

Seminar „Web Application Security anhand der OWASP Top 10 (2017 NEU!)“

Sicherheits-Risiken in Webanwendungen veranschaulicht dargestellt anhand der OWASP Top 10 (2017!) mit entsprechenden Querverweisen in den IT-Grundschutz-Baustein für Webanwendungen sowie Besprechung geeigneter Schutz-Maßnahmen.

Da noch keine offizielle Übersetzung vorliegt, werden einige geänderte oder neue Topics und zitierte Passagen der Folien in Englisch sein. Die Seminarsprache selbst ist Deutsch.

Veranstaltungs-Agenda: 9:45 Uhr – 17:15

9:45 – 11:15

- Kurzvorstellung OWASP als Organisation, OWASP Top 10 – 2017, mit Rückschau (Top 10: 2013, 2010, 2007, 2004), IT-Grundschutz-Baustein Webanwendungen, Dozent
- Prinzipielle Funktionsweise einer Anwendung basierend auf Client / Server / Repository Architektur
- Kurzeinführung in HTTP, SSL/TLS, HTML und JavaScript
- Vorstellung Intercepting HTTP-Proxies und geeigneter Browser-AddOns für sicherheitstechnische Betrachtungen

Kurze Pause

11:30 – 13:00

- OWASP Top 10 - A7 - 2017 - Cross-Site Scripting (XSS)
[aus didaktischen Gründen wird die A7 zuerst behandelt, um Grundlagen zu schaffen]
- OWASP Top 10 - A1 - 2017 - Injection

Mittagspause

14:00 – 15:30

- OWASP Top 10 - A2 - 2017 - Broken Authentication
- OWASP Top 10 - A3 - 2017 - Sensitive Data Exposure
- OWASP Top 10 - A4 - 2017 - XML External Entities (XXE)
- OWASP Top 10 - A5 - 2017 - Broken Access Control Restrictions
- OWASP Top 10 - A6 - 2017 - Security Misconfiguration Security
- OWASP Top 10 - A8 - 2017 - Insecure Deserialization

Kurze Pause

15:45 – 17:15

- OWASP Top 10 - A9 - 2017 - Using Components with Known Vulnerabilities
- OWASP Top 10 - A10 - 2017 - Insufficient Logging & Monitoring
- Cross-Site Request Forgery (CSRF) (Top 10 - A8 - 2013)
- Ungeprüfte Um- und Weiterleitungen (Top 10 - A10 - 2013)
- Clickjacking
- Information Gathering
- Zusammenfassung, Ausblick und weiterführende Möglichkeiten
- Offene Diskussion, ggf. begleitet von Live-Hacking Demonstration

Veranstaltungsort: Bürokomplex STOCKWERK, Gröbenzell

STOCKWERK <<http://www.stockwerk.de/>>
Konferenzraum 3, 3. Stock <<https://www.allianz-fuer-cybersicherheit.de/>>
Oppelner Str. 5
82194 Gröbenzell bei München

Durchführung der Veranstaltung: sic[!]sec GmbH, Gröbenzell

sic[!]sec GmbH <<http://www.sicsec.de/>> Tel: 08142-44250-30
Industriestr. 31 E-Mail: info@sicsec.de Fax: 08142-44250-39
82194 Gröbenzell bei München

Kapazität der Veranstaltung: 32 Teilnehmer

Maximale Teilnehmerzahl: 32; Mindestteilnehmerzahl: 4

Veranstaltungstermine für 2018

Nach Vereinbarung.

Anmeldeschluss (Anmeldungen ausschließlich über „info@sicsec.de“)

10 Arbeitstage vor dem vereinbarten Termin.

Seminarkosten

Unser „Sorglos-Paket“ zum Preis von EUR 490,00 netto zzgl. USt beinhaltet alle Seminarunterlagen in gedruckter und gebundener Form, Schreibzeug sowie alle Getränke, Snacks und Fingerfood während des Tages.

Bitte beachten Sie, dass wir 20 % dieses Betrages auch dann in Rechnung stellen müssen, wenn Sie am Veranstaltungstag verhindert sind und nicht bis zum Anmeldeschluss storniert haben.

Quellen und weiterführende Infos

IT-Grundschutz-Baustein für Webanwendungen, allgemeine Informationen
<https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2012/Neuer_IT-Grundschutz-Baustein_Webanwendungen_17102012.html>

IT-Grundschutz-Baustein für Webanwendungen, Download
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen.pdf?__blob=publicationFile>

IT-Grundschutz-Baustein für Webanwendungen, Goldene Regeln, Download
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen_Goldene_Regeln.pdf?__blob=publicationFile>

OWASP Top 10 – 2017, Download (aktuell nur auf Englisch)
<https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>

