# Hacking Day 2011

## Application Security Audit in Theorie und Praxis

Jan Alsenz & Robert Schneider





oneconsult®
IT Security & Strategic Consulting

# Agenda

- → Vorstellung
- → Application Security Audit
- → Optimaler Zeitpunkt
- → Testansatz
- → Schlussbericht
- → Live Demo
- → Fragen

# Vorstellung

# Referenten


Jan Alsenz
MSc ETH CS, OPST & OPSA
Team Leader Security Audits

jan.alsenz@oneconsult.com
+41 79 377 15 15



Robert Schneider
BSc FH CS, OPST
Security Consultant

robert.schneider@oneconsult.com
+41 79 269 29 29

# Unternehmen

## → OneConsult GmbH

- Gründung 2003
- IT Security Consulting & strategische Beratung
- Kein Verkauf von Hard- und Software
- 11 Mitarbeitende, wovon 9 Consultants
- Christoph Baumgartner, CEO & Inhaber
- Jan Alsenz, Teamleiter Security Audits & Teilhaber
- Dr. Cathrin Senn, Senior Consultant & Teilhaberin

## → Standorte

- Schweiz: Hauptsitz in Thalwil
- Österreich: Niederlassung in Wien

# Dienstleistungen

## → Security Audits

- Security Scan
- Penetration Test
- Application Security Audit
- Ethical Hacking
- Conceptual Security Audit

## → Consulting

- Strategy & Organisation
- Policies & Guidelines
- Processes & Documentation
- Business Continuity & Disaster Recovery
- Engineering & Project Management

## → Incident Response

- Emergency Response
- Computer Forensics

## → Training & Coaching

- OSSTMM Zertifizierungskurse
- Security Awareness Training
- Coaching

## → Security as a Service





oneconsult®
IT Security & Strategic Consulting

# Application Security Audit

# Definition

Gründliche, technische, unprivilegierte und privilegierte Sicherheitsüberprüfung einer Applikation und der zugehörigen Systeme aus der Perspektive eines Angreifers mit Skill Level «Hacker / Cracker».

# Berücksichtigt beispielsweise

- → Architektur
- → Infrastruktur
  - Vertrauensstellungen
  - Authentisierungs-mechanismen
- → Implementation
- → Source Code
- → Compliance
- → Verantwortlichkeiten
- → User Management
- → Dokumentationspflege
- → Umgang mit Source Code
- → Patching-Prozess

# Stichwörter

→ Applikationen
- Online-Shops
- Interbanking-Portale
- Mailserver
- Datenbanken
- Branchenlösungen
- Mobile Apps
- Etc.

→ Ansätze
- Client und Server
- Dediziert vs. virtualisiert (Cloud)
- Mobile Client
- Web Application vs. Web Service
- Etc.

→ Environment
- Betriebssystem
- Programmiersprache
- Framework
- Etc.

# Zweck und Nutzen

- → Qualitätssicherung dank (unabhängiger) IT Security-Analyse
- → Compliance: Nachweis bezüglich gesetzlicher Rahmenbedingungen und Vorgaben
- → Prävention: Ermöglicht (in der Zukunft) direkte und indirekte Kosteneinsparungen

# Zweck und Nutzen

- → Awareness auf allen Stufen
- → Know-how Transfer
- → Argumentationsgrundlage für zukünftige
  - IT Security-Investitionen
  - Aktivitäten

# Knackpunkte

- → Fach- und Sozialkompetenz der Tester und der am Projekt beteiligten Mitarbeiter
- → Vergleichbarkeit und Nachvollziehbarkeit von
  - Offerten
  - Vorgehen
  - Resultaten und Dokumentationen
- → Compliance zu Gesetzen, Standards und Vorgaben erwünscht, aber:
  - Nur rudimentäre Behandlung von technischen Audits in Standards (z.B. ISO/IEC 2700x)
  - Keine offiziellen Checklisten oder Guidelines verfügbar

