Pentests – more than just using the proper tools

TÜVRheinland®
Precisely Right.

Agenda

1. **Information Security @ TÜV Rheinland**
2. **Security testing**
3. **Penetration testing**
   - **Introduction**
   - **Evaluation scheme**
   - **Security Analyses of web applications**
   - **Internal Security Analyses (optional)**

Information security @TÜV Rheinland.

- **Providing information security services worldwide (Europe, North America, Asia, Middle East)**
- **Germany‘s leading vendor independent service provider for information security**
- **Over 500 security experts worldwide – 150 in Germany and growing**
- **For the 7th time:**

top ARBEITGEBER DEUTSCHLAND 2014
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

TÜVRheinland®
Precisely Right.

Agenda

1. **Information Security @ TÜV Rheinland**
2. **Security testing**
3. **Penetration testing**
   - **Introduction**
   - **Evaluation scheme**
   - **Security Analyses of web applications**
   - **Internal Security Analyses (optional)**

Security Testing. Goals.

Software testing

“ … an investigation conducted to provide stakeholders with information about the quality of the product or service under test.” (Wikipedia)

Goals of security testing

- Detection of security vulnerabilites
- Demonstrate vulnerability of systems
- Identify the potential damage caused by real attacks
- Identification of remedial measures

➔ Increase overall security level

Variations

- Black Box
- White Box
- any other color in between
- Vulnerability scans

Security Tests. Targets.

Evaluation Targets

- Applications
  - Web
  - Client-Server
  - Mainframe
  - Mobile
- Infrastructure
  - Server
  - DMZ
  - Intranet
- Special purpose hardware
- Processes and organizations

Agenda

1. **Information Security @ TÜV Rheinland**
2. **Security testing**
3. **Penetration testing**
   - **Introduction**
   - **Evaluation scheme**
   - **Security Analyses of web applications**
   - **Internal Security Analyses (optional)**

Penetration Tests. Definition. Pros and Cons.

Definition

"… an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data." (Wikipedia)

Pros

+ Verification of the security of complex systems including multiple security layers
+ Dynamical testing including tester's creativity, e.g. combination of low impact vulnerabilities
+ Using up-to-date attack vectors
+ Verify attack detection

Cons

– Security Snap-shot - Results valid for a limited time
– Quality of results depend upon tester's quality
– Very high complexity of finding previously unknown vulnerabilities

➔ Penetration testing is one important mechanism for security quality assurance

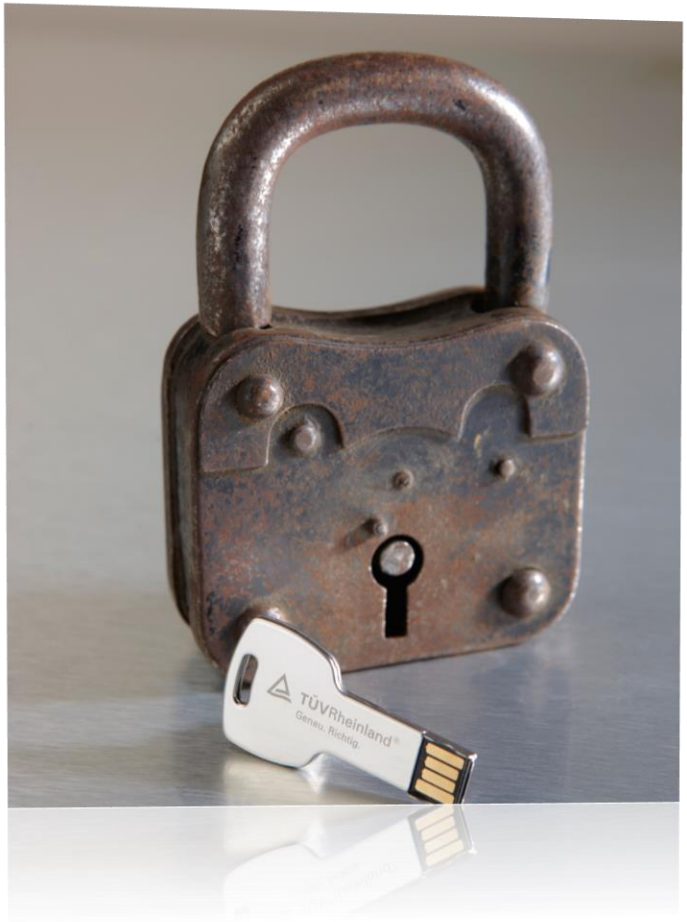
Penetration Test. Workflow.

