



Von der Idee zum Erfolg.

# ANECON Präsentation

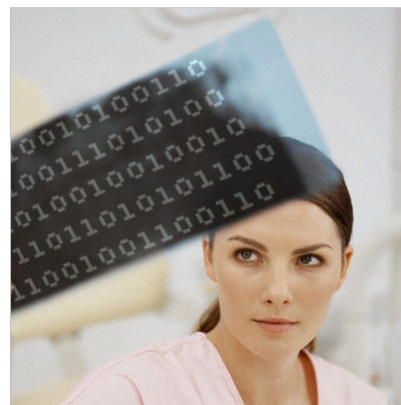
## Securitychecks im Softwaretest

Michael Lausch

© ANECON Software Design und Beratung G.m.b.H. | Alser Str. 4/Hof 1 | A-1090 Wien | Tel.: +43 1 409 58 90 | www.anecon.com | office@anecon.com

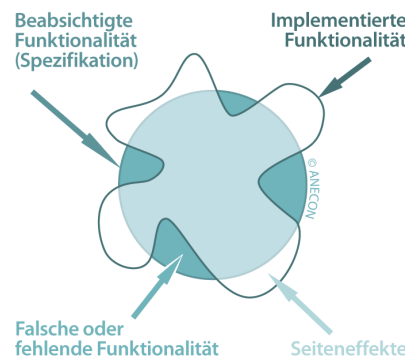
## Securitytests im Softwaretest

- Was testen Securitytests
- Die “Top Zwei” der Bedrohungsszenarien
- Einfaches Screening von Webapplikationen



## Was testen Securitytests

- Häufige Ursachen von Sicherheitsproblemen sind Seiteneffekte der Software
- Seiteneffekte sind nicht beabsichtigte Funktionen in der Software



3 | Securitytests im Softwaretest



## Die "Top 2" der Bedrohungen

- Cross Site Scripting
  - Gegen einen Benutzer der Applikation gerichtet
  - Wenn dieser Benutzer Administrationsrechte hat, kann auch die Applikation direkt betroffen sein.
- Injection Attacken
  - Direkt gegen die Applikation gerichtet
- Beide dienen als Basis für weiterführende Angriffe

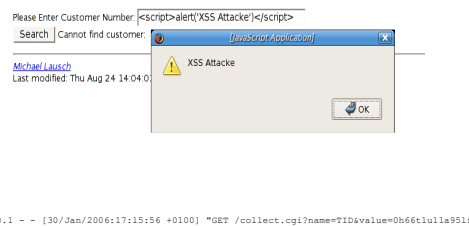
4 | Securitytests im Softwaretest



## Cross Site Scripting

- Ausführen von Code im Browser
- Angreifer kann Javascript im Browser des Opfers ausführen
- Cookie Diebstahl
- Netzwerk Scans

### XSS Attack



## Schnelltest für XSS Attacken

- Eingabe von Testwerten in Eingabefelder
- Prüfung der Anzeige dieser Testwerte
  - Werden sie angezeigt?
  - Wie werden sie angezeigt
- Eingabe von "<PLAINTEXT>" ändert das Layout
- Bei der Eingabe von ";!--"<XSS>=&{()}" wird "<XSS>" angezeigt (oder ist im HTML Source der Seite vorhanden)

## Injection Attacken

---

- Richten sich gegen die Applikation selbst
  - Ändern die Datenbestände der Applikation
  - Erlauben Zugriff auf geschützte Daten
- SQL Injection
  - Der Angreifer kann fast beliebiges SQL ausführen.
- LDAP Injection
  - Authentication wird unwirksam
- XML Injection
  - AJAX Requests können verfälscht werden

## SQL Attacken

---

- SQL Statements werden erst zur Laufzeit erzeugt
- Beispiel
  - `'SELECT * FROM users WHERE username='' + $username + ''';`
  - `SELECT * FROM users WHERE username="musteruser"`
  - `$username="' OR 1 OR username="'`
  - `SELECT * FROM users WHERE username="" OR 1 OR username=""`

## Test auf SQL Injection Attacken

---

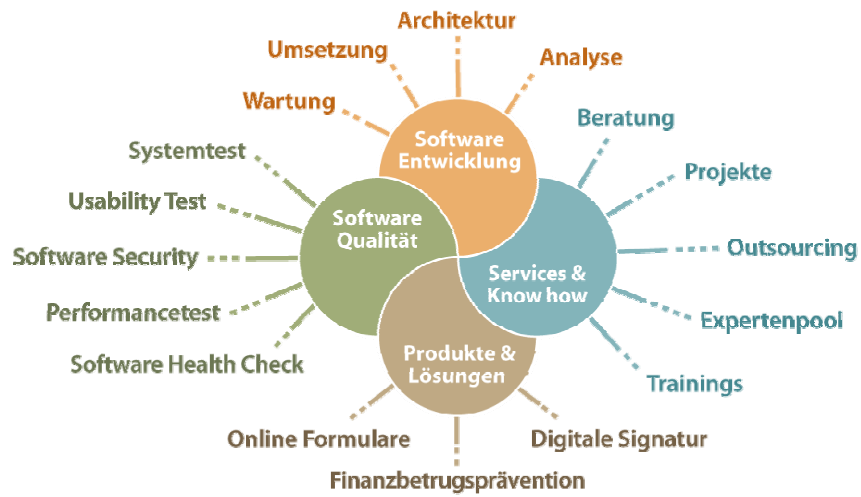
- Eingabe von " OR 1 OR "x" = "x"
- Test des Ergebnisses
  - Fehlermeldung die auf SQL Syntax Errors hinweisen
  - Anzeigen von Daten die nicht erwartet werden
  - Server Error (500 Internal Server Error)
- Alles ausser Fehlermeldungen die sich auf ungültigen Eingaben beziehen sind relevant

## Wir sind der richtige Partner...

---

- ...wenn Ihnen beim beim Testen ein Security Problem aufgefallen ist,
- oder wenn sie vermehrt auch komplexere Tests durchführen wollen,
- denn gut getestet ist halb gewonnen!

# ANECON Software Design und Beratung G.m.b.H.



11 | Securitytests im Softwaretest



Software  
ist unsere  
Leidenschaft

