Best Practice: Projektierung der Sicherheitsprüfung von Webanwendungen

Tobias Glemser
tglemser@tele-consulting.com

OWASP

Review: Marco Di Filippo ;-)

Appsec Germany Nürnberg 13.10.2009

The OWASP Foundation

http://www.owasp.org

Die Projektgruppe (alphabetical order)

- Marco Di Filippo
- Tobias Glemser
- Achim Hoffmann
- Barbara Schachner
- Dennis Schröder
- Feilang Wu

Um was geht's?

Artikelbaum - Artikel 1-10 von 29

Diesen Artikelbaum abonnieren ☐

<< Zurück | Weiter >> | 1 | 2 | 3

Pentest für Webserver **07.10.2009, 13:41**

Hallo Zusammen,

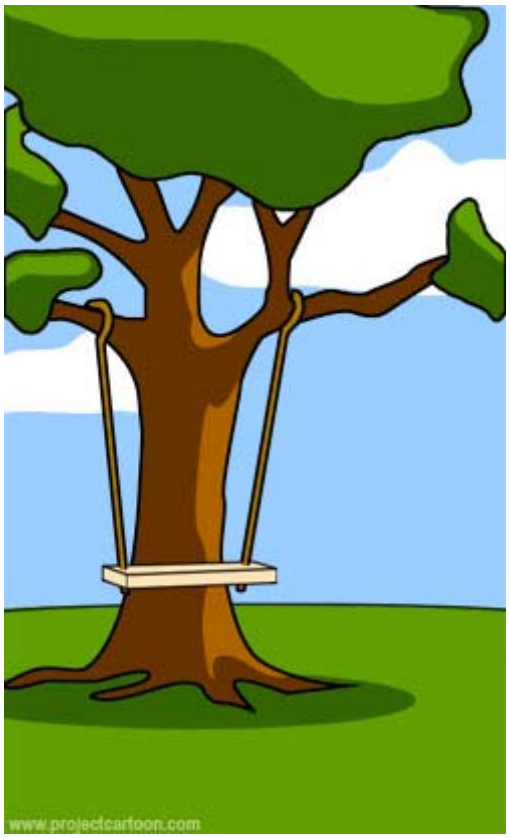
ich bin auf der Suche nach einem Anbieter für Pentest (u.a. Webserver).
Hat jemand schon Erfahrung gesammelt und kann uns daran teilhaben lassen?
(Preis, auf was achten, seriöser Anbieter, Kontakte...)

Vielen Dank

Grüße
Thomas

Eine Frage der Definition…

Wie der Kunde es erklärt hat

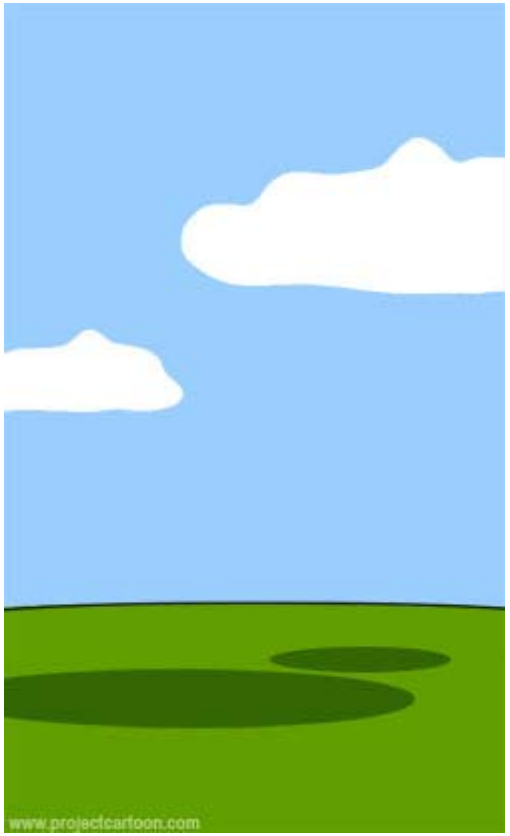


Wie der Projektleiter es verstanden hat

Wie der Analyst es auffasst

Eine Frage der Definition...

Wie der Wirtschaftsberater es verkauft



Wie das Projekt dokumentiert wurde

Wie es dem Kunden berechnet wurde

Eine Frage der Definition...

Was der Kunde wirklich gebraucht hätte

Um was geht's?

