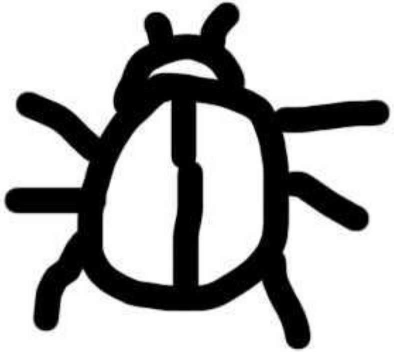
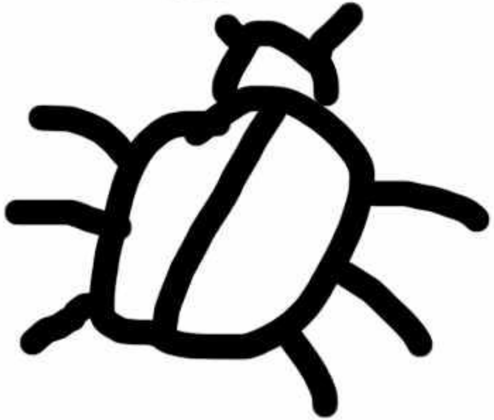
30(ish) Days of Security

With Grace and Catherine

ANITA BORG

A HEULLANT

High Quality

 bugs 

Catherine

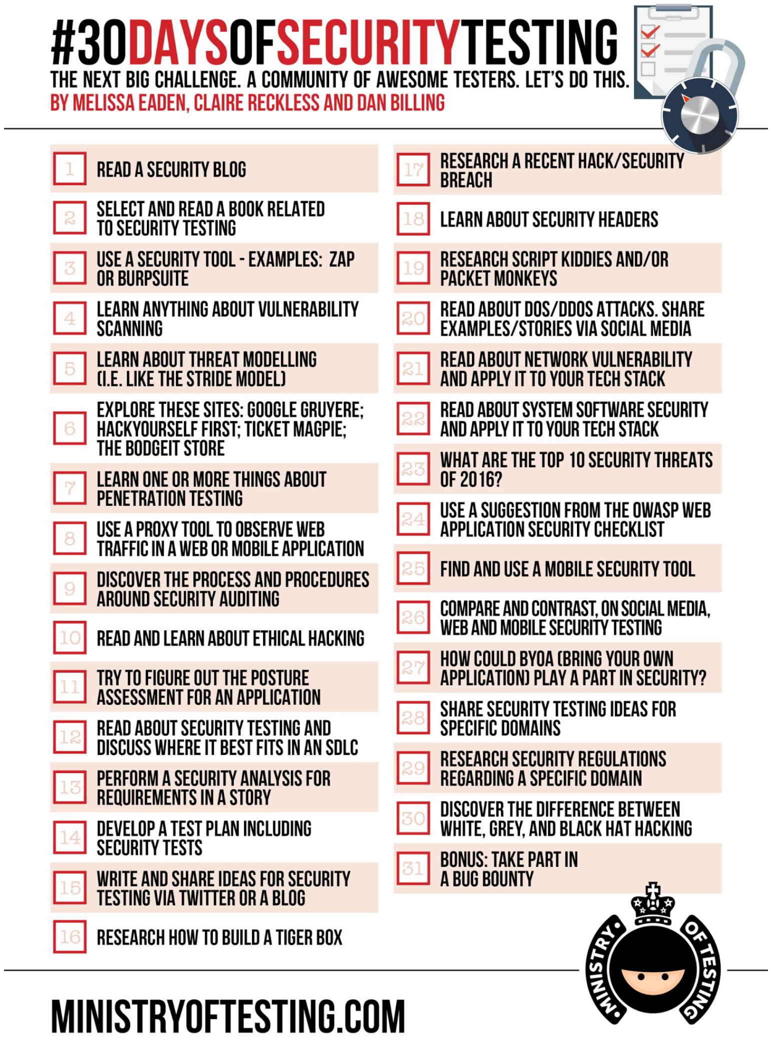
Grace

“HACKING”

I'M INTERESTED

“If you want to learn about something, the best way is to give a talk”

- Kanye West



#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?

