OWASP
Open Web Application Security Project

OWASP Top 10 – 2017

Die 10 kritischsten Sicherheitsrisiken für Webanwendungen

- Neuerungen & Hintergründe
- Aktuelles (20.11.2018)

OWASP
German Chapter

Über mich

Torsten Gigler:

- **Interner IT-Sicherheitsberater bei einer Bank**
  spezialisiert auf IT-Infrastruktur- und Anwendungs-Sicherheit (>20 Jahre)
- **In OWASP seit 6 Jahren aktiv:**
  - OWASP Top 10 – 2017 (Co-Leader)
  - OWASP Top 10 – 2013 (Contributor und Mitarbeit bei der deutschen Version)
  - OWASP Top 10 für Entwickler (seit 6 Jahren)
  - O-Saft – OWASP SSL Advanced Forensic Tool (Co-Entwickler seit 5 Jahren)
  - Stammtisch München (Mitglied im Organisations-Team seit 4 Jahren)
  - OWASP-Germany (Mitglied im Chapter-Board seit 1 Jahr)

Unsere Mission (1)

- **Awareness**

  Für **Entwickler, Anwendungs-Verantwortliche, Sicherheitstester** und **Manager:**

  – **Sensibilisierung und kompakter Einstieg** in die Sicherheit für Webanwendungen

  – **Verstehen** von (gefundenen) Schwachstellen und **Hilfe** beim Beseitigen

- **Security-by-Default**

  – Motivation für das Programmieren von Tools und Bibliotheken, die bereits mit **Standard-Einstellungen robust gegen Schwachstellen** sind.

Unsere Mission (2)

- **Nutzung als ‚De-Facto-Sicherheitsstandard‘**
  - **Meine Meinung: kein Standard**
    - → Vermittelt die Fähigkeit Risiken ‚zu sehen‘
    - → ‚Good Practices‘ für die 10 kritischsten Risiken
    - → **Guter erster Schritt** für mehr Anwendungssicherheit

Neuerungen: Methodik

- **Zusammensetzung der 10 Risiken:**
  - **8 Risiken** auf Basis einer **Datenerhebung** [+DAT]
    - **Rückschau**
    - **Häufigkeitsrate** auf Basis der **Anwendungen** mit einer bestimmten Schwachstelle (vorher: Anzahl der Schwachstellen)
    - **Rohdaten und Ergebnisse** sind öffentlich abrufbar
  - **2 Risiken** auf Basis einer **Expertenumfrage in der Community** [+DAT]
    - **Vorausschau**
- **Berechnung der Risiken:**
  - **Faktoren (1-Niedrig … 3-Hoch)** (vorher: umgekehrt) [+R]
  - Angabe des **Werts** [+RF]

Neuerungen: Risiken

OWASP Top 10 - 2017:

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Fehler in Authentifizierung und Session-Mgmt.	→	A2:2017-Fehler in der Authentifizierung
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Verlust der Vertraulichkeit sensibler Daten
A4 – Unsichere direkte Objektreferenzen [mit A7]	U	A4:2017-XML External Entities (XXE) [NEU]
A5 – Sicherheitsrelevante Fehlkonfiguration	↘	A5:2017-Fehler in der Zugriffskontrolle [vereint]
A6 – Verlust der Vertraulichkeit sensibler Daten	↗	A6:2017-Sicherheitsrelevante Fehlkonfiguration
A7 – Fehlerhafte Autorisierung auf Anw.-Ebene [mit A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Unsichere Deserialisierung [NEU, Community]
A9 – Nutzung von Komponenten mit bekannten Schwachstellen	→	A9:2017-Nutzung von Komponenten mit bekannten Schwachstellen
A10 – Ungeprüfte Um- und Weiterleitungen	☒	A10:2017-Unzureichendes Logging & Moniting [NEU, Community]

NEU

NEU, Community

NEU, Community

OWASP Open Web Application Security Project

Empfehlung: Nächste Schritte für…

- ‚Rollenbezogene‘ Seiten:
  - Software-Entwickler [+E]
  - Sicherheitstester [+T]
  - Organisationen [+O]
  - Anwendungs-Verantwortliche [+A]

- Geben Hinweise auf
  - weitere Vorgehensweise
  - Prozesse
  - weitere Sicherheitsmaßnahmen und ‚Best Practices‘
  - zusätzliche Dokumente und Tools von OWASP

Aktuelles: Deutsche Version

NEU

Deutschsprachiges Top 10-Team:

- Christian Dresen
- Alexios Fakos
- Louisa Frick
- Torsten Gigler
- Tobias Glemser
- Dr. Frank Gut
- Dr. Ingo Hanke
- Dr. Thomas Herzog
- Dr. Markus Koegel
- Sebastian Klipper
- Jens Liebau
- Ralf Reinhardt
- Martin Riedel
- Michael Schaefer

Hier beim German OWASP Day und als Download:

https://www.owasp.org/index.php/Germany/Projekte/Top_10

OWASP
Open Web Application Security Project

Dein/Ihr Einsatz

OWASP
Open Web Application Security Project