

OWASP TOP 10



2013

Project: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

With a full card, you and your team gets: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A1** ‘Injection<script>alert(‘lol’ ; -- | (password = \*)

**A2**

Broken Authentication and Session Management

**A5**

Security Misconfiguration

**A10**

Unvalidated Redirects and Forwards

**A8**

Cross-Site Request Forgery (CSRF)

A9

Using Components with Known Vulnerabilities

**A6**

Sensitive Data Exposure

**A3**

Cross-Site Scripting (XSS)

**A4**

Insecure Direct Object References

**A7**

Missing Function Level Access Control

Top 10: <https://www.owasp.org/index.php/Top_10_2013-Top_10>

Fresh Bingo Cards: [http://haxor.nl/bingo/](http://haxor.nl/bingo/OwaspTop10Bingo)

Note: the OWASP Top 10 does not cover everything and anything, or anything at all. But it is a well-documented list, which can help with explaining vulnerabilities. A full card means that the system is insanely and laughably vulnerable.

Elger “Stitch” Jonker

elgerjonker.nl