Drei Webapplikations-Scanner im Vergleich

Die schwächste Stelle

Martin Wundram

Wer auch nur einen Funken Risikobewusstsein hat, schaltet keine Webanwendung ohne vorherige Sicherheitstests frei. Werkzeuge für Auditoren und Einbruchstester existieren in allen möglichen Ausführungen und Preisklassen. Wie man mit ihnen vorgeht und was sie leisten, zeigt *iX* an drei Produkten.

Übung macht den Meister, so viel ist bekannt. Aber wie groß ist der Unterschied wirklich zwischen der „Out of the box"-Verwendung von Webapplikations-Scannern im Vergleich zu einer angepassten Vorgehensweise? Wo liegen Stärken und Schwächen verschiedener Programme, wie bedient man sie? Denn von kostenlos bis teuer bietet der Markt viel Auswahl, und gerade umfassende Suites mit grafischer Oberfläche sind aufgrund ihrer zahlreichen Helfer- und Komfortfunktionen für viele Penetrationstester interessant [1]. Ein praxisrelevanter Vergleich verfügbarer Produkte, bei dem Scanner zuerst vollautomatisiert und dann händisch betreut auf Testumgebungen losgelassen werden, soll diese Fragen beantworten.

Einige Experten haben bereits gute Vergleichstests durchgeführt und veröffentlicht, die jedoch bisweilen zu unterschiedlichen Ergebnissen kommen. Denn die Resultate hängen bei weiterführenden Tests stark von der Methodik des Experten und natürlich von der Testumgebung ab. So darf man beispielsweise bei den von Scanner-Herstellern angebotenen Testumgebungen [a, b] getrost davon ausgehen, dass die jeweiligen Produkte dort alle Schwachstellen zuverlässig finden.

Adam Doupé, Marco Cova und Giovanni Vigna von der University of California kamen 2010 nach einer Untersuchung [c] und einem Vergleich der Scanner Acunetix, AppScan, Burp Suite, Grendel-Scan, Hailstorm, Milescan, N-Stalker, NTOSpider, Paros, w3af und Webinspect zu dem Ergebnis, dass das Crawling moderner Webanwendungen eine echte Hürde für die aktuell verfügbaren Webapplikations-Scanner darstellt. So ließ ein Image-Upload-Formular, das verschiedene Schwachstellen enthält, die Mehrheit der Programme scheitern.

Auch das Erkennen und Umsetzen anwendungsspezifischer Verarbeitungslogik stößt an Grenzen. Die Forscher erklärten, dass Blackbox-Scanner nur schwerlich vollautomatisch zu guten

iX-TRACT

- Da Webanwendungen zu den größten Einfallstoren für Hacker zählen, sollte niemand seine Website ungeprüft freischalten. Für solche Penetrationstests oder Sicherheitsaudits existieren zahlreiche freie und kommerzielle Werkzeuge.
- Alle Scanner und Test-Suites haben ihre Eigenheiten sowie Vorzüge und Nachteile. Die besten Resultate erzielt, wer mehrere Werkzeuge kombiniert.
- Zwar bieten automatisierte Tests Ungeübten einen guten Einstieg und finden bereits die ein oder andere kritische Schwachstelle, ohne Expertenwissen kann man aber keine Website auf Herz und Nieren prüfen und absichern.

