Kai Jendrian

Überprüfung von Webanwendungen mit dem „OWASP Application Security Verification Standard 2009“

Zur vereinheitlichten Vorgehensweise bei Sicherheitsanalysen von Webanwendungen sowie zur Vergleichbarkeit von deren Ergebnissen wurde im Rahmen des Open Web Application Security Projects (OWASP) ein Standard mit Vorgaben zu Umfang und Tiefe von Sicherheitsprüfungen sowie Form und Inhalt von Berichten erstellt und veröffentlicht.

Sicherheitstests von Webanwendungen

Herausforderungen

Dynamische Webanwendungen sind aus dem heutigen Internet nicht mehr wegzudenken. Ohne diese Anwendungen wären Techniken, wie „Soziale Netzwerke“, „Web 2.0“ und Einkaufen im Web überhaupt nicht möglich.

Neue Techniken, die Anwendungen im Browser immer mehr wie native Programme auf einem PC erscheinen lassen, führen allerdings zu immer komplexeren Architekturen von Webanwendungen, die vielfältige Angriffsmöglichkeiten mit sich bringen.

Die Sicherheit von Webanwendungen muss frühzeitig bedacht und geplant werden. Schon in der Entwurfsphase führen Bedrohungs- und Risikoanalysen zu angemessenen Schutzmaßnahmen, die in eine Webanwendung integriert werden.

Im Verlauf der Entwicklung der Software und vor allem vor der Freigabe hat es sich bewährt, die Sicherheit von Webanwendungen durch verschiedene Tests überprüfen zu lassen.

In der Praxis liegt der Schwerpunkt der meisten Tests immer noch im Aufspüren von Sicherheitsproblemen in der Anwendung[2],[3]. Häufig sind solche Sicherheitstests von Webanwendungen durch die individuellen Vorgehensweisen der betrauten Tester und die Fähigkeiten der eingesetzten Werkzeuge bestimmt.

Aussagen zur Sicherheit über die gefundenen Fehler hinaus sind bei den traditionellen Pentests für Sicherheitsanalysen in der Regel nur ansatzweise möglich und nicht vergleichbar.

OWASP

Im „Open Web Application Security Project“[1] (OWASP) [4] haben sich viele verschiedene Personen zusammengeschlossen, die im Umfeld der Sicherheit von Webanwendungen aktiv sind. Im Rahmen des Projekts werden die vielfältigen und umfangreichen Arbeitsergebnisse gebündelt und allen Interessierten zur Verfügung gestellt. Die Dokumente und Werkzeuge aus dem OWASP decken alle Phasen der Anwendungsentwicklung vom Entwurf über die Programmierung bis hin zum Testen ab.

Der in diesem Artikel vorgestellte „Application Security Verification Standard“ [7] ist eines der im Rahmen von OWASP entstandenen richtungweisenden Dokumente.

1 Siehe: http://www.owasp.org

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und OWASP-Mitglied.
Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

Application Security Verification Standard

Bei der Festlegung von Sicherheitsanforderungen und Plänen zum Testen der Sicherheit von Webanwendungen wird schnell deutlich, dass diese Aufgabe häufig sehr schwierig ist.

Mit der Erstellung und Veröffentlichung des „Application Security Verification Standards“ (ASVS) hat das OWASP eine Arbeitshilfe geschaffen, die einen Weg zu standardisierten und vergleichbaren Sicherheitstests von Webanwendungen bezüglich Umfang und Teststrenge aufzeigt.

Die Prüfung von Webanwendungen orientiert sich an der (Datenfluss-)Logik der zu untersuchenden Anwendung, die im Standard als „Target of Verficiation (TOV)“ bezeichnet wird. Es liegt in der Verantwortung des jeweiligen Testers, zu überprüfen und dokumentieren, ob eine Webanwendung die festgelegten Sicherheitsanforderungen erfüllt.

