itsc.
Die Lösung zählt

itsc Admin-Tag

OWASP Top 10

Tobias Ellenberger – COO & Co-Partner
OneConsult GmbH

oneconsult®
IT Security & Strategic Consulting

Agenda

- → Vorstellung
- → Open Web Application Security Project (OWASP)
- → Die OWASP Top 10 (2013 – RC1)
- → OWASP Top 3 in der Praxis
- → Fazit

Über mich

- Tobias Ellenberger
- Ausbildung als Mediamatiker
- Stetige Weiterbildung in den Bereichen Security, Netzwerk und Betriebssysteme
- Seit 2002 in den Bereichen Consulting und Engineering tätig
- OSSTMM Professional Security Tester & OSSTMM Professional Security Analyst
- COO & Co-Partner der OneConsult GmbH

Agenda

- → Vorstellung
- → **Open Web Application Security Project (OWASP)**
- → Die OWASP Top 10 (2013-RC1)
- → OWASP Top 3 in der Praxis
- → Fazit

Open Web Application Security Project

- → Gegründet 01.12.2001 in der USA
- → Fördern von Applikationssicherheit mit
  - Vorträgen
  - Veröffentlichungen (OWASP Top 10, Bücher, Guidelines)
  - Veranstaltungen
  - Projekten
- → Frei verfügbar (www.owasp.org)
- → Diverse Tools (z.B WebGoat, DirBuster) stehen zur Verfügung

Agenda

- → Vorstellung
- → Open Web Application Security Project (OWASP)
- → **Die OWASP Top 10 (2013-RC1)**
- → OWASP Top 3 in der Praxis
- → Fazit

Die OWASP Top10 (2013 – RC1)

→ A1 Injection
→ A2 Broken Authentication and Session Management
→ A3 Cross-Site Scripting (XSS)
→ A4 Insecure Direct Object References
→ A5 Security Misconfiguration
→ A6 Sensitive Data Exposure
→ A7 Missing Function Level Access Control
→ A8 Cross-Site Request Forgery (CSRF)
→ A9 Using Known Vulnerable Components
→ A10 Unvalidated Redirects and Forwards

Die OWASP Top10 (2010 - 2013)

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Agenda

- → Vorstellung
- → Open Web Application Security Project (OWASP)
- → Die OWASP Top 10 (2013-RC1)
- → **OWASP Top 3 in der Praxis**
- → Fazit

Die OWASP Top10 (2013-RC1)

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components
- A10 Unvalidated Redirects and Forwards

A1: 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
- Beispiele:
  - SQL-Injections
  - HTML-Injections (Defacements)
  - XML-Injections
  - LDAP-Injections
  - etc.

A1: Injection

Webshop mit Büchern:

→ Suche nach Literatur von «Addison»
SELECT author, title FROM books WHERE publisher = 'addison'

→ Such nach Bücher von «O'reilly»
SELECT author, title FROM books WHERE publisher = 'o'reilly'

→ Resultat?
Incorrect syntax near 'reilly'.
Unclosed quotation mark before the character string '

A1: Injection

→ Angreifer sucht nach: «addison' OR 1=1 --»
SELECT author, title FROM books
WHERE publisher = 'addison' OR 1=1 --'

→ Resultat? -> alle Bücher werden ausgegeben

→ Grund:
Dies wird ermöglicht durch die Erweiterung der "WHERE" Klausel durch eine dauerhaft wahre Bedingung.
WHERE publisher = 'addison' OR 1=1 --'
WHERE wahr/falsch OR wahr --'

A1: Injection

→ BTW: «Injection»