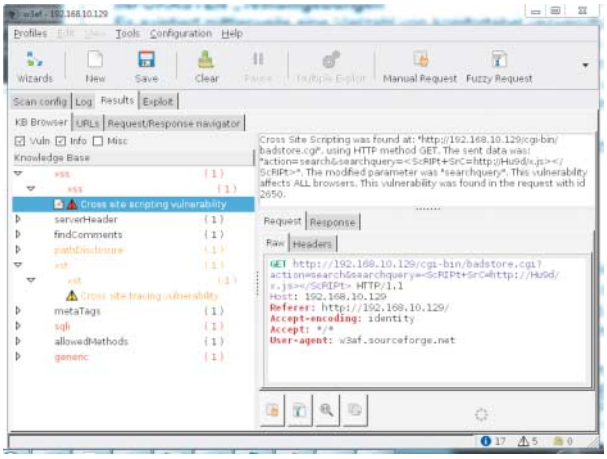
Ergebnissen kommen, sondern erst in den Händen von Fachleuten zu effektiven Hilfsmitteln werden. Zu vergleichbaren Ergebnissen kamen bereits 2008 Sean McAllister, Engin Kirda und Christopher Kruegel von der Universität Wien [d]. Damit Scanner „tiefer“ in Webanwendungen hineinblicken können, muss der Benutzer sie an die Hand nehmen und führen.

Der Sicherheitsforscher Shay-Chen hat sich intensiv mit dem Vergleich von über 40 kostenfrei verfügbaren Scannern beschäftigt, das Web Application Vulnerability Scanner Evaluation Project – WAVSEP – ins Leben gerufen (siehe Kasten „Testumgebungen für …“) sowie 2010 und 2011 zwei umfangreiche Blog-Einträge zur Bewertung von Webapplikations-Scannern verfasst [e, f]. Neben vielen Einzelergebnissen kommt er dort zu dem Schluss, dass eine Kombination mehrerer Programme die besten Ergebnisse liefert.

Im Folgenden werden mit *w3af*, Burp Suite Pro und Acunetix WVS drei leistungsfähige Webapplikations-Scanner näher betrachtet, die weltweit von Penetrationstestern eingesetzt werden und bei den zitierten Tests insgesamt gut abgeschnitten hatten. Außerdem deckt diese Auswahl das Spektrum von kostenlos bis kostenpflichtig ab.

w3af (Web Application Attack and Audit Framework), von Andreas Riancho und anderen entwickelt, ist Open Source und kostenlos verfügbar. Auf der Download-Webseite finden sich auch Dokumentationen und Informationen über die Mailing-Liste. Seit dem 25. Mai gibt es die stabile Version 1.0 mit etlichen maßgeblichen Verbesserungen und neuen Funktionen, etwa einen PHP static code analyzer. Sie ist aber (noch) nicht auf Deutsch verfügbar.

w3af läuft auf vielen Architekturen (Windows, Linux, Mac OS X, xBSD) und bietet neben einer grafischen Oberfläche eine Konsolenvariante. Sicherlich besonders interessant ist die Option, Exploits einzusetzen und so zum Beispiel über eine Schwachstelle im Anwendungscode eigene Systembefehle ausführen zu lassen. Das Werkzeug *w3af* bringt dafür sogar eine virtuelle Shell und eine Metasploit-Anbindung mit. Hilfreich ist die Möglichkeit, aus dem reichhaltigen Angebot an Test- und Discovery-Verfahren die in den jeweiligen Profilen getroffene Auswahl zu speichern. Dieser Scanner enthält überdies einige vorkonfigurierte Profile wie die Suche nach den OWASP Top 10 [g], den zehn größten Risiken für Webanwendungen.



Anders als andere Werkzeuge hält *w3af* die Beschreibung der Scan-Ergebnisse recht knapp (Abb. 1).

Auch die Burp Suite des Herstellers PortSwigger hat einiges zu bieten und ist, da in Java geschrieben, auf vielen Architekturen ohne Installation direkt lauffähig. Die Suite bietet mit der seit dem 3. Juni verfügbaren Version 1.4 leistungsfähige neue Features, unter anderem einen Headless-Betrieb (also ohne grafische Ausgabe). Neben der kostenfrei verfügbaren Basisversion bietet die Pro-Variante für 210 Euro jährlich zusätzliche Funktionen wie das automatische Suchen nach Sicherheitslücken. Sie ist aber ebenso wenig wie *w3af* auf Deutsch verfügbar.

