



GUIDE:

Sécurité des Applications Web — Comment Minimiser les Risques d'Attaques les plus Courants

Sommaire

I. L'essentiel	2
II. Les bases de la sécurité des applications Web	2
III. Types de vulnérabilités inhérentes aux applications Web	3
IV. Détection des vulnérabilités dans les applications Web	5
V. QualysGuard WAS automatise la détection des vulnérabilités	6
IV. Protection de vos applications Web	8
V. À propos de Qualys	8

L'essentiel

Les vulnérabilités au sein des applications Web sont désormais le vecteur le plus important des attaques dirigées contre la sécurité des entreprises. L'an dernier, près de 55% des vulnérabilités dévoilées concernaient des applications Web ¹. Selon ce même rapport, à la fin de l'année, aucun patch de remédiation n'était disponible pour 74% des vulnérabilités affectant les applications Web. Les récits sur les exploits qui compromettent des données sensibles mettent souvent en cause des attaques à base de « scripts intersite », d'« injection de code SQL » et de « débordement de la mémoire tampon ». Les vulnérabilités de ce genre ne relèvent généralement pas de l'expertise traditionnelle des responsables de la sécurité réseau. Par conséquent, l'obscurité relative des vulnérabilités des applications Web est précieuse pour mener des attaques. Comme l'ont constaté de nombreuses entreprises, ces attaques résisteront aux défenses classiques du réseau d'entreprise, à moins que vous ne preniez de nouvelles précautions. Pour vous aider à savoir comment minimiser ces risques, Qualys vous propose ce guide d'introduction à la sécurité des applications Web. Ce guide fait le point sur les vulnérabilités qui affectent généralement les applications Web. Il compare aussi les options de détection disponibles et présente la solution Web Application Scanning (WAS) de la suite QualysGuard, un nouveau service à la demande fourni par Qualys pour automatiser la détection des vulnérabilités les plus courantes au sein des applications Web personnalisées.

Les bases de la sécurité des applications Web

Les attaques contre les vulnérabilités des applications Web ont commencé à voir le jour en même temps qu'émergeait le Web, c'est-à-dire au milieu des années 1990. Ces attaques s'appuient généralement sur l'injection de fautes, une technique permettant d'exploiter les vulnérabilités de la syntaxe et de la sémantique d'une application Web. Avec un navigateur Web standard et une connaissance de base du protocole HTTP et du langage HTML, un pirate tente un exploit particulier en modifiant automatiquement un lien URI (Uniform Resource Indicator) qui, à son tour, est capable de déclencher un exploit tel qu'une injection de code SQL ou du script intersite

http://example/foo.cgi?a=1

http://example/foo.cgi?a=1'

http://example/foo.cgi?a=<script> ...

< Injection de code SQL

< Script intersite (XSS)

Certaines attaques tentent d'altérer le workflow logique. Les pirates mènent également ces attaques en modifiant automatiquement une URI.

http://example/foo.cgi?admin=false

http://example/foo.cgi?admin=true

< Augmentation des privilèges

Un nombre important d'attaques exploitent des vulnérabilités au niveau de la syntaxe et de la sémantique. Nombre de ces vulnérabilités peuvent être découvertes à l'aide d'un outil d'analyse automatisé. Les vulnérabilités logiques sont très difficiles à tester avec un outil d'analyse. En effet, elles imposent de

procéder manuellement pour inspecter et analyser le code source de l'application Web et pour effectuer des tests de sécurité.

En règle générale, les vulnérabilités de sécurité au sein des applications Web sont liées à des erreurs de programmation avec un langage de programmation d'application Web (par exemple Java, .NET, PHP, Python, Perl et Ruby), à une bibliothèque de codes, à un trait de conception ou à l'architecture.

Ces vulnérabilités peuvent être complexes et se produire dans de nombreuses circonstances. Utiliser un firewall pour applications Web peut aider à contrôler les effets de certains exploits, mais il ne permettra pas de résoudre les vulnérabilités sous-jacentes.

Types de vulnérabilités des applications Web

Les applications Web peuvent comporter chacune une vingtaine de types de vulnérabilités. Les consultants en sécurité qui effectuent des tests de pénétration s'attachent à trouver les principales vulnérabilités, notamment celles figurant dans une liste publiée par le projet OWASP (Open Web Application Security Project - www.owasp.org). Parmi les autres initiatives visant à classer de manière systématique les vulnérabilités au sein des applications Web figurent six catégories publiées par le consortium WASC (Web Application Security Consortium - www.webappsec.org). Les descriptions de vulnérabilités Web qui suivent s'appuient sur le schéma WASC.