- Erfahrungswerte von Dienstleistern und Kunden
- Wie projektiere ich intern?
- Wie definiere ich meine Anforderungen?
- Wie finde ich geeignete Dienstleister?

Projektverlauf

- Diskussion am OWASP Stand auf der IT-SA Oktober 08
- Erste Anfrage an OWASP Mailing-Liste: 26.11.08
- Erste Antwort: 27.11.08
- Grober Projektablaufplan: Januar 09
- Erster Draft: Februar 09

Projektverlauf

- Problem: Keine Kunden ☹
- Lösung: 04.03. - 2 Kunden ☺
- Zweiter Draft: April 09
- Dritter Draft: Juni 09 (inkl. ein Ausstieg aus berufl. Gründen)
- „Kick-Off“ Workshop im August
- Finalisierungs-WS Mitte September
- Version 1.01 auf owasp.org: 9. Oktober

Aufbau des Papers

- Einführung und Zielsetzung
- Anforderungen: Kundenseite
- Anforderungen: Dienstleister
- Checkliste: Anforderungen Kundenseite
- Checkliste: Anforderungen Dienstleister-Angaben

Einführung

- Kunde: Betreiber von Webanwendungen auf der Suche nach einem Dienstleister
- Dienstleister (intern oder extern): Abteilung oder Unternehmen mit Expertise bei der Durchführung von Sicherheitsprüfungen von Webanwendungen
- Webanwendung: Auf Webtechnologien aufsetzende Anwendung
  - klassische Internetpräsenz
  - Web-API
  - Web-Frontend von Anwendungsservern
  - ...

Einführung

- Zielgruppe:
  - Betreiber von Webanwendungen
  - (Dienstleister)
- Abgrenzung
  - „untechnisch“
  - Technische Erläuterungen, wenn für den Gesamtkontext wichtig
- Aktualisierungen
  - Mal schauen ☺
  - Feedback jederzeit und gerne erwünscht!

Anforderungen: Kundenseite

- Art der Prüfung
  - Vulnerability-Assessment (VA) / Penetrationstest der Webanwendung
    - Wahl der Vorgehensmodells
      - BSI: Durchführungskonzept für Penetrationstests
      - Open Source Security Testing Methodology Manual (OSSTMM)
      - OWASP Testing Guide
      - OWASP Application Security Verification Standard
    - Blackbox/Whitebox
    - Lasttests/DoS
    - SaaS - Software as a Service

Anforderungen: Kundenseite

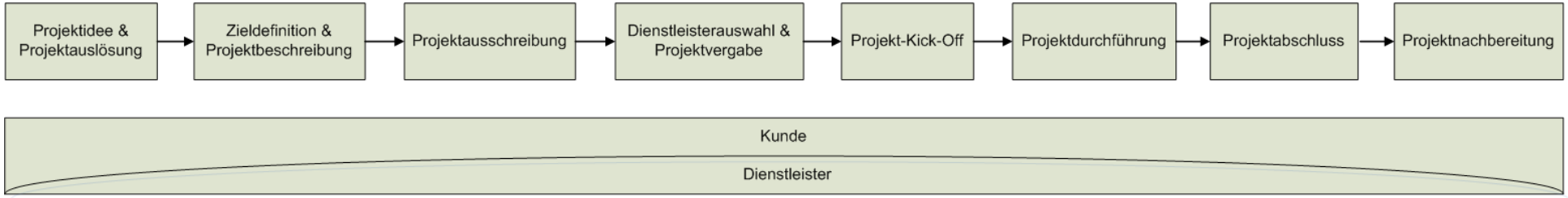
- Art der Prüfung II
  - Quellcode-Analyse
  - Architektur-Analyse
  - Prozess- und Dokumentations-Analyse (z. B. auf Basis IT-Grundschutz oder ISO 27001 „native“)

Anforderungen: Kundenseite

- Zielformulierung
  - Definition der Testziele
  - Beschreibung der Umgebung, u. A.
    - Überblick
    - Zugriffswege
    - Rechteprofile
    - Umfang
    - Architektur
    - Datenflußdiagramm

Anforderungen: Kundenseite

- Organisatorische Aspekte: Initialisierung



  - Zieldefinition und Projektbeschreibung
    - Ausgangssituation und Begründung
    - Ziele und Meilensteine
    - Randbedingungen und Abgrenzungen