# Optimaler Zeitpunkt

# Typische Szenarien

→ Neuentwicklung

→ Neuer Release

→ Bestehende Lösung

# Typische Zeitpunkte

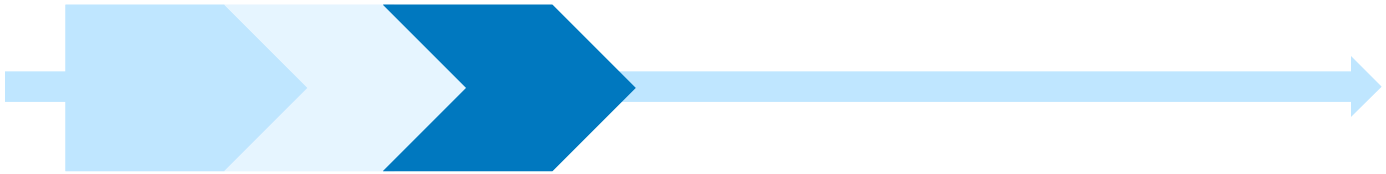
# Typische Zeitpunkte

→ Frühe Entwicklung: Eher Konzept-Review

# Typische Zeitpunkte

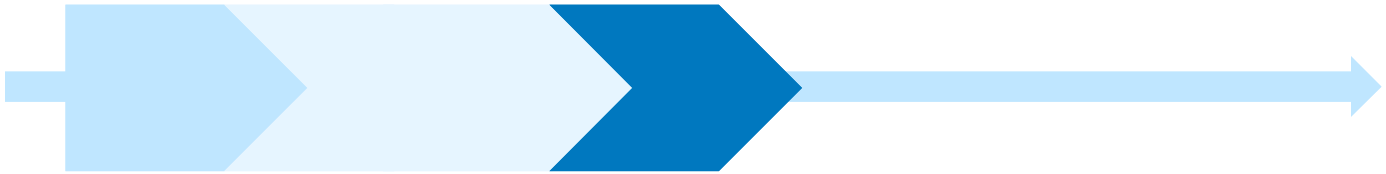
→ Frühe Entwicklung: Eher Konzept-Review

→ In der Entwicklung: Eher Code-Review



# Typische Zeitpunkte

- → Frühe Entwicklung: Eher Konzept-Review
- → In der Entwicklung: Eher Code-Review
- → Gegen Ende der Entwicklung:
  - Häufig noch nicht alles fertig oder nicht funktionierend (-)
  - Nicht finales Umfeld (-)



# Typische Zeitpunkte

- → Frühe Entwicklung: Eher Konzept-Review
- → In der Entwicklung: Eher Code-Review
- → Gegen Ende der Entwicklung:
  - Häufig noch nicht alles fertig oder nicht funktionierend (-)
  - Nicht finales Umfeld (-)
- → In der Test-Phase:
  - Nicht finales Umfeld (-)
  - Teilweise noch nicht alles fertig / komplett funktionierend (-)

# Typische Zeitpunkte

→ In Produktiv-Umgebung vor Go-Live: optimal

- Funktion komplett (+)
- In Zielumgebung (+)
- Noch nicht produktiv (+)
- Meistens dedizierte Testingzeit nötig (-)

# Typische Zeitpunkte

→ In Produktiv-Umgebung vor Go-Live: optimal

- Funktion komplett (+)
- In Zielumgebung (+)
- Noch nicht produktiv (+)
- Meistens dedizierte Testingzeit nötig (-)

→ Live:

- Funktion komplett (+)
- In Zielumgebung (+)
- Produktiv (evtl. Ausfälle) (-)


# Testansatz


# Typische Phasen

- → Offerte
- → Kick-off
- → Audit
- → Report (Diskussion/Präsentation)


# Typische Stolpersteine

→ Offerte
- Kein Geld/Budget eingeplant
- Offerte zu früh: genauer Scope noch nicht bekannt
- Offerte zu spät: zu wenig Zeit vor Go-Live

→ Kick-off
- Parteien kommunizieren auf unterschiedlichen Ebenen
- Zu viele/falsche Personen sind anwesend
- Änderung des Scopes

→ Audit
- Verschiebungen
- Applikation/Umgebung noch nicht fertig
- Kundenseitige Vorbereitungen nicht abgeschlossen


# OneConsult Testansatz

Mischung aus zwei bekannten und verbreiteten Methoden

→ OSSTMM

→ OWASP


# OSSTMM

- **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual
- Entwicklung unter der Leitung von ISECOM,
  **I**nstitute for **SEC**urity and **O**pen **M**ethodologies,
  http://www.osstmm.org
- Erstausgabe 2001, aktueller offizieller Release OSSTMM 3.0
- Offene und frei verfügbare Methode zur
  - Planung
  - Durchführung
  - Grobdokumentation

  von (technischen) Security Audits


# OSSTMM

- Sicherheitsniveau als neutraler Zahlenwert (Risk Assessment Value)
- Umfassender Verhaltenskodex (Rules of Engagement)
- Compliant zu ISO/IEC 17799/27001, ITIL, BSI-Standard-100-1/4, SOX, Basel II etc.
- Optionale Zertifizierung (Projekte, Personen und Organisationen) durch ISECOM
- OneConsult
  - ISECOM Licensed Auditor (Platinum Level)
  - ISECOM Partner (akkreditierter Schulungsanbieter)
  - Aktive Mitarbeit am OSSTMM: 3 Mitarbeiter im ISECOM Core Team
  - Mehr als 300 Projekte nach OSSTMM seit 2003