1. **Kick-Off / Preparation**
2. **Information gathering and -analysis (manually and automated)**
   - Online search engines
   - Scanning Tools (port-, vulnerability-scanner, etc.)
3. **Information evaluation / risk analysis**
   - Based on results of phase 1 and information of phase 2
   - Identification of vulnerabilities
4. **Active Intrusion**
   - Exploitation of vulnerabilities (mostly manually)
   - Use of exploit code
5. **Finalization**
   - Result evaluation
   - Report generation

Agenda

1. **Information Security @ TÜV Rheinland**
2. **Security testing**
3. **Penetration testing**
   - **Introduction**
   - **Evaluation scheme**
   - **Security Analyses of web applications**
   - **Internal Security Analyses (optional)**

DREAD Risk assessment model



DREAD risk evaluation model

Damage - how bad would an attack be?

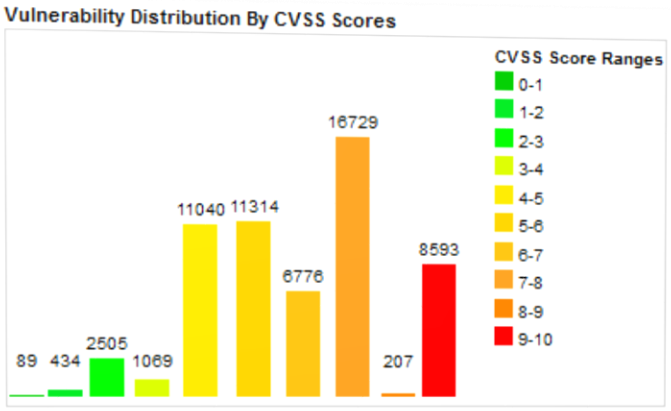
Reproducibility - how easy is it to reproduce the attack?

Exploitability - how much work is it to launch the attack?

Affected users - how many people will be impacted?

Discoverability - how easy is it to discover the threat?

Common Vulnerability Scoring System (CVSS)



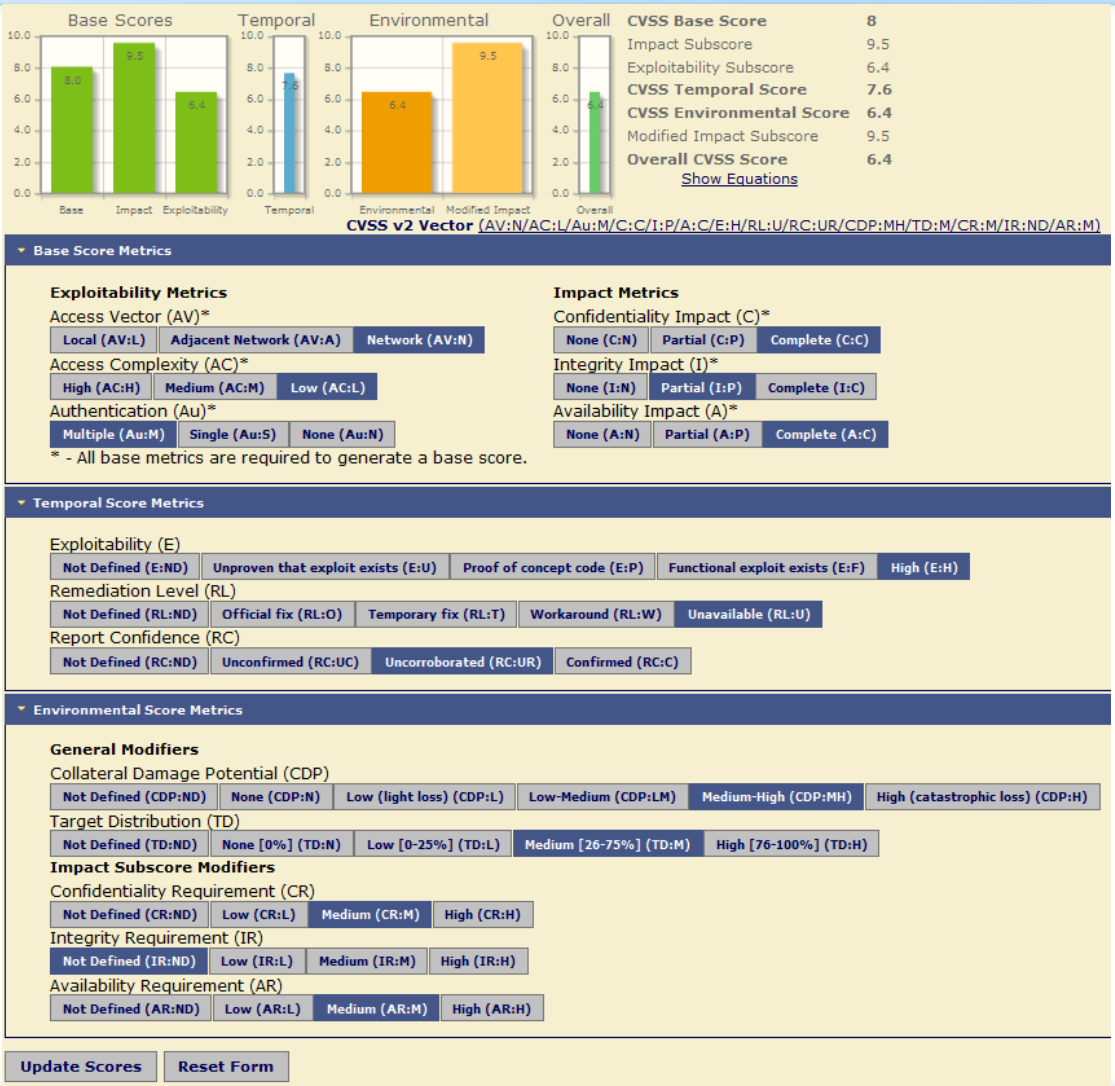
Common Vulnerability Scoring System (CVSS)

