QUALYS®
ON DEMAND SECURITY

LEITFADEN:

Web Application Security — So minimieren Sie das allgegenwärtige Angriffsrisiko

Inhalt

Überblick

Schwachstellen in Webanwendungen haben sich mittlerweile zum Hauptvektor für Angriffe auf die Unternehmenssicherheit entwickelt. Laut einer IBM-Studie betrafen im vergangenen Jahr fast 55% aller veröffentlichten Schwachstellen Webanwendungen.[1] Derselben Studie zufolge gab es Ende des Jahres für 74% aller Anfälligkeiten in Webanwendungen noch keinen Korrekturpatch. Wenn man von Exploits hört, die sensible Daten kompromittieren, ist vielfach von Übeltätern wie „Cross-Site Scripting“, „SQL-Injection“ und „Buffer Overflow“ die Rede. Solche Schwachstellen fallen oft nicht in den traditionellen Kompetenzbereich von Netzwerk-Sicherheitsmanagern. Deshalb bleiben Sicherheitslücken in Webanwendungen vergleichsweise häufig unbemerkt und lassen sich somit gut für Angriffe nutzen. Wie viele Unternehmen feststellen mussten, umgehen diese Angriffe die herkömmlichen Abwehrmechanismen in Unternehmensnetzwerken, sofern keine neuen Vorsichtsmaßnahmen getroffen werden. Um Ihnen einen Überblick darüber zu geben, wie sich derartige Risiken minimieren lassen, stellt Ihnen Qualys diesen Leitfaden zur Sicherung von Webanwendungen zur Verfügung. Er bietet eine Übersicht über typische Sicherheitslücken in Webanwendungen, vergleicht die Optionen für ihre Erkennung und stellt die Lösung QualysGuard Web Application Scanning vor – einen neuen On-Demand-Service von Qualys, mit dem sich die meistverbreiteten Sicherheitslücken in maßgeschneiderten Webanwendungen automatisch finden lassen.

Grundlagen der Web Application Security

Angriffe auf Schwachstellen in Webanwendungen begannen mehr oder weniger schon in den Anfangstagen des World Wide Web, Mitte der 1990er Jahre. Sie basieren zumeist auf dem gezielten Einschleusen von Fehlern, wobei Schwachstellen in der Syntax und Semantik einer Webanwendung ausgenutzt werden. Mit einem Standard-Browser und grundlegenden HTTP- und HTML-Kenntnissen kann ein Angreifer versuchen, einen bestimmten Exploit anzuwenden, indem er automatisch einen Uniform Resource Indicator (URI)-Link verändert, was wiederum Exploits wie SQL-Injection oder Cross-Site Scripting möglich machen kann.

http://example/foo.cgi?a=1
http://example/foo.cgi?a=1’ < SQL Injection
http://example/foo.cgi?a=<script> … < Cross-site Scripting (XSS)

Manche Angriffe versuchen den logischen Programmablauf zu manipulieren. Auch solche Angriffe werden mittels automatischer Veränderung eines URI durchgeführt.

http://example/foo.cgi?admin=false
http://example/foo.cgi?admin=true < Increase privileges

Eine beträchtliche Zahl von Angriffen nutzt Schwachstellen in der Syntax und Semantik aus. Viele dieser Schwachstellen können Sie mit einem automatisierten Scanning-Tool finden. Logische Schwachstellen sind dagegen mit einem

1 IBM ISS X-Force Trend- & Risiko-Report 2008, http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

Scanning-Tool sehr schwer zu testen und machen es erforderlich, den Quellcode der Webanwendung manuell zu analysieren und manuelle Sicherheitstests durchzuführen. Ursache von Sicherheitslücken in Webanwendungen sind in der Regel Fehler in einer Programmiersprache für Webanwendungen (z.B. Java, . NET, PHP, Python, Perl und Ruby), in einer Code-Bibliothek, einem Entwurfsmuster oder einer Architektur.

Diese Sicherheitslücken können komplex sein und unter verschiedensten Umständen auftreten. Eine Web Application Firewall kann die Folgen mancher Exploits verhindern, doch die ihnen zugrunde liegenden Schwachstellen behebt sie nicht.

Arten von Schwachstellen in Webanwendungen

In Webanwendungen können rund zwei Dutzend verschiedene Arten von Schwach-stellen auftreten. Security Consultants, die Penetrationstests durchführen, können sich auf die Ermittlung der kritischsten Schwachstellen konzentrieren, etwa die aus einer Liste, die vom Open Web Application Security Project (www.owasp.org) veröffentlicht wird. Ergebnis eines anderen Projekts zur systematischen Definition von Schwachstellen in Webanwendungen sind die sechs Kategorien, die das Web Application Security∑ Consortium (WASC) veröffentlicht hat (www.webappsec.org). Die nachfolgenden Beschreibungen von Schwachstellen in Webanwendungen orientieren sich am WASC-Schema.

