



Sichere Programmierung von Web-Anwendungen

Applikationssicherheit verstehen

Inhaltsverzeichnis

Sichere Programmierung von Web-Anwendungen.....	1
Motivation: Angriffe auf Web-Anwendungen.....	4
Typische Angriffe.....	4
Ursachen.....	5
Hacking-Anatomie.....	5
Programmierfehler und (Web-)Anwendungssicherheit.....	7
Fehlerhafte Input-Validierung.....	8
Fehlerhaftes Output-Encoding.....	9
Generische Sicherheitsfunktionen.....	10
Sichere Programmierung:.....	10
Klassifizierte Angriffsformen und ihre Abwehr.....	11
[01] Code/Command Injection.....	11
Beschreibung.....	11
Vereinfachtes Codebeispiel mit Sicherheitslücke:.....	11
Sichere Programmierung:.....	11
[02] (No)SQL-Code-Injection.....	12
Beschreibung.....	12
Vereinfachtes Codebeispiel mit Sicherheitslücke:.....	12
Sichere Programmierung:.....	12
[03] Cross-Site-Request-Forgery (CSRF).....	13
Beschreibung.....	13
Beispiel mit Sicherheitslücke:.....	13
Sichere Programmierung:.....	14
[04] Cross-Site-Scripting (XSS).....	15
Beschreibung.....	15
Sichere Programmierung:.....	16
[05] Open-Redirection.....	16
Beschreibung.....	16
Beispiel mit Sicherheitslücke:.....	16
Sichere Programmierung:.....	17
[06] Remote File Inclusion (RFI) sowie Local File Inclusion (LFI) bzw. Directory/Path Traversal.....	18
Beschreibung.....	18
Beispiel mit Sicherheitslücke:.....	18
Sichere Programmierung:.....	19
[07] Clickjacking.....	19
Beschreibung.....	19
Sichere Programmierung:.....	20
[08] Session-Hijacking.....	21
Beschreibung.....	21
Sichere Programmierung:.....	21
[09] Information Disclosure.....	22

Beschreibung.....	23
Sichere Programmierung:.....	23
[10] Angriffe auf Schwachstellen der Authentifizierung.....	23
Beschreibung.....	23
Sichere Programmierung:.....	24
[11] Denial of Service.....	25
Beschreibung.....	25
Sichere Programmierung:.....	25
[12] Middleware.....	26
[13] Third-Party-Software.....	26
Abschließende Anmerkungen.....	27
Zusammenfassung.....	28
Weiterführende Informationsquellen.....	29
Rechtliche Hinweise.....	30

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