Bee Ware : La liste des failles Internet les plus couramment utilisÃ©es
Internet
PostÃ© par : JulieM
PubliÃ©e le : 27/5/2013 13:30:00

CommunautÃ© dÃ©diÃ©e Ã la sÃ©curitÃ© des applications Web, l'OWASP (Open Web Application Security Project) a rÃ©cemment publiÃ©e une **version actualisÃ©e des dix menaces Web les plus critiques**. Expert en sÃ©curisation des flux HTTP, Bee Ware revient sur la mise Ã jour de ce document.

L'OWASP est une communautÃ© regroupant de nombreux spÃ©cialistes de la sÃ©curitÃ© des applications web. Libre et ouverte Ã tous, cette communautÃ© concentre son attention sur des projets de veille, de mise en place de standards ou de logiciels d'audit.

Parmi ces projets, le "Top Ten" est un document recensant les failles les plus couramment utilisÃ©es pour compromettre les systÃ¨mes d'information. L'objectif premier de ce rapport est donc d'informer et d'Ã©vangÃ©liser les responsables de la sÃ©curitÃ© des systÃ¨mes d'information sur les risques encourus lors de publication d'applications sur le net.

Pour Ãªtre le plus efficace possible, ce rapport est rÃ©guliÃ¨rement mis Ã jour par les membres de l'OWASP. La nouvelle version du Top Ten venant d'Ãªtre publiÃ©e, Bee Ware revient sur les Ã©volutions notables apparues depuis 2010 (date de la derniÃ¨re mise Ã jour du Top Ten).

Il est tout d'abord intÃ©ressant de noter que de nombreuses menaces prÃ©sentes dans le Top Ten 2010 sont toujours d'actualitÃ© et maintiennent leur place dans ce palmarÃ¨s...:

â¢ Les injections SQL

o Les zones de saisies de caractÃ¨res des sites web dynamiques sont utilisÃ©es comme console, permettant ainsi d'injecter des bouts de codes SQL non prÃ©vus par le systÃ¨me et atteignant

directement le coeur du site : les bases de donnÃ©es.

â¢ Le Cross-Site Scripting (XSS)

o A l'instar des injections SQL, le Cross-Site scripting utilise les zones de saisies de caractÃ¨res des sites pour injecter, non pas des requÃªtes SQL, mais n'importe quel code Ã©crit dans un langage supportÃ© par le navigateur (JavaScript, Java, Flash, HTML5, etc.).

â¢ La violation de gestion d'authentification et de session

o Cette menace se dÃ©cline sous plusieurs formes, dont notamment :

ï§ L'utilisation de la force brute (test d'un grand nombre de possibilitÃ©s) pour valider une authentification ou voler un identifiant de session

ï§ La demande de rÃ©initialisation de mot de passe (en s'appuyant par exemple sur les donnÃ©es personnelles visibles sur les rÃ©seaux sociaux)

ï§ L'hameÃ§onnage (technique consistant Ã soutirer ses identifiants de connexion Ã une victime, en lui faisant croire qu'elle s'adresse Ã un tiers de confiance)

â¢ Les rÃ©fÃ©rences directes et non sÃ©curisÃ©es Ã un objet

o Certaines applications ne vÃ©rifient pas les autorisations d'accÃ¨s des personnes effectuant des requÃªtes, leur permettant ainsi d'accÃ©der Ã des donnÃ©es (sensibles ou non) dont la visibilitÃ© ne leur Ã©tait pas autorisÃ©e

â¢ Les mauvaises configurations de sÃ©curitÃ©

o Ne pas modifier un mot de passe par dÃ©faut ou ne pas mettre Ã jour les composants d'une application (systÃ¨me d'exploitation, modules complÃ©mentaires, etc.) laisse la possibilitÃ© aux personnes malveillantes d'utiliser les failles de sÃ©curitÃ© publiques non corrigÃ©es.

â¢ La falsification de requÃªtes intersites (cross-site request forgery, ou XSRF)

o PrÃ©sente depuis 6 ans dans le Top Ten de l'OWASP, la falsification de requÃªte intersites consiste Ã manipuler un utilisateur lambda en vue de lui faire effectuer, sans qu'il ne s'en rende compte, une attaque de type XSS.

â¢ La redirection et les renvois non validÃ©s

o Cette technique consiste Ã rediriger (via un lien) un utilisateur vers une page n'appartenant pas Ã l'application visÃ©e, sans que ce dernier ne s'en aperÃ§oive.

D'autres failles prÃ©sentes dans le Top Ten 2010 ont Ã©voluÃ©es au cours de ces derniÃ¨res annÃ©es, donnant ainsi lieu en 2013 Ã de nouvelles menaces :

â¢ La dÃ©faillance dans la restriction des accÃ¨s Ã une URL est devenue l'absence de fonction contrÃ´lant le niveau de contrÃ´le d'accÃ¨s (Missing Function Level Access Control)

o Cela englobe les mauvaises configurations ou l'absence de code vÃ©rifiant l'identitÃ© et les droits de la personne souhaitant accÃ©der Ã des fonctionnalitÃ©s critiques de l'application

â¢ Le stockage de donnÃ©es cryptographiques non sÃ©curisÃ©es a Ã©tÃ© fusionnÃ© avec la protection insuffisante des couches de transport pour donner la divulgation de donnÃ©es sensibles

o Le risque de divulgation de donnÃ©es sensible est principalement dÃ» au fait que ces derniÃ¨re ne sont pas cryptÃ©es, ou lorsqu'elles le sont, que les clefs et logiciels de chiffrement utilisÃ©s sont trop faibles. Il est alors possible d'intercepter ces donnÃ©es lorsqu'elles transitent entre deux applications ou plus simplement, directement sur leur lieu de stockage.

Enfin, une nouvelle menace fait en 2013 son apparition dans le Top Ten de l'OWASP :

â¢ L'utilisation de composants connus pour Ãªtre vulnÃ©rables (Using known vulnerable components)

o De nombreuses applications s'appuient sur des composants dont les failles de sÃ©curitÃ© sont connues et d'ores et dÃ©jÃ diffusÃ©es... Une fois la prÃ©sence de ces composants identifiÃ©e, il ne reste plus qu'Ã adapter l'exploit pour atteindre l'application visÃ©e...

Il est aujourd'hui indispensable de connaÃ®tre et de maÃ®triser l'ensemble des failles sÃ©curitaires prÃ©sentes dans le Top Ten de l'OWASP pour se prÃ©munir contre la majoritÃ© des attaques visant les applications Web. Cependant, d'autres menaces non listÃ©es dans ce document sont Ã©galement Ã prendre en compte...

JÃ©rÃ´me Clauzade, Product Manager chez **Bee Ware** explique : "*Le Top Ten de l'OWASP est un document de rÃ©fÃ©rence et doit servir de base Ã la sÃ©curisation des flux HTTP. Cette derniÃ¨re ne repose plus uniquement sur le filtrage des donnÃ©es, mais englobe Ã©galement les problÃ©matiques d'authentification, de fiabilitÃ©, de SLA, etc. Avec plus de 10 ans d'expÃ©rience dans le domaine de la sÃ©curitÃ© web, Bee Ware est aujourd'hui le seul Ã©diteur Ã proposer une solution intÃ©grant un pare-feu applicatif, un pare-feu XML et un contrÃ´le des accÃ¨s au sein d'une plate-forme unique. Nous protÃ©geons ainsi nos clients contre l'ensemble des menaces applicatives susceptibles de leur nuire*.".