limitées quand à leur capacité d'infection. Ce sont ces premières générations qui ont été utilisées lors de la récente guerre Russie/Georgie. Les prochaines générations devraient pouvoir être intégrées de façon furtive dans les trafics HTTPS tout en développant une capacité de mutation (un peu comme les virus maintenant). Néanmoins, cela ne signifie pas la fin des Bot IRC, mais il est clair que ces derniers ne sont plus les plus « populaires » depuis quelque temps.

Actuellement le Botnet HTTP le plus actif serait le BlackEnergy avec une capacité d'attaques en DDOS. Son implantation serait principalement en Russie avec comme cible principale les jeux d'argent.

Clickjacking : Les 0-days de Robert & Jeremiah

Le fameux talk sur le clickjacking (un exploit 0-day) n'a pas été totalement annulé, nos deux compères n'ont donc pas totalement cédé à la pression, même s'ils ne nous ont pas totalement tout dévoilé (en l'occurrence nous n'avons pas pu avoir un slide ou une démo...). Ce fameux procédé permet à n'importe quelle personne dont vous visitez le site Web de prendre contrôle de votre navigateur ; ou plus exactement de prendre contrôle des « liens » des pages visitées. Tout navigateur est impacté hormis lynx ; ce n'est pas une faille liée à javascript mais réellement à la façon de fonctionner

du navigateur.

J'ai ensuite eu l'occasion de discuter avec Jeremiah et RSnake (que j'avais déjà croisé ailleurs) sur l'analyse du problème (confirmée par la suite par les PoC publiés) est la suivante :« ***L'exploitation de la faille passe par une iFrame (clairement lynx ne les gère pas...) qui cache le contenu malicieux. Le contenu principal doit être un flash (ou un autre contenu de type ActiveX, Applet Java). Tous les clics de l'utilisateur sur le contenu principal sont alors utilisés pour générer du trafic (des faux clics) dans l'iFrame malicieuse..*** »

Présentation sur les Java RMI

Un talk sur les Java RMI (Remote Method Invocation) plutôt intéressant, sur la façon d'effectuer des intrusions sur les frameworks Java actuels. Le présentateur nous a présenté la manière dont Java traite les requêtes RMI. Il a expliqué en particulier que lors de l'invocation d'une RMI, il existe une clef d'authentification. Le présentateur nous a indiqué qu'il avait découvert une faiblesse dans l'algorithme de génération de ces clefs, qui permet d'effectuer des appels RMI avec une clef faible.

L'ensemble des outils présentés (tous écrits en Java) seront bientôt ajoutés au projet OWASP.

L'annonce de l'ISC2

La journée s'est close sur la fameuse annonce de l'ISC2 : le lancement de la certification CSSLP (Certified Secure Software Lifecycle Professional) . Il s'agit d'une certification similaire à la CISSP, mais qui s'adresse au monde des développeurs et des chefs de projets techniques. Cette certification sera officiellement lancée en 2009, une population teste les examens sur cette fin 2008 et une autre finalise la rédaction du CSSLP CBK (le livre de référence à apprendre par cœur...).

Deuxième Jour des conférences

La seconde journée fut plus calme mais avec quand même des présentations intéressantes.

Présentation du Chapitre Allemand sur les Web Application Firewalls (WAFs)

Une présentation du Guide sur les meilleures pratiques d'implémentation et d'utilisation des WAF, effectuée par le leader du chapitre allemand de l'OWASP. Le document est disponible sur le site de l'OWASP.

Le Framework W3AF

L'outil W3AF est un outil (framework) d'audit Web écrit en python, assez similaire dans son approche à l'outil "metasploit". C'est clairement un très bon outil, disposant de l'avantage de pouvoir rajouter des plugins. Son auteur indique qu'il lui reste cependant à stabiliser le code du framework et à optimiser la rapidité et la consommation mémoire. L'OWASP a sponsorisé le GUI (écrit en GTK) via le "Summer of Code 2008" de l'OWASP.