Schon preislich bildet der unter Windows lauffähige Web Vulnerability Scanner (WVS) von Acunetix das Schwergewicht. Eine Jahreslizenz zum Eigengebrauch für eine Domain ist ab 995 Euro und eine Lizenz für Consultants ab 3100 Euro zu haben. Pro-Support, etwa per Telefon, gibt es gegen Aufpreis. Es ist ebenfalls eine kostenfreie Version verfügbar, sie testet jedoch nur auf Cross-Site-Scripting(XSS)-Verwundbarkeit. WVS ist zwar auch nicht auf Deutsch erhältlich, bietet dafür aber einige hilfreiche Funktionen wie ein Firefox-Plug-in und eine AcuSensor genannte Technik. Durch serverseitige Integration dieser Technik in .Net- oder PHP-Code verspricht Acunetix, mehr Sicherheitslücken in kürzerer Zeit zu finden und diese direkt auf den Source-Code oder einzelne SQL-Abfragen beziehen zu können.

Diese drei Webapplikations-Scanner sind auch deshalb leistungsfähig, weil sie sich erweitern oder in andere Programme beziehungsweise Prozesse integrieren lassen. Dazu später mehr.

Nicht immer werden Tests von erfahrenen Penetrationstestern durchgeführt. Anfänger setzen gerade die günstigen oder kostenfreien Scanner gerne ein, insbesondere um eigene Webseiten auf Schwachstellen zu untersuchen. Aber auch Experten haben nicht jederzeit eine knackige Beschreibung aller Problemtypen, ihre Bedeutung und Auswirkungen parat. Umfangreiche Webapplikations-Scanner helfen hier mit einem eingebauten Expertensystem. Sie bewerten eine gefundene Schwachstelle, geben Erklärungen für mögliche Ursachen und Folgen sowie Gegenmaßnahmen ab. Das spart Zeit und kann helfen, Fehlinterpretationen zu vermeiden.

Webapplikations-Scanner als „Expertensystem“

Die Burp Suite und der Scanner von Acunetix sind in diesem Punkt besonders ausführliche Helfer. Beide klassifizieren eine gefundene Schwachstelle, geben Hintergrundinformationen über Ursachen und beschreiben die daraus resultierenden Gefahren. Schließlich geben beide zum Teil ausführliche Erklärungen, wie man die jeweiligen Schwachstellen grundsätzlich beseitigen kann. *w3af* hingegen beschränkt sich auf das Wesentliche und liefert für die gefundenen Lücken lediglich eine Kategorisierung und Klassifizierung inklusive einer knappen Beschreibung (Abb. 1).

Für den vorliegenden Test wurden *w3af*, Burp Suite Pro und Acunetix hauptsächlich im vollautomatischen Modus auf drei Testumgebungen losgeschickt. Dazu dienten die Damn Vulnerable Web Application (DVWA), die als schlüsselfertige virtuelle Maschine inklusive Webserver und Datenbank verfügbar ist, der BadStore, den man sich ebenfalls als „No config“-Maschine samt Apache und MySQL herunterladen kann, und die Acunetix-Testseite als Hersteller-Testumgebung. Der Kasten „Testumgebungen für Webapplikations-Scanner“ listet weitere Systeme nebst URLs auf.

Die Resultate sind positiv und decken sich mit den oben zitierten Testergebnissen. Zwar finden die Scanner nicht alle Schwachstellen, die Ergebnisse sind aber insgesamt überzeugend. Out of the

Der Penetrationstester wählt die zu manipulierenden Parameter aus (Abb. 2).

Box arbeitet die Suite von Acunetix besonders gründlich und listet neben den Ergebnissen eines Portscans auch noch gefundene Backup-Dateien, ungeschützte phpMyAdmin-Frontends, veraltete Softwareversionen, Injection-Schwachstellen im Apache sowie unsichere SSL-Versionen auf und berücksichtigt außerdem noch die Google Hacking Database (GHDB). Auch das Werkzeug *w3af* sucht übrigens via GHDB nach Verwundbarkeiten.

