Die Software-Risiken, die ich rief...

Dr. Dirk Wetter
Dr. Wetter IT-Consulting
mail bei drwetter punkt eu
+49-(40)-2442035-1

Security Forum 2012

The OWASP Foundation
http://www.owasp.org

/me

- **Beruf:**
  - **Selbständiger IT-Sicherheitsberater**
    - Technisch: Audits, Absichern, Forensik, Technologie-Beratung
    - Organisatorisch: Prozesse, Konzepte, Workshops
  - **Ehrenamt**
    - Aktiv in OWASP, insbesondere 
    - GUUG
    - Schreibe gerne

Zauberlehrling

Und nun komm, du alter Besen!
Nimm die schlechten Lumpenhüllen;
bist schon lange Knecht gewesen:
nun erfülle meinen Willen!
Auf zwei Beinen stehe,
oben sei ein Kopf,
eile nun und gehe
mit dem Wassertopf!

Walle! walle
manche Strecke,
daß, zum Zwecke,
Wasser fließe
und mit reichem, vollem Schwalle
zu dem Bade sich ergieße

Ach, er läuft und bringt behende!
Wärst du doch der alte Besen!
Immer neue Güsse
bringt er schnell herein,
Ach! und hundert Flüsse
stürzen auf mich ein.
[..]
O du Ausgeburt der Hölle!
Soll das ganze Haus ersaufen?
Seh ich über jede Schwelle
doch schon Wasserströme laufen.
Ein verruchter Besen,
der nicht hören will!
Stock, der du gewesen,
steh doch wieder still!

Die ich rief, die Geister, werd' ich nun nicht los

II. OWASP

- **Open Web Application Security Project**
  - **Non-profit Organisation (US: 501c3)**
    - Weltweite Organisation
    - > 10 Jahre
    - 20k Leute, denen an OWASP gelegen ist
    - ~13k Webseiten @ owasp.org
- **Mission**
  - **Applikationssicherheit verbessern**
  - *The Open Web Application Security Project (OWASP) [... is] trying to make the world a place where insecure software is the anomaly, not the norm [..]*

II. OWASP: O wie Open

- **Alles ist „open“, i.e.**
  - **Vendor unabhängig**
  - **ohne kommerzielle Intentionen**
  - **frei in Benutzung**
    - und Modifizierung
    - Open-Source-Lizenzen
  - **Jeder kann mitmachen**
  - **Transparenz!**
    - von Finanzen bis Code
    - Governance: Board

II. OWASP: P wie Projekte

- **OWASP-Projekte**
  - **~ 140 (!)**

    → **Des OWASPs Kern ;-)**
  - **Zielgruppe**
    - Entwickler
    - Betrieb
    - Pentester
    - Projektmanager
    - Verantwortungsträger
  - **~ Zweiteilung**
    - Tools / Guides

III. OWASP-Projekte

- **Bekanntestes: OWASP Top 10**
  - **Großes Presseecho**
  - **1. Ausgabe 2003, letzte 2010**
    - Auch deutsche Übersetzung
  - **Neu in 2010 (vs. 2007)**
    - Keine Schwachstellen, sondern

  - **Konsequent + r/wichtig**
    - Wichtig fürs Geschäft ist immer Risiko
      - Allerdings Top 10: *technisches* Risiko
      - Biz Risiko: Betriebswirtschaftlicher Kontext Firma

III. OWASP-Projekte

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
_____	Ausnutzbarkeit	Verbreitung	Detektierbarkeit	Auswirkung	_____
Wer kann das anstellen?	So geht's	Die Ursache von Problem X ist, dass ... es trifft häufig in <diesen> Applikationen auf , Dies ist für den Angreifer relativ einfach durch <.....> zu entdecken.		Problem X hat diese oder jene technische Konsequenz diesen Ausmaßes	Geschäftliche Konse-sequenz eines Daten-verlustes, -modifika-kation oder Nichtver-fügbarkeit?
Angreifer	Schwachstelle			technisch	monetär

Wie einfach auszunutzen

Verbreitungs -grad Lücke

Detektier-barkeit

Eintrittswahrscheinlichkeit

Schaden, potenziell

Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	Easy	Widespread	Easy	Severe	?
?	Average	Common	Average	Moderate	?
?	Difficult	Uncommon	Difficult	Minor	?

