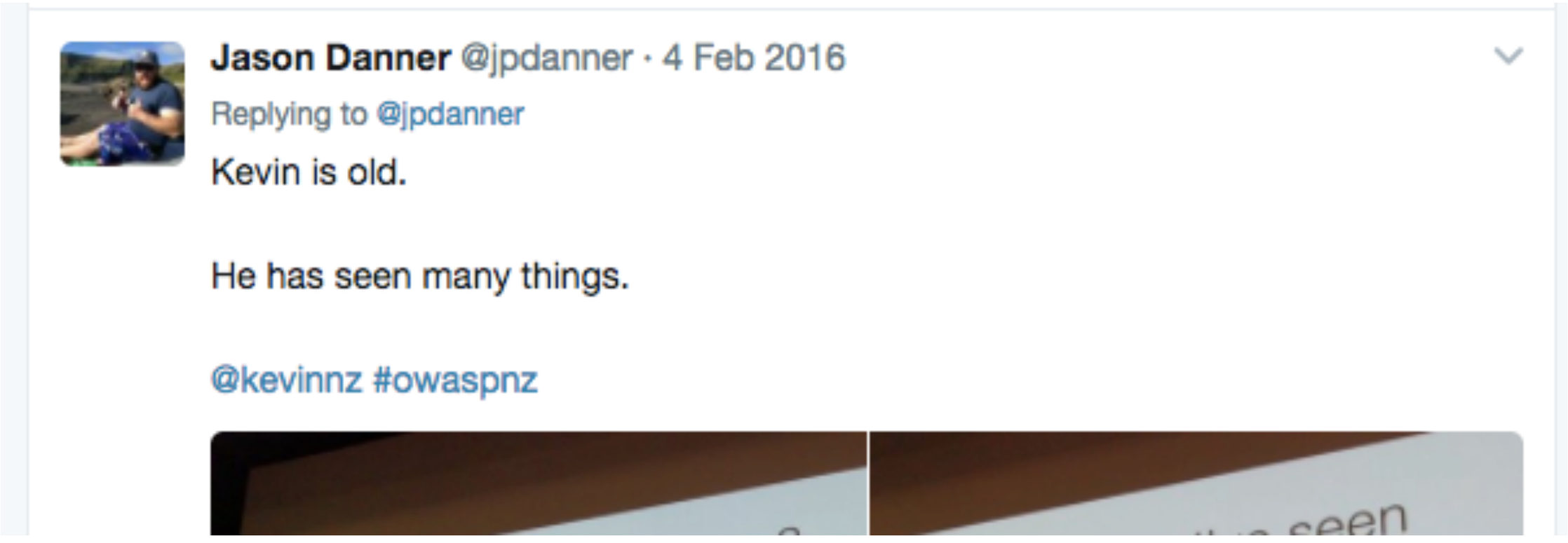
Top 10 Review and ~~Preview~~

Kevin Alcock, OWASP Day NZ 20 April 2017

OWASP
Open Web Application Security Project

Obligatory Who is



The Top 10

- Open Web Application Security Project (OWASP)
- The OWASP Top Ten provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

Who is it for?

Attackers

Defenders

Developers

Testers

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 Known Vulnerable Components
A10 - Unvalidated Redirects and Forwards

2017

A10 - Underprotected APIs (NEW)

- Increased exposure through Mobile, Micro Services
- Just because it is not “published” doesn’t mean it is is not discoverable
- Secure your comms, credentials, tokens and keys
- Harden your parsers
- Implement Access control where possible

A9 -Using Components with Known Vulnerabilities

- WordPress plugins, anyone?
- Audit your third party dependences
- Regularly check vendor and CVE’s
- Check to see if you really do need it
- Way up if you should Upgrade, replace, rewrite or virtual patch

A8 - Cross-Site Request Forgery (CSRF)

- A Phishers dream
- Use the CSRF defence in your framework
- Grab CSRF Cheat Sheet from owasp.org

A7 - Insufficient Attack Protection (NEW)

- Do you know when you are under attack?
- WAF's, IDS, Firewalls, Honeypots
- Actively monitor and respond accordingly

A6 - Sensitive Data Exposure

- Passwords, credit card numbers, health records, and personal information
- Don’t store sensitive data unnecessarily
- Ensure strong standard algorithms and strong keys are used, and proper key management is in place.
- Ensure passwords are stored with an algorithm specifically designed for password protection, such as bcrypt, PBKDF2, or scrypt.

A5 - Security Misconfiguration

- Are you rolling with default settings, anywhere?
- Is your software up to date?
- IaaS - treat your configurations like code
- Test Test Test

A4 - Broken Access Control (Original category in 2003/2004)

- Don’t just hide features
- Check access!!

A3 - Cross-Site Scripting (XSS)

- Stored, reflected, server, client
- Escape untrusted data

A2 - Broken Authentication and Session Management

- Don’t put session tokens in the URL
- Use analytics to fine tune your timeouts
- Make sure you do invalidate your tokens
- Validate credentials on sensitive operations

A1 - INJECTION!

