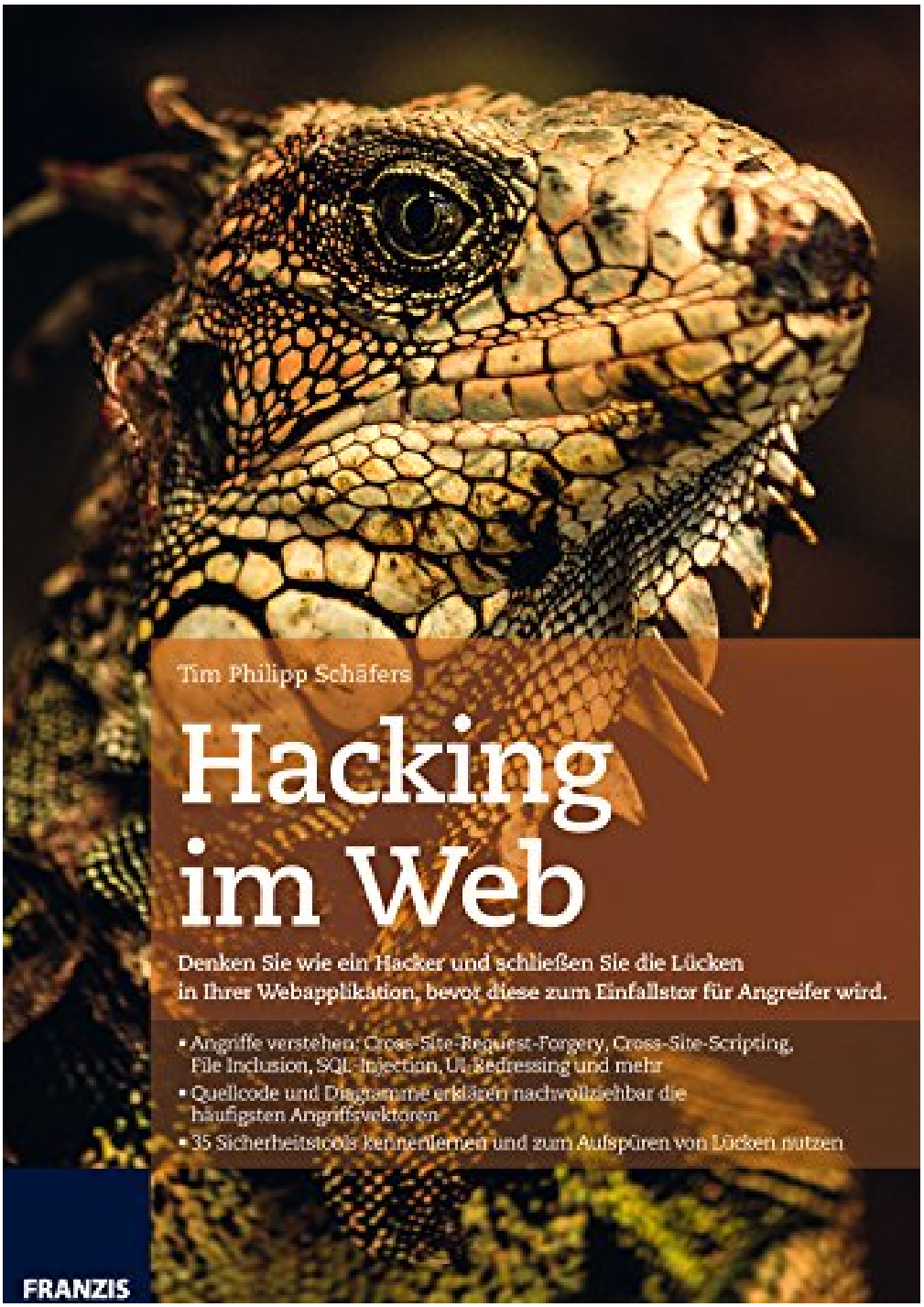
Hacking im Web: Cross-Site-Scripting, SQL Injections, File Inklusion, Header Injection, Cross-Site-Request-Forgery und Clickjacking: Schließen Sie die Lücken in Ihrer Webanwendung



Datum: 11. April 2016
Verlag: Franzis Verlag
Autor: Tim Philipp Schäfers
Seitenzahl: 504 Seiten
Sprache: Deutsch

PDF

Der Erfolg des E-Commerce hat auch seine Schattenseiten: Hackerangriffe im Web gehören inzwischen zum Alltag. Es geht dabei nicht nur um unsichere Firewalls oder Fehler in Betriebssystemen, häufig stellt die selbst programmierte Webapplikation das größte Einfallstor dar. Um sich vor Hackern zu schützen, ist es wichtig, wie ein Hacker zu denken. In diesem Buch lernen Sie die häufigsten Angriffsmethoden kennen und erhalten Tipps, wie Sie sich davor schützen können. Analysieren Sie Ihren Programmcode auf Schwachstellen und schließen Sie die Lücken direkt in der Implementierungsphase.

Die wichtigsten Angriffsvektoren

Browser, HTML, JavaScript, PHP, Java und SQL sind nur Beispiele für die bei einer Webanwendung eingesetzten Technologien. Meist werden sie in Kombination verwendet, sodass die potenziellen Schwachstellen unzählbar sind. Ob SQL-Injection, Cross-Site-Scripting oder Session-Hijacking: Lernen Sie die Funktionsweise dieser Angriffe kennen und schützen Sie sich mit den aufgeführten Tipps erfolgreich davor.

Werkzeuge kennen und nutzen

Entwickler sind keine Sicherheitsexperten und können nicht jede Schwachstelle der eingesetzten Programmiersprache und Bibliotheken kennen. Umso wichtiger ist es, die entstandene Webanwendung auf ihre Schwachpunkte zu testen. Schäfers stellt in einem ausführlichen Anhang zahlreiche Werkzeuge vor, mit denen Sie effektiv nach Schwachstellen suchen können.

Aus dem Inhalt:

- Basiswissen: HTTP, Cookies, URL, DOM, Browsersicherheit, Same-Origin-Policy und Codierung
- Session-Angriffe
- Cross-Site-Scripting
- Injections: Code, Cookie, HTTP-Header, LDAP, SMTP-Header, SQL und XPath
- Grundlagen von LDAP
- XPath
- Sicherheit von Authentifizierungsmechanismen
- Kryptografische Hashfunktionen
- Passwortcracking
- File Inclusion
- Zugriffsrechte
- Cookie-Manipulation
- Informationspreisgabe
- UI-Redressing
- Google-Bombing und -Dorking

• Exploits
• Hackertools

Übersichtliche Diagramme erläutern das Vorgehen bei einem Angriff.

Überall sind anfällige Webanwendungen in Betrieb, selbst in Biogasanlagen.

https://k2s.cc/file/904f498ae974c/GgFDuc1Yt.pdf.rar