A2: Broken Authentication and Session Management

→ Bedeutung

Ein Angreifer kann Passwörter, Sessiontokens oder ähnliches kompromittieren

→ Impact

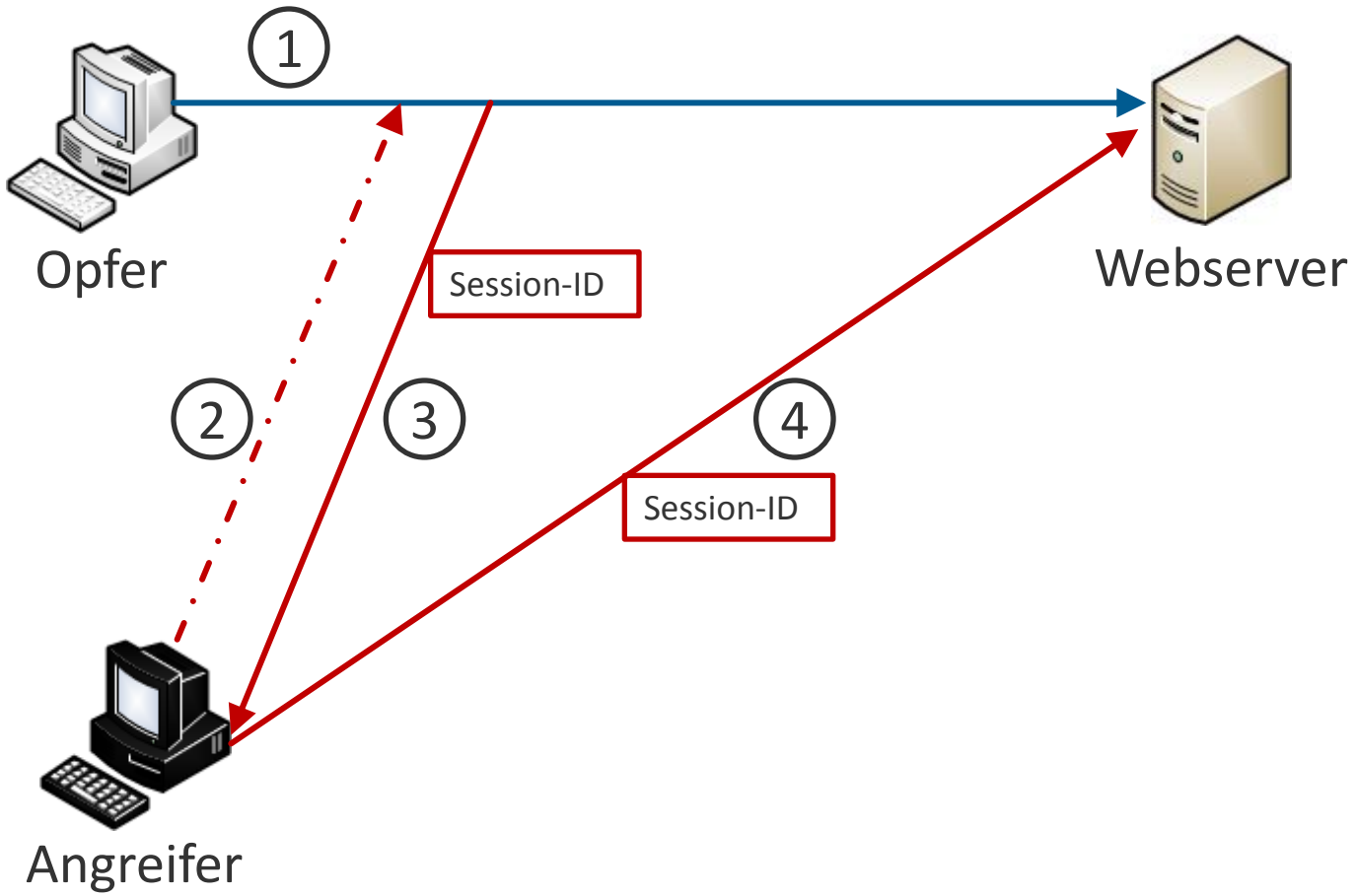
Durch die Fehlimplementierung der Anwedungsfunktion erhält der Angreifer so die Möglichkeit