Erste Penetrationstests gehen mit *w3af* und Acunetix besonders intuitiv von der Hand, denn sie fragen zu Beginn nach der zu testenden Webseite/URL und nach dem zu verwendenden Testprofil. Danach geht es mit der automatischen Suche nach Sicherheitslücken auch gleich los. Die Burp Suite hingegen startet ohne gesonderte Meldung einen Proxy und wartet auf „vorbeikommende“ Requests. Der Penetrationstester muss also zunächst in seinem Browser den Burp-Proxy einstellen und die zu testende Seite ansteuern. Auf diesem Wege gelangt das gewünschte Ziel in die Liste des Scanners, der nebenbei passiv auf mögliche Sicherheitslücken prüft.

Nun kann man in der Burp Suite zu jedem Zeitpunkt unter Angabe eines zu testenden Bereichs einen Spider-Prozess starten, der die Webseite so vollständig wie möglich durchläuft und analysiert. Den hierbei ebenfalls passiv mitlaufenden Scanner kann der Penetrationstester im Anschluss im aktiven Modus starten, damit er auch mit invasiven Techniken nach Schwachstellen sucht. Die Burp Suite arbeitet damit nicht ganz so „vollautomatisch“ wie die beiden anderen Scanner.

Vulnerabilities und Profile

Nicht nur gute Heuristiken und generische Testschemata sind für einen zielführenden Penetrationstest wichtig. Eine ergänzende Vulnerability-Datenbank gibt die Sicherheit, dass ein Werkzeug bereits bekannte Schwachstellen zuverlässig und schnell finden kann. Acunetix enthält als einziger der Scanner eine umfangreiche Datenbank.

w3af verfügt immerhin über Plugins, die etwa in Google und Bing nach relevanten Informationen über eine untersuchte Webseite fahnden, sowie über ein Plug-in, das verwandte Wörter aus einer Datenbank sucht und verwendet (etwa „schwarz“ und „weiß“ als Ergänzung zu einem gefundenen Parameter „blau“). Außerdem bieten beide Scanner mit anpass- und speicherbaren Profilen die Möglichkeit, aus den enthaltenen Modulen die für einen bestimmten Penetrationstest relevanten auszuwählen. Schon vorbereitet sind bei beiden beispielsweise die Suche nach den oben genannten OWASP Top 10 oder spezielle Brute-Force-Tests.

Testumgebungen für Webapplikations-Scanner

Es existieren mittlerweile viele komfortabel verwendbare Testumgebungen, die Interessierte zum Einarbeiten in das Themenfeld Web-Security und natürlich zum Testen von Webapplikations-Scannern verwenden können. Für einen eigenen Test ist es aber auch empfehlenswert, selbst eine Testumgebung zu erstellen oder eine existierende an die eigenen Bedürfnisse anzupassen beziehungsweise zu erweitern. Einige der verfügbaren Umgebungen sind hier aufgeführt:

BadStore: ebenfalls erhältlich als ISO-Image (www.badstore.net);

BodgeIt Store: beziehbar als Anwendung zum Einbinden in einen eigenen Webserver (code.google.com/p/bodgeit);

DVWA: verfügbar als ISO-Image, zum Beispiel zur Benutzung in einer VM, und als Webseite, etwa zur Verwendung in einer eigenen Umgebung (www.dvwa.co.uk);

Vicnum: verfügbar als betriebsfertige virtuelle Maschine (sourceforge.net/projects/vicnum);

OWASP Broken Web Applications Project: ebenfalls vorhanden als VM (https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project);

Web Application Vulnerability Scanner Evaluation Project (WAVSEP): verfügbar als Anwendung (code.google.com/p/wavsep).

