



OWASP

Open Web Application  
Security Project

# Ein Best-of-Konzept für Sicherheitsanalysen von Webanwendungen

Katharine Brylski  
iT-Cube Systems AG

# Agenda

- Motivation
- Was ist eine Sicherheitsanalyse?
- Bekannte Konzepte
- Entwicklung eines Best-of-Konzepts für Webanwendungen

# Motivation

30.04.2015 18:01

## eBay ignoriert XSS-Lücke ein Jahr lang

 vorlesen / MP3-Download



(Bild: dpa, Bernd Thissen/Archiv)

**Eine Schwachstelle in eBay erlaubt es Angreifern eine Session mitzuschneiden und im schlimmsten Fall einen Account zu übernehmen. Die Lücke ist ein Jahr alt und wurde immer noch nicht geschlossen.**

Quelle: <http://heise.de/-2630964>

15.12.2014 08:10

« Vorige | Nächste »

## l+f: Paypal kämpft mit XSS-Problemen

 vorlesen / MP3-Download

**Nur weil keiner mehr über Cross Site Scripting berichtet ist es längst nicht tot.**



In letzter Zeit ist es stiller geworden um [Cross Site Scripting](#). Das bedeutet längst nicht, dass das Problem aus der Welt geschafft wäre. Selbst auf Seiten, bei denen man erwarten sollte, dass sie das langsam mal in den Griff bekommen, tauchen immer wieder XSS-Lücken auf. Paypal etwa fixte in den letzten Wochen allein zwei davon. [Eine XSS-Lücke](#) entdeckte Sebastien Lekies

Quelle: <http://heise.de/-2489125>



**OWASP**

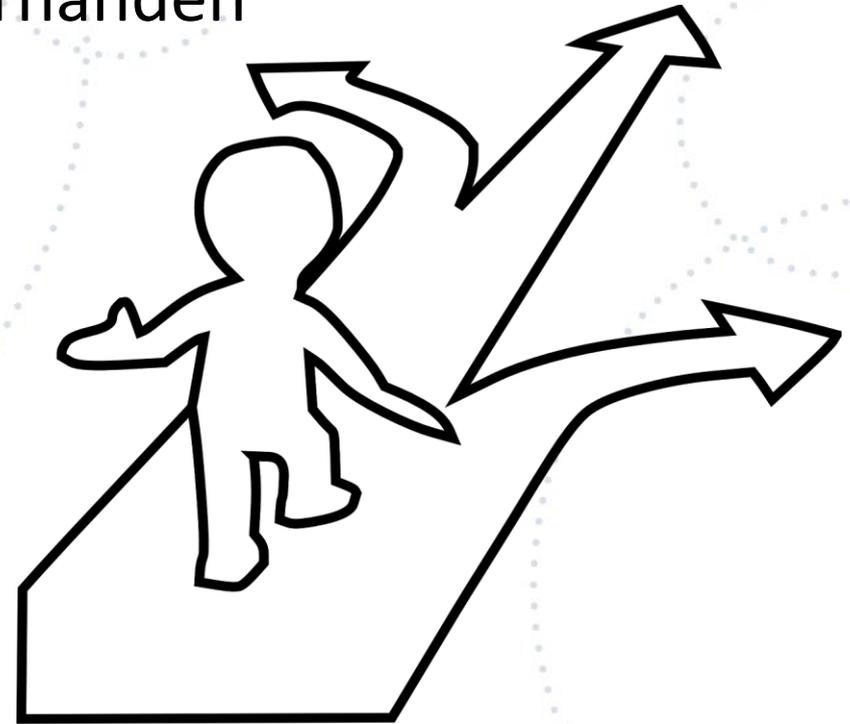
Open Web Application  
Security Project

#18 | OWASP Stammtisch Frankfurt | 30.07.2015

[WWW.OWASP.ORG](http://www.owasp.org)

# Motivation

- Sicherheit muss gewährleistet werden!
- Problem: viele Konzepte vorhanden
- Welches ist das **Richtige**?