- Sich als anderen User auszugeben
- Sich später oder gleichzeitig mit einer anderen User die Session zu teilen
- Die Applikation zu benutzen ohne ein gültiges Login zu besitzen

→ Beispiel

- Man-in-the-Middle Attacken (MitM)

A2: Broken Authentication and Session Management



A2: Broken Authentication and Session Management

→ Beispiele:

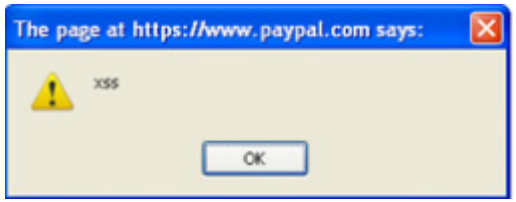
- «Verschlüsselter» Session Token
  dXNlcj1yYW5kb207ZGF0dW09MDEuMDEuMTk3MA==
  user=random;datum=01.01.1970
- Passwort Attacken
  - Brute-Force Attacke auf ein Login
  - Wörterbuch Attacke auf ein Login
- Fehlermeldungen
  Benutzername nicht bekannt
  Passwort nicht richtig

A3 Cross-Site Scripting (XSS)

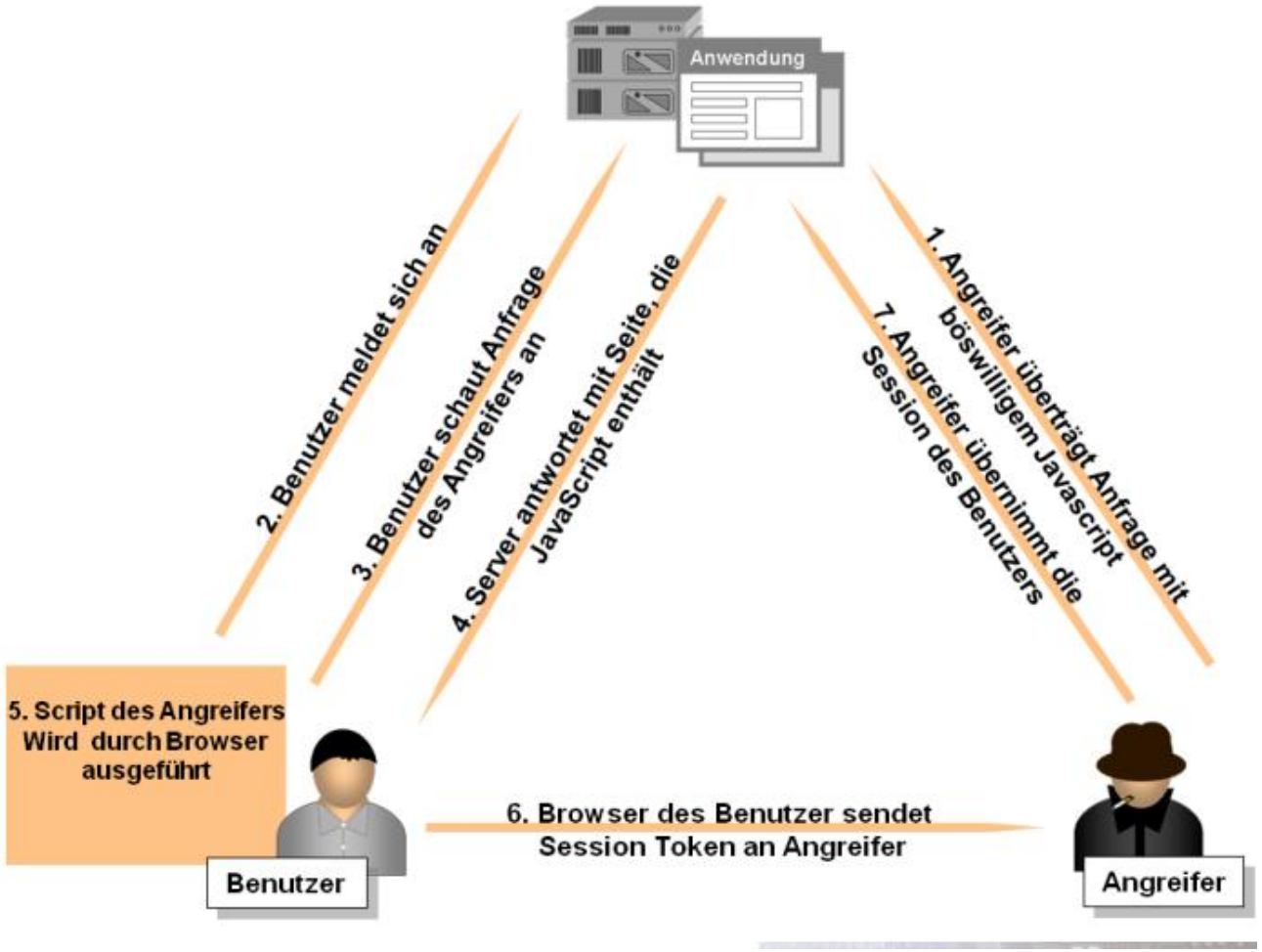
- → Bedeutung
  - Rohdaten eines Angreifers werden an den Browser eines Users gesendet
- → Rohdaten
  - In Datenbank abgespeichert: Stored XSS
  - Von Web-Input reflektiert: Reflected XSS
    - › Formularfeld, verstecktes Feld, URL, etc.
- → Impact
  - Stehlen von
    - › Aktiven Benutzer-Sessions
 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

