

Les attaques contre les applications PHP une menace pour le Web

Internet

Posté par : JulieM

Publié le : 12/9/2013 11:30:00

Le nouveau rapport Hacker Intelligence Initiative de Imperva montre que les attaques contre les applications PHP peuvent avoir des conséquences sur la sécurité et la santé du World Wide Web.

Imperva, Inc, pionnier et leader d'une nouvelle catégorie de solutions de sécurité professionnelles pour les applications critiques et les données à haute valeur ajoutée dans les datacenters, publie son rapport Hacker Intelligence Initiative, "PHP : Superglobales : Problèmes XXL". Le rapport de septembre présente une vue approfondie des récentes attaques contre les applications PHP, incluant les attaques qui impliquent les variables "superglobales" PHP, et permet de mieux comprendre la nature des activités de hacking et les conséquences pour l'intégrité de l'ensemble du World Wide Web.



«Parce que des serveurs hackés peuvent être utilisés comme botnets pour attaquer d'autres serveurs, les attaques contre les applications PHP peuvent affecter la sécurité générale et la santé de l'ensemble du Web», explique **Amichai Shulman**, Directeur Technique de Imperva. «Les répercussions de ces attaques peuvent être importantes tant donné que la plate-forme PHP est de loin la plus populaire pour le développement d'applications web, équipant plus de 80% des sites internet, incluant Facebook et Wikipedia. De toute évidence, il est temps pour les professionnels de la sécurité de consacrer plus d'attention à ce sujet.»

Le rapport montre également que les hackers sont de plus en plus aptes à combiner des niveaux élevés de sophistication dans de scripts simples. Ils identifient les variables «superglobales» du PHP comme une cible de choix qui donne un retour sur investissement élevé.

Les variables «superglobales» du PHP gagnent en popularité au sein de la communauté des hackers car elles intègrent de multiples problèmes de sécurité lors d'une menace Web avancée qui peut briser la logique d'application, compromettre les serveurs et aboutir sur des transactions frauduleuses et du vol de données. En un mois, l'équipe de recherche d'Imperva a noté une moyenne de 144 attaques par application qui contenaient des vecteurs d'attaque liés à des variables «superglobales». En outre, les chercheurs ont observé des campagnes d'attaque de plus de cinq mois avec des salves de requêtes allant jusqu'à 90 par minute sur une

seule application.

Voici les principaux enseignements du rapport :

â€¢ **Les principales expositions dans les infrastructures** tiers d'Imperva montrent la nécessité d'un modèle de sécurité "opt-out". Le rapport révèle une vulnérabilité dans l'application très populaire PhpMyAdmin (PMA) utilisée pour gérer les bases de données MySQL dans des environnements PHP. Parce qu'il est souvent associé à d'autres applications utilisant la fameuse base de données MySQL, avoir cette application vulnérable présente sur le serveur, (même si elle n'est pas utilisée par l'administrateur) peut l'exposer aux attaques d'exécution de code, et en conséquence, au contrôle total du serveur. Par conséquent, Imperva recommande un modèle de sécurité en "opt out".

â€¢ **Les modèles de sécurité positifs sont les meilleurs.** Seul un mécanisme de sécurité positif qui spécifie les noms des variables autorisées pour chaque ressource peut empêcher un attaquant de profiter de la faiblesse d'une manipulation de variable externe qui donne à quiconque la possibilité d'envoyer des paramètres externes avec le même nom de variables internes, et donc de remplacer la valeur de ces dernières.

â€¢ **Les hackers sont à la pointe.** Les chercheurs de la cellule HII d'Imperva ont observé que les hackers sont capables de monter des attaques complexes et de les packager en un outil simple à utiliser. Cependant, pour une impressionnante démonstration de la force d'une attaque, la méthode PHP peut présenter des failles. Une solution de sécurité d'application qui permet de détecter et de réduire une seule étape de l'attaque peut rendre toute l'attaque inutile.

â€¢ **Les variables « superglobale » dans une requête devraient être bloquées.** Il n'y a aucune raison de la présence de ces paramètres dans les requêtes, par conséquent, ils devraient être interdits.

Le rapport complet d'Imperva est disponible.