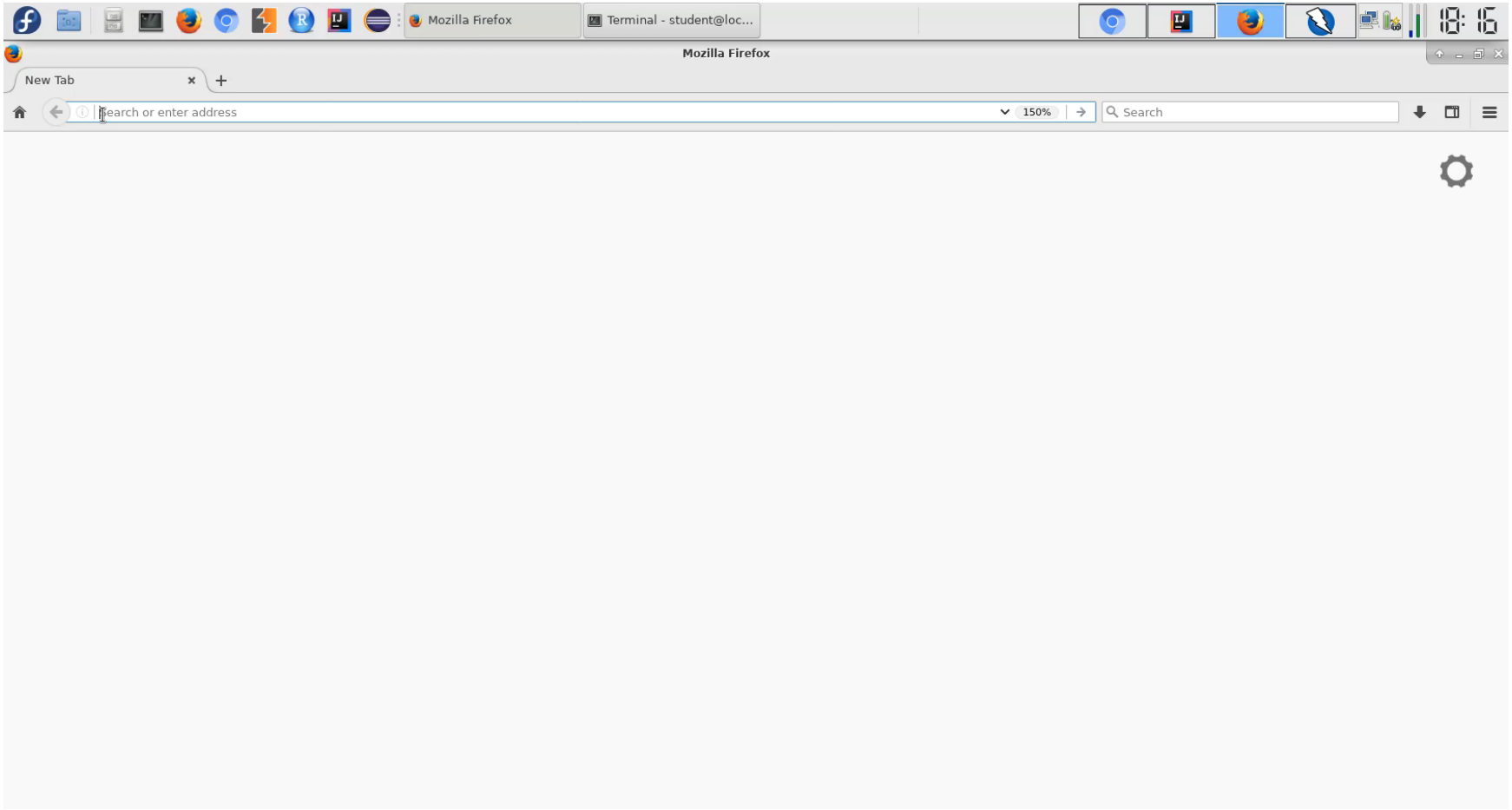
Warum ist Software nicht sicher?
I4.0 Round Table

Egon Teiniker
Software Design, IT & Mobile Security
FH JOANNEUM

22.3.2018

Warum ist Software nicht sicher?



Warum ist Software nicht sicher?

Unsichere Lösung

```
public List<User> findByUsername(String name)
{
    final String SQL = "SELECT * FROM user WHERE username='" + name + "'";

    PreparedStatement pstmt = null;
    ResultSet rs = null;
    List<User> users = new ArrayList<~>();

    try
    {
        pstmt = getConnection().prepareStatement(SQL);
        rs = pstmt.executeQuery();
```

Warum ist Software nicht sicher?