Anforderungen: Kundenseite

- Organisatorische Aspekte: Vorbereitung
  - Teilnehmer
  - Projektsteuerung und Feedback
  - Ort und Zeit
  - Scan-Freigaben
  - Vertraulichkeitserklärungen
  - Haftung

Anforderungen: Kundenseite

- Organisatorische Aspekte: Ausschreibung
  - Unkritische Informationen
  - So konkret als möglich
    - Allgemeine Kurzbeschreibungen der Systeme bzw. Komponenten
    - Vereinfachte Netzwerkpläne
    - Vereinfachte Datenflussdiagramme
- Organisatorische Aspekte: Dienstleister Auswahl
  - Eigenes Kapitel..

Anforderungen: Kundenseite

- Organisatorische Aspekte: Kick-Off
  - Übergabe der Informationen
  - Alle Beteiligten an einen Tisch
  - Abstimmung der Vorgehensweise
- Organisatorische Aspekte: Durchführung
  - Ständiger Ansprechpartner beim Kunden
  - Definierte Eskalationswege
  - Definierte Rückmelde-Strategien
- Organisatorische Aspekte: Projektabschluss
  - Bericht nach Vereinbarung (siehe Dienstleister-Auswahl)
  - Ggf. Präsentation

Anforderungen: Kundenseite

- Organisatorische Aspekte: Projektabschluss
  - Bericht nach Vereinbarung (siehe Dienstleister-Auswahl)
  - Ggf. Präsentation
- Organisatorische Aspekte: Projektnachbereitung
  - Risikograd-Einschätzungen verifizieren
  - Verantwortlichkeiten zuweisen
  - Behebung der Schwachstellen prüfen

Anforderungen: Dienstleister-Angaben

- Erforderliche Angaben: Unternehmensgeschichte
  - Anhaltspunkte für Qualität
  - Veröffentlichungen
  - Aktive Mitgliedschaften
- Erforderliche Angaben: Projektteam
  - Sollte von Beginn an feststehen!
  - Mitarbeiterprofile

Anforderungen: Dienstleister-Angaben

- Erforderliche Angaben: Methoden
  - Projektplan, pro Phase
    - Aufwand
    - Meilensteine
  - Methodik
    - Automatisierte Tests
    - Manuelle Tests mit „kreativer Komponente“
  - Individuelle Beschreibung der Vorgehensweise!
  - Nennung der Werkzeuge und Tools, ggf. inkl. Beschreibung

Anforderungen: Dienstleister-Angaben

- Erforderliche Angaben: Bericht
  - Executive Summary
  - Zusammenfassung der Schwachstellen
  - Ausführliche Beschreibung der Schwachstellen
    - Kurzbeschreibung,
    - Auswirkung der Schwachstelle
    - Risikoeinschätzung
    - Referenzen
    - ggf. genaue Vorgehensweise zur Ausnutzung der Schwachstelle

➔Reproduzierbarkeit und Transparenz

Anforderungen: Dienstleister-Angaben

- Weiche Faktoren: Referenzen
  - Fast immer (individuell) möglich
  - Prüfen!
- Weiche Faktoren: Veröffentlichungen
  - Fachartikel
  - Vorträge
- Weiche Faktoren: Mitgliedschaften
  - IT-Sicherheitsrelevante Organisationen
  - Aktiv/passiv

Anforderungen: Dienstleister-Angaben

- Weiche Faktoren: Zertifizierungen
  - z. B. ISO/IEC 27001 oder ISO 9001
- Weiche Faktoren: Umgang mit Daten
  - Verschlüsselter Transfer
  - Sichere Speicherung
- Weiche Faktoren: Haftpflicht
  - Greift nur bei Fahrlässigkeit

Fazit

- IT-Sicherheit ist kein Voodoo
- Gemeinsame Sprache und gemeinsames Verständnis der Ziele aller Beteiligter oberstes Gebot
- Wiederholbarkeit der Prüfungen
- Nachvollziehbarkeit der Ergebnisse
- Interne Nachbereitung

Danke

- Alle Infos und Download auf http://www.owasp.org/index.php/Projektierung_der_Sicherheitspr%C3%BCfung_von_Webanwendungen
- Konstruktive Kritik an einen der Autoren per Mail
- Morgen (14.10.) OWASP Stand auf der IT-SA
- Aus ☺