# Open Web Application Security Project (OWASP)

Idee

→ Unternehmen können mit Hilfe von OWASP-Bordmitteln Applikationen

- Entwickeln
- Beschaffen und
- Pflegen

OWASP
The Open Web Application Security Project

Ziel

→ Mehr Sicherheit in Applikationen





oneconsult®
IT Security & Strategic Consulting


# Open Web Application Security Project (OWASP)

Gratis und offen für jeden, der den Sicherheitsaspekt von Applikationen verbessern möchte.

→ OWASP Top 10
→ Tools
→ Dokumente
→ Foren
→ Teilnahme an Meetings der Ortsverbände

OWASP
The Open Web Application Security Project

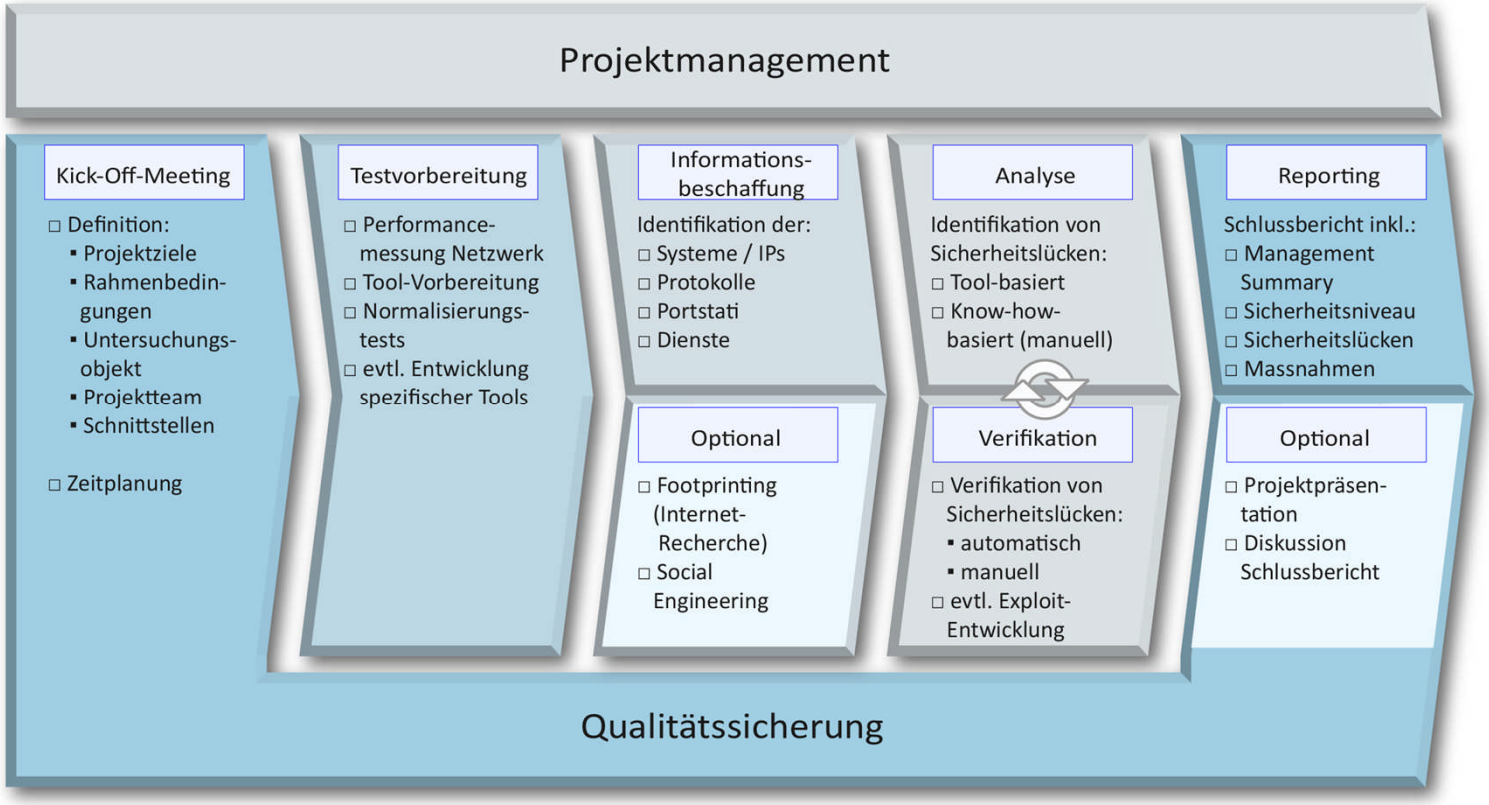
http://www.owasp.org





oneconsult®
IT Security & Strategic Consulting


# Generischer Ablauf Application Security Audit








oneconsult®
IT Security & Strategic Consulting

# Schlussbericht

# Schlussbericht

Die Dokumentation sollte mindestens die folgenden Punkte beinhalten:

- → Kurze und prägnante Zusammenfassung (Management Summary)
- → Liste mit den detektierten Risiken (inkl. Kategorisierung)
- → Massnahmen und Empfehlungen (inkl. Priorisierung)