Les Web Services/XML

Une présentation sur les Web Services et la sécurité XML réalisée par Gunnar Peterson (spécialiste du sujet des SOA et XML). Il a annoncé la sortie imminente d'un guide similaire au Top10 Web de l'OWASP qui sera totalement orienté XML/SOA/WebServices.

Gunnar donnait une formation les jours précédents sur le sujet.

Revue de code

Différentes sessions sur la revue de code toutes plus intéressantes les unes que l'autres. Avec la présentation des concepts, des outils et des méthodes à employer.

La Sécurité de Lotus Domino

Une présentation très intéressante autour des problématiques de sécurité que l'on peut trouver dans Domino. La présentation a débuté sur une approche globale de Domino, son modèle de sécurité ainsi que son langage de programmation qui n'est pas immunisé contre les problématiques classiques de sécurité Web.

La présentatrice a passé en revue l'ensemble des types de problèmes classique en expliquant les fonctions Domino permettant de tirer partie des failles.

Globalement, on retiendra que tout ce que l'on trouve en Web classique est possible de base dans Domino, et la sécurité de Domino est rarement « **auditée** ».

L'injection de paramètres dans les applications Flash

Et pour finir une présentation sur l'injection de paramètres dans les applications Flash/Flex faite par deux israéliens d'IBM (ex WatchFire) très bien abordée et présentée, avec des exemples concrets.

Il est a noter que le principal problème de Flash est qu'il a été créé pour un public de « WebDesigner » et donc comporte un modèle de sécurité faible. De plus les « Webdesigner » n'ont explicitement aucune connaissance en programmation et donc joue avec les souplesses de Flash...

Leur approche d'injection a permis de montrer qu'il est facile d'effectuer du Phishing ou des injections de codes malicieux pour récupérer le contenu de bases de données ou tout simplement les contenus d'éléments du navigateur.

Sébastien Gioria (sebastien.gioria@owasp.fr)

Président et évangéliste de l'OWASP France.

A propos de l'OWASP

L'OWASP (Open Web Application Security Project) est une organisation communautaire mondiale ouverte et indépendante. Elle a pour objectif d'organiser, promouvoir, développer et maintenir des applications sûres.

Tous les projets et manifestations de l'OWASP sont libres et ouverts aux personnes intéressées par la sécurité des applications Web.

L'OWASP est une organisation d'un nouveau genre, sa liberté par rapport aux influences commerciales lui permettant de fournir des informations pratiques et non influencées concernant la sécurité des applications Web.

L'OWASP n'est liée à aucune société commerciale, bien qu'elle puisse fournir des informations à propos des technologies de ces dernières sociétés. Comme beaucoup d'organisations Open Source, l'OWASP produit différents contenus et outils dans un esprit collaboratif et ouvert.

L'OWASP est dirigée par un bureau composé d'experts dans leur domaine respectif et permettant de couvrir tous les aspects de la sécurité Applicative (Education, Technique, Juridique, ...). Une fondation américaine permet de récolter des fonds alimentant les programmes de recherches sponsorisés par l'OWASP.

L'OWASP organise chaque année plusieurs conférences sur le thème de la sécurité applicative. La dernière vient d'avoir lieu au Portugal du 3 au 7 novembre 2008. Ces conférences sont le moment de démontrer des concepts et de présente des projets, tout comme former aux dernières techniques

La problématique de la sécurité applicative.

La sécurité n'est pas un évènement ponctuel. Sécuriser un code juste une fois ne suffit pas.

Une démarche de programmation sécurisée doit composer avec toutes les étapes du cycle de vie d'un programme. Les applications web sécurisées sont seulement possibles quand un SDLC (i.e. Software Development Life Cycle) sécurisé est utilisé. Les programmes sûrs sont sécurisés par conception, pendant le développement et par défaut. Il y a au moins 300 problèmes affectant l'ensemble de la sécurité d'une application web. Ces 300 problèmes sont détaillés dans le Guide de l'OWASP, lecture essentielle et indispensable à toute personne développant des applications web aujourd'hui.