OWASP
Open Web Application Security Project

Top 10 Privacy Risks Project

Initial results presentation @ IPEN Workshop

Florian Stahl (Project Lead, msg systems, Munich)
Stefan Burgmair (Master Student, Univ. of Applied Sciences Munich)

26 September 2014, Berlin State Parliament

msg
Sponsored by

Background

- OWASP is an open source and non-profit organization and known for its Top 10 Web Application Security Risk list (de facto standard)
- No such list or standard for privacy risks available
- Top 10 Privacy Risks Project founded in early 2014
- Goal: Identify the most important technical and organizational privacy risks for web applications
- Nearly 100 privacy and security experts from all over the world participated (62 participated in survey)
- Method is explained on the project website
- Member of IPEN

OWASP
Open Web Application Security Project

Top 10 Privacy Risks Results v1.0

P1	Web Application Vulnerabilities
P2	Operator-sided Data Leakage
P3	Insufficient Data Breach Response
P4	Insufficient Deletion of personal data
P5	Non-transparent Policies, Terms and Conditions
P6	Collection of data not required for the user-consented purpose
P7	Sharing of data with third party
P8	Outdated personal data
P9	Missing or Insufficient Session Expiration
P10	Insecure Data Transfer