# Live Demo

# Live Demo

Live-Vorstellung der Beispiel-Applikation

Credits

→ Für die Live Demo wird Hacme Bank v2.0 von McAfee (Foundstone) verwendet.

http://www.mcafee.com/

# Typische Schwachstellen

→ Typische Schwachstellen-Liste:

- Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects und Forwards

# SQL Injection

→ Bedeutung
- Applikation wird so angesprochen, dass diese (vom Betreiber nicht gewünschte) Kommandos an die Datenbank weiterleitet.

→ Datenbank
- Führt die eingeschleusten Kommandos aus

→ Impact
- Auslesen und unter Umständen Modifikation der gesamten Datenbank
- Voller Datenbank-Schema-, Account- oder sogar OS-Level-Zugriff

# SQL Injection

Inputfeld

Submit

```
ID:
First name:
Surname:
```

1

```
$id = $_GET['id'];
$querry = "SELECT name FROM users WHERE id = '$id'";
```

Webserver

2

Submit

```
ID: ' union all select table_name
First name: CHARACTER_SETS
Surname: -

ID: ' union all select table_name
First name: COLLATIONS
Surname: -

ID: ' union all select table_name
First name: COLLATION_CHARACTER_SI
Surname: -

ID: ' union all select table_name
First name: COLUMNS
Surname: -
```