Der ASVS gliedert sich in eine Beschreibung der Verifikationslevel, detaillierte Prüfvorgaben sowie Vorgaben zu Berichten über die Sicherheitsprüfungen.

Wie in Abbildung 1 verdeutlicht, sollte der ASVS im Rahmen zur iterativen Verbesserung der Sicherheit von Web-Anwendungen genutzt werden.

Verifikationslevel 1-4

Um den verschiedenen Anforderungen an die Sicherheit von Webanwendungen so-

Abbildung 1 |

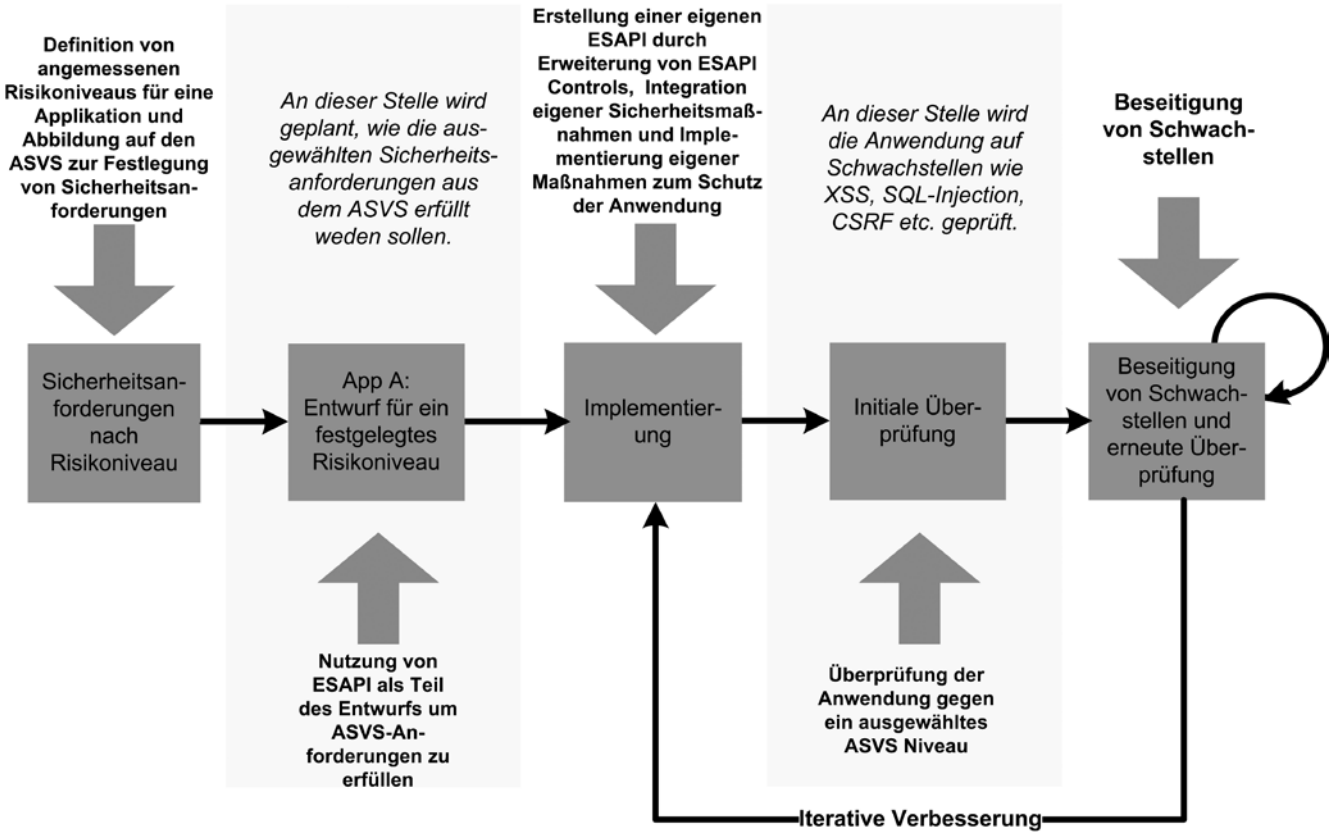
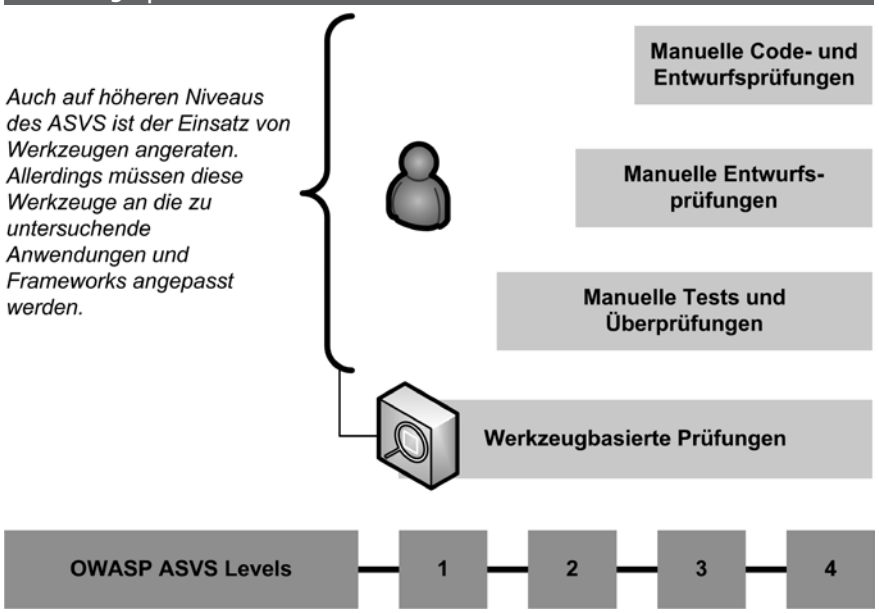