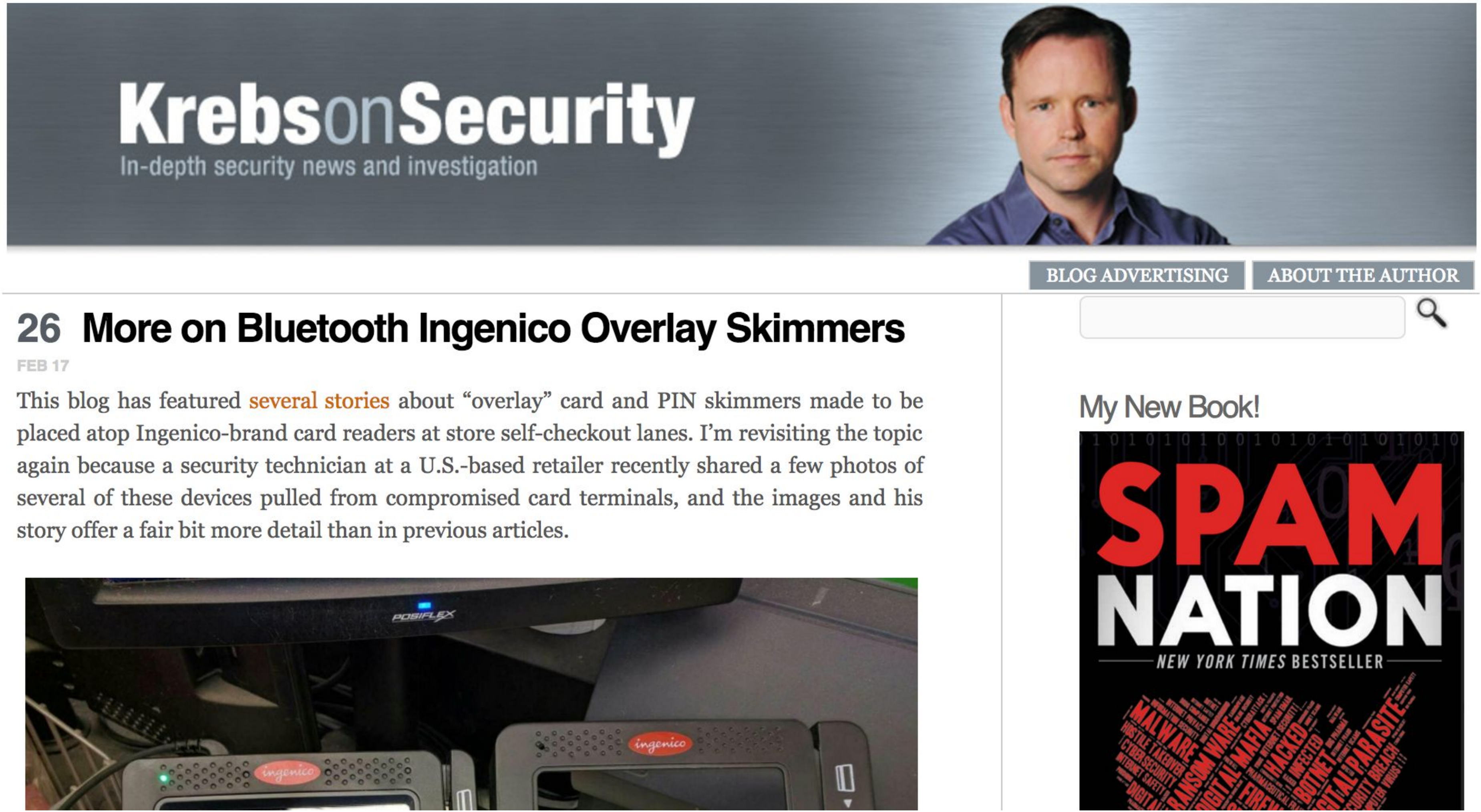
28 SHARE SECURITY TESTING IDEAS FOR SPECIFIC DOMAINS

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

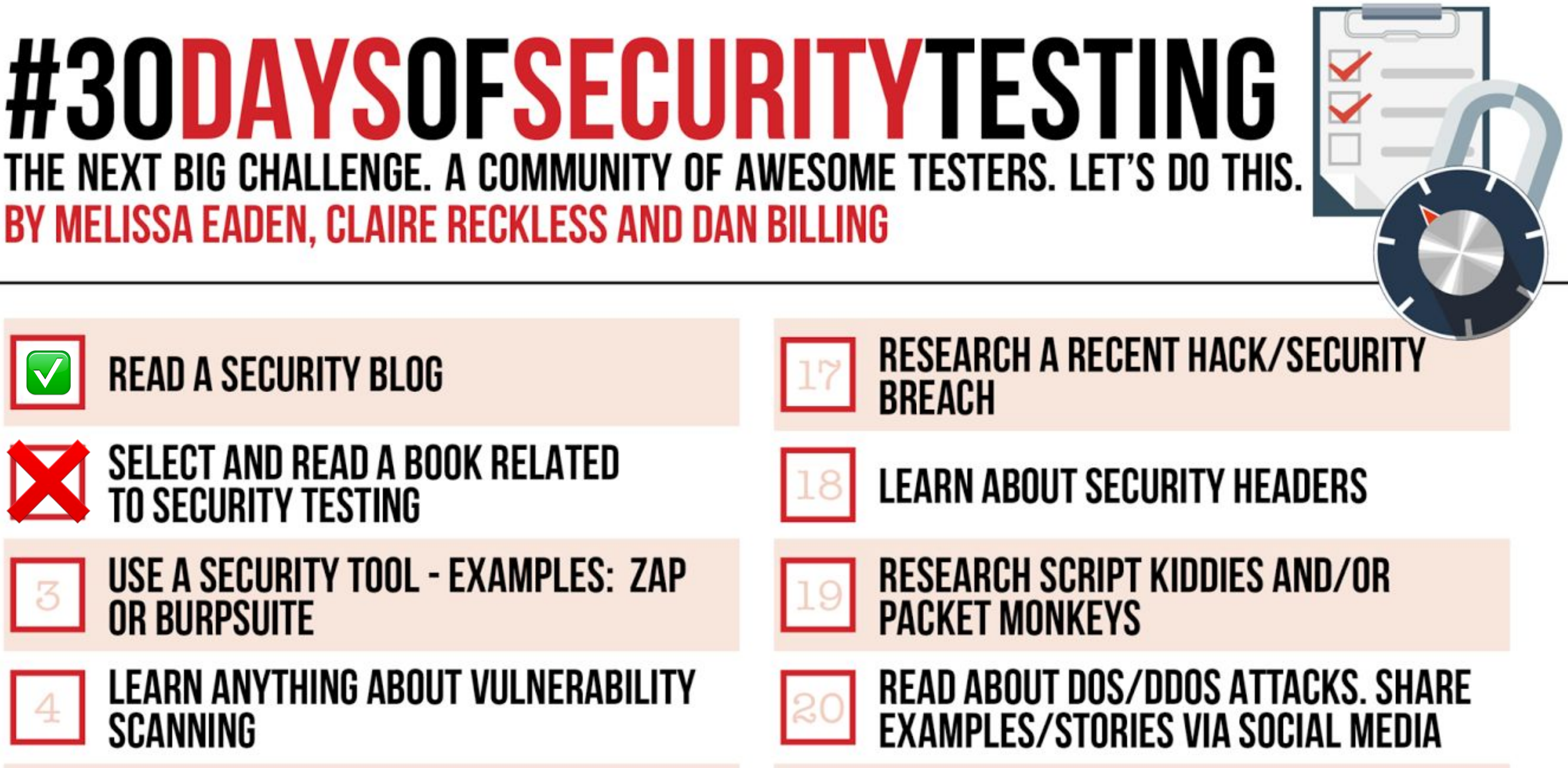
MINISTRYOFTESTING.COM



26 More on Bluetooth Ingenico Overlay Skimmers

FEB 17

This blog has featured several stories about “overlay” card and PIN skimmers made to be placed atop Ingenico-brand card readers at store self-checkout lanes. I’m revisiting the topic again because a security technician at a U.S.-based retailer recently shared a few photos of several of these devices pulled from compromised card terminals, and the images and his story offer a fair bit more detail than in previous articles.