Authentification – vol des identités de compte utilisateur

- **L'attaque par Force brute** (ou Brute Force) automatise un processus d'essais et d'erreurs destiné à deviner le nom d'utilisateur, le mot de passe, le numéro de carte de crédit ou la clé cryptographique d'une personne.
- **L'attaque par authentification insuffisante** (ou Insufficient Authentication) permet à un pirate d'accéder à du contenu ou à une fonctionnalité sensible sans authentification appropriée.
- **La faiblesse de la validation de restauration du mot de passe** (ou Weak Password Recovery Validation) permet à un pirate d'obtenir, de modifier ou de récupérer de manière illégale le mot de passe d'un autre utilisateur.

Autorisation – accès illégal à des applications

- **La prédiction de certificat/session** (ou Credential/Session Prediction) est une méthode pour pirater ou dépersonnaliser un utilisateur.
- **L'attaque par autorisation insuffisante** (ou Insufficient Authorization) permet d'accéder à du contenu sensible ou à une fonctionnalité qui devrait exiger davantage de restrictions en matière de contrôle d'accès.
- **L'attaque par expiration de session insuffisante** (ou Insufficient Session Expiration) permet à un pirate de réutiliser des certificats ou des identifiants de session périmés pour bénéficier d'une autorisation.

“ Les solutions d'analyse des applications Web pour l'entreprise sont plus larges et doivent inclure un large éventail de tests des principales classes de vulnérabilités des applications Web, notamment les injections de code SQL, les scripts intersite et les traversées de répertoires. Le Top 10 de l'OWASP est une bonne liste de départ pour identifier les principales vulnérabilités, mais une solution d'entreprise ne devrait pas se limiter à une seule liste ou à une catégorie de vulnérabilités. En effet, une solution d'entreprise doit également permettre d'analyser de nombreuses applications, de suivre les résultats dans le temps et aussi de fournir un puissant reporting (en particulier des rapports de conformité) ainsi que des rapports personnalisés aux exigences locales. ”

Livre blanc sur le développement d'un programme de sécurité des applications Web
Securosis.com

- **Des attaques de type Fixation de session** (ou Session Fixation) forcent l'identifiant de la session d'un utilisateur sur une valeur explicite.

Attaques côté client – exécution illégale de code étranger

- **L'usurpation de contenu** (ou Content Spoofing) leurre un utilisateur en lui faisant croire qu'un certain contenu s'affichant sur un site Web est légitime et qu'il ne provient pas d'une source externe.
- **Le script intersite** (ou Cross-site Scripting - XSS) force un site Web à relayer le code exécutable fourni par un pirate et à le charger dans le navigateur Web de l'utilisateur.

Exécution de commandes – prise de contrôle d'une application Web

- **Les attaques par débordement de la mémoire tampon** (ou Buffer Overflow) altèrent le flux d'une application en écrasant certaines parties de la mémoire.
- **Une attaque de type Format String** altère le flux d'une application en utilisant les fonctionnalités d'une bibliothèque de formatage de chaînes pour accéder à un autre espace mémoire.
- **Les attaques par injection LDAP** exploitent les sites Web en construisant des instructions LDAP à partir des informations saisies par l'utilisateur.
- **La prise de contrôle à distance du système d'exploitation** (ou OS Commanding) exécute des commandes du système d'exploitation sur un site Web en manipulant les données entrées dans l'application.
- **L'injection de code SQL** construit des instructions SQL sur une application de site Web à partir des informations saisies par l'utilisateur.
- **L'injection SSI** (Server-Side Include) envoie du code dans une application Web qui est ensuite exécutée localement par le serveur Web.
- **L'injection XPath** construit des requêtes XPath à partir des informations saisies par un utilisateur.

Divulgaration d'informations – affichage des données sensibles pour les pirates

- **L'indexation de répertoires** (ou Directory Indexing) est une fonction automatique de serveur Web pour le listage/l'indexation de répertoires qui affiche tous les fichiers d'un répertoire demandé en l'absence du fichier de base normal.
- **Une fuite d'informations** se produit lorsque un site Web divulgue des données sensibles telles que les commentaires d'un développeur ou des messages d'erreur, ce qui peut aider un pirate à exploiter le système.
- **Une attaque par traversée de répertoires** (ou Path Traversal) force l'accès aux fichiers, dossiers et commandes pouvant se trouver en dehors du dossier racine du document Web.
- **Une attaque sur les lieux prévisibles des ressources** (ou Predictable Resource Location) révèle le contenu et les fonctionnalités cachés d'un site Web.

Attaques logiques – interférence avec l'utilisation de l'application

- **Une attaque par abus de fonctionnalités** (ou Abuse of Functionality) utilise les propres caractéristiques et fonctionnalités d'un site Web pour consommer, détourner ou faire échouer les mécanismes de contrôle d'accès.
- **Les attaques par déni de service** (ou Denial of Service - DoS) empêchent un site Web de satisfaire l'activité normale d'un utilisateur.
- **On parle de mesures d'anti-automatisation insuffisantes** (ou Insufficient Anti-automation) lorsqu'un site Web permet à un pirate d'automatiser un processus qui ne devrait pouvoir être exécuté que manuellement.
- **Une validation de processus insuffisante** (ou Insufficient Process Validation) permet à un pirate de contourner ou de faire échouer le flux légitime d'une application.