Webapplikationen mit Ajax stellen für Scanner eine echte Herausforderung dar, weil die technische und logische Komplexität grundsätzlich höher und durch asynchrone, kleinschrittige Operationen noch weniger im Ganzen erfassbar ist. Im Übrigen gilt das ganz allgemein für jede Form komplexerer Business-Logik, also etwa für das Durchlaufen ganzer Prozessketten. Woher sollen die Programme auch wissen, dass zuerst ein Login nötig ist, dann das Hinzufügen von Artikeln in den Warenkorb, das Erreichen eines Mindestbestellwertes, das Auswählen einer Zahlungsoption und schließlich der Checkout? Ein einfaches Beispiel soll die Schwierigkeiten zeigen. Es handelt sich dabei um ein Ajax-Tool zum gemeinsamen Gestalten und Verwalten von Trainingsplänen, das der Autor für seinen Sportverein „gestrickt“ hat.

Ohne gültiges Login sind hier offensichtlich kaum relevante Ergebnisse zu erzielen, es sei denn, es lassen sich per Brute Force gültige Zugangsdaten finden. Aber auch mit gültigen Login-Daten schaffte es der Spider der Burp-Suite nicht, das Ajax-Login-Formular korrekt abzuschicken. Ein vollständiges Durchsuchen und Analysieren der Webseite war somit erst einmal nicht möglich. Stattdessen funktionierte es, sich im Browser einzuloggen und den Scanner danach das gültige Session-Cookie sniffen und verwenden zu lassen.

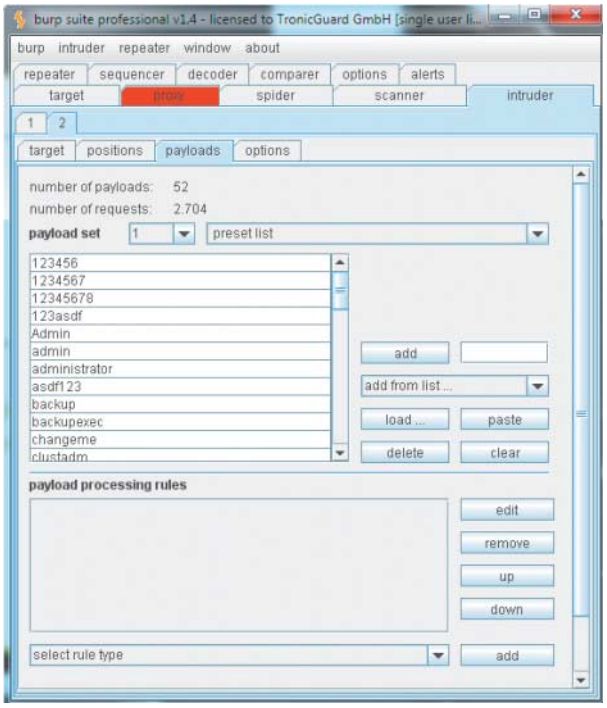
Ajax – eine besondere Herausforderung

Nun gelang es der Burp Suite, nahezu die gesamte Webseite zu erfassen („spidern“). Bei der anschließenden Suche nach Schwachstellen kam sie jedoch wieder nicht mit der Ajax-Implementierung zurecht und versandte Aktionen per GET statt POST – obwohl die Anwendung alle Daten per POST erwartet und die Aktionen dementsprechend konfiguriert sind. So wurde ein beachtlicher Teil der Webanwendung überhaupt nicht getestet, denn der Scanner sah statt Folgeschritten nur 500er-Fehler. Auch Acunetix und *w3af* kamen mit dem umständlichen Ajax-Login nicht zurecht, obwohl die korrekten Login-Daten konfiguriert waren.

Um erfolgreich die verschlungenen Pfade komplexer Webanwendungen zu meistern – und das geht mit allen hier betrachteten Webapplikations-Scannern –, müssen Penetrationstester eingreifen und die wesentliche Arbeit

selbst machen, insbesondere die Verarbeitungslogik einer Webanwendung erkennen und berücksichtigen. Die Webapplikations-Scanner übernehmen dann eher unterstützende und gut automatisierbare Arbeiten. Sie folgen dem Experten, indem sie als Proxy zwischen Browser und Webanwendung alle Datenströme mitlesen und bei Bedarf verändern können.