Abbildung 2 |



wie den unterschiedlichen bereitstehenden Ressourcen zur Überprüfung Rechnung zu tragen, definiert der ASVS vier verschiedene Test-Niveaus, die sich jeweils im Umfang und der Tiefe der durchzuführenden Tests unterscheiden. Dabei werden die Anforderungen mit wachsendem Niveau immer strenger.

Level 1 – Automated Verification

Im (Einstiegs-)Level 1, im Standard mit „Automated Verification" bezeichnet, sollen Tests durchgeführt werden, die ein grundlegendes Vertrauen in die Verwendung von Schutzmaßnahmen in einer Webanwendung erlauben. Der Schwerpunkt der Tests im Level 1 liegt auf automatisierten Tests, die teilweise durch manuelle Prüfungen ergänzt werden können.

Das Level 1 ist noch einmal in die Level 1A und 1B unterteilt. Das Level 1A kann durch den Einsatz von automatischen Applikationsscannern[2] erreicht werden, das Level 1B durch den Einsatz von automatisierten Quellcode Analysetools[3]. Um Level 1 zu erreichen, müssen die Anforderungen sowohl aus Level 1A als auch aus Level 1B erfüllt sein.

Im Level 1 müssen alle Bestandteile der Anwendung überprüft werden, die neu erstellt oder angepasst wurden. Alle Feststellungen der angewendeten Werkzeuge für die Prüfungen nach Level 1A oder 1B müssen manuell verifiziert werden, um im Sinne der Anforderungen des Standards akzeptiert zu werden.

2 dynamische Sicherheitsanalyse
3 statische Sicherheitsanalyse

Level 2 – Manual Verification

Anwendungen mit höheren Anforderungen an die Sicherheit sollten mindestens nach den Vorgaben aus Level 2 geprüft werden. Dabei kann ein gewisses Vertrauen geschaffen werden, dass angemessene Schutzmaßnahmen zum Einsatz kommen und korrekt arbeiten.

