OWASP Top Ten in Österreich

Florian Brunner

florian.brunner@owasp.org

these slides are licensed CC-BY-SA based on content from Dave Wichers, Juergen Grieshofer and Seba Deleersnyder
Florian Brunner?

- 11 Jahre Programmiererfahrung
- 5 Jahre IT-Sicherheitsberatung
- Geschäftsführer
  Holistic Security Consulting GmbH
- OWASP Austria board member
- www.owasp.org
OWASP Top 10 - 2010

A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Failure to Restrict URL Access
A8: Insecure Cryptographic Storage
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards
What Didn’t Change

It’s About Risks, Not Just Vulnerabilities

• Title is: “The Top 10 Most Critical Web Application Security Risks”

OWASP Top 10 Risk Rating Methodology

• Based on the OWASP Risk Rating Methodology, used to prioritize Top 10

Based on the slides by Dave Wichers, OWASP
<table>
<thead>
<tr>
<th>OWASP Top 10 – 2010 (old)</th>
<th>OWASP Top 10 – 2013 (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2010-A2 – Cross Site Scripting (XSS)</strong></td>
<td><strong>2013-A2 – Broken Authentication and Session Management</strong></td>
</tr>
<tr>
<td><strong>2010-A3 – Broken Authentication and Session Management</strong></td>
<td><strong>2013-A3 – Cross Site Scripting (XSS)</strong></td>
</tr>
<tr>
<td><strong>2010-A4 – Insecure Direct Object References</strong></td>
<td><strong>2013-A4 – Insecure Direct Object References</strong></td>
</tr>
<tr>
<td><strong>2010-A5 – Cross Site Request Forgery (CSRF)</strong></td>
<td><strong>2013-A5 – Security Misconfiguration</strong></td>
</tr>
<tr>
<td><strong>2010-A6 – Security Misconfiguration</strong></td>
<td><strong>2013-A6 – Sensitive Data Exposure</strong></td>
</tr>
<tr>
<td><strong>2010-A7 – Insecure Cryptographic Storage</strong></td>
<td><strong>2013-A7 – Missing Function Level Access Control</strong></td>
</tr>
<tr>
<td><strong>2010-A8 – Failure to Restrict URL Access</strong></td>
<td><strong>2013-A8 – Cross-Site Request Forgery (CSRF)</strong></td>
</tr>
<tr>
<td><strong>2010-A9 – Insufficient Transport Layer Protection</strong></td>
<td><strong>2013-A9 – Using Known Vulnerable Components (NEW)</strong></td>
</tr>
<tr>
<td><strong>2010-A10 – Unvalidated Redirects and Forwards (NEW)</strong></td>
<td><strong>2013-A10 – Unvalidated Redirects and Forwards</strong></td>
</tr>
</tbody>
</table>

**3 Primary Changes:**

- **Merged:** 2010-A7 and 2010-A9 -> 2013-A6
- **Added New 2013-A9: Using Known Vulnerable Components**
- **2010-A8 broadened to 2013-A7**

Provided by **Dave Wichers**, OWASP
OWASP Top 10 - 2013

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 Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards
OWASP Top 10 – 2013

Austria?
You can compare the OWASP Top 10 with the OWASP Top 10 based on the test results of the last 15 web application penetration tests by the author. Only those vulnerabilities are counted that fall into those categories.
Subscribe mailing list

www.owasp.at

Keep up to date!