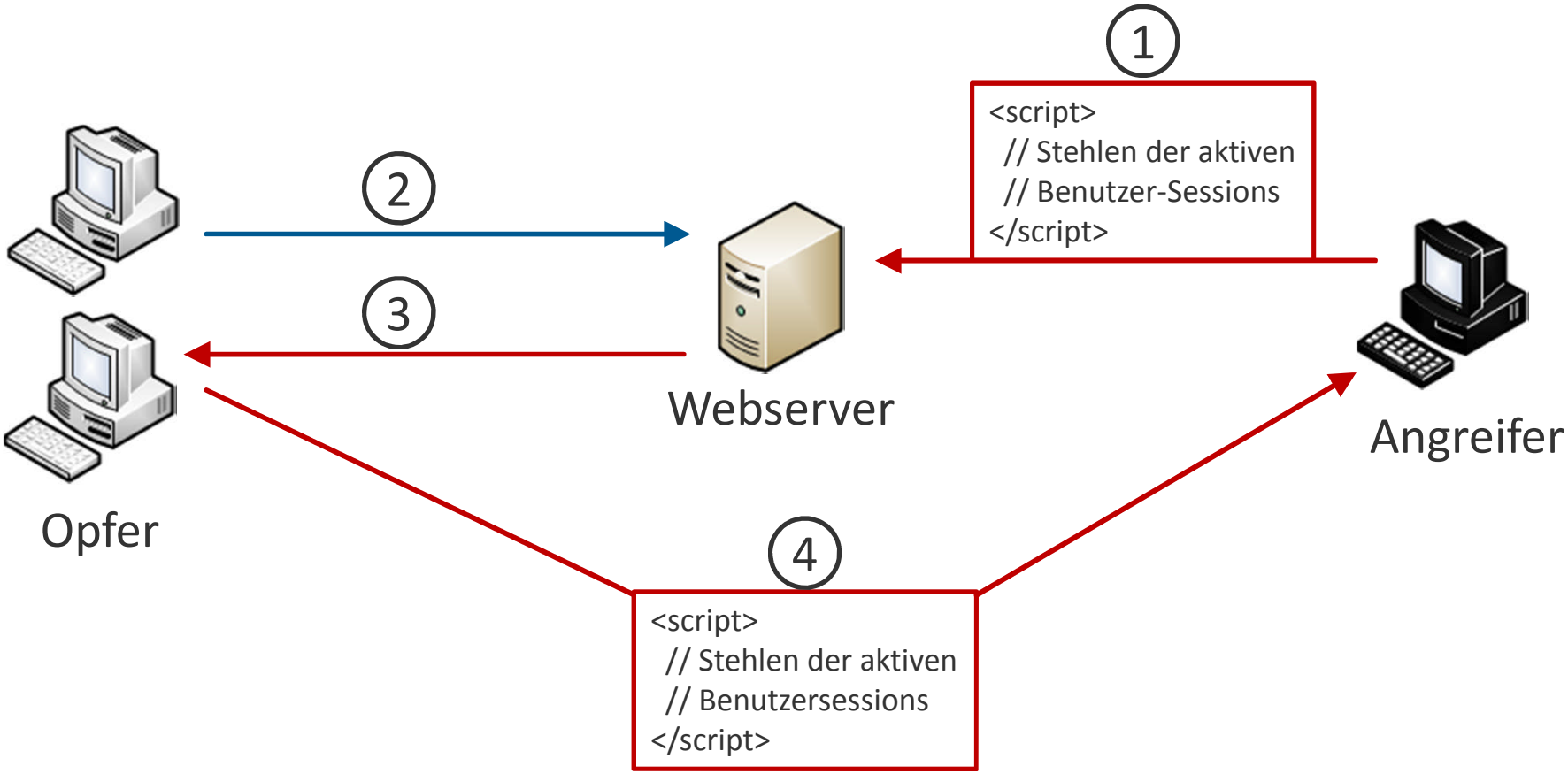
# SQL Injection: Abhilfe

- → Verwendung einer Schnittstelle welche Bind-Variablen unterstützt (Prepared Statements, Stored Procedures)
- → Encoding der Benutzereingaben vor Übergabe an Datenbank
- → Inputvalidation anhand einer „White List“
- → Minimalberechtigungen für Datenbankuser

# Cross Site Scripting (XSS)

- → Bedeutung
  - Rohdaten eines Angreifers werden an den Browser eines Users gesendet
- → Rohdaten
  - In Datenbank abgespeichert: Stored XSS
  - Von Web-Input reflektiert: Reflected XSS
    - › Formularfeld, verstecktes Feld, URL, etc.
- → Impact
  - Stehlen von
    - › Aktiven Benutzer-Sessions
    - › Sensitiven Daten
    - › Benutzer-Zugangsdaten (Phishing)
  - Umschreiben der Webseite (Defacement)
  - Installation eines XSS-Proxys
    - › Monitoring und Steuerung des Benutzerverhaltens
    - › Umleiten auf andere Seiten

# Cross Site Scripting (XSS)








oneconsult®
IT Security & Strategic Consulting

# Cross Site Scripting (XSS): Abhilfe

→ Unterbinden der Schwachstelle
- Keine vom Benutzer gelieferten Eingaben in Seiten einbinden