- SQLi is 18 years old and its still a thing!
- it is not just SQL:
  check your LDAP, XPath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, expression languages, etc.
- DON’T TRUST INPUT!

OWASP TOP 10 (2017)

A1 - Injection

A2 - Broken Authentication and Session Management

A3 - Cross-Site Scripting (XSS)

A4 - Broken Access Control (Original category in 2003/2004)

A5 - Security Misconfiguration

A6 - Sensitive Data Exposure

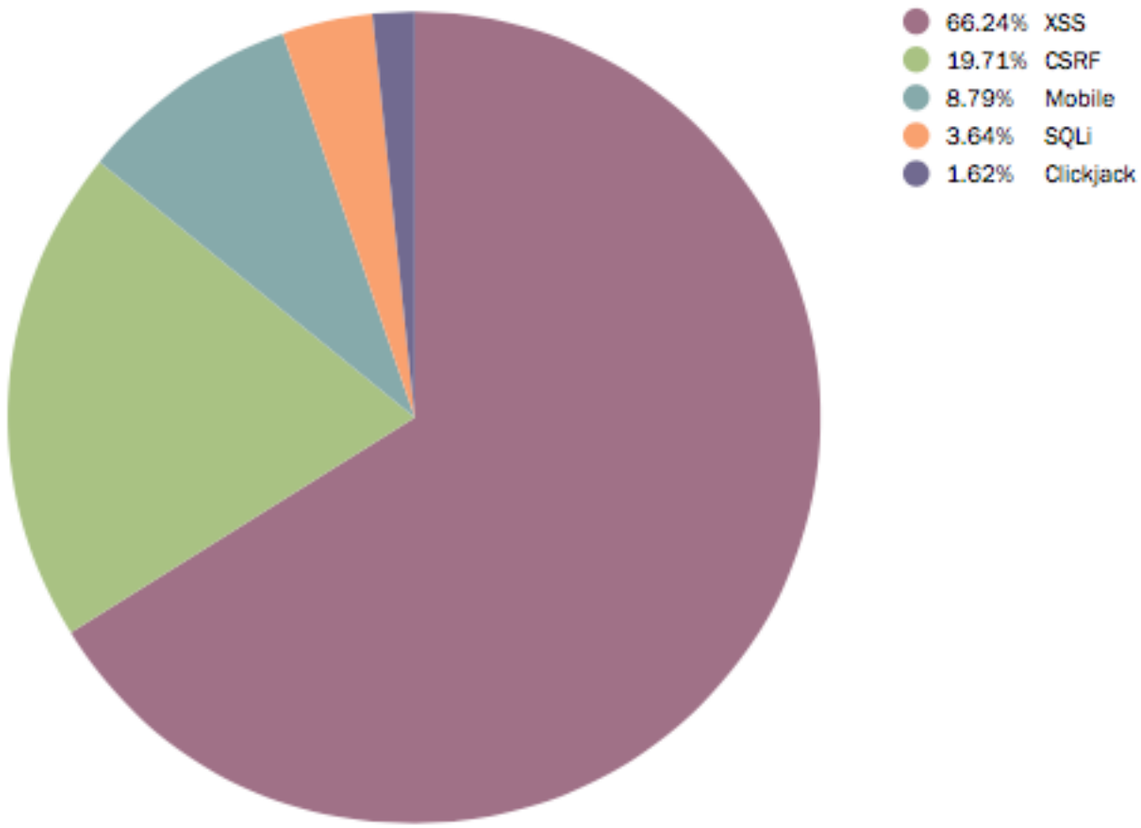
A7 - Insufficient Attack Protection (NEW)

A8 - Cross-Site Request Forgery (CSRF)

A9 - Using Known Vulnerable Components

A10 - Underprotected APIs (NEW)

How does that compare



* The State of the Bug Bounty - 2016 *(Bugcrowd)*

But there’s more…

- Clickjacking (CAPEC-103)
- Denial of Service (CWE-400) (Was 2004 Top 10 – Entry 2004-A9)
- Deserialization of Untrusted Data (CWE-502)
- Expression Language Injection (CWE-917)
- Information Leakage (CWE-209) and Improper Error Handling (CWE-388) (Was part of 2007 Top 10 – Entry 2007-A6)
- Hotlinking Third Party Content (CWE-829)
- Malicious File Execution (CWE-434) (Was 2007 Top 10 – Entry 2007-A3)
- Mass Assignment (CWE-915)
- Server-Side Request Forgery (SSRF) (CWE-918)
- Unvalidated Redirects and Forwards (CWE-601) (Was 2013 Top 10 – Entry 2013-A10)
- User Privacy (CWE-359)

Where to from here?

