Mob Learning with the OWASP Top Ten and 30 Days of Security Testing

Michael Clarke

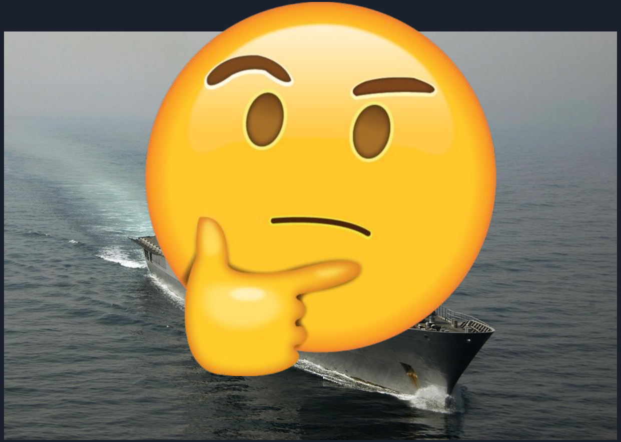
InfoSec is exciting, but how do you get started?

- New Zealand (and the world) needs more security professionals
- InfoSec is exciting and interesting, why aren’t more people getting involved?

A bit about me

- Software Tester - Erudite Software
- Non-technical background
- Was always interested in IT, but thought entry requirements were too daunting

How did I get started in software?



Talk to mountain climbers and those familiar with mountains.

Find people that have made it to where you want to be - talk to them

Make it clear that you want to learn, and that you’ll put the effort in.

Learn how they got started

Listen

Find the stones in the mountain, and share the load

- SMART goals, cliche but useful
- Make your goals accountable

Climb with others

- Find like minded people and learn together
- Learn from their experiences
- Learn by teaching