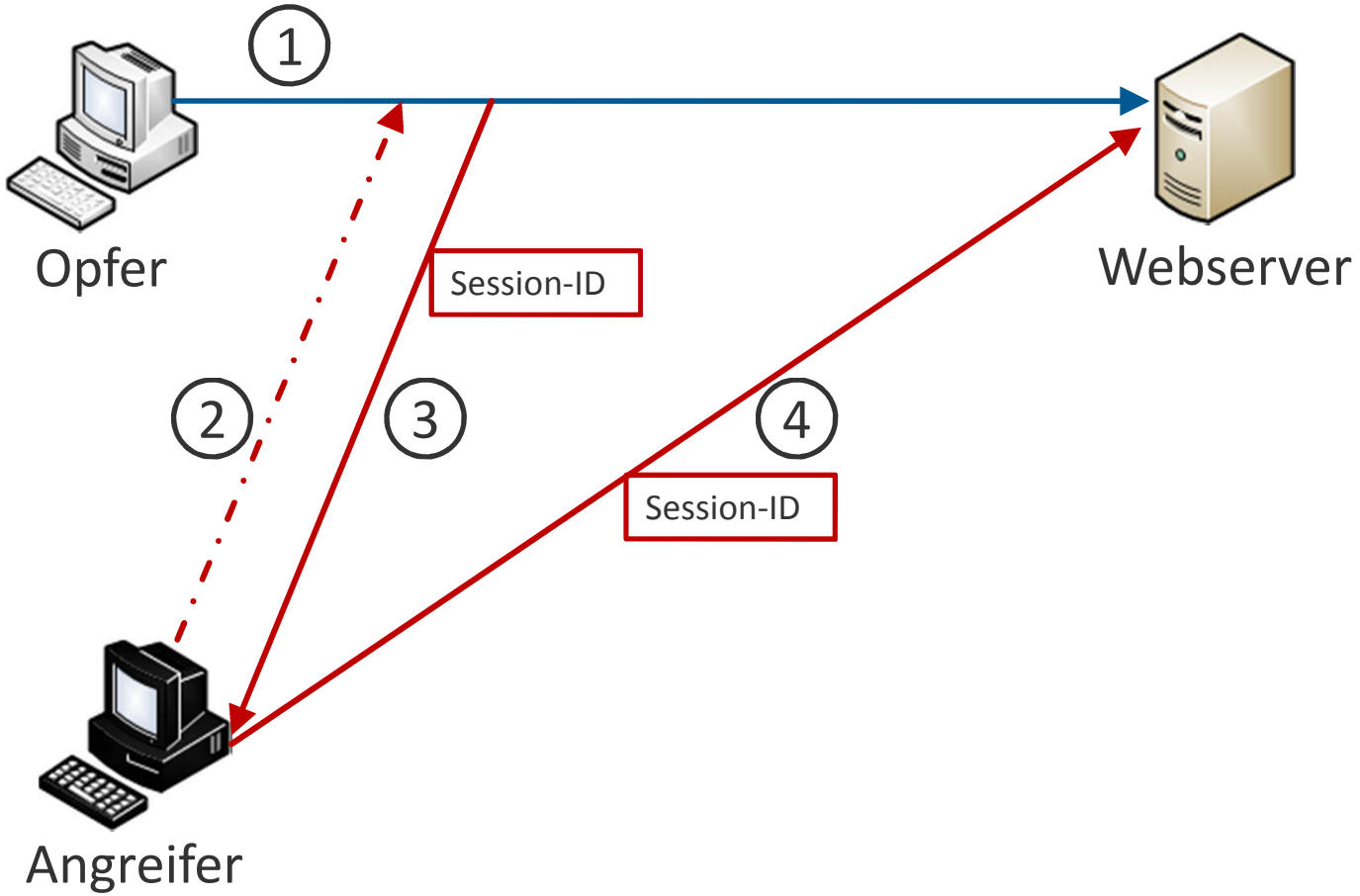
→ Schutzmassnahmen
- Output Encoding
  - › Benutzereingaben werden vor der Ausgabe encodiert
- Inputvalidation
  - › Benutzereingaben werden mittels „White List“-Ansatz validiert

# Session-Handling

→ Bedeutung
- Session-IDs ermöglichen es aus dem ansonsten statuslosen HTTP, statusorientierte Anfragen zu versenden
- Session-IDs können oft an den folgenden Stellen ausgelesen werden:
  - Netzwerke (WLAN)
  - Browser (Cookie)
  - Logs
  - Etc.

→ Impact
- Session Hijacking
  - Angreifer gelangt an gültige Session-ID
  - Im Kontext des betroffen Benutzers agieren