Mit dem Burp Intruder, einem Werkzeug aus der Burp Suite, können die Zuständigen recht komfortabel eigene Tests und Angriffe vorbereiten und automatisiert durchführen lassen. Dazu gehören etwa das Füttern von Requests mit Zufallsdaten („Fuzzing“) auf der Suche nach XSS- oder SQL-Injection-Schwachstellen, Brute-Force-Tests gegen Formulare sowie das Session-Handling und parallele Requests zum Finden von Race Conditions.



Bei einem Brute-Force-Angriff auf das Login besteht die Payload aus einer Datei mit Benutzernamen und Passwörtern (Abb. 3).

Dank des Intruders benötigt ein Brute-Force-Angriff auf das Login-Formular der DVWA nur wenige Schritte. Zunächst stellt der Tester den Proxy so ein, dass er alle Requests abfängt und nach Rückfrage testweise einen Login-Request an den Intruder weiterleitet. Dort wählt er anschließend aus, welche Parameter manipuliert werden sollen (Abb. 2). Für beide manipulierenden Parameter muss er nun eine Payload aussuchen, in unserem Fall jeweils eine Textdatei mit Benutzernamen und Passwörtern (Abb. 3). Erfolgreiche Logins kann das Werkzeug abschließend leicht aus der Masse der fehlerhaften herausfiltern, da bei ihnen der Umfang der zurückgelieferten Webseite einige Byte größer ausfällt.

Auch komplexere Angriffe wie die Suche nach blinden SQL-Injections

iX-Wertung

w3af

⊕ Open Source und vollständig anpassbar

⊕ Exploit-orientiert

⊖ noch nicht so stabil wie erwartet

⊖ kann Ergebnisse und Bearbeitungsstand nicht speichern

Burp Suite

⊕ Java-API und Headless-Betrieb

⊕ leistungsstarker Intruder

⊖ keine vorgefertigten Profile

Acunetix WVS

⊕ umfangreiche Helfer

⊕ umfangreiche Reports

⊕ Datenbank mit erfassten Schwachstellen

⊖ nativ nur unter Windows lauffähig

Nicht ohne Ecken und Kanten

Ganz ohne Fehler und Hakeleien sind auch die besten Werkzeuge oder Testumgebungen nur selten. Kennt man sie, lassen sich aber Fehlinterpretationen oder misslungene Tests vermeiden oder zumindest in den Ergebnissen berücksichtigen. So funktioniert die virtuelle Maschine von DVWA in der aktuellen Version 1.0.7 anscheinend nicht ganz korrekt, ein Login ist initial nicht durchführbar – es fehlen die Tabellen in der MySQL-Datenbank. Diese kann man durch händisches Aufrufen der *setup.php* anlegen. Danach ist das Login mit den angegebenen Daten (admin:password) problemlos möglich.

Die aktuelle Version der Firefox-Erweiterung von Acunetix ist nicht mit den Browser-Versionen 4 und 5 kompatibel. Unter blog.bursali.eu/2011/03/23/firefox-4-alte-addons-installieren findet sich jedoch ein Workaround, mit dem zumindest der FF4 funktioniert.

Leider stürzte im Test *w3af* nach einem automatischen Update auf die aktuelle Version unter Windows reproduzierbar beim Durchlaufen verschiedenster Profile ohne nachvollziehbare Ursachen mehrfach ab. Abhilfe brachte ein Downgrade auf 1.0 und das Entfernen aller lokalen *w3af*-Einstellungen.

sind möglich. Dafür manipuliert der Tester wieder relevante Parameter und übergibt als Payload beispielsweise Abwandlungen der Benchmark-Funktion (BENCHMARK(50000,SHA1(4711))). Eine potenzielle Lücke wird erkennbar, wenn bei einer oder mehreren der getesteten Payloads eine deutlich längere Zeit vergeht, bis der Server die Antwort geliefert hat.