OWASP Top Ten

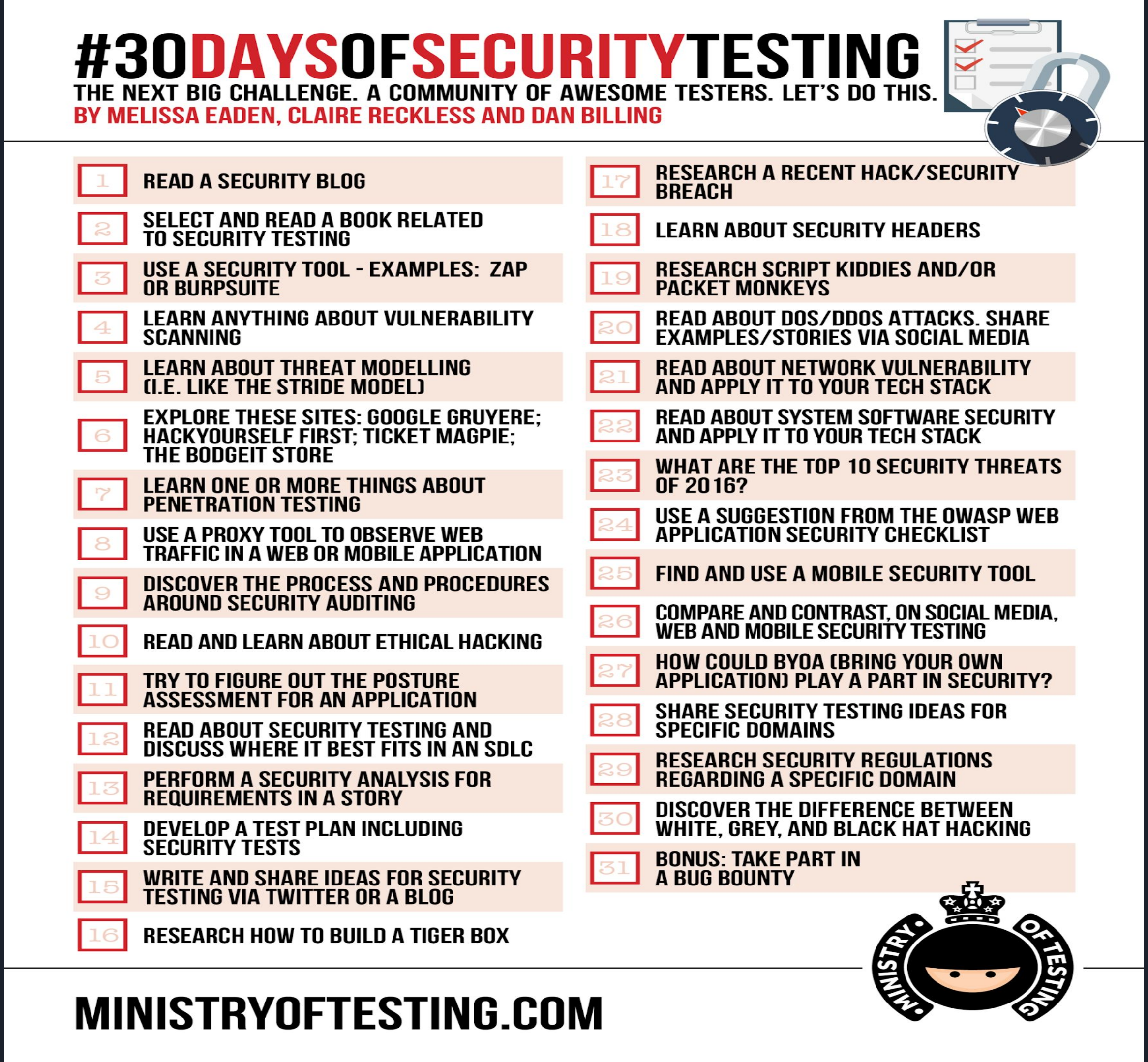
MINISTRY OF TESTING PODCASTS

A Podcast Workshop - Goal Setting
with Tom Griffin and Mike Clarke

In partnership with The Super Testing Bros

Irritable ***B***owel ***S***yndrome, ***E***xternal ***B***owel ***S***yndrome, ***C***rying ***I***n ***U***r ***I***ntestines

1. **I**njection
2. **B**roken Authentication
3. **S**ensitive Data Exposure
4. **E**xternal XML Entities
5. **B**roken Access Control
6. **S**ecurity Misconfiguration
7. **C**ross Site Scripting
8. **I**nsecure Deserialisation
9. **U**sing Components with Known Vulnerabilities
10. **I**nsufficient Logging and Monitoring



#30DAYSOFSECURITYTESTING

THE NEXT BIG CHALLENGE. A COMMUNITY OF AWESOME TESTERS. LET'S DO THIS.

