OWASP Top Ten in Österreich

Florian Brunner

florian.brunner@owasp.org

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

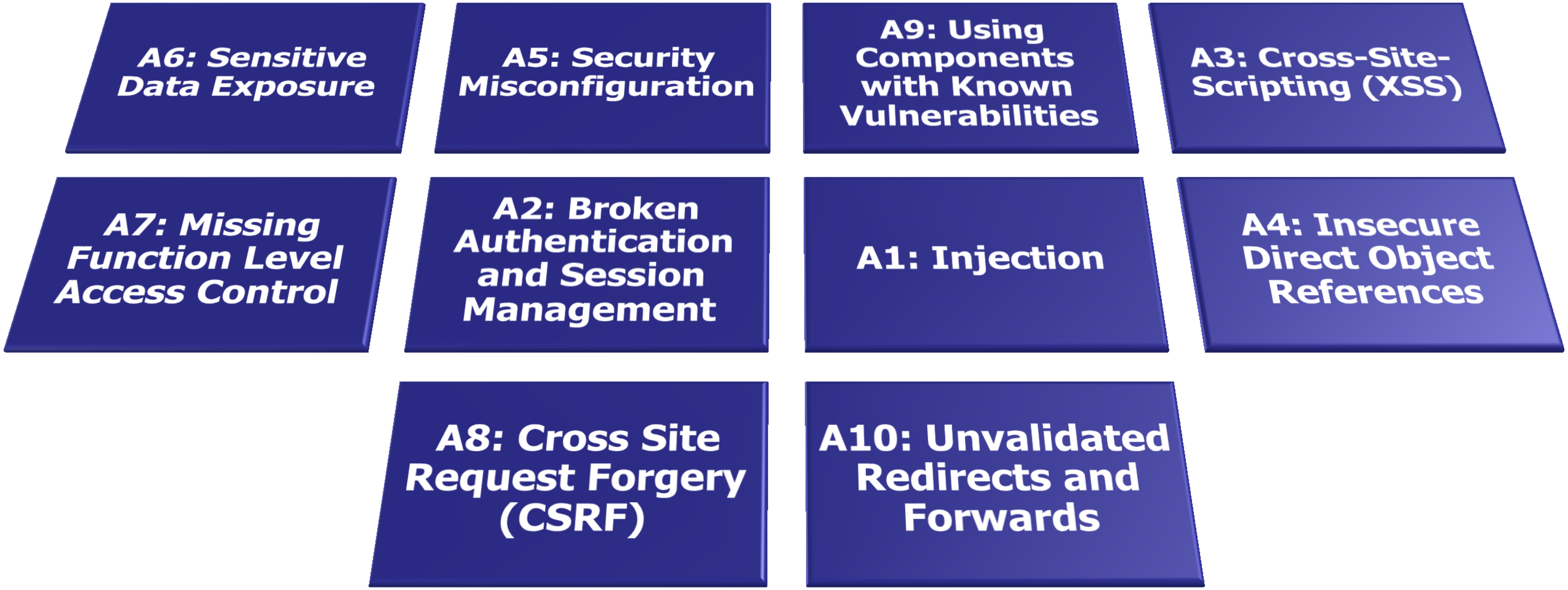
OWASP Top 10 – 2010 (old)	OWASP Top 10 – 2013 (New)
2010-A1 – Injection	**2013-A1 – Injection**
2010-A2 – Cross Site Scripting (XSS)	**2013-A2 – Broken Authentication and Session Management**
2010-A3 – Broken Authentication and Session Management	**2013-A3 – Cross Site Scripting (XSS)**
2010-A4 – Insecure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



A6: Sensitive Data Exposure

A5: Security Misconfiguration

A9: Using Components with Known Vulnerabilities

A3: Cross-Site-Scripting (XSS)