Sichere Lösung

```
public List<User> findByUsername(String name)
{
    final String SQL = "SELECT * FROM user WHERE username=?";

    PreparedStatement pstmt = null;
    ResultSet rs = null;
    List<User> users = new ArrayList<~>();

    try
    {
        pstmt = getConnection().prepareStatement(SQL);
        pstmt.setString( parameterIndex: 1, name);
        rs = pstmt.executeQuery();
```

Warum ist Software nicht sicher?

Unsichere Lösung

```
public List<User> findByUsername(String name)
{
    final String SQL = "SELECT * FROM user WHERE username='" + name + "'";

    PreparedStatement pstmt = null;
    ResultSet rs = null;
    List<User> users = new ArrayList<~>();

    try
    {
        pstmt = getConnection().prepareStatement(SQL);
        rs = pstmt.executeQuery();
```

Warum ist Software nicht sicher?

Sichere Lösung

```
public List<User> findByUsername(String name)
{
    final String SQL = "SELECT * FROM user WHERE username=?";

    PreparedStatement pstmt = null;
    ResultSet rs = null;
    List<User> users = new ArrayList<~>();

    try
    {
        pstmt = getConnection().prepareStatement(SQL);
        pstmt.setString( parameterIndex: 1, name);
        rs = pstmt.executeQuery();
```

Warum ist Software nicht sicher?

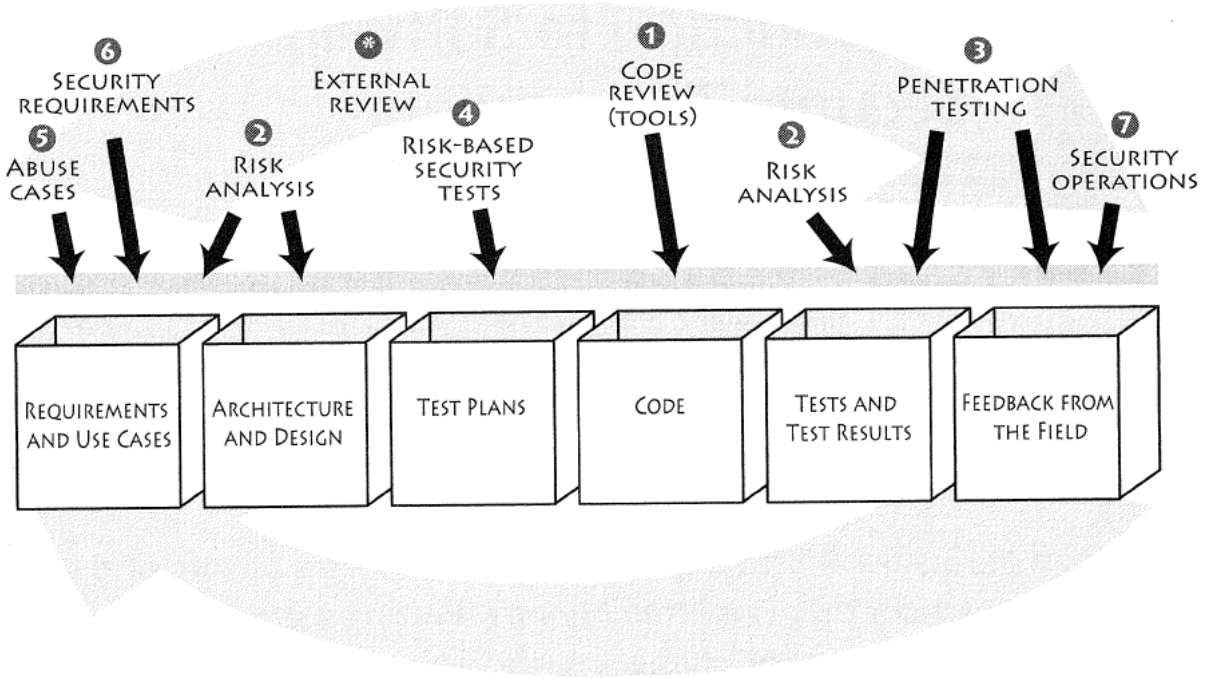
Bekannte Probleme

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Quelle: https://www.owasp.org/index.php/Top_10-2017_Top_10

Warum ist Software nicht sicher?

Software Security in der Ausbildung



Quelle: Gary McGraw (2006). Software Security. Addison-Wesley

Warum ist Software nicht sicher?

Software Security in I4.0 & IoT

- Critical functionality
- Replication
- Security assumptions
- Not easily patched
- Long life cycle
- Proprietary/industry specific protocols
- Deployed outside of enterprise security perimeter

Quelle: http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things