M183 Applikationssicherheit Implementieren # 18

By Jürg Nietlispach

Recap M183

1. Login / Authentifizierung (Idetification using Username, Password, API-Token)
    - Attacken:
        - (Stored, Reflected, DOM-Based)
        - UI-Redress via Phishing
    - Gegenmassnahmen
        - Two Factor Authentication
        - Single Sign On

2. Sessions (Persistente Authentifizierung mittels Digest Auth, HTTP-Cookies, Parameters)
    - Attacken:
        - Session-ID Theft (XSS) & Eavesdropping (Traffic)
        - ID-Guessing (Brute-Force)
        - Session Fixation
    - Gegenmassnahmen:
        - Use a CSRF-Token, Cookie-Flags

Recap M183

3. Authorization & Access Control (DAC, MAC, Role-Based, Hybrid, Permission Models)
    - Attacken:
        - Forceful Browsing
        - Parameter Tampering
        - Error Handling
    - Gegenmassnahmen:
        - Check Permissions at every Request
        - Use a CSRF-Token

4. Data Access (Databases, HTTP-Ressources)
    - Attacken:
        - SQL-Injection, XSS, File Enumeration, Directory Traversial, File Inclusion
    - Gegenmassnahmen
        - Prepared Statements, Filtering, Whitelisting

Recap M183

5. Data Integrity (Data in Transit & Data at Rest)
    - Attacken
        - Data Theft
    - Gegenmassnahmen
        - Encryption (Symmetric, Asymmetric),
        - Hasing

6. Intrusion Detection (Logging & Audit Trails)
    - Attacken
        - Invstigation of possible Security holes
    - Gegenmassnahmen
        - Logging & Auswertung von applikationsfremden Verhalten

Recap M183

Principles for Building secure Applications (**and other Systems**)

- Security Principles (Prevent Security by obscurity etc.)
- 3x3 Matrix
- Attacks are possible on every OSI Layer!
- …

How the situation looks today?

37%	Cross-site scripting
16%	SQL injection
5%	Path disclosure
5%	Denial-of-service attack
4%	Arbitrary code execution
4%	Memory corruption
4%	Cross-site request forgery
3%	Data breach (information disclosure)
3%	Arbitrary file inclusion
2%	Local file inclusion
1%	Remote file inclusion
1%	Buffer overflow
15%	Other, including code injection (PHP/JavaScript), etc.

How the situation looks today?

Nearly Weekly information about new security leaks

- Spectre, Meltdown
- Creditcard-Information stolen
- Heartbleed (SSL)
- …

Challenges

- Blockchains
- Quantum-Computers which are able to solve Encryption Algorithms fast
- IoT
- Quantum Cryptography
- …

Lab

Feedback of the M183-Module (20’)

Finish the Paper von Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf

Have a look to https://www.udemy.com/the-bitcoin-course/

Search for Quantum Cryptography Informations