DuD
Datenschutz und Datensicherheit

Open Web Application Security Project

Dirk Fox

Hintergrund

Das „Open Web Application Security Project" (OWASP)[1] wurde im Jahr 2004 mit dem Ziel initiiert, Unternehmen und Organisationen bei der Entwicklung und Pflege vertrauenswürdiger Anwendungen zu unterstützen. OWASP ist eine unternehmensunabhängige Organisation. Um einen langfristigen Fortbestand sicher zu stellen, wurde die OWASP Foundation gegründet, der Einzelpersonen und Unternehmen beitreten können (jährlicher Mitgliedsbeitrag: 100 bis 9.000 US$). Alle Einnahmen und finanziellen Unterstützungen werden direkt in OWASP-Projekte investiert.

Die Aktivitäten und Ergebnisse von OWASP werden in einem Wiki dokumentiert (d. h. einem Open-Source Content Management System, das von jedem Besucher auch inhaltlich verändert und weiterentwickelt werden kann). Ähnlich zahlreichen Open-Source-Projekten entstehen die meisten OWASP-Materialien in einem offenen Kooperationsprozess. Auf den jährlichen, zweitägigen OWASP AppSec Konferenzen (eine in den USA, eine in Europa) werden die neuesten Entwicklungen im Gebiet der Anwendungssicherheit vorgestellt und diskutiert.

Ergebnisse

Anwendungssicherheit umfasst im Verständnis von OWASP sowohl Technik als auch Prozesse und die beteiligten Menschen. Wirksame Verbesserungen der Anwendungssicherheit müssen alle diese drei Bereiche berücksichtigen und betreffen.

OWASP-Projekte umfassen die Untersuchung und Dokumentation sicherheitsrelevanter Aspekte spezifischer Programmiersprachen und Anwendungsentwicklungen ebenso wie allgemeine, System unabhängige Empfehlungen, Tipps und Hinweise.

Alle im Rahmen von OWASP erstellten Hilfsmittel, Dokumente, Foren und Veröffentlichungen sind unter einer Open Source-Lizenz frei zugänglich und richten sich an alle, die sich für die Weiterentwicklung von Anwendungssicherheit interessieren. OWASP-Dokumente umfassen Tools, Lehrmaterialien, Richtlinien und Checklisten zur Entwicklung sicheren Codes. Zu den wichtigsten Ergebnissen der bisherigen OWASP-Aktivitäten zählen der knapp 300 Seiten starke „OWASP Guide" zur Entwicklung sicherer Web-Anwendungen sowie die „OWASP Top Ten" der Sicherheitsmängel in Web-Applikaitonen.

Unternehmen, die Mitglied der OWASP Foundation sind, können OWASP-Materialien innerhalb ihrer Organisation unter einer kommerziellen Lizenz nutzen, ändern und verbreiten.

Die „OWASP Top Ten"

Die „OWASP Top Ten" konnten sich inzwischen als eine Art „Minimalstandard für Web-Anwendungssicherheit" etablieren: Zahlreiche Unternehmen und Organisationen haben sich zur Vermeidung dieser häufigsten und kritischsten Fehler bei der Entwicklung von Web-Anwendungen verpflichtet. Kurz zusammengefasst sind dies:

A1 Ungeprüfte Eingaben

Werden Eingaben z.B. in Web-Formularen nicht auf Gültigkeit geprüft, können Angreifer die Hintergrundsysteme über die Web-Anwendung durch Fehleingaben attackieren. Das kann so weit gehen, dass sie das Hintergrundsystem komplett „übernehmen".

A2 Überwindbare Zugangsbeschränkung

Werden Berechtigungseinschränkungen legitimer Nutzer nicht korrekt überprüft und durchgesetzt, können Angreifer über einen normalen Nutzeraccount auf sensible Daten zugreifen oder Funktionen ausführen, zu denen sie eigentlich nicht berechtigt sind.

A3 Fehler im Session Management

Kann ein Angreifer die Sitzung eines berechtigten Nutzers „übernehmen" oder die Authentisierungsdaten eines fremden Accounts gewinnen oder raten, kann er auf die Dienste unter Vortäuschung der Identität des berechtigten Nutzers zugreifen.

A4 Cross Site Scripting

Eine Web-Anwendung kann dazu missbraucht werden, Angriffscode auf das System eines Endbenutzers zu bringen. Darüber lassen sich dann Authentisierungsdaten des Nutzers ausspähen oder weitere Berechtigungsdaten gewinnen.

A5 Pufferüberlauf

In einigen Programmiersprachen oder Web-Anwendungsmodulen werden Eingaben nicht sauber überprüft, sodass Angreifer Anwendungen zum Absturz bringen oder Systeme übernehmen können, indem sie ausführbaren Code in den Speicher schreiben. Betroffen sind unter anderem CGI-Scripte, in C(++) entwickelte Bibliotheken und Treiber.

A6 Injizierte Fehler

Web-Anwendungen geben bei Aufrufen von externen Systemen und dem Zugriff auf das lokale Betriebssystem Parameter mit. Können diese von einem Angreifer manipuliert werden, so kann dieser Schaden stiftende Kommandos ausführen lassen.

A7 Unsaubere Fehlerbehandlung

Werden Fehlerfälle von einer Anwendung nicht korrekt behandelt (was häufig für seltene Fehler gilt), können sie einem Angreifer wertvolle Informationen über das System liefern oder die Möglichkeit eines Störangriffs (Denial of Service) bieten.

A8 Unsichere Speicherung

Web-Anwendungen verwenden kryptographische Funktionen zum Schutz von Daten und Authentisierungsinformationen. Fehlerhafte Implementierung können den Schutz dieser sensiblen Daten bedrohen.

A9 Denial of Service-Anfällgikeit

Angreifer können die Ressourcen einer Web-Anwendung durch automatisierte Tools, die ständig weitere Nutzer „simulieren", so beanspruchen, dass eine Nutzung der Anwendung durch legitime Nutzer praktisch unmöglich wird. Sie können legitime Nutzer auch z.B. durch Passwort-Fehleingaben aus ihren Accounts aussperren oder durch Denial-of-Service-Angriffe auf den Webserver, auf dem die Anwendung betrieben wird, diese zum Absturz bringen.

A10 Unsichere Konfiguration

Die verwendeten Web-Server müssen sauber und streng konfiguriert sein, denn eine unsichere Serverkonfiguration beeinträchtigt direkt auch die Sicherheit der auf diesem Server betriebenen Webanwendungen. Das ist meist nicht einfach, denn kein Web-Server ist sicher vorkonfiguriert.

[1] http://www.owasp.org