A3 Cross-Site Scripting (XSS)

```
<tr>
<td><font size="2" face="Arial"><strong>XSS Example</
strong></font></td>
</tr>
<tr>
<td><font size="2" face="Arial">
<strong>
<script>alert("XSS")</script>
</strong></font></td>
</tr>
<tr>
<td> </td>
</tr>
```



A3 Cross-Site Scripting (XSS)



A3 Cross-Site Scripting (XSS)

→ Umgehen von Filtern:

- Groß-/Kleinschreibung: <ScRiPt>
- Leerzeichen im Tag-Code: < Script>
- Zusätzliche Zeichen: < <script>
- Beendigung des Filters: html text... %00<script>
- Nicht-Rekursive Filter: <scr<script>ipt>
- Endcoding: %3cscript%3e, %253cscript%253e

Agenda

- → Vorstellung
- → Open Web Application Security Project (OWASP)
- → Die OWASP Top 10 (2013-RC1)
- → OWASP Top 3 in der Praxis
- → **Fazit**

Sicherheits - Tipps

- → Hersteller Guidelines / Security Guidelines
- → Integrieren der Security Themen in die Entwicklung
- → Berücksichtigen von bestehendem Know-How (z.B OWASP)
- → Sicherheitsspezifische Aspekte durch Spezialisten (IT-Abteilung, Security-Abteilung, Externe Partner) beurteilen und ausarbeiten lassen.
- → Kontinuierliche Änderungen

Fazit

- Wenig Änderungen bei den OWASP Top 3
  (Seite mehr als 5 Jahren!)
- Applikationen werden noch attraktiver (Web, Mobile etc.)
- Angriffe sind an der Tagesordnung
- Man kann sich schützen (80 / 20 Regel)

Danke für Ihre Aufmerksamkeit!

Tobias Ellenberger
Mediamatiker EFZ, MCITP, OPST & OPSA
COO & Co-Partner

tobias.ellenberger@oneconsult.com
+41 79 314 25 25

Hauptsitz
OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

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

Büro Deutschland
Niederlassung der OneConsult GmbH
Karlstraße 35
80333 München
Deutschland

Tel +49 89 452 35 25 25
Fax +49 89 452 35 21 10
info@oneconsult.de

Büro Österreich
Niederlassung der OneConsult GmbH
Wienerbergstraße 11/12A
1100 Wien
Österreich

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