QUALYSGUARD® WEB APPLICATION SCANNING

WEBOVÁ APLIKACE PROVĚŘÍ BEZPEČNOST NEOMEZENÉHO POČTU WEBOVÝCH STRÁNEK – SLUŽBA NA VYŽÁDÁNÍ

Zranitelnosti webových aplikací představují dnes nejvýznamnější trend bezpečnostních útoků na firmy. Zprávy o bezpečnostních dírách kompromitujících data často označují za pachatele metody typu “cross-site scripting,” “SQL injection,” a “web site misconfiguration”. Zranitelnosti webových aplikací spadají mnohdy mimo tradiční oblast působení sítových bezpečnostních manažerů a nejasnosti kolem nich vytvářejí příležitosti pro specifické útoky. Jak mnoho organizací už zjistilo, zmíněné útoky budou obcházet tradiční firemní síťovou ochranu do té doby, dokud nebudou implemetována nová opatření.

Bezpečnostní zranitelnost webové aplikace většinou vzniká z důvodu chyby v konfiguraci nebo programátorské chyby v programovacím jazyce (např. Java, .NET, PHP, Python, Perl, Ruby), knihovnách, designu nebo architektuře. Tyto zranitelnosti mohou být velice komplexní a mohou nastat za různých podmínek.

Úvod do QualysGuard® Web Application Scanning

Aby mohli zákazníci hodnotit a sledovat zranitelnosti jejich webových aplikací, Qualys uvádí nového člena skupiny QualysGuard® Security a Compliance Suite – službu QualysGuard Web Application Scanning (WAS) 1.0. Nová služba na vyžádání sleduje a testuje webové aplikace, přičemž identifikuje jejich zranitelnosti, například ty v seznamech OWASP Top 10 a WASC klasifikaci hrozeb, zahrnujících metody SQL Injection a Cross-Site Scripting. Uživatelé tak mohou řídit webové aplikace a generovat reporty prostřednictvím intuitivního uživatelského rozhraní QualysGuard.

Výhody QualysGuard WAS

- Snižuje celkové provozní náklady pomocí automatizovaných a opakovatelných testovacích procesů.
- Identifikuje syntaktické a sémantické zranitelností webových aplikací.
- Profiluje cílové aplikace, vykonává autentizované prohledávání a audit.
- Zvyšuje přesnost a snižuje počet falešně pozitivních nálezů prostřednictvím profilování webové stránky.
- Skenování libovolného počtu interních nebo externích webových aplikací, v ostrém nebo vývojovém prostření, s použitím platformy QualysGuard Software-as-a-Service (SaaS).

“Podniková třída skenovacích řešení webových aplikací je širší, a měla by obsahovat široký rozsah testů pro hlavní třídy bezpečnostních zranitelností, jako jsou SQL injection, cross-site scripting, a directory traversal. Podnikové řešení by mělo také umožňovat vícenásobné skenování aplikací, průběžné sledování výsledků, nabízet rozsáhlé reportovací možnosti (zejména reporty o opatřeních) a možnost přizpůsobovat reporty specifickým požadavkům.”

Building a Web Application Security Program Whitepaper
Securosis.com

“Počet zranitelností webových aplikací vzrostl enormní rychlostí. V roce 2008 zastupovaly zranitelnosti ovlivňující web-serverové aplikace 54 procent z celkového počtu objevených zranitelností a představovaly jeden z hlavních faktorů celkového nárůstu zranitelností odhalených během zmíněného roku.”

IBM X-Force® 2008 Trend & Risk Report

Vlastnosti QualysGuard WAS :

Procházení a hledání odkazů — Vestavěný webový průzkumník vybírá z kódu HTML a JavaScript webové odkazy. Automaticky při prohledávání vyrovná šířku a hloubku zahrnutých odkazů až do počtu 5000 odkazů na aplikaci.

Autentizace — Autentizace HTTP Basic, Digest a NTLM. Jednoduchá formulářová autentizace.

Black List — Zabraňuje průzkumníkovi procházet specifikované odkazy ve webových aplikacích.

White List — Nařizuje průzkumníkovi procházet pouze definované webové odkazy.

Ladění výkonu — Případné snížení výkonu aplikace zapříčiněné testováním může uživatel regulovat stanovením velikosti zpřístupněné šířky pásma paralelního skenování.

Citlivý obsah — Umožňuje automatizované vyhledávání specifikovaných výrazů nebo citlivých informací na jednotlivých webových stránkách.

Workflow pro definování skenů a generování specifických reportů — Vlastní workflow pro každou webovou aplikaci. Detailní a srozumitelné reporty o zranitelnostech.

Create Web Application(s)

WAS Scan Options

WAS Scan Results

Jak pracuje QualysGuard WAS :

Etapa zkoumání

Sofistikovaný skenovací nástroj disponuje několika efektivními technikami pro zkoumání webových stránek. Stačí poskytnout pouze uživatelské jméno a heslo, průzkumník automaticky identifikuje stránku HTML s přihlašovacím formulářem, testuje průběh přihlášení, monitoruje neustále stav přihlášení, aby zajistil skenování pod danými právy. Průzkumník se pokouší otestovat funkčnost webových stránek nastavením různé šířky a hloubky skenování, a přitom se vyhýbá redundantním a rekurzivním odkazům. Průzkumník také profiluje běžné chování webových stránek, aby odhalil jejich chyby a taktéž používá informace profilu k redukci chyb během testování.

Etapa hodnocení

V testovací fázi WAS vyhledává zranitelnosti typu SQL injection, cross-site scripting, source disclosure, a directory traversal. Testovací engine používá mix signatur a profilů stránek, pomocí nichž upřesňuje rozhodnutí o přítomnosti zranitelností. Testování se současně zaměřuje na vznik problémů zapříčiněných chybami a když to je možné, tak rozeznává mezi zneužitelnými problémy a prostým prozrazením informací.

Vyhodnocení a reporting

Reportovací engine vypisuje ke každé stránce problémy týkající se zranitelností, jako jsou cross-site scripting nebo SQL injection a taktéž vytváří souhrnné reporty i pro celé skupiny aplikací. QualysGuard WAS zavádí nový mechanismus pro řízení přístupu ke skenování jednotlivých webových aplikací pro případ diferencovaných postupů nápravných opatření nebo testování určitých specifických webových aplikací.

Cenová kalkulace a dostupnost :

QualysGuard WAS je k dispozici jako část QualysGuard Security a Compliance Suite. Roční předplatné služby QualysGuard WAS je licencováno podle počtu webových aplikací. Licence zahrnující neomezené skenování, automatické aktualizace a zákaznickou podporu 24×7 jsou stanoveny na rok.

Více informací na http://www.qualys.cz.

Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Praha 2
Česká republika
telefon: +420 221 628 400
fax: +420 221 628 401
email: qualys@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.

QUALYS®
www.qualys.com