For Devs

- Application Security Requirements
- Application Security Architecture
- Standard Security Controls
- Secure Development Lifecycle
- Application Security Eduction

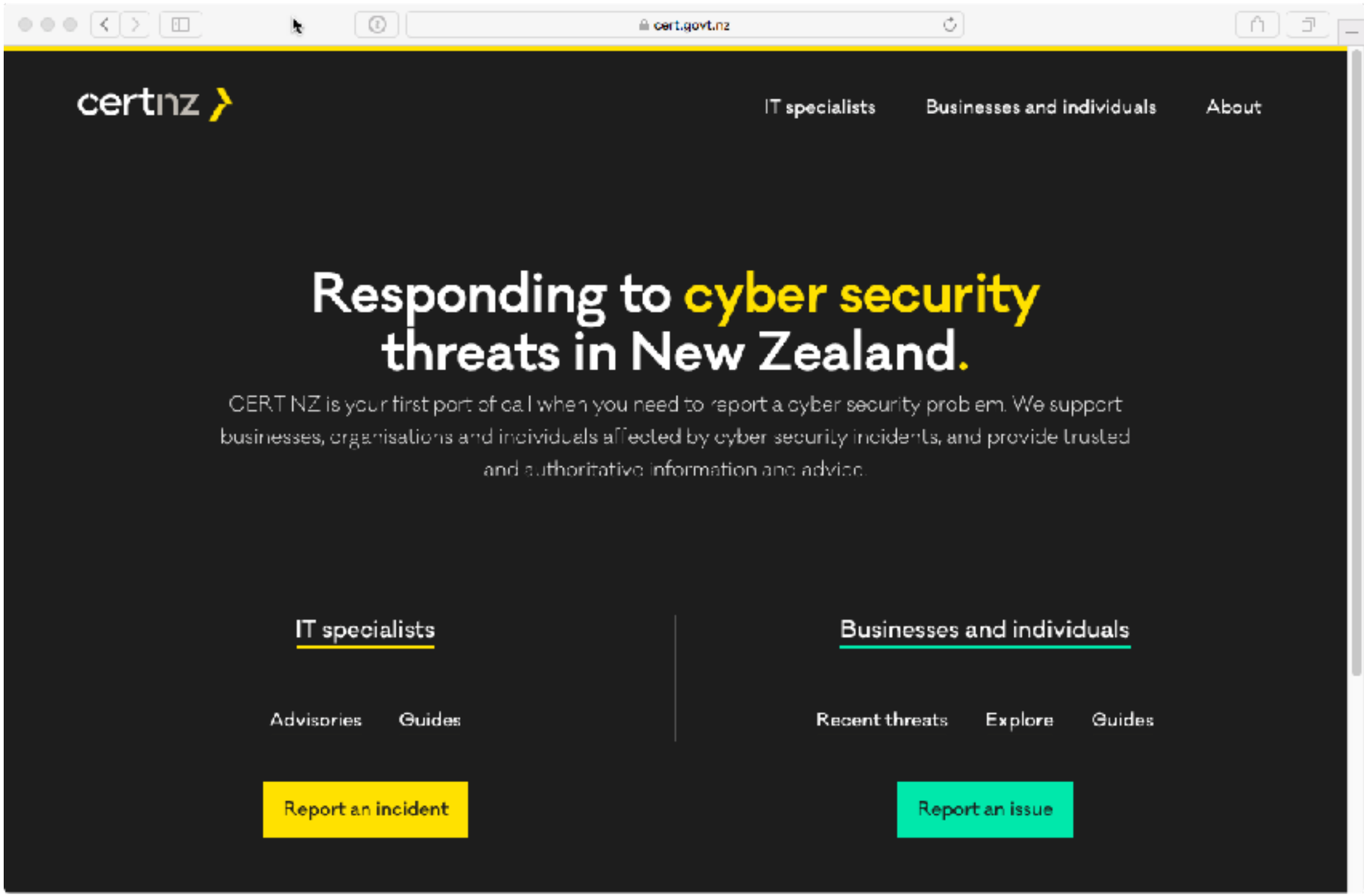
For Testers

- Understand the Threat Model
- Understand your SDLC
- Testing Strategies
- Achieving Coverage and Accuracy
- Make Findings Awesome

For Everyone

- Support OWASP
- And your local chapter!

Shout out!


cert.govt.nz
certnz
IT specialists
Businesses and individuals
About
Responding to cyber security threats in New Zealand.
CERT NZ is your first port of call when you need to report a cyber security problem. We support businesses, organisations and individuals affected by cyber security incidents, and provide trusted and authoritative information and advice.
IT specialists
Advisories
Guides
Report an incident
Businesses and individuals
Recent threats
Explore
Guides
Report an issue

Credits

- old-guy https://twitter.com/jpdanner/status/695087811158880256
- attackers https://twitter.com/malwareunicorn/status/853359887568445440
- defenders https://images.nasa.gov/#/details-GRC-1973-C-01775.html
- developer https://twitter.com/ProObject/status/849683334473150464
- tester http://imgur.com/gallery/3IxOlz2
- bugcrowd https://pages.bugcrowd.com/2016-state-of-bug-bounty-report
- where2 https://www.nasa.gov/sites/default/files/images/297755main_GPN-2001-000009_full.jpg