“ Le nombre de vulnérabilités affectant les applications Web s'est développé à une vitesse vertigineuse. En 2008, les vulnérabilités affectant les applications de serveur Web représentaient 54% de toutes les vulnérabilités connues. Elles étaient l'un des principaux facteurs de l'augmentation globale des vulnérabilités dévoilées au cours de l'année. ”

Rapport IBM X-Force® sur les tendances et risques pour 2008

Détecter les vulnérabilités des applications Web

Il n'existe pas de solution miracle pour détecter les vulnérabilités des applications Web. Pour ce faire, la stratégie est la même que l'approche multi-couche utilisée pour garantir la sécurité sur un réseau. La détection et la remédiation de certaines vulnérabilités impose l'analyse du code source, en particulier pour les applications Web d'entreprise complexes. La détection des autres vulnérabilités peut également nécessiter des tests de pénétration sur site. Comme mentionné plus avant, la plupart des vulnérabilités courantes des applications Web peuvent également être détectées à l'aide d'un scanner automatisé.

Un scanner automatisé des vulnérabilités des applications Web enrichit et complète les formes de test manuelles. Il offre cinq avantages majeurs :

- Réduction du coût total de fonctionnement en automatisant des processus de test répétables
- Identification des vulnérabilités de syntaxe et de sémantique au sein d'applications Web personnalisées
- Navigation authentifiée
- Profilage de l'application cible
- Précision garantie par réduction réelle des fausses alertes et des alertes non pertinentes

Comme un scanner n'a pas accès au code source d'une application Web, le seul moyen pour lui de détecter les vulnérabilités est de simuler des attaques contre l'application cible. La durée de l'analyse varie, mais simuler une attaque d'envergure sur une application prend beaucoup plus de temps que d'effectuer

une analyse des vulnérabilités du réseau sur une seule adresse IP. L'un des prérequis majeurs pour un scanner de vulnérabilités des applications Web est de pouvoir analyser pleinement les fonctionnalités de l'application cible. Si la couverture est partielle, le scanner ignorera les vulnérabilités existantes.

QualysGuard WAS détecte automatiquement les principales vulnérabilités des applications Web

La solution QualysGuard Web Application Scanning (WAS) est un service à la demande intégré à la suite QualysGuard de sécurité et de conformité fournie sous la forme de services (SaaS). Pour utiliser QualysGuard WAS, aucune connaissance spécifique de la sécurité Web n'est requise. Grâce à ce service, un administrateur informatique ou chargé de la sécurité du réseau peut exécuter des analyses de vulnérabilité complètes et précises sur des applications Web personnalisées, notamment des formulaires d'achat, des pages de connexion et autres types de contenu dynamique. L'étendue de la couverture se concentre sur les tests de sécurité des applications Web.

Principaux avantages. WAS automatise des techniques répétables utilisées pour identifier les vulnérabilités Web les plus courantes telles que l'injection de code SQL et le script intersite. Cette solution associe la reconnaissance des caractéristiques et l'observation des comportements pour identifier et vérifier avec précision les vulnérabilités. Le service WAS identifie et profile les formulaires de connexion, l'état d'une session, les pages d'erreur et autres fonctionnalités personnalisées de l'application cible, même si cette dernière s'étend sur de nombreux sites Web. Grâce aux données issues du profil du site, la solution WAS s'adapte aux modifications à mesure que l'application Web est optimisée. Fort de cette capacité d'adaptation, le scanner peut être utilisé pour des applications Web inconnues ou propriétaires pouvant contenir des informations sur des pages d'erreur ou autre comportement. WAS fournit donc une détection hautement précise tout en réduisant le nombre de fausses alertes. De par sa nature automatisée, le module Web Application Scanning permet d'effectuer régulièrement des tests pour obtenir des résultats cohérents. De plus, cette solution s'adapte facilement à un grand nombre de sites Web.

Fonctionnalités actuelles. Le tableau ci-après décrit les fonctionnalités complètes de QualysGuard WAS pour évaluer et suivre des vulnérabilités au sein d'applications Web. Qualys prévoit d'ajouter d'autres fonctionnalités au cours du 2ème/3ème trimestre 2009.

Navigation & découverte de liens

Un navigateur Web embarqué analyse le code HTML et une partie du code JavaScript pour en extraire des liens. Pondération automatique de l'étendue et de la profondeur des liens découverts pour parcourir jusqu'à 5000 liens par application Web.

Authentification

Authentification HTTP de base et NTLM depuis un serveur. Authentification par formulaire simple.