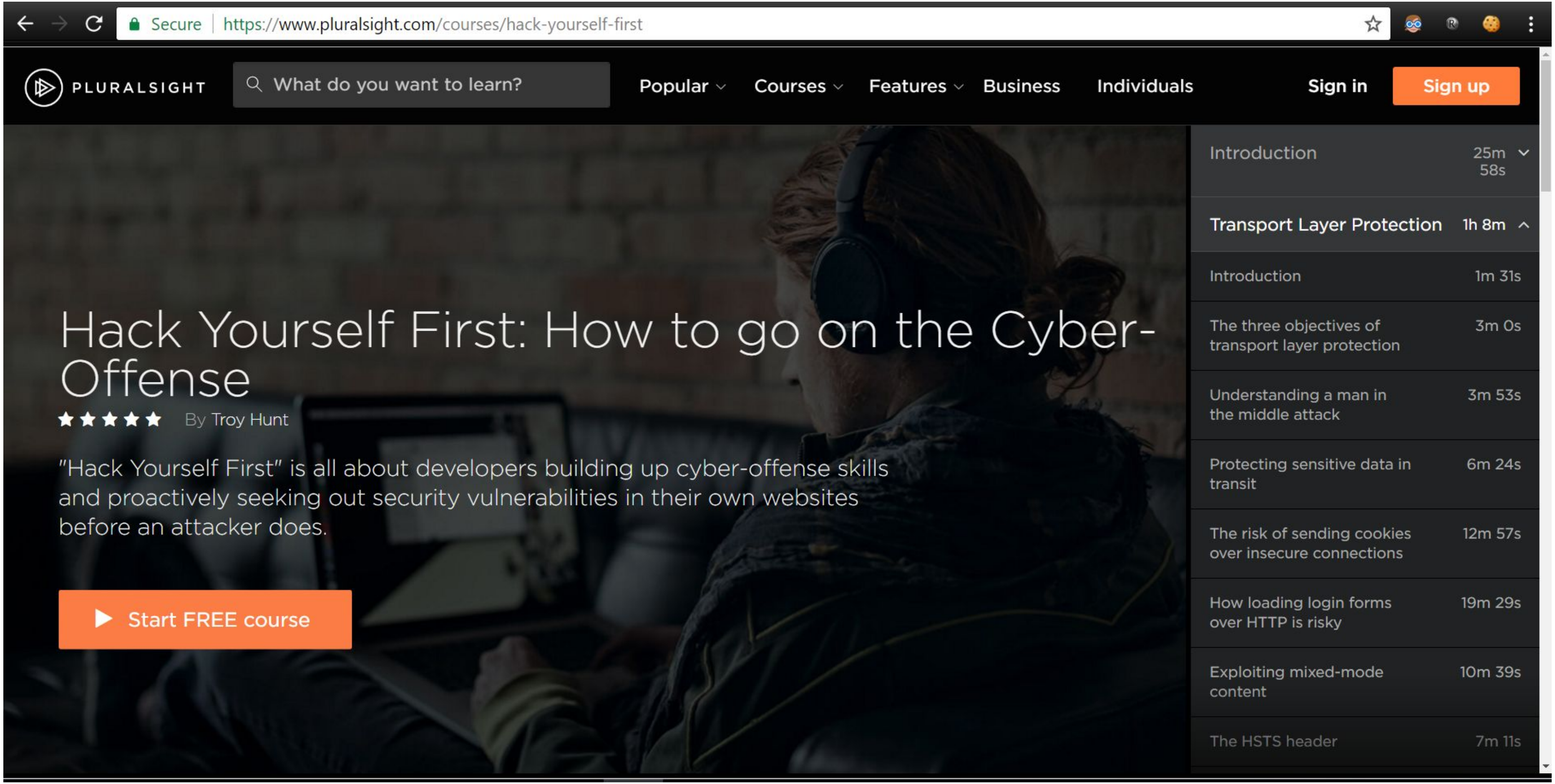


#30DAYSOFSECURITYTESTING

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

BY MELISSA EADEN, CLAIRE RECKLESS AND DAN BILLING

- ✅ READ A SECURITY BLOG
- ❌ SELECT AND READ A BOOK RELATED TO SECURITY TESTING
- 3 USE A SECURITY TOOL - EXAMPLES: ZAP OR BURPSUITE
- 4 LEARN ANYTHING ABOUT VULNERABILITY SCANNING
- 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



Hack Yourself First: How to go on the Cyber-Offense

★★★★★ By Troy Hunt

"Hack Yourself First" is all about developers building up cyber-offense skills and proactively seeking out security vulnerabilities in their own websites before an attacker does.

Introduction	25m 58s
Transport Layer Protection	**1h 8m**
Introduction	1m 31s
The three objectives of transport layer protection	3m 0s
Understanding a man in the middle attack	3m 53s
Protecting sensitive data in transit	6m 24s
The risk of sending cookies over insecure connections	12m 57s
How loading login forms over HTTP is risky	19m 29s
Exploiting mixed-mode content	10m 39s
The HSTS header	7m 11s