BY MELISSA EADEN, CLAIRE RECKLESS AND DAN BILLING

1 READ A SECURITY BLOG

2 SELECT AND READ A BOOK RELATED TO SECURITY TESTING

3 USE A SECURITY TOOL - EXAMPLES: ZAP OR BURPSUITE

4 LEARN ANYTHING ABOUT VULNERABILITY SCANNING

5 LEARN ABOUT THREAT MODELLING (I.E. LIKE THE STRIDE MODEL)

6 EXPLORE THESE SITES: GOOGLE GRUYERE; HACKYOURSELF FIRST; TICKET MAGPIE; THE BODGEIT STORE

7 LEARN ONE OR MORE THINGS ABOUT PENETRATION TESTING

8 USE A PROXY TOOL TO OBSERVE WEB TRAFFIC IN A WEB OR MOBILE APPLICATION

9 DISCOVER THE PROCESS AND PROCEDURES AROUND SECURITY AUDITING

10 READ AND LEARN ABOUT ETHICAL HACKING

11 TRY TO FIGURE OUT THE POSTURE ASSESSMENT FOR AN APPLICATION

12 READ ABOUT SECURITY TESTING AND DISCUSS WHERE IT BEST FITS IN AN SDLC

13 PERFORM A SECURITY ANALYSIS FOR REQUIREMENTS IN A STORY

14 DEVELOP A TEST PLAN INCLUDING SECURITY TESTS

15 WRITE AND SHARE IDEAS FOR SECURITY TESTING VIA TWITTER OR A BLOG

16 RESEARCH HOW TO BUILD A TIGER BOX

17 RESEARCH A RECENT HACK/SECURITY BREACH

18 LEARN ABOUT SECURITY HEADERS

19 RESEARCH SCRIPT KIDDIES AND/OR PACKET MONKEYS

20 READ ABOUT DOS/DDOS ATTACKS. SHARE EXAMPLES/STORIES VIA SOCIAL MEDIA

21 READ ABOUT NETWORK VULNERABILITY AND APPLY IT TO YOUR TECH STACK

22 READ ABOUT SYSTEM SOFTWARE SECURITY AND APPLY IT TO YOUR TECH STACK

23 WHAT ARE THE TOP 10 SECURITY THREATS OF 2016?

24 USE A SUGGESTION FROM THE OWASP WEB APPLICATION SECURITY CHECKLIST

25 FIND AND USE A MOBILE SECURITY TOOL

26 COMPARE AND CONTRAST, ON SOCIAL MEDIA, WEB AND MOBILE SECURITY TESTING

27 HOW COULD BYOA (BRING YOUR OWN APPLICATION) PLAY A PART IN SECURITY?

28 SHARE SECURITY TESTING IDEAS FOR SPECIFIC DOMAINS

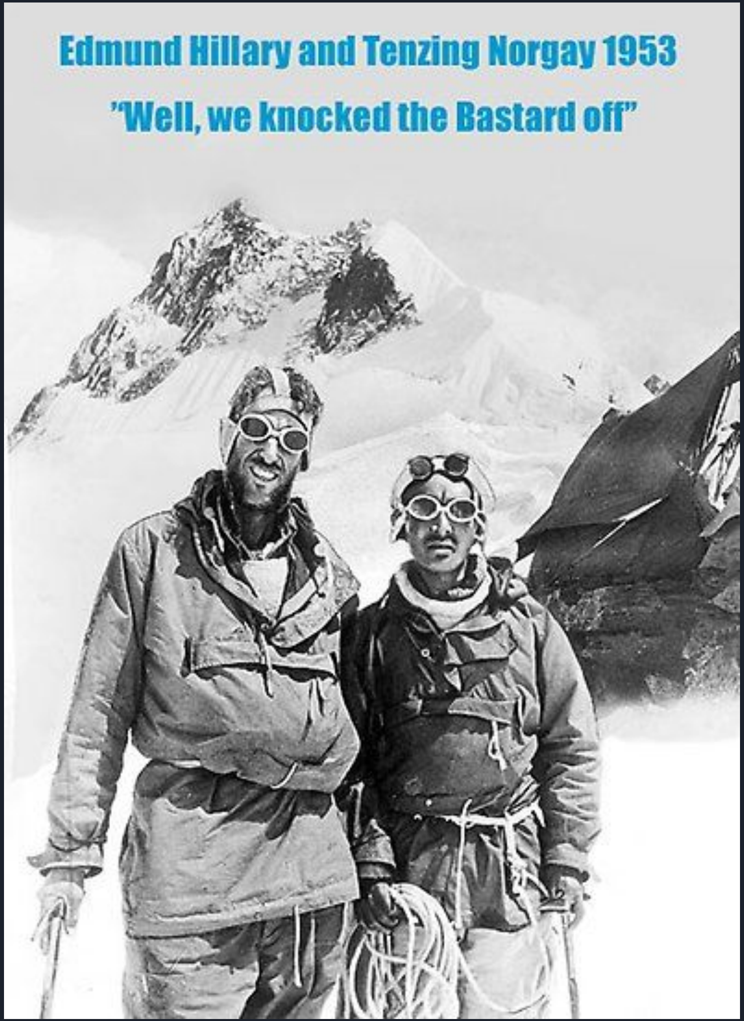
29 RESEARCH SECURITY REGULATIONS REGARDING A SPECIFIC DOMAIN

30 DISCOVER THE DIFFERENCE BETWEEN WHITE, GREY, AND BLACK HAT HACKING

31 BONUS: TAKE PART IN A BUG BOUNTY

MINISTRY OF TESTING

MINISTRYOFTESTING.COM


Edmund Hillary and Tenzing Norgay 1953
"Well, we knocked the Bastard off"

Thanks to the following:

Murray Polson - Erudite Software

Dan and James from the Super Testing Bros
Tom Griffin

Brendan Seerup, Santhosh Tuppad
Erin Okoko, Teresa Wetherall, Rasha Taher,
Swapna Soni, Prachi Jain,
Jasmin Liu, Ali Haydar - WeTest Slack

Francois Marais - Defend Ltd
Shofe Miraz - ZX Security
Jeremy Stott - Vend

Questions?

How to reach me

I’m always interested to talk testing and learn something new.
If you’d like to get in touch you can find me here:

Twitter - @TesterMikeNZ https://twitter.com/TesterMikeNZ

LinkedIn - https://www.linkedin.com/in/michael-clarke-nz/

My blog - https://mikethetesternz.wordpress.com/

On the Minstry of Testing Auckland Slack group
or at one of our Meetups