RISK	Attack Vectors → Exploitability	Security Weakness → Prevalence	Security Weakness → Detectability	Technical Impacts
A1 - Injection	EASY	COMMON	AVERAGE	SEVERE
A2 - XSS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE
A3 – Broken Auth.+Session Mgmt.	AVERAGE	COMMON	AVERAGE	SEVERE
A4 – Insecure Direct Object Reference	EASY	COMMON	EASY	MODERATE
A5 - CSRF	AVERAGE	WIDESPREAD	EASY	MODERATE
A6 – Security Misconfiguration	EASY	COMMON	EASY	MODERATE
A7 – Insecure Crypto	DIFFICULT	UNCOMMON	DIFFICULT	SEVERE
A8 – Direct URL Access	EASY	UNCOMMON	AVERAGE	MODERATE
A9 – Insufficient Transport Protectition	DIFFICULT	COMMON	EASY	MODERATE
A10 - Unvalidated Redirects	AVERAGE	UNCOMMON	EASY	MODERATE

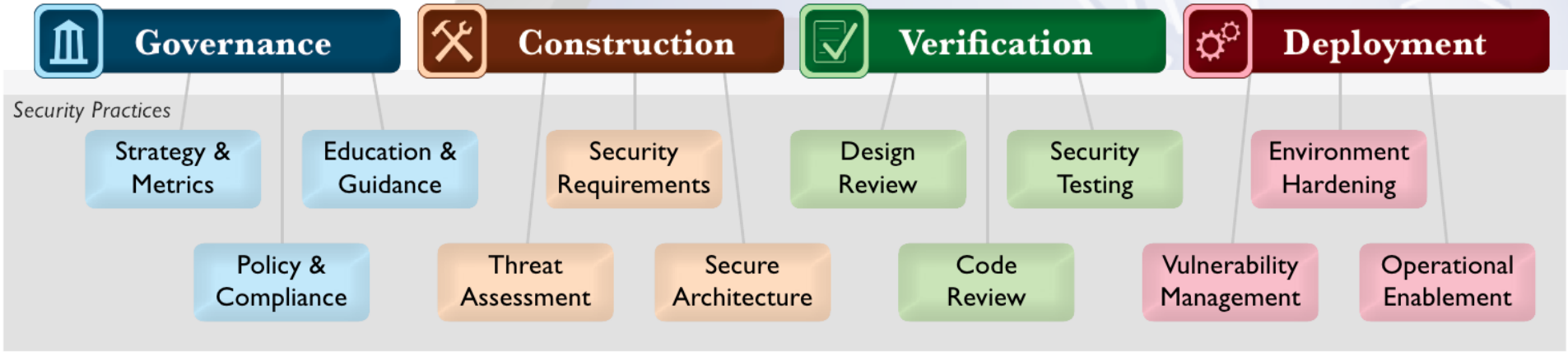
III. OWASP-Projekte

- **Nachhaltig: (Open)SAMM**

  - **Mehr als Reifemodell**
    - Wie entwickle ich in meiner Firma nachhaltig sichere Software?
    - SDLC!