Obfuscation Output Encoding

Reflected Data

SQL Injection

Malware TCP Cookies

Black Hat

Fuzzing

XSS

Domains

Traffic UDP

Encryption

Verb Tampering

HTTP DNS

Spoofing

Payload

NAT

Whitelisting

Input Validation

Pen Testing

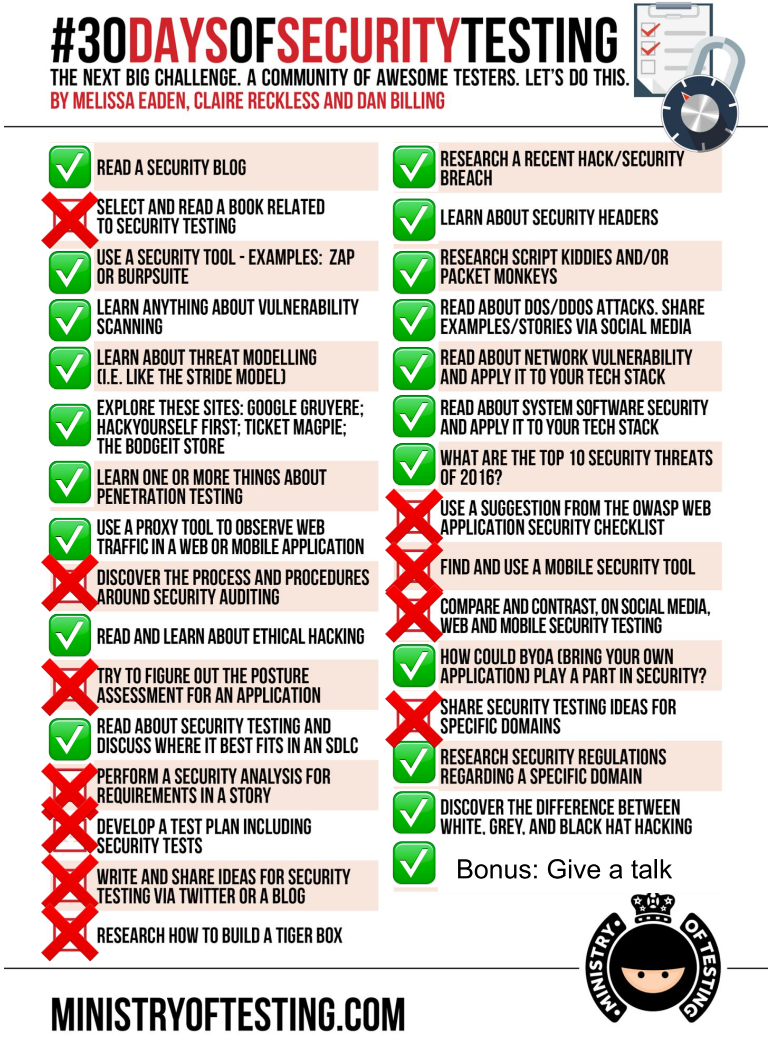
DDOS

Untrusted Data

Binary

End of Project

30 days review



#30DAYSOFSECURITYTESTING

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

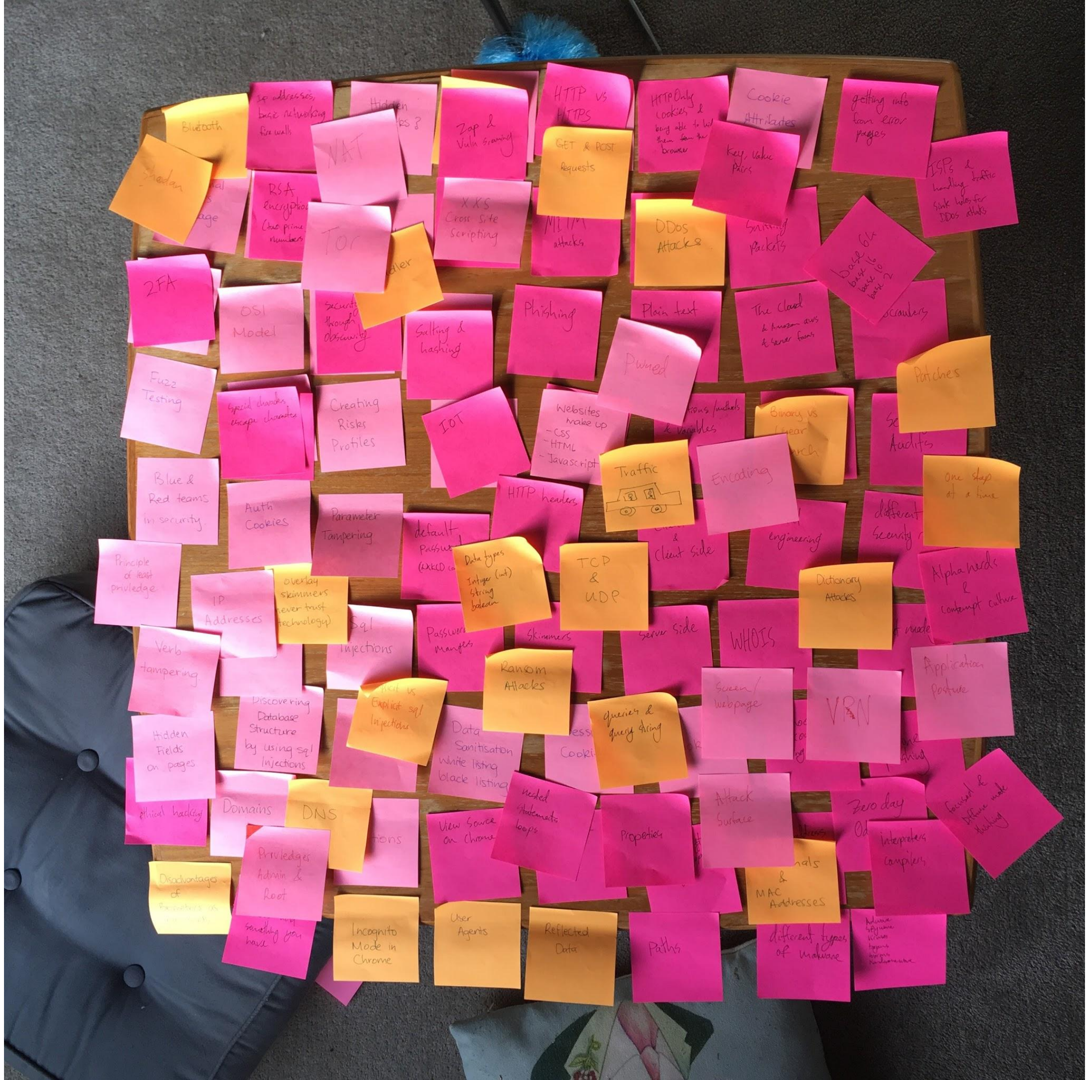
BY MELISSA EADEN, CLAIRE RECKLESS AND DAN BILLING

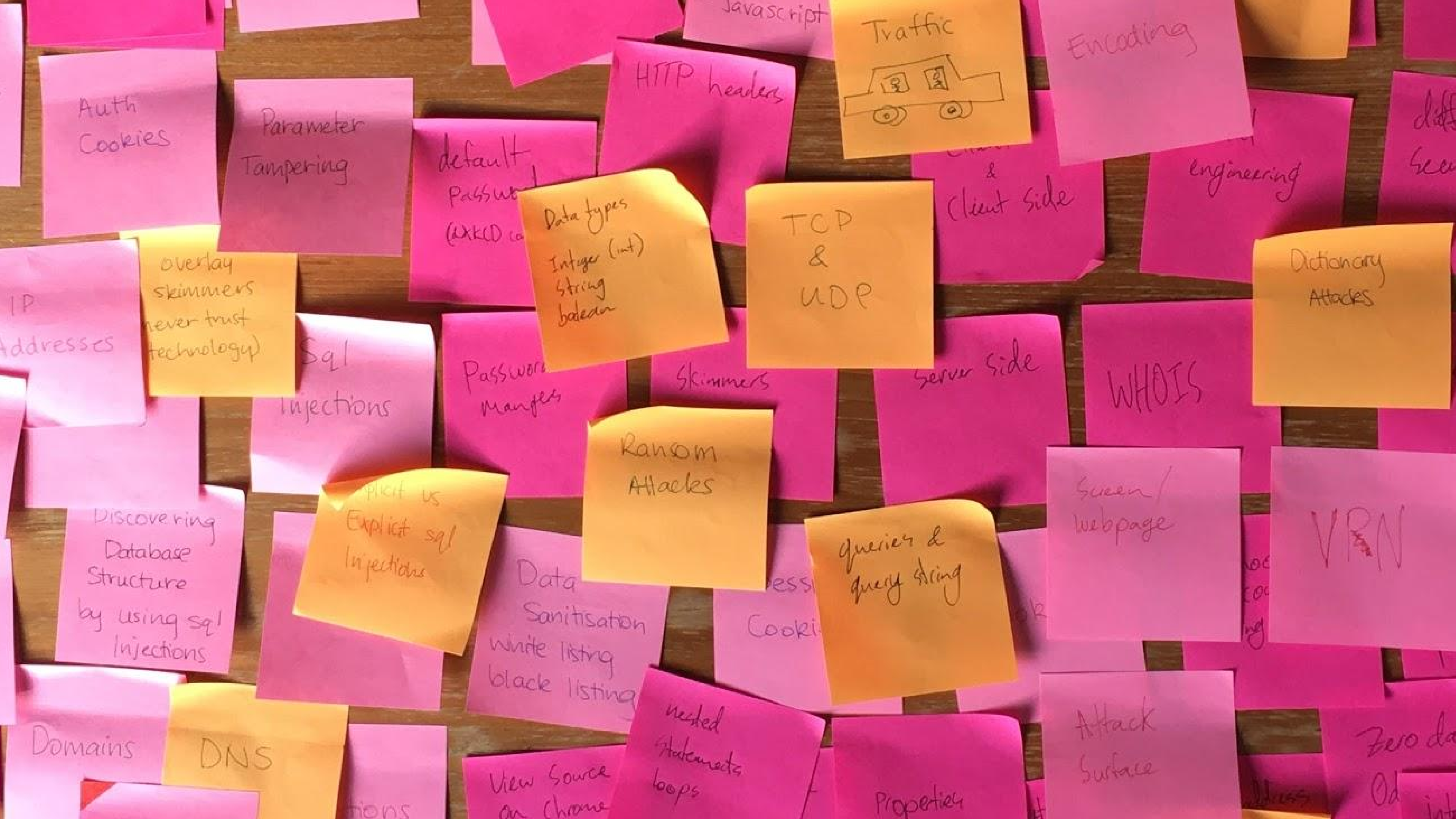
- ✓ READ A SECURITY BLOG
- ✗ SELECT AND READ A BOOK RELATED TO SECURITY TESTING
- ✓ USE A SECURITY TOOL - EXAMPLES: ZAP OR BURPSUITE
- ✓ LEARN ANYTHING ABOUT VULNERABILITY SCANNING
- ✓ LEARN ABOUT THREAT MODELLING (I.E. LIKE THE STRIDE MODEL)