So wie Level 1 ist auch Level 2 unterteilt in die Level 2A und 2B, die Vorgaben zur teilweisen manuellen Prüfung der Anwendung (2A) und zur teilweisen manuellen Prüfung des Quellcode (2B) machen.

Alle für Level 1 zu betrachtenden Anwendungsbestandteile müssen auch für Level 2 untersucht werden. Zusätzlich müssen in diesem Level auch alle weiteren Komponenten überprüft werden, die Sicherheitsfunktionen für die Anwendung beisteuern.

Auch wenn Level 2 strengere Anforderungen stellt als Level 1, müssen zum Erreichen von Level 2 nicht zwingend automatisierte Tests durchgeführt werden. Sie können allerdings unterstützend eingesetzt werden.

Die Strenge der Test erhöht sich im Level 2 merklich, da hier erste konkrete Prüfvorgaben gemacht werden. Zum Beispiel wird gefordert, dass alle technischen Schutzmaßnahmen, die Sicherheitsentscheidungen treffen, einen White-List-Ansatz umsetzen. Eine weitere wichtige Anforderung ab diesem Level ist der ausschließliche Einsatz zentralisierter Sicherheitsmaßnahmen.

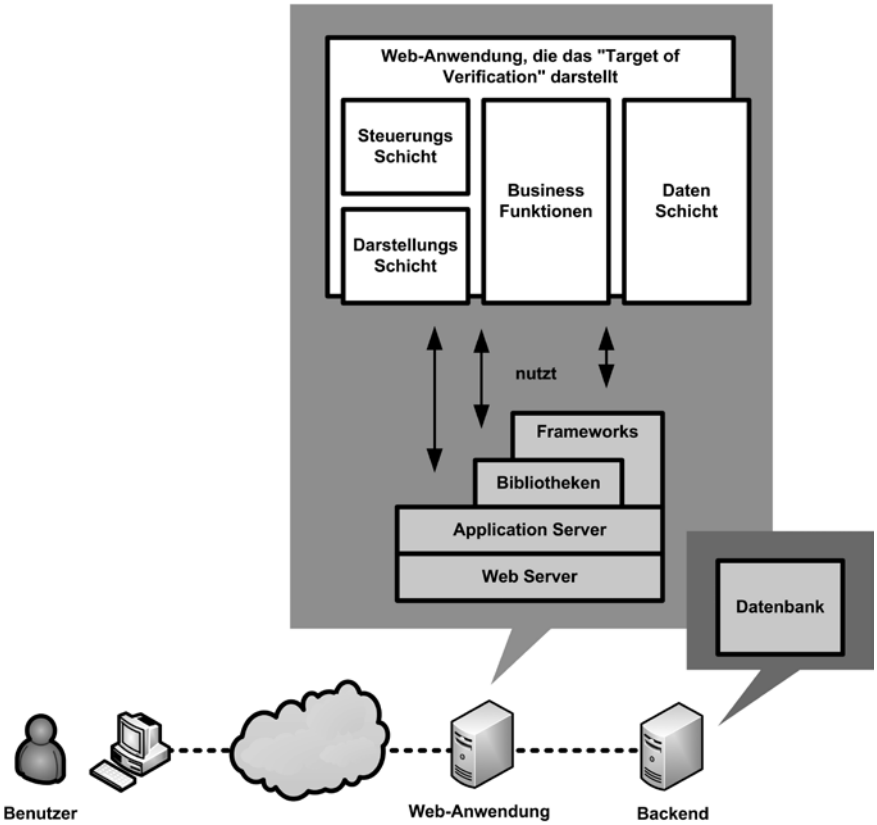
Die konkreten durchzuführenden Tests für die Level 2A und 2B sind im Standard nachfolgend in detaillierten Prüfvorgaben festgelegt.

