

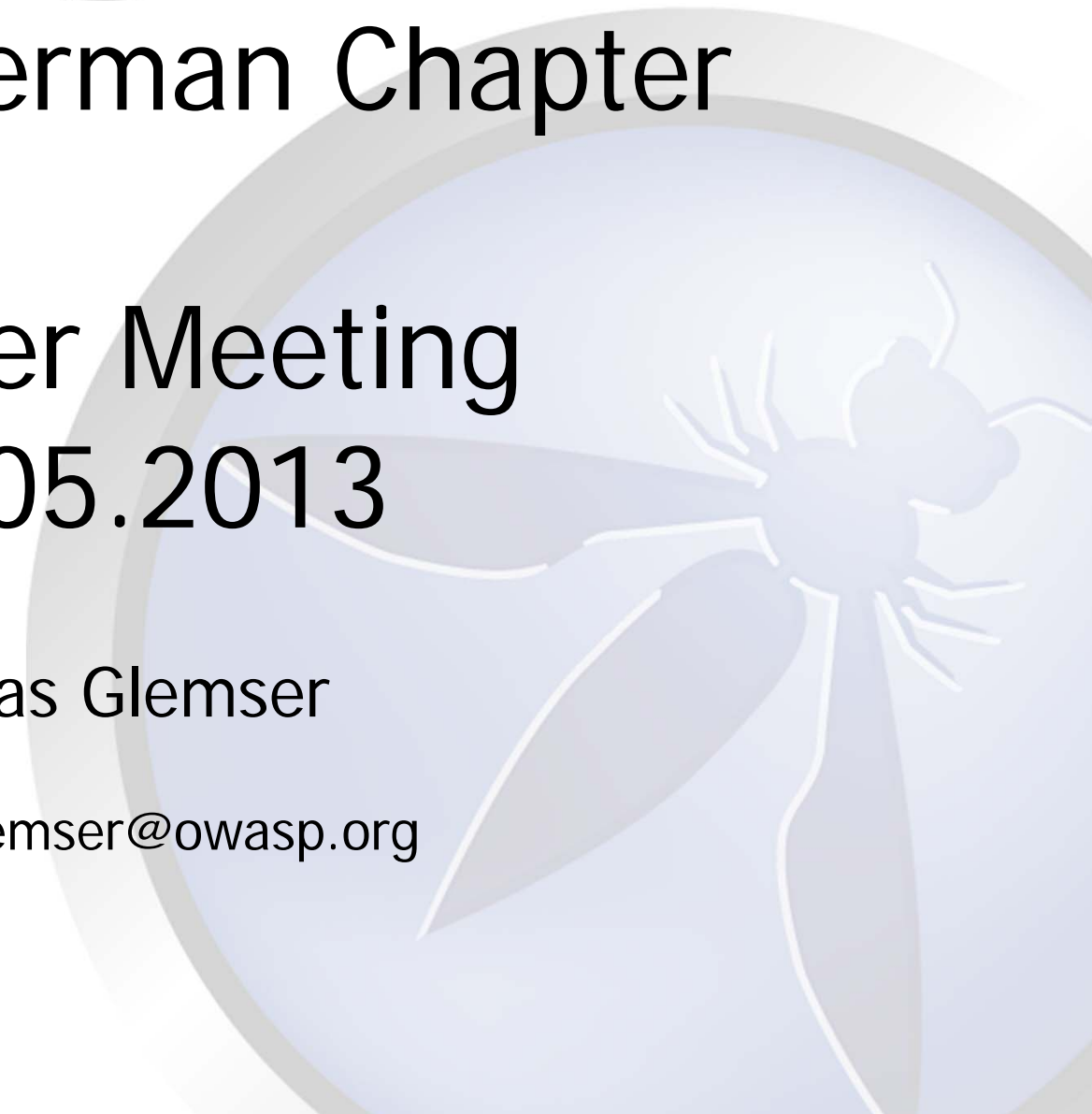


OWASP German Chapter

Chapter Meeting 17.05.2013

Tobias Glemser


tobias.glemser@owasp.org



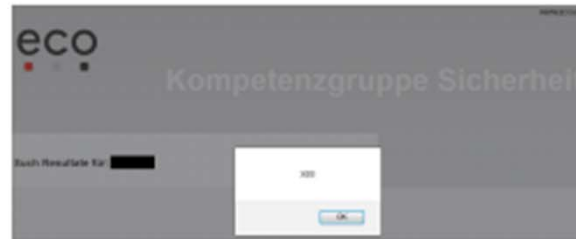



Was ist OWASP?

Heise-Leser entdeckt Sicherheitslücken auf 150 Webseiten

 vorlesen / MP3-Download

Florian Gumbel, ein 19-jähriger Leser von heise online und heise Security, hat Schwachstellen auf über 150 namhaften Webseiten wie Bitkom.org, Buhl.de, Eco.de, Ferrari.com, KabelBW.de, Kicker.de, IHK.de, Wetter.de und Zurich.de entdeckt. Bei den Lücken handelt es sich um sogenannte Cross-Site-Scripting-Lücken (XSS), die ein Angreifer dazu nutzen kann, um eigenen Code in die verwundbaren Seiten einzuschleusen; etwa, um Zugangsdaten zu stehlen oder Schadcode zu verbreiten.



Durch XSS-Lücke eingebetteter JavaScript-Code. 

Außer der schieren Anzahl der verwundbaren Webseiten überrascht auch der Anteil der überregional bekannten und mutmaßlich gut besuchten Internet-Präsenzen. Dabei ist Cross-Site-Scripting bei weitem kein neues Phänomen: heise Security berichtete bereits im Jahr 2003 ausführlich über daraus resultierende Gefahren. Unser Leser hat nach eigenen Angaben rund 12 Stunden gebraucht, um die uns vorliegende Liste mit verwundbaren Seiten zusammenzustellen.