- Common standard
- Description of vulnerability‘s severity
- Evaluation based on „Metrics“
  - Base (Access Vector, Access Complexity, Authentication, Confidentiality, Integrity, Availability)
  - Environmental (Confidentiality Requirement, Integrity Requirement, Availability Requirement, Collateral Damage Potential, Target Distribution)
  - Temporal (Exploitability, Remediation Level, Report Confidence)
- Allows to compare vulnerabilities

CVSS-calculator:

http://nvd.nist.gov/cvss.cfm?calculator&version=2

Common Vulnerability Scoring System (CVSS)



Generic evaluation and risk classification.

Risk classification is performed from an IT security perspective in relation to infrastructure, systems, services and processes in the area of observation

→ Risk Rating for the business processes is done by the internal risk management of our customer.

Recommendation	Suggestions to improve the overall security situation, though a concrete threat is not present. Includes i.e. out-of-scope-observations.	
Low Risk	The implemented security mechanisms to ensure • confidentiality and integrity of sensible data • availability of necessary systems has a **minor deficit**.	
Medium Risk	The implemented security mechanisms to ensure • confidentiality and integrity of sensible data • availability of necessary systems has a **deficit**.	
High Risk	The implemented security mechanisms to ensure • confidentiality and integrity of sensible data • availability of necessary systems has a **severe deficit**.	

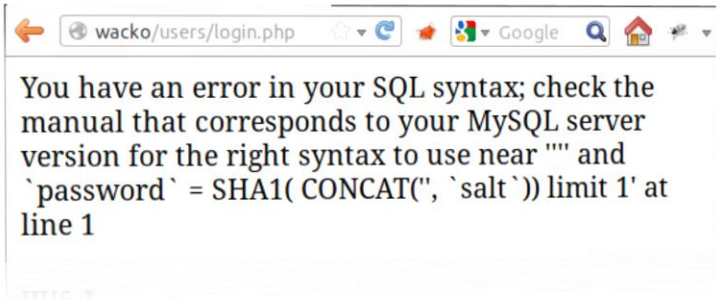
Agenda

1. **Information Security @ TÜV Rheinland**
2. **Security testing**
3. **Penetration testing**
   - **Introduction**
   - **Evaluation scheme**
   - **Security Analyses of web applications**
   - **Internal Security Analyses (optional)**

Open Web Application Security Project (OWASP) – Top 10

1. Injection
2. Cross Site Scripting
3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross Site Request Forgery
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Top 1. Injection.



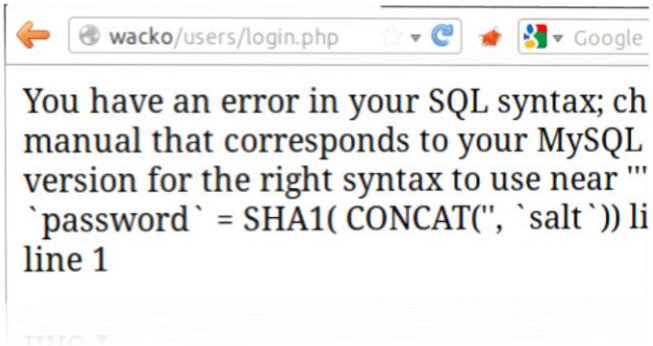
1. **Injection**
2. Cross Site Scripting
3. Broken Authentication and Session Management
4. Insecure Direct Object References
5. Cross Site Request Forgery
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

Injections. Basics.