# Session-Handling



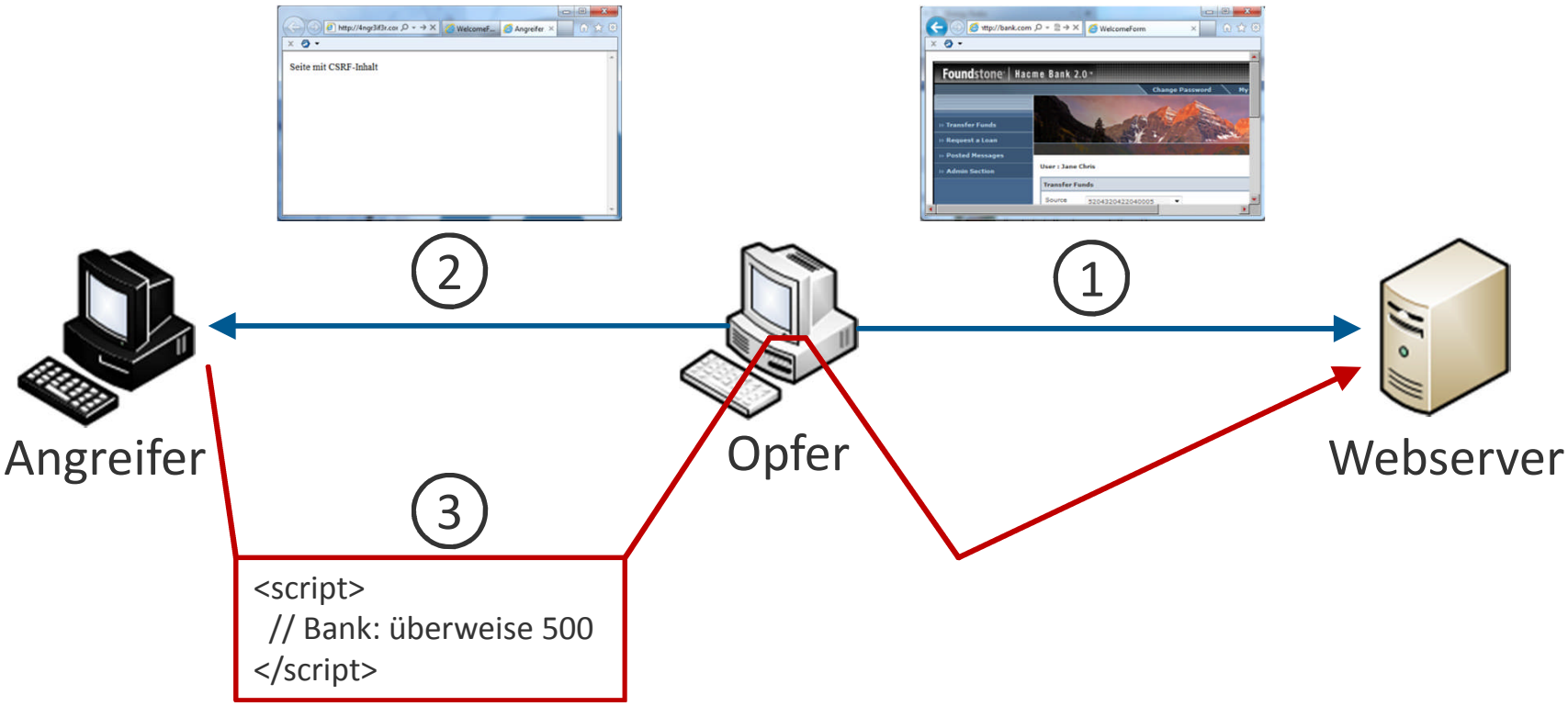
# Session-Handling: Abhilfe

- → Session-IDs sollten immer durch SSL geschützt werden
- → Oder zusätzlich an IP oder Browser-Merkmale gebunden werden
- → Session-IDs sollten zufällig und nicht vorhersagbar sein
- → Session-ID sollte bei der Anmeldung ausgetauscht werden
- → Zerstören der Session bei der Benutzerabmeldung / Timeout

# Cross Site Request Forgery (CSRF)

- Bedeutung
  - Browser des Opfers führt ungewollt Aktionen auf einer vom Angreifer gewählten verwundbaren Seite aus.
  - Funktioniert weil Browser automatisch einen Grossteil der Authentisierungsdaten an jede abgesendete Anfrage anhängt
    - Session-Cookies
    - Basic Authentication Header
    - IP-Adresse
    - Client-seitige SSL Zertifikate
    - Windows-Domänen-Authentisierung
- Impact
  - Initiieren von Transaktionen
    - Überweisungen
    - Benutzerlogout
    - Etc.
  - Änderung von Kontendaten
  - Ausnutzen von XSS

# Cross Site Request Forgery (CSRF)








oneconsult®
IT Security & Strategic Consulting

# Cross Site Request Forgery (CSRF): Abhilfe

→ Verwenden eines nicht automatisch übermittelten Tokens für alle Aktions-Anfragen