Level 3 – Design Verification

Mit weiter steigenden Anforderungen an die Sicherheit der zu betrachtenden Webanwendung, steigen auch die Anforderungen an die Überprüfung der Sicherheit im Level 3. Hier wird Vertrauen in die korrekte Arbeitsweise sowie die durchgängige Verwendung von Sicherheitsmaßnahmen geschaffen. Im Gegensatz zu den beiden vorherigen Level sind weder Level 3 noch Level 4 weiter unterteilt.

Zusätzlich zu den schon in den vorigen Levels zu betrachtenden Bestandteilen müssen ab dem Level 3 auch alle verwendeten Frameworks, Bibliotheken und Dienste einer Prüfung unterzogen werden.

Abbildung 3 |



Beachtenswert ist, dass ab dem Level 3 der „Weg" der Daten einer Benutzeranfrage durch die Applikation grundsätzlich zu dokumentieren ist. Diese müssen dann auch umfassend bei der Prüfung untersucht werden.

Auch bei der Durchführung der Tests gelten verschärfte Anforderungen. Neben den schon im Level 2 durchzuführenden manuellen Prüfungen (2A und 2B) muss die Sicherheitsarchitektur einer Anwendung dokumentiert werden. Durch eine Bedrohungsanalyse soll sichergestellt werden, das für die identifizierten Schutzziele ein angemessenes Design sowie passende Sicherheitsmaßnahmen gewählt wurden.

Verglichen mit Level 2 erhöht sich ebenfalls der Umfang der detaillierten Prüfvorgaben.

Level 4 – Überprüfung der Interna

Die strengste Form der Überprüfung nach dem ASVS findet durch Prüfungen nach dem Level 4 statt. Dieses Level kann und sollte für kritische Anwendungen genutzt werden. Das können beispielsweise Anwendungen im medizinischen Bereich sein, die Leib und Leben schützen, aber auch Anwendungen, die signifikanten Einfluss auf die öffentliche Ordnung oder Sicherheit haben.

Durch eine Überprüfung nach Level 4 soll sichergestellt sein, dass eine Anwendung auch den Bedrohungen durch fähige und motivierte Angreifer mit hohem Know-How widerstehen kann.

Zusätzlich zu dem Vertrauen aus Level 3, wird in Level 4 daher noch das Vertrauen geschaffen, dass alle Sicherheitsmaßnahmen auch nach Prinzipien der sicheren Softwareentwicklung implementiert wurden.

Eine wesentliche Erweiterung der Prüfvorgaben auf Level 4 ist die Einführung von manuellen Code-Reviews auf Basis der detaillierten Prüfvorgaben.

Detaillierte Prüfanforderungen

Nachdem in den Verifikationsleveln die abstrakten Anforderungen an die Sicherheitsprüfungen vorgegeben wurden, legt der Abschnitt „Detailed Verification Requirements" des ASVS die detaillierten Prüfanforderungen für jedes Level fest.

Abbildung 4 |

Dabei werden im Standard die folgenden 14 Sicherheitsthemen betrachtet:

V1. Sicherheitsarchitektur (Security Architecture)
V2. Authentifizierung (Authentication)
V3. Sitzungsverwaltung (Session Management)
V4. Zugriffskontrolle (Access Control)
V5. Eingabevalidierung (Input Validation)
V6. Ausgabekodierung (Output Encoding)
V7. Kryptographie (Cryptography)
V8. Fehlerbehandlung (Error Handling and Logging)
V9. Schutz von Daten (Data Protection)
V10. Kommunikationssicherheit (Communication Security)
V11. HTTP Sicherheit (HTTP Security)
V12. Sicherheitskonfiguration (Security Configuration)
V13. Suche nach schadhaftem Code (Malicious Code Search)
V14. Interne Sicherheit (Internal Security)

Auf 15 Seiten werden im ASVS die insgesamt 121 konkreten Prüfanforderungen aus den genannten Bereichen und deren Anwendung auf die jeweiligen Level beschrieben.