Authentifizierung – Diebstahl von Benutzeridentitäten

- ***Brute Force-Attacke*** Ein automatisierter Angriff, bei dem versucht wird, durch Ausprobieren den Benutzernamen, das Passwort, die Kreditkartennummer oder den Geheimschlüssel eines Benutzers zu erraten.
- ***Unzureichende Authentifizierung*** Ermöglicht es einem Angreifer, auf sensible Inhalte oder Funktionen zuzugreifen, ohne sich korrekt authentifiziert zu haben.
- ***Schwache Passwort-Recovery-Funktion*** Ermöglicht es einem Angreifer, das Passwort eines anderen Benutzers unerlaubt auszulesen, zu verändern oder wiederzugewinnen.

Autorisierung – unerlaubter Zugriff auf Anwendungen

- ***Credential / Session Prediction*** Eine Methode, um die Session eines Benutzers zu übernehmen oder sich als dieser Benutzer auszugeben.
- ***Ungenügende Autorisierung*** Ermöglicht Zugriff auf sensible Inhalte oder Funktionen, die eigentlich erhöhte Zugriffsrechte erfordern.
- ***Mangelhaft Konfigurierter Session-Ablauf*** Versetzt einen Angreifer in die Lage, alte Session-Berechtigungen oder Session-IDs zur Autorisierung weiterzuverwenden.
- ***Session Fixation*** Angriffsmethode, die die Session-ID eines Benutzers auf einen festen Wert setzt.

> *“Enterprise-Lösungen zur Sicherheitsanalyse von Webanwendungen sind umfang-reicher und sollten ein breites Spektrum von Tests auf die wichtigsten Klassen von Schwachstellen in Webanwendungen bieten, wie etwa SQL-Injection, Cross-Site Scripting und Directory Traversals. Die OWASP Top 10-Liste für kritische Schwachstellen ist eine gute Ausgangsbasis, doch eine Lösung der Enterprise-Klasse sollte sich nicht auf eine einzige Schwachstellen-Liste oder -Kategorie beschränken. Au-ßerdem sollte eine Enterprise-Lösung in der Lage sein, vielerlei Anwendungen zu scannen, die Resultate über längere Zeiträume zu verfolgen, robuste Berichterstattung zu bieten (insbesondere Compliance-Reports) und auch Berichte zu liefern, die auf lokale Anforderungen zugeschnitten sind.”*
>
> Building a Web Application Security Program Whitepaper
> **Securosis.com**

Clientseitige Angriffe – unerlaubte Ausführung von fremdem Code

- ***Content Spoofing*** Täuscht einem Benutzer vor, dass ein bestimmter Inhalt, der auf einer Website erscheint, legitim ist und nicht aus einer externen Quelle stammt.
- ***Cross-Site Scripting*** (XSS) Zwingt eine Website, vom Angreifer eingeschleusten, ausführbaren Code zu verteilen, der dann im Browser eines Anwenders ausgeführt wird.

Befehlsausführung – Übernahme der Kontrolle über eine Webanwendung

- ***Buffer Overflow*** Angriffe dieser Art verändern den Programmablauf einer Anwendung, indem sie Teile des Speichers überschreiben.
- ***Format-String-Angriff*** Manipuliert den Programmablauf einer Anwendung, indem er Funktionen der String-Formatting-Library ausnutzt, um auf andere Bereiche des Programmspeichers zuzugreifen.
- ***LDAP-Injection*** Nutzt Websites aus, indem aus Benutzereingaben LDAP-Statements generiert werden.
- ***OS Commanding*** Führt mittels Manipulation der Benutzereingaben in eine Anwendung Betriebssystembefehle auf einer Website aus.
- ***SQL Injection*** Konstruiert aus Benutzereingaben in eine Webanwendung unzulässige SQL-Statements.
- ***SSI Injection*** (auch als Server-Side Include bezeichnet) Sendet einer Webanwendung Code, der dann später lokal auf dem Webserver ausgeführt wird.
- ***XPath Injection*** Konstruiert aus Benutzereingaben Xpath-Anfragen.