Reale Gefahr?

kylex (167 Beiträge seit 20.06.01)

XSS ist bei Nutzergenerierten Inhalten relevant.

Was aber bei einem Suchfeld gefährlich sein soll, dessen Inhalt nur der Nutzer selbst ausgegeben bekommt, erschließt sich mir nicht wirklich.

Der Fall, dass jemand einen Link erstellt, in dessen URL via GET irgendwas mitgeschickt wird und auf dessen Anklicken gehofft wird, halte ich doch für ein bisschen paranoid.



Was ist OWASP?

- ~~Fear, Uncertainty and Doubt" (FUD)~~
- Angstkultur < > Wissen





Was ist OWASP?

Das Open Web Application Security Project
hilft damit

- Entwicklern
 - Entscheidern
 - QA-Spezialisten
 - Penetrationstestern
- ➔ Ihnen



Was ist OWASP?

Werte

- Offen
- Innovativ
- Weltweit vertreten
- Integer





Was ist OWASP?

Prinzipien

- Frei und Offen
- Getrieben durch Konsens und funktionierenden Code
- Ausgerichtet an Werten
- Non-profit
- Nicht von kommerziellen Interessen getrieben
- Risiko basierte Ansätze



Was ist OWASP?

Organisationsstruktur

- Board
- Chapter
- Mitglieder





Was ist OWASP?

Chapter

- Lokale Organisationseinheiten
- Kann jeder überall einrichten (auch in einzelnen Städten/Regionen)
- Grundlegen im Chapter Handbook



Was ist OWASP?

Mitglieder

- Firmen
- Einzelpersonen
- Edukative Einrichtungen





Projekte

- Unterteilt in
 - Code
 - Tools
 - Documents





Projekte

- Viele, viele, viele Projekte (Stand 05/13)
 - Flagship (4 Code, 3 Tools, 8 Doku)
 - Labs (26 Tools, 8 Doku)
 - Incubator (19 Code, 39 Tools, 41 Doku)



Bekannteste Projekte

- OWASP Top 10 (2004, 2007, 2010, 2013)
- OWASP Development Guide
- OWASP Code Review Guide
- OWASP Testing Guide
- OWASP Zed Attack Proxy (ZAP)
- OWASP WebGoat
- OWASP ModSecurity Core Rule Set Project



Das deutsche Chapter

- Derzeit ein Chapter in Deutschland
- Aktuell 6 Personen im Board
- Regelmäßige lokale Stammtische in
 - München
 - Frankfurt
 - Stuttgart
 - Köln
 - Hamburg
 - Karlsruhe
 - Nürnberg (Neustart?)
 - Berlin (Neustart?)
 - Dresden (im Aufbau)



Das deutsche Chapter

- Projekte
 - Best Practices: Web Application Firewalls (2008 abgeschlossen)
 - Projektierung der Sicherheitsprüfungen von Webanwendungen (2009 abgeschlossen)
 - Top 10 2010 Übersetzung (2011 abgeschlossen)



Das deutsche Chapter

- Projekte
 - Review BSI-Grundschutz Baustein Webanwendungen (2012 abgeschlossen), 2 Vorträge auf dem GS-Tag 2012
 - German Language Project (aktiv)
 - OWASP Top 10 fuer Entwickler (aktiv, später mehr)
 - OWASP Top 10 2013 Übersetzung (geplant)



Das deutsche Chapter

- Konferenz OWASP Day Germany
 - Ehemals AppSec Germany
 - Seit 2008
 - Größter Event zu Webanwendungssicherheit in Deutschland
- 2013 AppSec EU Research in Hamburg (später mehr)



Das deutsche Chapter

- Messestand it-sa
 - Seit 2008 (IIRC) jedes Jahr
 - Sehr gute Kontaktfläche
 - Mehr Unterstützung am Stand notwendig



Das deutsche Chapter

- Chapter Sponsoring
 - Seit 2012
 - 500 EUR/Jahr
 - Direkte Unterstützung des Chapters

SCHUTZWERK

Tele-Consulting
security | networking | training gmbh



sic [✓] sec

CYBERDAY®



Die Zukunft

- Basis der Stammtische verbreitern
- Mehr Projekte und Projekteilnehmer
- Höhere Reichweite, insbesondere „Neulinge“ und Studenten (Zeit 😊)
- Weitere Aspekte von Anwendungssicherheit (Mobility)
- Mehr Mitglieder
 - Firmen
 - Personen



Kontakt und Informationen

<http://www.owasp.de/>

<https://www.owasp.org/>

[https://lists.owasp.org/mailman/listinfo/
owasp-germany](https://lists.owasp.org/mailman/listinfo/owasp-germany) (eintragen!)

Tobias Glemser

tobias.glemser@owasp.org



Agenda

- 14:30h Laurent Levi: DevOps and Security: It's Happening. Right Now.
- 15:15h Dirk Wetter: OWASP Day 2012 und Ausblick AppSec EU Research 2013
- 15:45h Pause (15 min)
- 16.00h Jim Manico: Top Ten Web Defenses
- 16.45h Torsten Gigler: OWASP Top 10 fuer Entwickler
- 17.00h Chapter Board Wahl
- 17.15h offene Runde: OWASP Germany im kommenden Jahr



Boardwahl

- „It is always advisable to avoid elections“
- (If electing) "elections should be held for a 24 months term"
- Bislang jährlich. OK?
- Wer hat Lust sich zu engagieren?