Die verschiedenen Prüfniveaus werden deutlich, wenn für das Level 1B genau zwei der 15 Prüfungen des Abschnitts „V2 – Authentication Verification Requirements" durchgeführt werden müssen, für das Level 4 aber alle 15. Ein ähnliches Verhältnis der Prüftiefe ergibt sich für alle Sicherheitsthemen.

Beispielhaft wird an dieser Stelle eine Prüfanforderung vorgestellt, damit sich auch derjenige ein Bild machen kann, der sich nicht tiefer in den Standard einarbeiten will.

Die Prüfvorgabe V2.9, die für die Level 2A, 2B, 3 und 4 angewendet werden muss, fordert beispielsweise „Verify that users can safely change their credentials using a mechanism that is at least as resistant to attack as the primary authentication mechanism." Das bedeutet hier konkret, dass die Angabe des Geburtsnamens der Mutter für das Rücksetzen eines Passworts keine geeignete Kontrollfrage ist.

Für die tatsächliche Durchführung der Prüfungen existiert sowohl im Umfeld des Open Web Application Security Projects als auch in der Literatur gutes unterstützendes Material zur Prüfung von Webanwendungen ([5], [6], [8]).

Berichtsanforderungen

Für die Vergleichbarkeit der Ergebnisse von Sicherheitsprüfungen ist eine gewisse Einheitlichkeit der Darstellung notwendig. Der ASVS trägt dieser Erkenntnis dadurch Rechnung, dass der letzte Abschnitt des Standards „Verification Reporting Requirements" sich grundlegenden Anforderungen an die zu erstellenden Berichte widmet.

Alle Berichte nach den Vorgaben des ASVS müssen zur Vergleichbarkeit die folgenden Bestandteile enthalten:

- Einführung (Introduction)
- Beschreibung (Description)
- Architektur (Architecture)
- Ergebnisse (Results)

Es werden allerdings keine zwingenden Anforderungen and die genaue Struktur oder das Format eines Berichtes gestellt. Zusätzliche oder weiterführende Informationen dürfen ebenfalls in einem Bericht enthalten sein.

Auch wenn keine zwingenden Vorgaben zu Struktur oder Format gemacht werden, ist es doch erforderlich, dass neben der Vollständigkeit der Ergebnisse auch die Nachvollziehbarkeit gewährleistet ist. Dazu müssen alle notwendigen Informationen, wie z. B. Konfigurationen und Quellcode-Auszüge, dokumentiert sein.

An die Einführung in den Bericht sind vier konkrete Anforderungen gestellt. Sowohl der Bericht selbst, als auch die überprüfte Anwendung (TOV) müssen identifizierbar sein. Der Gesamteindruck zum Vertrauen in die Sicherheit muss klar ausgedrückt sein, die Hauptrisiken aus Geschäftssicht beim Betrieb der Anwendung müssen herausgearbeitet sein und alle Einschränkungen bei der Überprüfung müssen deutlich werden.

Die Beschreibung der Anwendung muss so detailliert und ausführlich sein, dass ein Verständnis des Betriebs und der Umgebung, in der die Anwendung betrieben wird, für den Leser möglich ist.

Die Dokumentation der Architektur im Bericht muss zusätzliche Detailbeschreibungen der Anwendung bereitstellen, um dem Leser die Beurteilung zu ermöglichen, dass die Überprüfung sowohl vollständig als auch korrekt durchgeführt wurde. Die notwendigen Details sind abhängig vom jeweiligen Level der Prüfung.

Die Ergebnisse der konkreten Prüfschritte sind für jede konkrete detaillierte Prüfvorgabe nach dem gleichen Schema darzustellen.

Für jede Prüfvorgabe ist entweder ein „Pass" (bestanden) oder „Fail" (nicht bestanden) als Urteil anzugeben.