Offenlegung von Informationen – zeigt Angreifern sensible Daten

- ***Directory Indexing*** Eine automatische Verzeichnislisting-Funktion des Webservers, die bei Fehlen der üblichen Standarddatei alle Dateien in einem abgefragten Verzeichnis zeigt.
- ***Information leakage*** Liegt vor, wenn eine Website sensible Daten ausgibt – z.B. Kommentare der Entwickler oder Fehlermeldungen –, die einem Angreifer helfen können, das System zu missbrauchen.
- ***Path-Traversal*** Ermöglicht Zugriff auf Dateien, Verzeichnisse und Befehle, die potenziell außerhalb des Document Root-Verzeichnisses des Webservers liegen.
- ***Predictable Resource Location*** Angriffsmethode, um versteckte Inhalte oder Funktionalitäten einer Website zu finden.

Logische Angriffe – Eingriffe in die Abläufe bei der Nutzung einer Anwendung

- ***Funktionsmissbrauch*** Eigenschaften und Funktionen einer Website selbst werden genutzt, um Zugangskontrollen auszuschalten, zu überlisten oder zu umgehen.
- ***Denial-of-Service*** (DoS) Angriffstechnik, die das Ziel verfolgt, die üblichen Benutzeraktivitäten auf einer Website zu verhindern.
- ***Ungenügende Anti-Automation*** Erlaubt einem Angreifer, einen Prozess automatisiert auszuführen, der eigentlich nur manuell ausgeführt werden sollte.
- ***Ungenügende Prozessprüfung*** Erlaubt einem Angreifer, den vorgesehenen Anwendungsablauf zu umgehen.

“Die Zahl der Schwachstellen, die Webanwendungen betreffen, nimmt rasend schnell zu. 2008 machten Anfälligkeiten in Webserver-Anwendungen 54 Prozent aller veröffentlichten Schwachstellen aus und waren einer der Hauptgründe für den Gesamtanstieg der veröffentlichten Schwachstellen im Lauf dieses Jahres.”

IBM X-Force® Trend- & Risiko-Report 2008

Ermittlung von Schwachstellen in Webanwendungen

Für die Entdeckung von Schwachstellen in Webanwendungen gibt es keine „Wunderlösung“. Die Strategie zu ihrer Ermittlung entspricht dem mehrschichtigen Ansatz, der für die Sicherung eines Netzwerks praktiziert wird. Zur Entdeckung und Beseitigung einiger Sicherheitslücken muss der Quellcode analysiert werden, besonders dann, wenn es um komplexe Webanwendungen von Unternehmen geht. Zur Entdeckung anderer Schwachstellen können auch Penetrationstests vor Ort erforderlich sein. Die meistverbreiteten Schwachstellen in Webanwendungen lassen sich jedoch, wie bereits erwähnt, auch mit einem automatischen Scanner aufspüren.

Ein automatischer Schwachstellenscanner für Webanwendungen ergänzt und unterstützt die manuellen Testmethoden. Er bietet fünf entscheidende Vorzüge:

- Senkt die Gesamtbetriebskosten durch Automatisierung wiederholbarer Testprozesse
- Ermittelt Schwachstellen in der Syntax und Semantik unternehmenspezifischer Webanwendungen
- Führt authentifiziertes Crawling durch
- Erstellt ein Profil der Zielanwendung
- Gewährleistet Genauigkeit durch effektive Verminderung von False Positives und False Negatives

Da ein Scanner nicht auf den Quellcode einer Webanwendung zugreifen kann, kann er Schwachstellen nur ermitteln, indem er wahrscheinliche Angriffe auf die Zielanwendung durchführt. Die Scandauer ist unterschiedlich, doch wird für einen umfassenden simulierten Angriff auf eine Anwendung erheblich mehr Zeit benötigt als für einen Netzwerk-Schwachstellenscan einer einzelnen IP. Eine

zentrale Anforderung an einen Schwachstellenscanner für Webanwendungen besteht darin, dass er die Funktionalitäten der Zielanwendung umfassend abdeckt. Ist dies nicht der Fall, wird der Scanner bestehende Sicherheitslücken übersehen.

