

# ThreadFix als Beispiel eines Vulnerability Management Systems

Mirko Dziadzka

*<http://mirko.dziadzka.de/>  
@MirkoDziadzka*

OWASP Stammtisch München - 18.03.2014

## Worum soll es heute gehen

- ▶ Ich habe mich im Rahmen eines Projektes mit ThreadFix beschäftigt, und wollte darüber was erzählen und kurz was zeigen
- ▶ Eher von der Position eines Integrators, nicht eines wirklichen Anwenders

# DISCLAIMER

- ▶ Ich arbeite für einen WAF Hersteller
- ▶ Ich gebe hier meine Meinung wieder
- ▶ das ist nicht notwendigerweise auch die Meinung meines Arbeitgebers.

## Wer bin ich - Kurzfassung

- ▶ Old School Unix Geek, currently interested in
  - ▶ IT-Security
  - ▶ Software Development
  - ▶ Unix
  - ▶ Python
  - ▶ Distributed Systems

## Wer bin ich - Kurzfassung

- ▶ 80er: Studium Mathe/Informatik
- ▶ 90er:
  - ▶ System- und Netzwerkadmin
  - ▶ Dozent: Unix und Security
  - ▶ Autor: Linux Kernel Programmierung
- ▶ ab 1999: Entwicklung + Betrieb im Schweizer Bankumfeld.
  - ▶ unter anderem Implementation von Web-Input-Filtern und Authentisierungs-Proxies
- ▶ seit 2005 bei art of defence / Riverbed in Regensburg

- ▶ Vulnerability Management System
- ▶ Denim Group, Open Source, Java
- ▶ <https://github.com/denimgroup/threadfix>
- ▶ Zur RSA im Februar in der Version 2.0 erschienen

- ▶ Versucht dem Entwickler und/oder Betreiber von Webapplikationen ein Mittel in die Hand zu geben, um
- ▶ die Ergebnisse von Vulnerability Scans, Audits zu verwalten
- ▶ daraus Aktionen abzuleiten (Priorisierung, Bug Tickets)
- ▶ in der Zwischenzeit Regeln für WAF und IDS abzuleiten

# ThreadFix Integration

- ▶ REST interface (ändert sich grade öfter mal)
- ▶ Plugin System für integration neuer Komponenten
- ▶ clone on github, pull request -> legal documents



- ▶ Importiert Vulnerabilities aus verschiedenen Quellen
  - ▶ ca. 15 Scanner
  - ▶ ca. 5 Source Code Scanner (beta)
  - ▶ per Hand vom Audit
- ▶ Erlaubt das klassifizieren, mergen, priorisieren, verwalten, ... dieser Findings
- ▶ Statistiken, Reports, .... wie entwickeln sich meine Apps

- ▶ Generiert aus den Findings Issues in diversen Issue Trackern
  - ▶ bugzilla
  - ▶ Jira(?)
  - ▶ Microsoft Team Foundation Server (in Entwicklung)
- ▶ und stellt fest, wenn diese (angeblich) gefixt sind

- ▶ Generiert Real Time Protectionrules für diverse WAFs ....  
mod-security, snort, diverse kommerzielle
- ▶ und kann die Logs (einiger) dieser WAFs wieder importieren  
um die wirksamkeit der mitigations zu tracken
- ▶ ABER: Die Qualität der WAF Anbindungen ist  
diskussionswürdig
  - ▶ die in 2.0 vorhandenen WAF Anbindungen wurden von  
ThreadFix implementiert und zeichnet sich durch overblocking  
aus
  - ▶ in 2.0 haben nur 2(?) WAF Anbindungen den logfile import  
implementiert
  - ▶ das ist IMHO eher ein proof of concept
- ▶ ABER: Besserung ist in Sicht

- ▶ Kurze Vorführung der ThreadFix GUI
- ▶ Zusammenspiel zwischen
  - ▶ ThreadFix
  - ▶ OWASP ZAP
  - ▶ Web Application Firewall

# Diskussion