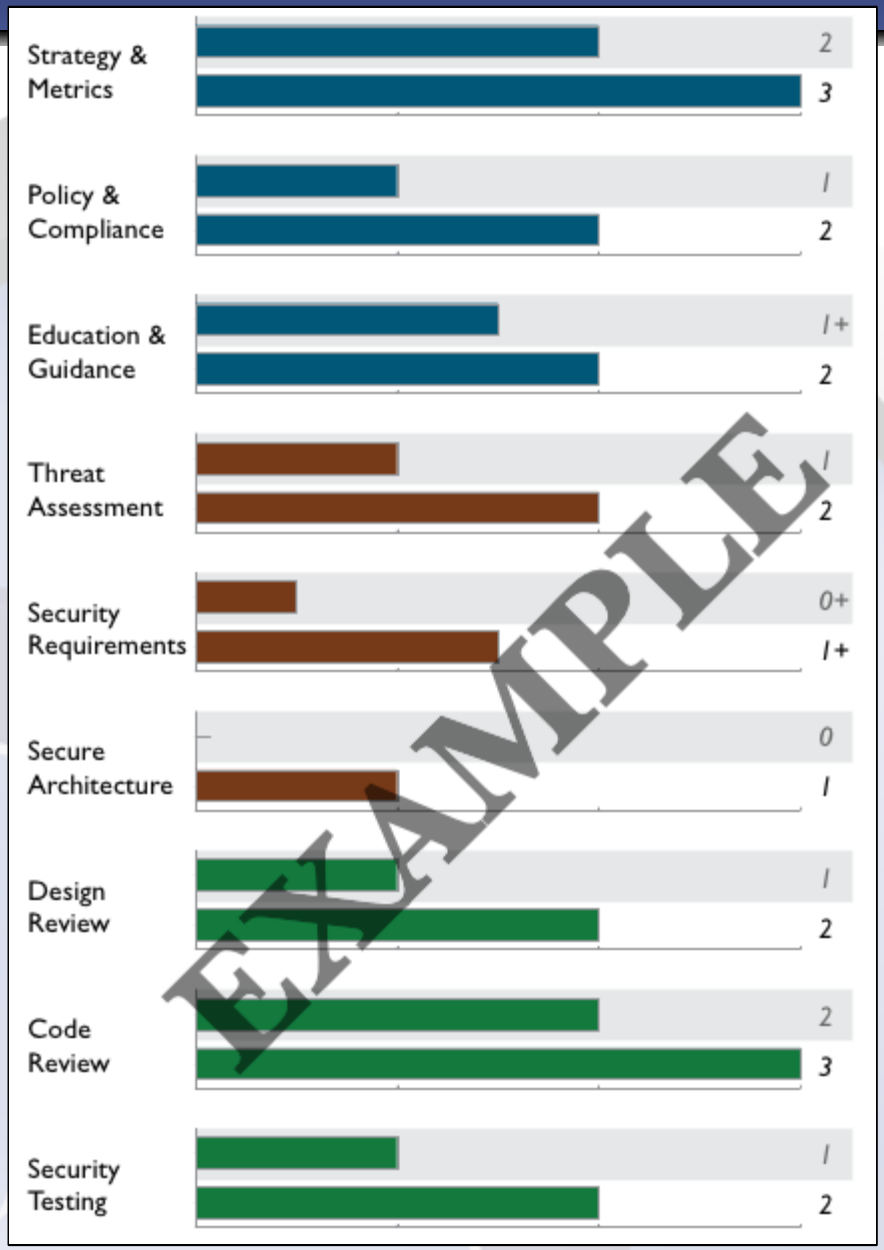
III. OWASP-Projekte

- **OpenSAMM**
  - **4 Kernfunktionen:**



III. OWASP-Projekte

- **OpenSAMM**
  - **Questionaire**
    - Ist-Analyse
      =Assessment
  - **Verbesserung**
    - Soll-Anpassung
  - **„Messung“**