- ✓ EXPLORE THESE SITES: GOOGLE GRUYERE; HACKYOURSELF FIRST; TICKET MAGPIE; THE BODGEIT STORE
- ✓ LEARN ONE OR MORE THINGS ABOUT PENETRATION TESTING
- ✓ USE A PROXY TOOL TO OBSERVE WEB TRAFFIC IN A WEB OR MOBILE APPLICATION
- ✗ DISCOVER THE PROCESS AND PROCEDURES AROUND SECURITY AUDITING
- ✓ READ AND LEARN ABOUT ETHICAL HACKING
- ✗ TRY TO FIGURE OUT THE POSTURE ASSESSMENT FOR AN APPLICATION
- ✓ READ ABOUT SECURITY TESTING AND DISCUSS WHERE IT BEST FITS IN AN SDLC
- ✗ PERFORM A SECURITY ANALYSIS FOR REQUIREMENTS IN A STORY
- ✗ DEVELOP A TEST PLAN INCLUDING SECURITY TESTS
- ✗ WRITE AND SHARE IDEAS FOR SECURITY TESTING VIA TWITTER OR A BLOG
- ✗ RESEARCH HOW TO BUILD A TIGER BOX
- ✓ RESEARCH A RECENT HACK/SECURITY BREACH
- ✓ LEARN ABOUT SECURITY HEADERS