Liste noire	Navigateur interdit de visiter certains liens d'une application Web.
Liste blanche	Le navigateur ne doit visiter que les liens définis de manière explicite dans cette liste.
Optimisation des performances	Niveau de bande passante déterminé par l'utilisateur pour une analyse en parallèle afin de contrôler l'impact sur les performances applicatives.
Contenu sensible	Recherche de contenu d'après des expressions spécifiées par l'utilisateur dans le code HTML, notamment les numéros de sécurité sociale.

The screenshot shows a web browser window displaying a 'Web Application Report' from QualysGuard Enterprise Suite. The report is dated February 27, 2009, and was generated with an evaluation version of QualysGuard. It includes a summary section and a detailed results table.

Web Application		Port		Owner		Statistics		# Vulns				# Sensitive Content			Total
Title	Authentication	Port	Owner	# Links	Scan Time	XSS	SQL	INFO	PATH	CC	SSN	Custom	Total		
Demo application	Basic	80	Stephen Bindarup	54	00:24:29	1	3	0	1	0	0	0	5		
Test Site 2	None	80	Bill Olson	1	00:01:07	0	0	0	0	0	0	0	0		
Test Web Scan	None	80	Bo Mendentall	3	00:01:18	0	0	0	0	0	0	0	0		
test for error	MG Demo	80	Margo Connell	54	00:24:48	1	3	0	1	0	0	0	5		
Demo website - AD	Demo auth record - AD	80	Amr Dushmakh	54	00:24:27	1	3	0	1	0	0	0	5		

Des rapports tels que le Web Application Scorecard offrent une vue globale et une visibilité en profondeur des vulnérabilités pour chaque application Web

Fonctionnement. QG WAS est fourni sous la forme d'un service à la demande totalement intégré aux solutions QualysGuard déjà utilisées par des milliers de clients pour la gestion des vulnérabilités et la conformité aux politiques. Il est possible de gérer les applications Web, de lancer des analyses et de générer des rapports depuis l'interface Web QualysGuard familière. Quant aux analyses WAS, elles peuvent être programmées ou exécutées à la demande. Le service WAS peut s'étendre aux applications Web les plus importantes et qui sont hébergées n'importe où dans le monde. Avec la gestion des droits d'un compte, une entreprise peut contrôler de manière centralisée les applications Web pouvant être analysées par des utilisateurs particuliers.

Enfin, grâce à QualysGuard WAS, une personne au minimum dans votre entreprise est responsable de la gestion de la remédiation des vulnérabilités découvertes dans vos applications Web.

Protéger vos applications Web

Le service QualysGuard Web Application Scanning vous permet de commencer à identifier immédiatement les vulnérabilités de sécurité les plus courantes qui sont à la merci d'exploits criminels. Le scanner sera un puissant complément des politiques de sécurité en place, notamment l'analyse du code source et les tests de pénétration. Ces mesures de contrôle sont indispensables, mais QualysGuard WAS automatisera la détection et les tests pour la plupart des menaces, celles publiées concernant le pillage d'informations confidentielles par des voleurs de données par le biais d'applications Web. En plus de tests complets et d'une détection précise, QualysGuard WAS est rentable. À l'instar de QualysGuard, WAS est un service à la demande convivial qui permet aux administrateurs d'exécuter des analyses sans aucune connaissance particulière en matière de sécurité des applications Web.

Les versions d'évaluation de QualysGuard WAS sont disponibles immédiatement. La diffusion générale est prévue pour avril 2009. Pour obtenir une version d'évaluation de QualysGuard WAS sans engagement de votre part, il vous suffit de nous contacter.

A propos de Qualys

Qualys, Inc. est le principal fournisseur de solutions « à la demande » pour la gestion des vulnérabilités et de la conformité sous la forme de services (SaaS). Déployables en quelques heures seulement partout dans le monde, les solutions SaaS de Qualys fournissent aux entreprises une vue immédiate et permanente de l'état de leur sécurité et de leur conformité.

Actuellement utilisé par plus de 3500 entreprises dans 85 pays, dont 40 des 100 premières sociétés mondiales du classement établi par Fortune, le service QualysGuard® réalise plus de 200 millions d'audits IP par an. Qualys a opéré le plus important déploiement de ressources de gestion des vulnérabilités au monde au sein d'une société figurant parmi les 50 premières entreprises mondiales du classement Fortune.

Qualys a signé des accords stratégiques avec des fournisseurs de services d'infogérance (« managed services ») de premier ordre et des cabinets de conseil tels que BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, SecureWorks, Symantec, Tata Communications, TELUS et VeriSign.

Pour de plus amples informations, rendez-vous sur www.qualys.com.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
Royaume-Uni – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Allemagne – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japon – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys Hong Kong Ltd. • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 2824 8488