Für positive Ergebnisse von Prüfungen nach Level 1 ist als Begründung für das Urteil jeweils die Konfiguration oder eine ergänzende Urteilsbegründung, unterlegt mit besonderen Fakten, anzugeben. Zusätzlich müssen die Features des verwendeten Tools den anzuwendenden detaillierten Prüfvorgaben zugeordnet werden, dies muss allerdings nur einmal pro Bericht erfolgen. Im Falle eines „Fail" sind entweder die konkrete URL samt Parametern oder die betroffene Quelldatei samt Zeilennummer, eine ausführliche Be-

schreibung sowie eine Bewertung des jeweiligen Risikos mit Begründung zu dokumentieren.

Für die Level 2-4 muss für jede Prüfvorgabe im positiven Fall das Urteil mit einer Begründung, die nachvollziehbare Argumente für die Vollständigkeit und Korrektheit der Prüfung sowie spezifische Belege enthält, dokumentiert werden. Auch hier müssen für ein negatives Prüfergebnis die konkrete URL oder die Stelle im Quellcode beschrieben werden. Eine Beschreibung der Prüfung einschließlich des betrachteten Pfades sowie der Dokumentation von Schritten zur Nachvollziehbarkeit der Tests ergänzen zusammen mit auch einer hier erforderlichen Bewertung des Risikos mit Begründung das jeweilige Urteil.

Für alle Fälle sollen Maßnahmen zur Beseitigung der Mängel aufgezeigt werden.

Auf der Webseite des ASVS finden sich konkrete Hinweise zur Erstellung von Berichten nach dem Standard[4].

4 Siehe http://www.owasp.org/index.php/How_to_meet_verification_reporting_requirements

Fazit

Durch „Application Security Verification Standard" wird eine Vorgehensweise zur Sicherheitsprüfung von Webanwendungen etabliert, die für bestimmte Sicherheitsanforderungen eine Vergleichbarkeit der Vorgehensweise und Ergebnisse ermöglicht.

Der Standard konzentriert sich durch seine doch recht abstrakten Vorgaben hauptsächlich auf das „Was" des Prüfens und weniger aus das „Wie". Dadurch werden zwar an den Prüfer gewisse Anforderungen bezüglich seiner Erfahrungen im Bereich des Testens von Webanwendungen gestellt, aber gleichzeitig wird dieser eben nicht in ein (nicht immer passendes) Korsett von kleinlichen Prüfvorgaben gezwungen.

Dank

Ein herzlicher Dank geht an die OWASP Foundation für die freundliche Genehmigung, Grafiken von OWASP für diesen Artikel unverändert oder modifiziert verwenden zu dürfen.

Literatur

[1] R. Giesecke, S. Fünfrocken, *Einfach zu mehr Software-Sicherheit*, in: DuD 12/2007, pp. 877-833.

[2] M. Borrmann, S. Schreiber, *Sicherheit von Web-Applikationen aus Sicht eines Angreifers*, in: DuD 10/2006, pp. 599-603.

[3] M. Schumacher, A. Wiegenstein, *Sichere Web-Anwendungen*, in: DuD 10/2006, pp. 611-615.

[4] Dirk Fox, *Open Web Application Security Project*, in: DuD 10/2006, p. 636.

[5] A. van der Stock, D. Cruz, J. Chapman, D. Lowery, E. Keary, M. Morana, D. Rook, J. Williams, P. Prego, *OWASP Code Review Guide, V1.1*, http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

[6] Matteo Meucci (Project Lead), *OWASP Testing Guide, v3*, http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[7] M. Boberski, J. Williams, D. Wichers, *OWASP Application Security Verification Standard 2009*, http://www.owasp.org/images/4/4e/OWASP_ASVS_2009_Web_App_Std_Release.pdf

[8] P. Hope, B. Walther, *Web Security Testing Cookbook*, O'Reilly 2008