- ✓ RESEARCH SCRIPT KIDDIES AND/OR PACKET MONKEYS
- ✓ READ ABOUT DOS/DDOS ATTACKS. SHARE EXAMPLES/STORIES VIA SOCIAL MEDIA
- ✓ READ ABOUT NETWORK VULNERABILITY AND APPLY IT TO YOUR TECH STACK
- ✓ READ ABOUT SYSTEM SOFTWARE SECURITY AND APPLY IT TO YOUR TECH STACK
- ✓ WHAT ARE THE TOP 10 SECURITY THREATS OF 2016?
- ✗ USE A SUGGESTION FROM THE OWASP WEB APPLICATION SECURITY CHECKLIST
- ✗ FIND AND USE A MOBILE SECURITY TOOL
- ✗ COMPARE AND CONTRAST, ON SOCIAL MEDIA, WEB AND MOBILE SECURITY TESTING
- ✓ HOW COULD BYOA (BRING YOUR OWN APPLICATION) PLAY A PART IN SECURITY?
- ✗ SHARE SECURITY TESTING IDEAS FOR SPECIFIC DOMAINS
- ✓ RESEARCH SECURITY REGULATIONS REGARDING A SPECIFIC DOMAIN
- ✓ DISCOVER THE DIFFERENCE BETWEEN WHITE, GREY, AND BLACK HAT HACKING
- ✓ Bonus: Give a talk