QualysGuard WAS entdeckt kritische Schwachstellen in Webanwendungen automatisch

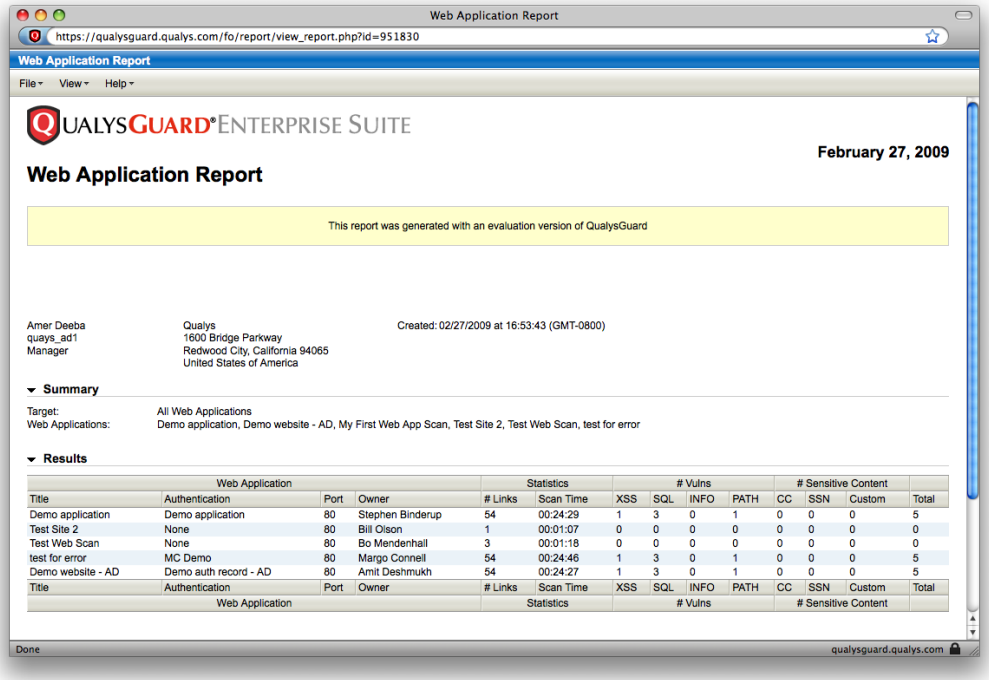
QualysGuard Web Application Scanning (WAS) ist ein On-Demand-Service, der in die Security und Compliance Suite QualysGuard integriert ist, die als Security-as-a-Service (SaaS) angeboten wird. Die Nutzung von QualysGuard WAS setzt keine speziellen Kenntnisse im Bereich Websicherheit voraus. Netzwerksicherheits- oder IT-Administratoren können mit dem Service umfassende, präzise Schwachstellenscans an unternehmensspezifischen Webanwendungen ausführen, wie etwa Einkaufswagen bei Webshop-Anwendungen, Formularen, Login-Seiten und dynamischen Inhalten anderer Art. WAS führt ein breites Spektrum von Tests durch und fokussiert dabei auf die Sicherheit von Webanwendungen.

Zentrale Benefits. WAS automatisiert wiederholbare Techniken, die eingesetzt werden, um die am weitesten verbreiteten Sicherheitslücken in Webanwendungen zu erkennen, wie etwa SQL-Injection- und Cross-Site Scripting-Schwachstellen. Auf Basis von Mustererkennung wie auch beobachteten Verhaltensweisen werden Schwachstellen präzise entdeckt und verifiziert. Der WAS-Service ermittelt und erstellt Profile für Login-Formulare, Sitzungszustand, Fehlerseiten und andere spezifische Merkmale der Zielanwendung – auch dann, wenn diese sich über mehrere Websites erstreckt. Mithilfe dieser Website-Profildaten kann sich WAS an Veränderungen anpassen, wenn sich die Webanwendung weiterentwickelt. Dank dieser Anpassbarkeit eignet sich der Scanner auch für unbekannte oder ältere Webanwendungen, für die wenig Informationen über Fehlerseiten oder sonstige Verhaltensweisen verfügbar sind. Auf dieses Weise kann WAS Schwachstellen außerordentlich präzise erkennen und Fehlalarme reduzieren. Da die Scans automatisiert ablaufen, können regelmäßig Tests durchgeführt werden, die konstant zuverlässige Resultate erbringen und leicht skalierbar sind, sodass sie auch auf eine hohe Zahl von Websites angewendet werden können.

Aktuelle Leistungsmerkmale. Die nachfolgende Tabelle gibt einen Überblick über die umfassenden Fähigkeiten zur Analyse und Verfolgung von Schwachstellen in Webanwendungen, die QualysGuard WAS derzeit bietet. Im Lauf des 2./3. Quartals 2009 wird Qualys voraussichtlich weitere Leistungsmerkmale implementieren.

Crawling & Link-Erkennung	Eingebetteter Webcrawler analysiert HTML und teilweise JavaScript, um Links zu extrahieren. Balanciert automatisch die Breite und Tiefe der gefundenen Links, um bis zu 5.000 Links pro Webanwendung crawlen zu können.
Authentifizierung	HTTP-Basic- sowie serverbasierte NTLM-Authentifizierung. Einfache Formularauthentifizierung.

