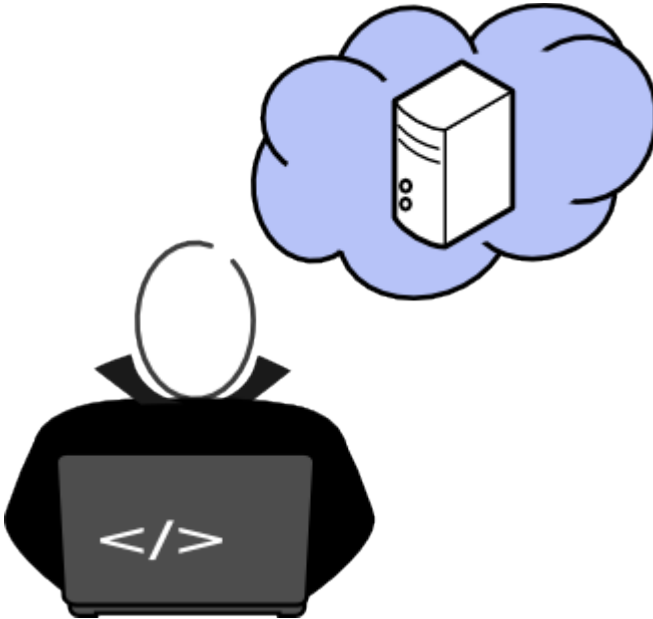Frank Hissen

Secure Programming of Web Applications

Web Application Security
for Software Developers
and Project Managers

Contents

Motivation: Web Application Attacks

We can read about numerous successful attacks on well-known web applications on a weekly basis. Reason enough to study the background of "Web Application Security" of custom-made / self-developed applications - no matter if these are used only internally or with public access.

This book DOES NOT cover related topics like secure (network) infrastructures, operating system security, patch management, firewall architectures etc. but instead focuses only at the application level - the central field of activity of a software developer.

Web applications are a generic expression for

- Internet applications
- Intranet applications
- Cloud services
- Web portals
- Web services
- Web APIs

Some of these types of applications are not affected by certain attack patterns. For instance, a pure backend for a mobile app usually cannot be attacked through clickjacking - but (No)SQL code injections are extremely relevant.

Typical Attack Patterns

The most common / typical attacks against web applications are:

- [01] Code/Command Injection in general
    - e.g. e-mail, header injection
- [02] (No)SQL Code Injection
- [03] Cross-Site Request Forgery (CSRF)
- [04] Cross-Site Scripting (XSS)
    - i.a. JavaScript, HTML
- [05] Open Redirection
- [06] Remote File Inclusion (RFI) and Local File Inclusion (LFI) resp. Directory/Path Traversal
- [07] Clickjacking
- [08] Session-Hijacking
    - i.a. manipulation of transactions
- [09] Information Disclosure
- [10] Attacks on Weaknesses of the Authentification
    - password handling, hashing, reset, configuration
    - alternative authentication methods / multifactor