# Was ist eine Sicherheitsanalyse?

- Überprüfung der Widerstandsfähigkeit von Systemen
- Aktive Eindringungsversuche am System
  - Penetrationstest
- Ergebnis
  - Empfehlungen für Maßnahmenbeseitigung

# Das richtige Konzept

- Viele Konzepte vorhanden
  - Vermeidung Beschreibung der Untersuchungsvorgehensweise
    - Gefahr Missbrauch als Hacking-Anleitung
  - Voraussetzungen für Sicherheitsanalyse unterschiedlich:
    - Untersuchungsgegenstand
      - Anwendung
      - Webserver
      - Infrastruktur
    - Umfang der Zugriffe auf Produktiv-/Testsystem
    - Quellcode gegeben?

# Bekannte Sicherheitsanalysen



**NIST**

Guideline on  
Network Security Testing



Sicherheitsüberprüfung  
von IT-Systemen  
mit Hilfe von „Tiger-Teams“



Bundesamt  
für Sicherheit in der  
Informationstechnik

Durchführungskonzept  
für Penetrationstests



Testing Guide



**OWASP**

Open Web Application  
Security Project

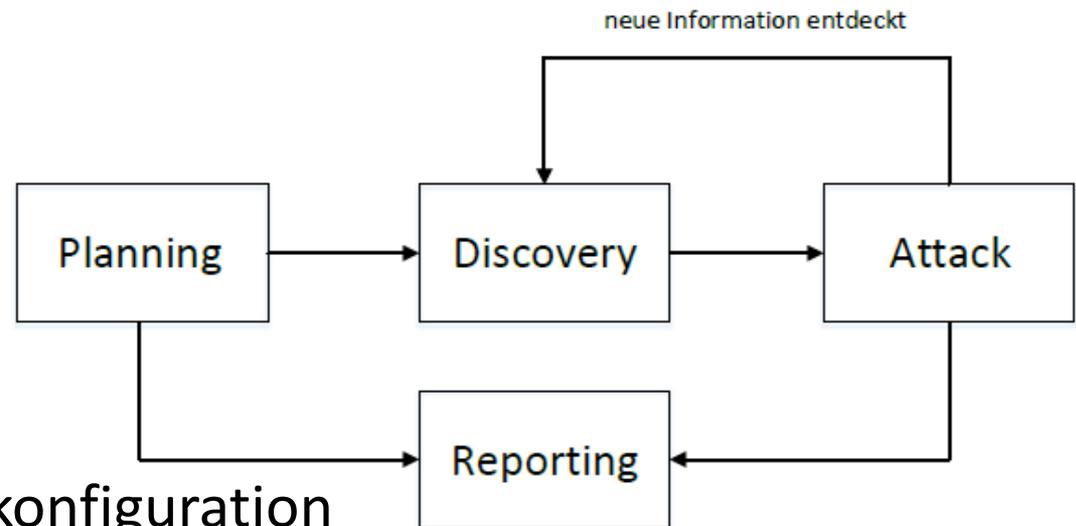
#18 | OWASP Stammtisch Frankfurt | 30.07.2015

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

## Guideline on Network Security Testing

- Techniken zur Überprüfung der **Netzwerksicherheit**  
z.B

- WLAN Testing
- Log Reviews
- **Penetration Testing**



→ Überprüfung Serverkonfiguration

- Offene Ports
- Softwareaktualität

# Sicherheitsüberprüfung von IT-Systemen mit Hilfe von „Tiger-Teams“

- 4 Phasen
  - Akquisition, Offerte und Vertrag
  - Risikoanalyse
  - Durchführung
  - Bericht und Präsentation
- Nur passive Angriffe
  - kein Schaden anrichten und keine Daten verändern
- Ergebnisse
  - Hinweise auf mögliche Schwachstellen



# Studie „Durchführungskonzept für Penetrationstests“

- Penetrationstest von **IT-Infrastrukturen**
- 5 Phasen
  - Vorbereitung
  - Informationsbeschaffung und –auswertung
  - Bewertung der Informationen / Risikoanalyse
  - Aktive Eindringversuche
  - Abschlussanalyse
- Anleitungen für Überprüfungen fehlen