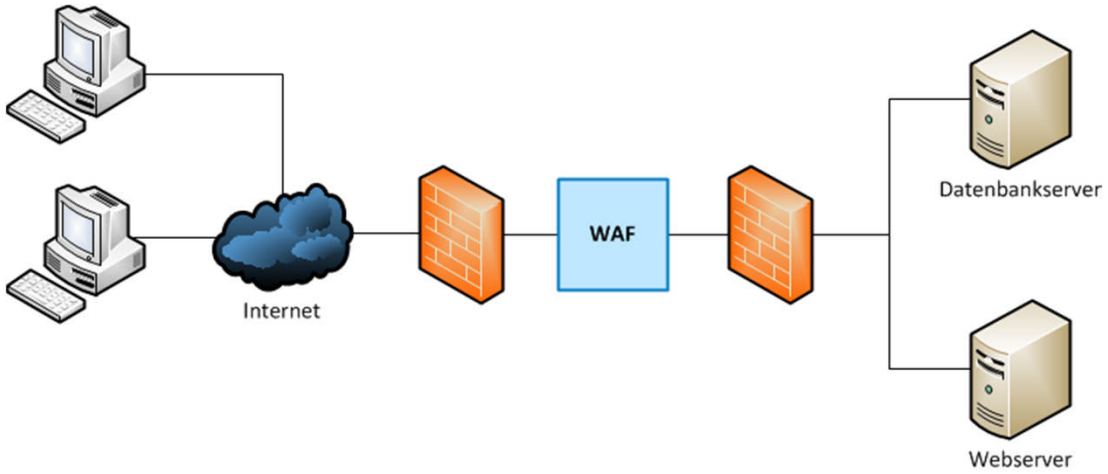
- Z.B. Hidden Post Parameter
- Token sollte kryptografisch stark zufällig sein

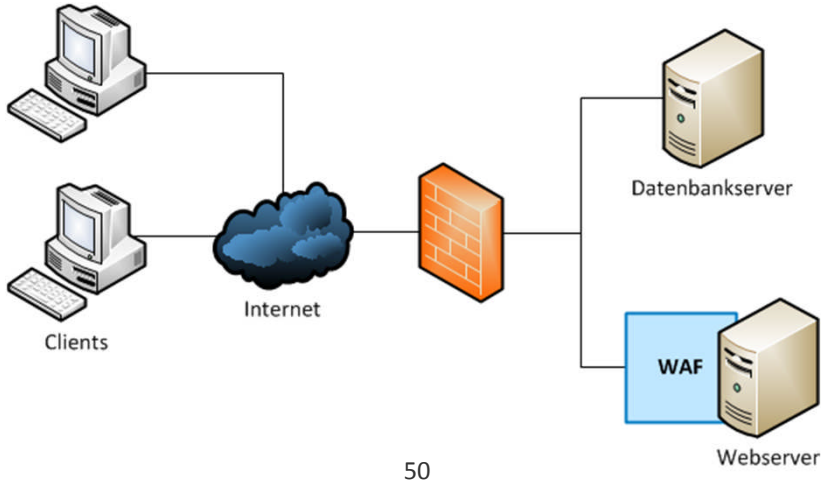
XSS Schwachstelle ermöglicht es diese Massnahme zu umgehen.

# Web Application Firewall (WAF)

- → Volle Unterstützung für HTTP:
  - Der Zugriff auf einzelne Felder (Feldinhalt, Länge, Anzahlfelder, etc.)
  - Gesamte Transaktion (beide, Anfrage und Antwort)
- → Kann gewisse Angriffe verhindern
  - CSRF
  - Session-Handling
- → Versucht andere Angriffe zu filtern
- → Anti-Evasion-Funktionen
  - Normalisierung
  - Kanonisierung
  - Transformation

# Web Application Firewall (WAF)








oneconsult®
IT Security & Strategic Consulting

# Web Application Firewall (WAF)

Eine WAF kann und wird NICHT alle Angriffe erkennen und verhindern können!

# Fragen

# OneConsult Ansprechpartner

Jan Alsenz
MSc ETH CS, OPST & OPSA
Team Leader Security Audits

jan.alsenz@oneconsult.com
+41 79 377 15 15

Robert Schneider
BSc FH CS, OPST
Security Consultant

robert.schneider@oneconsult.com
+41 79 269 29 29

**Hauptsitz**
OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22
Fax +41 43 377 22 77
info@oneconsult.com

**Büro Österreich**
Niederlassung der OneConsult GmbH
Twin Tower, Wienerbergstrasse 11/12A
1100 Wien
Österreich

Tel +43 1 99460 64 69
Fax +43 1 99460 50 00
info@oneconsult.at