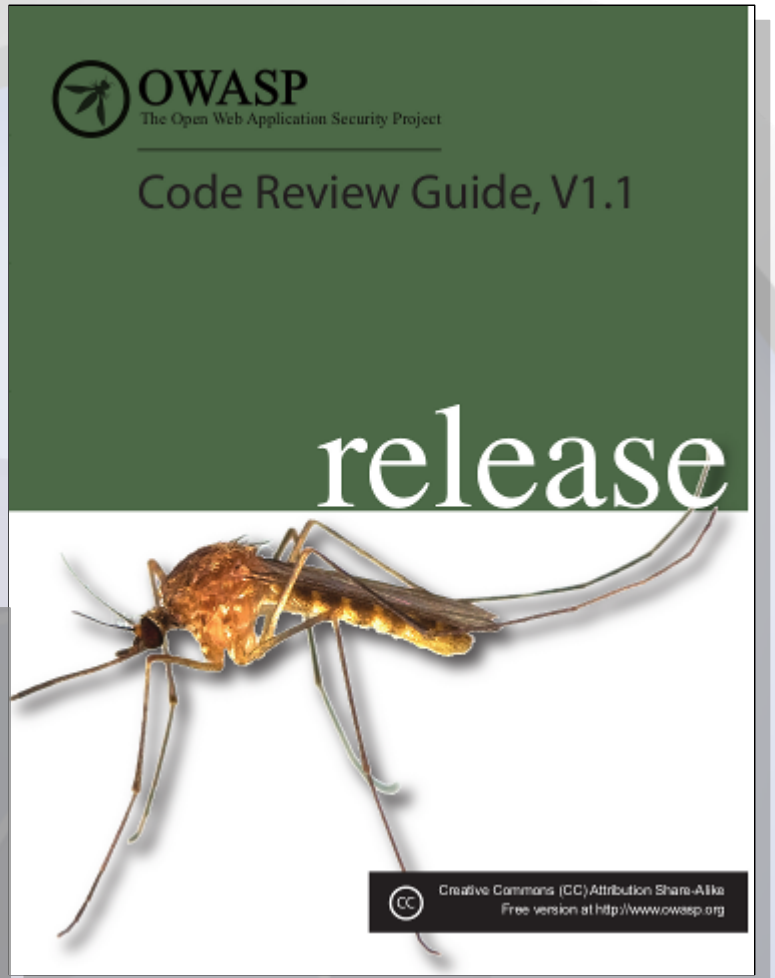
III. OWASP-Projekte

- **Developer's/Development Guide**
  - **Sprachenunabhängig**
  - **Kernpunkte sicherer Programmierung**
    - Data Validation, Canonicalization, Interpreter Injection
    - Session Management + Authorization
    - Error Handling, Logging
  - **Auch Webservices**
  - **Neuer Draft v3 in Arbeit**
    - Architektur
    - Extra Kapitel:
      - Input Validation
        +Output Escaping