Der Intruder verlangt einem Penetrationstester zwar profundes Wissen ab, ist dafür aber auch ein sehr flexibles Werkzeug, das mit fortgeschrittenen Verfahren Schwachstellen finden kann.

Hilfreich ist die Option, Arbeitsschritte samt der Ergebnisse zu konservieren und für einen Folgetest wieder zu verwenden. Eine Speicherfunktion hilft ebenfalls dabei, die eigene Arbeit zu dokumentieren. *w3af* kann lediglich Konfigurationsprofile speichern und ermöglicht damit kein Zwischenspeichern und Wiederaufnehmen eines laufenden Penetrationstests. Acunetix WVS kann Testergebnisse und Konfigurationsprofile speichern, und die Burp Suite unterstützt zwar keine Profile, ist dafür aber in der Lage, den kompletten aktuellen Bearbeitungsstatus zu speichern und später wieder einzulesen. Das ist ein sinnvolles Feature, weil so die erfasste Sitemap bei einem Folgetest als Ausgangsbasis dienen kann.

Nicht immer ist ein GUI von Vorteil. Gerade bei einer Vielzahl durchzuführender Tests, häufigen Wiederholungen gleichartiger Arbeitsabläufe und der Einbindung in umfangreiche Tests, an denen mehrere Programme in unterschiedlichen Testphasen beteiligt sind, kommt es auf gute Automatisierungsmöglichkeiten an. Der neue Headless-Betrieb der Burp Suite hilft in solchen Fällen weiter und ermöglicht das Parametrisieren per Konsolenaufruf. Auch die Java-API bietet vielfältige und leistungsfähige Automatisierungs- und Anpassungsmöglichkeiten.

w3af lässt sich mit Shell-Skripten, die die gewünschten Befehle für die Konsolenversion enthalten, ebenfalls automatisieren. Außerdem kann man neue Plug-ins selbst entwickeln sowie einbinden und den Scanner so stärker an eigene Bedürfnisse anpassen. Hier kommt besonders zum Tragen, dass die Software als Open Source verfügbar ist. Acunetix bietet zwar (noch) keine API an, hat aber mit *wvs_console.exe* eine Konsolenvariante, die sich durch Parameter konfigurieren lässt. Die Ergebnisse lassen sich als Report speichern und anschließend weiterverarbeiten.

Ergebnisse aufbereiten und präsentieren

Vor dem Abschluss eines erfolgreichen Penetrationstests steht das Anfertigen eines aussagekräftigen und verständlichen Reports, mit dem die jeweiligen Adressaten (Techniker und insbesondere Nicht-Techniker) auch etwas anfangen können. Die Herausforderung für den Penetrationstester liegt nicht nur in der Bewertung und Erläuterung der einzelnen Funde, sondern insgesamt in einer effizienten Arbeitsweise.

In diesem Punkt wird deutlich, welcher Scanner sich auf das Wesentliche konzentriert und welcher dem Penetrationstester mit einem umfangreichen Report Arbeit abnimmt. Zwar bieten alle drei getesteten Werkzeuge die Erstellung von Reports an, aber mit unterschiedlichem Komfort. *w3af* kann neben HTML- auch XML-Reports er-

Tabelle der gefundenen Schwachstellen

	w3af	Burp Suite Pro	Acunetix WVS
DVWA			
Reflected XSS	ja	ja	ja
Persistent XSS	ja	ja	ja
SQL-Inject	ja	ja	ja
SQL-Inject blind	nein	nein	nein
BadStore			
Reflected XSS	ja	ja	ja
Persistent XSS	nein	ja	nein
SQL-Inject	ja	ja	ja
SQL-Inject blind	nein	nein	nein
Test.acunetix.com			
Reflected XSS	ja	ja	ja
Persistent XSS	ja	nein	ja
SQL-Inject	ja	ja	ja
Ajax-Login	nein	nein	nein

Daten und Preise

w3af

Bezugsquelle: w3af.sourceforge.net

Preis: kostenlos

Burp Suite

Bezugsquelle: portswigger.net/burp

Preis: kostenlose Version; Professional Edition für 275 $ pro Benutzer und Jahr

Acunetix WVS

Bezugsquelle: www.acunetix.com/vulnerability-scanner

Preis: ab 995 Euro für eine Website (Small Edit.)

