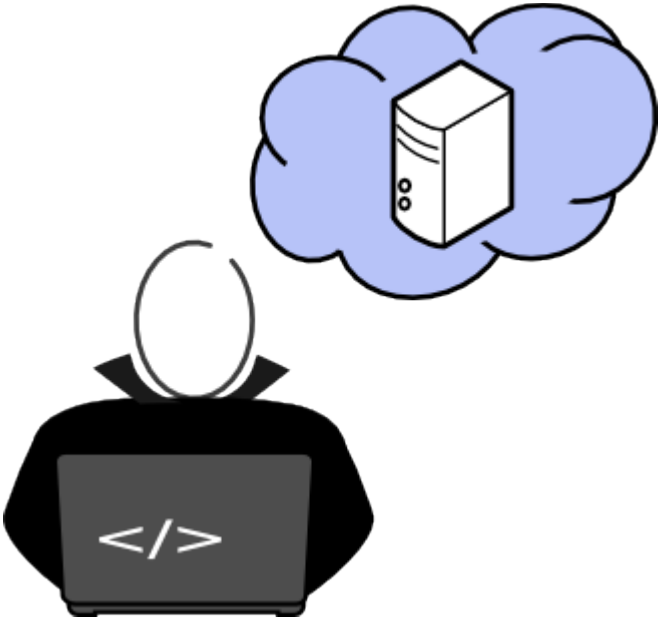
Frank Hissen



Sichere Programmierung von Web-Anwendungen

Applikationssicherheit verstehen

Inhaltsverzeichnis

Motivation: Angriffe auf Web-Anwendungen

Zahlreiche erfolgreiche Angriffe auf bekannte Web-Anwendungen finden wöchentlich Einzug in einschlägige Medien. Grund genug bei der Entwicklung eigener Anwendung - egal ob zur rein internen Nutzung oder mit öffentlichem Zugang - sich mit den Hintergründen der "Web Application Security" zu beschäftigen.

Dieses Buch behandelt dabei nicht verwandte Themen wie Sichere (Netzwerk-)Infrastrukturen, Betriebssystemsicherheit, Patch Management, Firewall Architekturen etc. sondern fokussiert sich ausschließlich auf die Anwendungsebene - dem zentralen Tätigkeitsfeld eines Softwareentwicklers.

Web-Anwendung steht hier generisch als Bezeichnung für

- Internet-Anwendungen
- Intranet-Anwendungen
- Cloud-Services / Cloud-Dienste
- Web-Portal
- Web-Services
- Web-APIs

Manche dieser Anwendungsgruppen sind von bestimmten, hier genannten Angriffsformen nicht betroffen. Ein reines Backend für eine mobile App etwa ist nicht von Clickjacking betroffen; (No)SQL-Code-Injections sind hingegen in Betracht zu ziehen.

Typische Angriffe

Die typischen bzw. häufigsten Angriffe auf Web-Anwendungen sind:

- [01] Code/Command Injection allgemein
    - z.B. E-Mail, Header-Injection
- [02] (No)SQL-Code-Injection
- [03] Cross-Site-Request-Forgery (CSRF)
- [04] Cross-Site-Scripting (XSS)
    - u.a. JavaScript, HTML
- [05] Open-Redirection
- [06] Remote File Inclusion (RFI) sowie Local File Inclusion (LFI) bzw. Directory/Path Traversal
- [07] Clickjacking
- [08] Session-Hijacking
    - u.a. Transaktionsmanipulation
- [09] Information Disclosure
- [10] Angriffe auf Schwachstellen der Authentifizierung