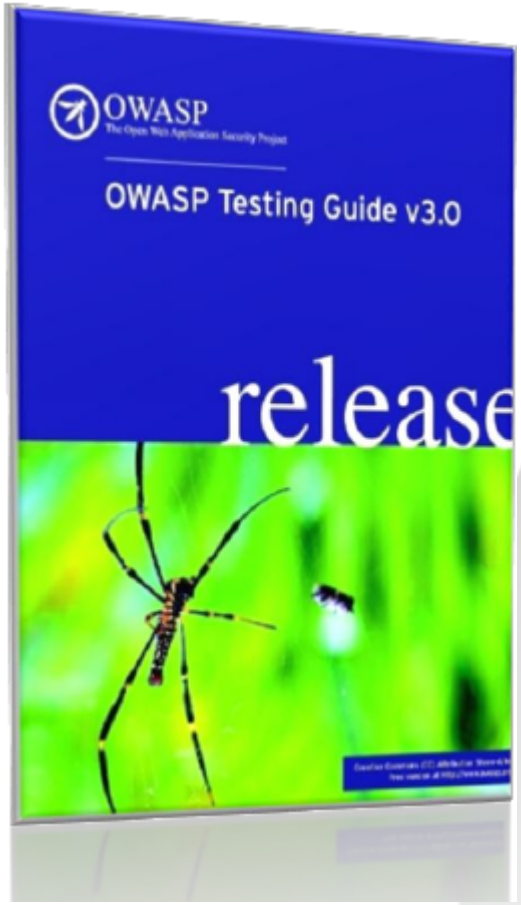
III. OWASP-Projekte

- **Code Review Guide**
  - „Code doesn't lie“

Reviewing by technical control: Authentication 70
Reviewing by technical control: Authorization 77
Reviewing by technical control: Session Management 83
Reviewing by technical 87
Reviewing by technical 90
Reviewing by technical 105
Reviewing Code for OS Inj 127
Reviewing Code for SQL In 132
Reviewing Code for Data 138
Reviewing Code for Cross- 153
Reviewing code for Cross- 160
Reviewing Code for Logging Issues 165
Reviewing Code for Session Integrity issues 170
Java gotchas .....
Java leading security practice .....
Classic ASP Design Mistakes .....
PHP Security Leading Practice .....
Strings and Integers .....
Reviewing MySQL Security .....
Reviewing Flash Applications .....
Reviewing Web services .....
How to write an application code review finding .....



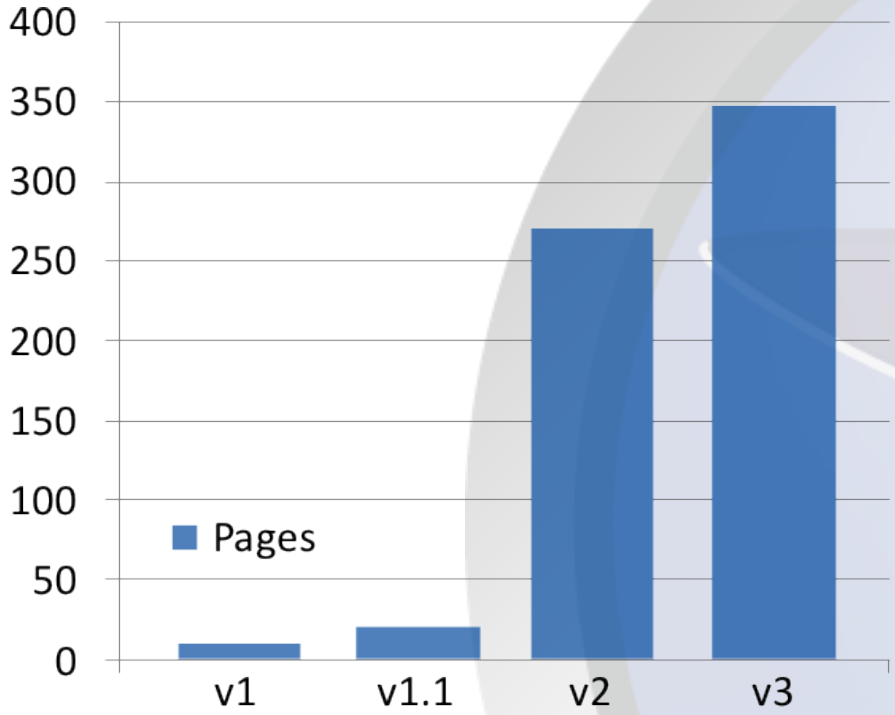
III. OWASP-Projekte



- **Testing Guide**
  - **Siehe SAMM (und Code Review Guide): keine sichere SW ohne Testing**
  - **2002: erste Gedanken zur Testmethodik**
  - **v1, v1.1: 2004**
  - **v2 (2007): erheblich erweitert**
    - Orientierte sich u.a. auf Verwundbarkeiten der OWASP Top 10
    - SOAP, XML, RESTful, Ajax
    - Wie Report?
      - Risiko!
  - **v3 (2008):**
    - OWASP Risk Rating Methology
    - Siehe OWASP Top 10 2010