# OWASP Testing Guide

- Sammlung von passiven und aktiven Angriffen
  - Erklärung der Ausführung und Verwendung der Tools
- Schwerpunkt Black-Box-Testing
  - aber auch z.T. Gray- und White-Box



# Zusammenfassung

				
Detaillierte Vorgehensweise der Überprüfung				✓
Untersuchungsschwerpunkt: Webanwendungen				✓
Strukturierte Vorgehensweise: Auftrag bis Übergabe	✓	✓	✓ ✓	

# Zusammenführung der Konzepte

- Fünf Phasen
  - Gemäß „Durchführungskonzept für Penetrationstests“ des BSI
- How To
  - OWASP „Testing Guide“
  - „Web Application Hacker's Handbook“

# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



# Beispielanwendung: demo.testfire.net

**Altoro Mutual** Sign In | Contact Us | Feedback | Search

**ONLINE BANKING LOGIN** **PERSONAL** **SMALL BUSINESS** **INSIDE ALTORO MUTUAL**

**PERSONAL**

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

**SMALL BUSINESS**

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

**INSIDE ALTORO MUTUAL**

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)

**Online Banking with FREE Online Bill Pay**  
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.



**Real Estate Financing**  
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.



**Business Credit Cards**  
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

**Retirement Solutions**  
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

**Privacy and Security**  
The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.



**Win an 8GB iPod Nano**  
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

[Privacy Policy](#) | [Security Statement](#) | © 2015 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.



**OWASP**

Open Web Application  
Security Project

#18 | OWASP Stammtisch Frankfurt | 30.07.2015

WWW.OWASP.ORG

# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



## Phase 1

# Vorbereitung

- Ist-Zustand erfassen
  - Welche Informationen stehen zur Verfügung?
  - Gibt es Abhängigkeiten zu anderen Systemen?
    - Auswirkungen auf andere Systeme
    - Notfallplan
  - Zeitliche Einschränkungen?
  - Was soll das Ergebnis sein?
    - Reine Auflistung der Schwachstellen
    - Lösungsvorschläge

→ Definition der Zielvereinbarung



# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



## Phase 2 Informationsbeschaffung

- Überblick verschaffen
  - Wie arbeitet die Anwendung
  - Kommunikation mit Nutzer
- Wie?
  - Abarbeitung einer Checkliste
    - Informations-Module (I-Module)

## Phase 2

# I-Module

- I-M.1: Untersuchung sichtbarer Inhalte
- I-M.2: Öffentliche Ressourcen befragen
- I-M.3: Untersuchung von versteckten Inhalten
- I-M.4: Serverseitige Technologien

## Phase 2

# I-M.1: Untersuchung sichtbarer Inhalte

- Manuelles Browsen
  - passives Spidern mit OWASP ZAP bzw. BurpSuite
  - mit/ohne JavaScript
  - mit/ohne SessionCookie
  - Unterschiedliche Browser
- Automatisierter Spider

## Phase 2

# I-M.1: Untersuchung sichtbarer Inhalte

HTTP-Methode	Rest-URL	Beschreibung	Parameter	Java Script	Sichtbar für
GET	~	Startseite			Alle
GET	~/search.aspx?txtSearch=xxxx	Suchfunktion	Suchstring: <i>txtSearch=xxxx</i>		Alle
GET	~/bank/login.aspx	Anmeldeseite			Alle
Post	~/bank/login.aspx	Anmelden	Anmeldedate: <i>uid=user&amp;passw=password&amp;btnSubmit=Login</i>	Ja	Alle

→ Zusammenfassung aller HTTP-Methoden, übermittelten Parameter, sowie eine Beschreibung

## Phase 2 I-M.2: Öffentliche Ressourcen befragen

- Suchmaschinen bzw. Cache
    - z.B. <https://www.google.de/search?q=cache:URL>
  - Wayback Machine
    - Welche Ressourcen öffentlich zugänglich sind
- Versteckte oder vergessene (Test-)Seiten entdecken