Onlinequellen

[a]	Acunetix-Testseite	test.acunetix.com
[b]	Watchfire-Testseite	demo.testfire.net
[c]	Untersuchung von Blackbox-Scannern	www.cs.ucsb.edu/~adoupe/static/black-box-scanners-dimva2010.pdf
[d]	Untersuchung zur Benutzerinteraktion bei Applikationstests	www.cs.ucsb.edu/~chris/research/doc/raid08_xss.pdf
[e]	Blog-Eintrag zur Scanner-Bewertung	sectooladdict.blogspot.com/2010/12/web-application-scanner-benchmark.html
[f]	Blog-Eintrag zu Myth Breaker	sectooladdict.blogspot.com/2011/01/myth-breaker-best-open-source-web.html
[g]	OWASP (Open Web Application Security Project) Top 10	https://www.owasp.org/index.php/Top_10_2010

stellen und sogar Funde per E-Mail versenden. Allerdings muss man schon vorher genau wissen, was man will – die Report-Einstellungen sind vor dem Audit gemeinsam mit allen anderen Optionen vorzunehmen, am Ende eines Tests besteht keine Auswahlmöglichkeit mehr. Die HTML-Reports sind knapp und es besteht keine Individualisierungsmöglichkeit.

Die Burp Suite erstellt Reports inklusive Einschätzungen und Ratschlägen des Expertensystems sowohl als spartanische, aber übersichtliche HTML-Datei als auch als XML-Datei für eine weitere Verwendung durch Drittprogramme. Der Benutzer kann vieles selbst anpassen, und das Erstellen des Reports lässt sich jederzeit aktivieren.

Auch Acunetix WVS exportiert Ergebnisse per XML und punktet darüber hinaus mit dem Anfertigen optisch ansprechender, umfangreicher und anpassbarer Reports im PDF-Format. Dazu gehören unter anderem Compliance Reports, zum Beispiel nach dem Payment Card Industry Data Security Standard (PCI-DSS) oder dem Sarbanes-Oxley Act. Mit *w3af* und Burp Suite kann man solche Berichte mit mehr Aufwand auch selbst aus den exportierten Ergebnissen „bauen“.

Fazit

Bei den drei hier näher betrachteten Webapplikations-Scannern handelt es sich durchweg um exzellente Programme, die zu Recht weltweit im Einsatz sind. Einen Vergleich aber darauf zu reduzieren, welcher Scanner bei den Testumgebungen zahlenmäßig die meisten Resultate geliefert hat, greift zu kurz. Jedes Programm hat seine Stärken und Schwächen, was sich auch jeweils in der Komplexität der grafischen Oberfläche und der jeweils implementierten Helfer widerspiegelt, insbesondere bei Acunetix.

Erfahrene Penetrationstester ersetzen Mängel im Experten- und Report-System durch eigenes Können und profitieren von den wirklich interessanten Features wie dem Burp Intruder, der Acunetix-AcuSensor-Technik oder der Modularität und Exploit-Orientierung von *w3af*. Um eine Kombination verschiedener Programme wird man daher kaum herumkommen. (ur)

MARTIN WUNDRAM

ist Geschäftsführer der TronicGuard GmbH und beschäftigt sich dort mit der Sicherheit von Webanwendungen.

Literatur

[1] Martin Wundram; Auf Mängelsuche; Scanner für Webanwendungen; *iX* extra 7/2011, S. V – IX

Alle Links: www.ix.de/ix1109072