III. OWASP-Projekte

- **Testing Guide**
  - **Immens gewachsen über all die Jahre**

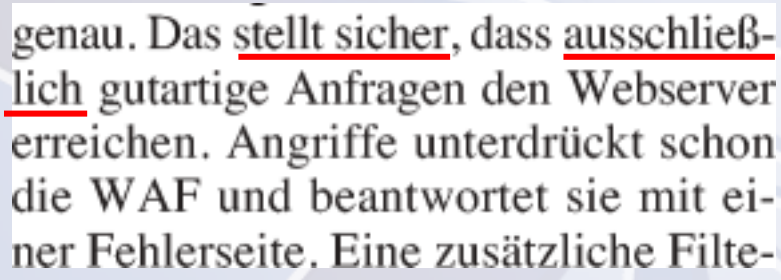


  - **v4 in Arbeit**
    - OWASP Vulnerability List
      =Gemeinsame Nummerierung d. Verwundbarkeiten
      - Auch Top 10, Code Review, Developers, ASVS
    - Ergänzungen zu WS
    - Übliche Updates

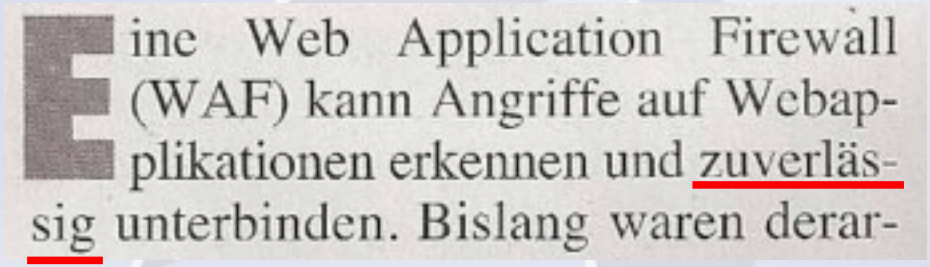
III. OWASP-Projekte

- **Best Practices WAF**
  - **Deutsches Vorzeigeprojekt**
    - Aber auch in Englisch
  - **Aufklärung teurer + nicht selten missverstandener Technologie**

iX 08/2008:


genau. Das stellt sicher, dass ausschließlich gutartige Anfragen den Webserver erreichen. Angriffe unterdrückt schon die WAF und beantwortet sie mit einer Fehlerseite. Eine zusätzliche Filte-

iX 06/2009:


Eine Web Application Firewall (WAF) kann Angriffe auf Webapplikationen erkennen und zuverlässig unterbinden. Bislang waren derar-

III. OWASP-Projekte

- **Best Practices WAF**
  - **„Tools drauf werfen"-Denken:** *If you think technology can solve your security problems then you don't understand the problems and you don't understand the technology (Bruce Schneier)*
  - **Leider**
    - WAFs können leider nicht alles
      - Was kann man erwarten?
      - Was nicht?
    - Und schon gar nicht nach Einstöpseln + von alleine
      - Wer macht's?
    - WAFs beheben Probleme nicht an der Wurzel
      - Wann sinnvoll?
    - WAF ist nicht gleich WAF
      - Architektur
      - Funktionsweise

IV. OWASP (cont'd)

- **Aktivitäten**
  - **Recht lebhafte Community**
    - Mailing-Liste
    - http://lists.owasp.org/mailman/listinfo/owasp-germany
    - Lokale Treffen in Metropolen
  - **Spannende deutsche Konferenzen seit 2007**
    - Steigende Zuschauerzahlen

IV. OWASP (cont'd)

- **Alles via owasp.org (auch: 

, )**
  - **Vieles auch in Buchform (lulu.com)**
    - Selbstkostenpreis

- **Konferenzen lohnen sich:**
  - **AppSec EU (USA)**
  - **OWASP Days**
    - Auch Benelux

Danke. Fragen?

Dirk Wetter

mail]ät[drwetter]punkt[eu
dirk]ät[owasp]punkt[org

@drwetter
gplus.to/drwetter