Blacklist	Verhindert, dass der Crawler bestimmte Links in einer Webanwendung besucht.
Whitelist	Weist den Crawler an, nur Links zu be-suchen, die in dieser Liste ausdrücklich aufgeführt sind.
Performance-Tuning	Benutzerdefinierte Brandbreite für paralleles Scannen, um die Auswirkungen auf die Leistung der Webanwendung zu steuern.
Sensible Inhalte	Ermöglicht bei HTML-Inhalten eine benutzerdefinierte∑ Suche nach Ausdrücken, zum Beispiel Sozialversicherungsnummern.



Reports wie die Web Application Scorecard liefern einen Überblick über die Schwachstellen in jeder Webanwendung sowie Informationen in wählbarer Detailtiefe

Funktionsweise. QG WAS wird als On-Demand-Service bereitgestellt und ist vollständig in die QualysGuard-Lösungen integriert, die bereits von Tausenden von Kunden genutzt werden, um Schwachstellenmanagement durchzuführen und Policy-Compliance zu gewährleisten. Über die vertraute QualysGuard-Bedienoberfläche können die Nutzer Webanwendungen verwalten, Scans starten und Reports erzeugen. Die WAS-Scans können vorab geplant oder nach Bedarf durchgeführt werden. Der WAS-Service ist skalierbar und damit selbst für die größten Webanwendungen geeignet, unabhängig davon, wo auf der Welt sie gehostet werden. Die Kontorechteverwaltung gibt Unternehmen die Möglichkeit, zentral zu regeln, welche Webanwendungen von bestimmten Anwendern gescannt werden dürfen.

Zudem erfordert QualysGuard WAS, dass mindestens eine Person in Ihrem Unternehmen für die Beseitigung der in Ihren Webanwendungen gefundenen Schwachstellen verantwortlich ist.

Schützen Sie Ihre Webanwendungen

Der QualysGuard Web Application Scanning Service hilft Ihrem Unternehmen, umgehend die meistverbreiteten Sicherheitsanfälligkeiten zu ermitteln, die von Kriminellen ausgenutzt werden können. Der Scanner ergänzt wirksam bereits bestehende Sicherheitsmaßnahmen wie etwa Quellcode-Analysen und Penetrationstests. Solche Maßnahmen sind zwar unerlässlich, doch QualysGuard WAS automatisiert die Tests zur Erkennung der Mehrzahl der Bedrohungen – eben jener, die immer wieder Schlagzeilen machen, wenn sich Datendiebe mithilfe von Webanwendungen vertrauliche Informationen beschaffen. Neben umfassenden Analysen und präziser Erkennung zeichnet sich QualysGuard WAS auch durch Kosteneffizienz aus. Genau wie QualysGuard ist WAS ein benutzerfreundlicher On-Demand-Service, mit dem Administratoren Scans durchführen können, ohne spezielle Kenntnisse über die Sicherheit von Webanwendungen besitzen zu müssen.

QualysGuard WAS kann jetzt kostenfrei getestet werden. Ab Mai 2009 wird der Service voraussichtlich allgemein verfügbar sein. Wenn Sie QualysGuard WAS kostenlos testen möchten, setzen Sie sich bitte mit Qualys in Verbindung.

Über Qualys

Qualys, Inc. ist der führende Anbieter von On-Demand-Lösungen für IT-Sicherheits- und Compliance-Management, die als Service bereitgestellt werden. Die Software-as-a-Service-Lösungen von Qualys können innerhalb von Stunden an jedem Ort der Welt verfügbar gemacht werden und vermitteln den Kunden einen sofortigen und kontinuierlichen Überblick über ihre Sicherheits- und Compliance-Aufstellung.
Der Service QualysGuard® wird derzeit von mehr als 3.500 Unternehmen in 85 Ländern genutzt – darunter 35 der Fortune Global 100 – und führt pro Jahr mehr als 200 Mio. IP-Audits durch. Bei einem Unternehmen der Fortune Global 50 betreibt Qualys die weltweit größte Installation einer Schwachstellenmanagement-Lösung mit mehr als 223 Appliances, die auf 53 Länder verteilt sind und mehr als 700.000 Systeme scannen. Qualys hat strategische Vereinbarungen mit führenden Managed Service Providern und Consulting-Firmen geschlossen, darunter BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, SecureWorks, Symantec, TELUS und Verisign.

Weitere Infos unter ***www.qualys.com***.

QUALYS®
www.qualys.com

USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – 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
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

ON DEMAND SECURITY