## Phase 2 I-M.3: Untersuchung von versteckten Inhalten

- Kommentar des Clientcodes
  - Verlinkungen
  - Geheimnisse

```
76
77 <h1>Online Banking Login</h1>
78
79 <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
80 <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:1
81
82 <form action="login.aspx" method="post" name="login" id="login" onsubmit="return
83 <table>
```

- BruteForce nach Standard-Seiten
  - Nikto oder OWASP DirBuster

## Phase 2 I-M.4: Serverseitige Technologien

- Informationen anhand von Serververhalten
  - (HTTP-Header / Reihenfolge)
- Software auf Schwachstellen (CVE) prüfen
- Offene Ports
  - Portscan mit Nmap

Phase 2

# Zwischenergebnis

- detaillierte Übersicht
  - potenziellen Angriffspunkte, beziehungsweise Sicherheitsmängeln

→ Basis für eigentlichen Test

# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



# Risikoanalyse

- Bewertung der Ergebnisse aus Phase 2
  - Wo kann eine Schwachstelle auftauchen
  - Zeitlichen Rahmen überprüfen

Schwachstelle	Auftreten	Auswirkung bei Ausnutzung	Analyseaufwand
XSS	Sehr häufig: <ul style="list-style-type: none"><li>- Textfelder</li><li>- Parameter in URL</li></ul>	<ul style="list-style-type: none"><li>-Schadcode beständig auf Site</li><li>-Diebstahl sensibler Daten</li></ul>	Mittel: Eingabe von Teststrings →ausreichende Filterung

# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



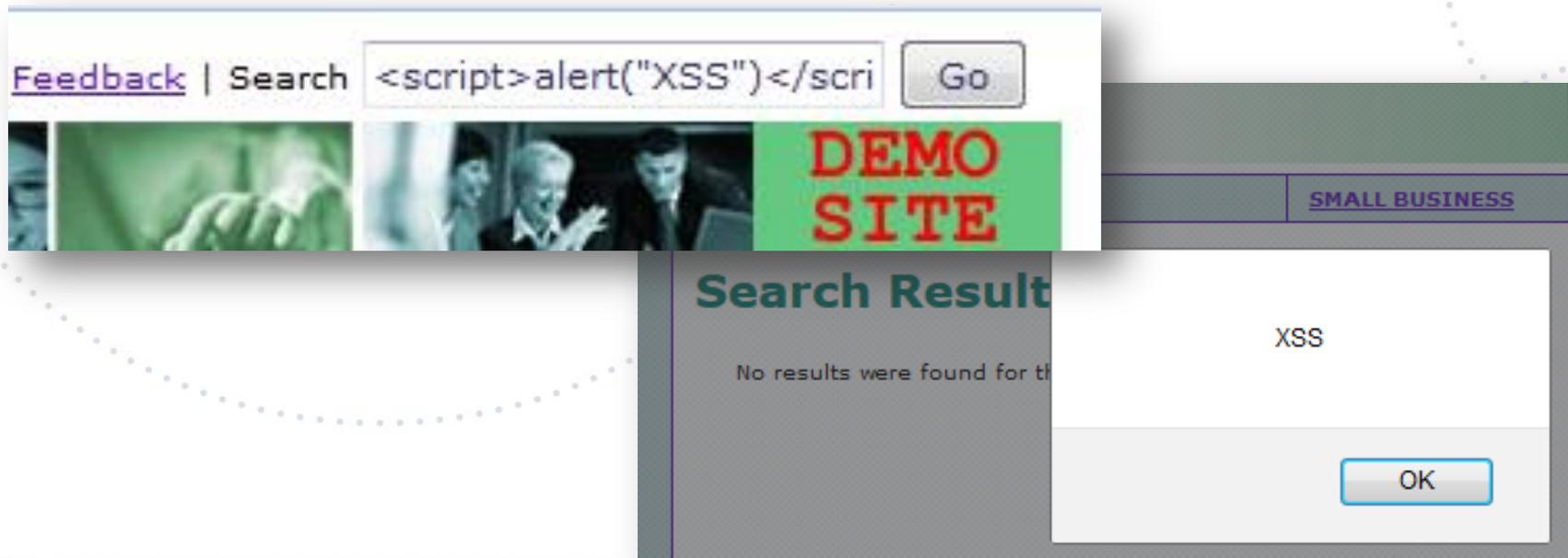
# Phase 4 Eindringungsversuche

- E(indringungs)-Module (Anlehnung OWASP Top 10)
  - E-M.1: Injection
  - E-M.2: Fehler in Authentifizierung und Session-Management
  - E-M.3: Cross-Site Scripting (XSS)
  - E-M.4: Unsichere direkte Objektreferenzen
  - E-M.5: Sicherheitsrelevante Fehlkonfiguration
  - E-M.6: Verlust der Vertraulichkeit sensibler Daten
  - E-M.7: Fehlerhafte Autorisierung auf Anwendungsebene
  - E-M.8: Cross-Site Request Forgery (CSRF)
  - E-M.9: Verwendung von Komponenten mit bekannten Schwachstellen
  - E-M.10: Ungeprüfte Um- und Weiterleitungen

→ eindeutig Schwachstellen identifizieren

## Phase 4 E-M.3: Cross-Site Scripting (XSS)

- Grundlage: Übersicht aus Phase 2
  - Verdächtig: Eingabefelder, Parameter in URL



# Durchführung des Best-of-Konzepts

Phase 1

- Vorbereitung

Phase 2

- Informationsbeschaffung

Phase 3

- Risikoanalyse

Phase 4

- Eindringungsversuche

Phase 5

- Abschlussanalyse



## Phase 5

# Abschlussanalyse

- Beispiel: Suchfeld

Beschreibung des Tests	Soll-Zustand	Ist-Zustand	Ergebnis
Einschleusung von aktiven Inhalten	Verhinderung der Ausführung von eingeschleusten Skript	Code ausführbar, nicht beständig	Anfällig; nicht-persistenter XSS
Filterung von Metazeichen oder Strings	Bestandteile für Skripte werden gefiltert	Keine Filterung	Anfällig
Escapen von Metazeichen	Metazeichen werden escapt	Keine	Anfällig

- Lösungsvorschlag: Verwendung Bibliotheken, WAF, Whitelists,...

# Fazit

- Anwendung muss sicher sein!
  - Imageschaden
  - Datendiebstahl
- Strukturierte Überprüfung anhand 5 Phasen
  - Vom Auftrag bis Berichterstattung
- Ausblick
  - Nach Beseitigung erneute Überprüfung in periodischen Abständen



# Quellen

- Fotos: <https://pixabay.com/de/>
- [BSI03] Studie: Durchführungskonzept für Penetrationstests. (November 2003).  
[https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/pentest/index\\_htm.html](https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/pentest/index_htm.html)
- [DS11] Dafydd Stuttard, Marcus P.: The Web Application Hacker's Hand-book: Finding and Exploiting Security Flaws. Wiley, 2011. - ISBN 1118026470
- [OWA08] OWASP TESTING GUIDE. (2008).  
[https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
- [OWA13] OWASP Top 13 - 2010 The Ten Most Critical Web Application Security Risks. (2013).  
[http://www.owasp.org/index.php/Top\\_10](http://www.owasp.org/index.php/Top_10)
- [Tig99] Sicherheitsüberprüfung von IT-Systemen mit Hilfe von "Tiger-Teams", ISACA Switzerland Chapter, SI Fachgruppe Security, 1999.  
[http://www.isaca.ch/home/isaca/files/Dokumente/04\\_Downloads/DO\\_03\\_Arbeitsgruppen/A\\_N\\_01\\_Diverse/tigerteam.pdf](http://www.isaca.ch/home/isaca/files/Dokumente/04_Downloads/DO_03_Arbeitsgruppen/A_N_01_Diverse/tigerteam.pdf)
- [WTS03] Wack, John ; Tracy, Miles ; Souppaya, Murugiah: The Open Source Security Testing Methodology Manual, NIST, Oktober 2003 (NIST special publication ; 800-42. Computer security). <http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf>