Fundamental Trouble

- Input is not completely validated
- Data provided by the user is interpreted:
  - Data base (SQL-Injection)
  - Operation system calls (Command Injection)
  - XML-Tags and Entities (XML Injection)
  - Scriptcode (i.e. Ruby, PHP) gets executed (Code-Injection)

SQL-Injection. Description.



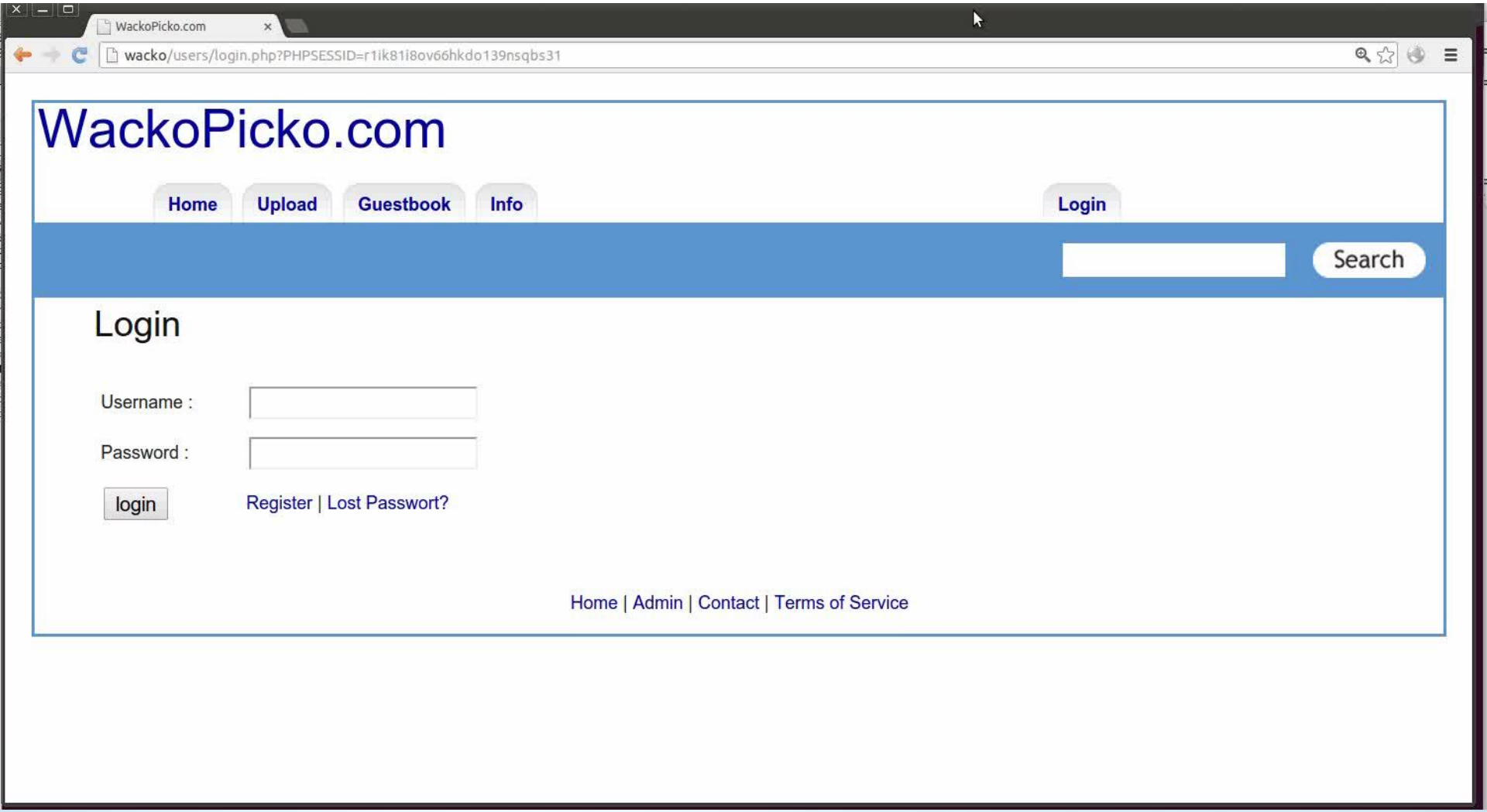
Issue

- Data provided by the user is not validated completely
- User can execute SQL queries

Consequences

- An Attacker can execute almost arbitrary SQL queries
  - Login without password
- Attacker can extract data from the database

SQL-Injection. Demo.



Thank you for your attention and questions!

Dr. Daniel Hamburg
Head of Security Engineering

T: +49 221 56783 220
E-Mail: daniel.hamburg@i-sec.tuv.com