A7: Missing Function Level Access Control

A2: Broken Authentication and Session Management

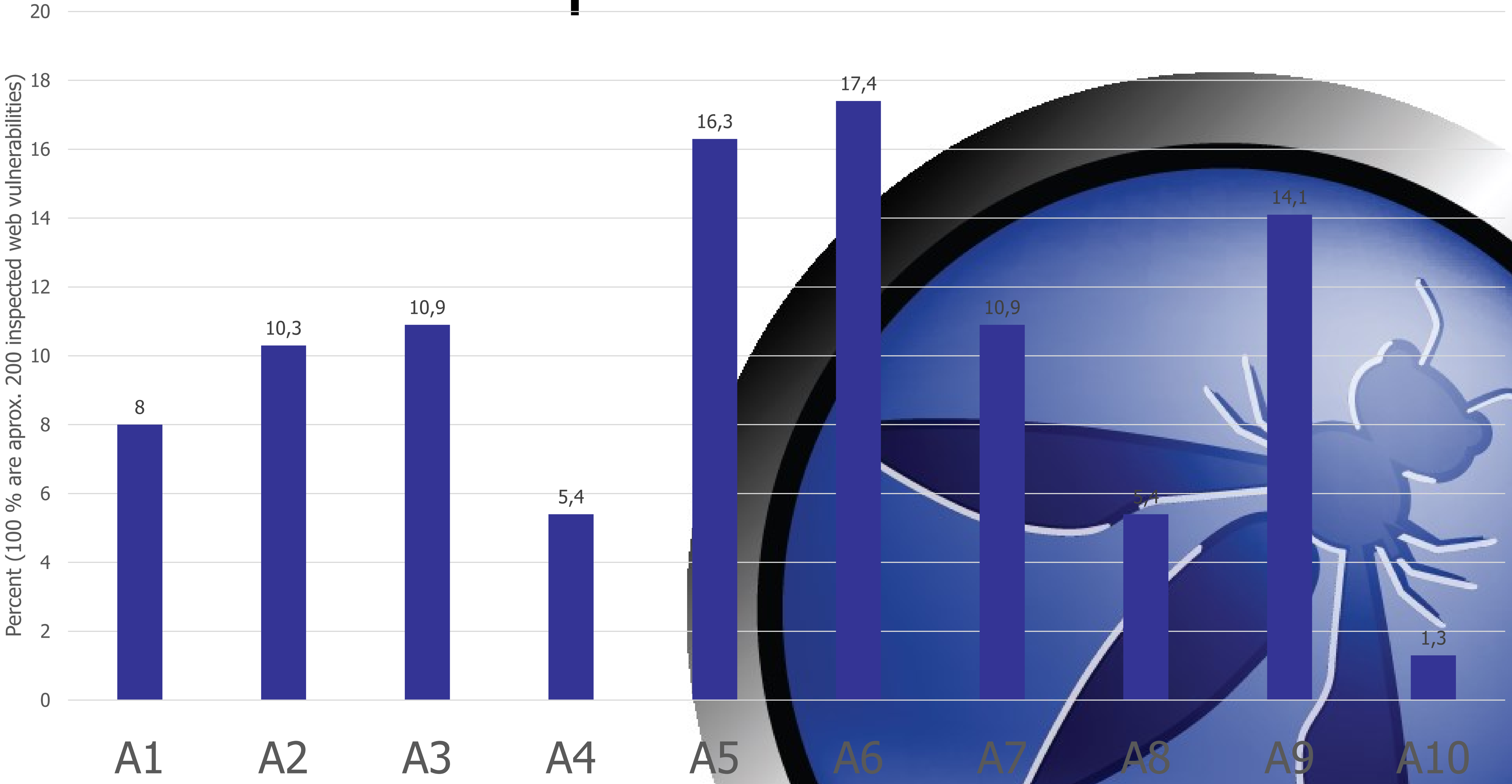
A1: Injection

A4: Insecure Direct Object References

A8: Cross Site Request Forgery (CSRF)

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!