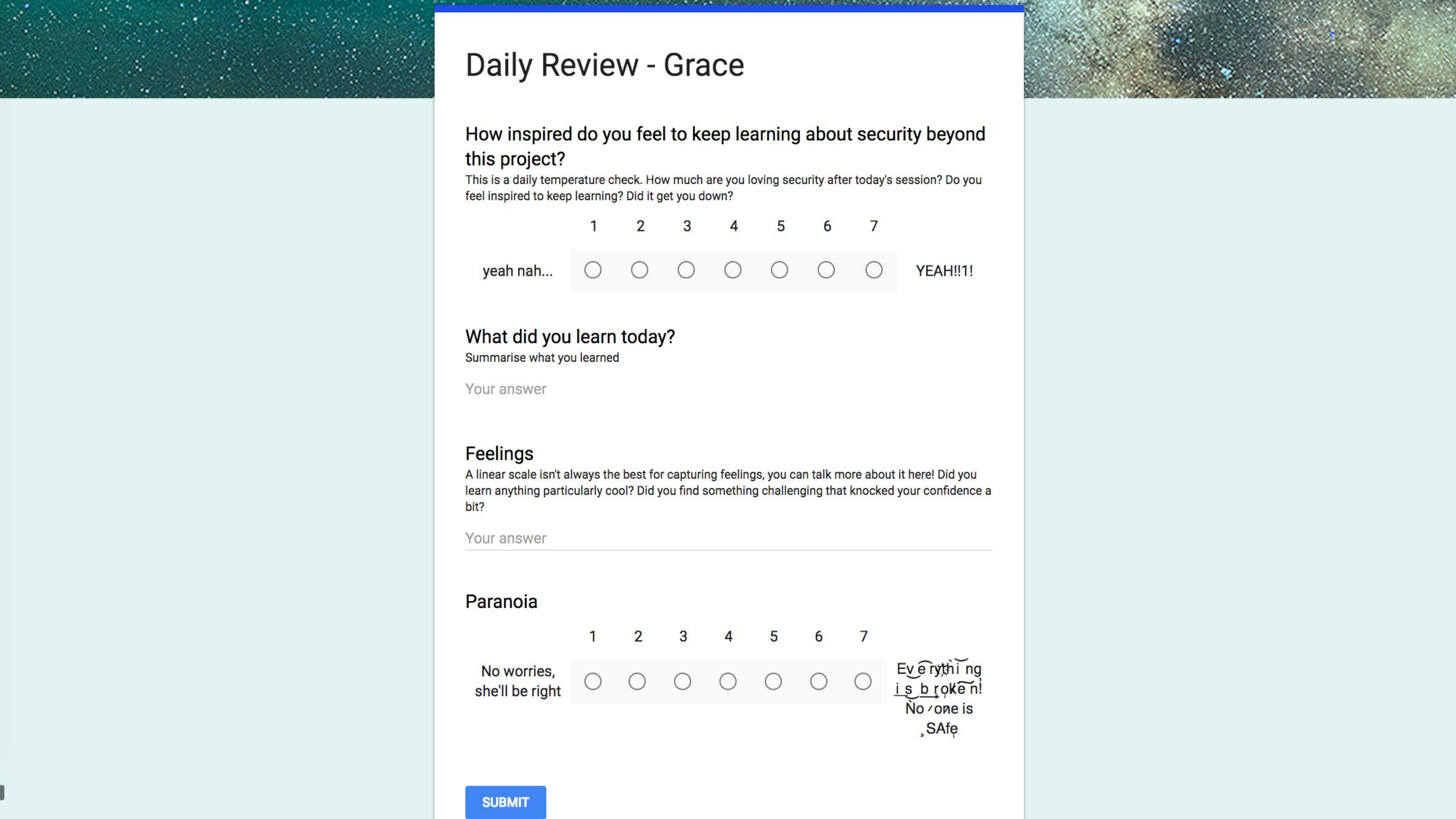
MINISTRY OF TESTING

MINISTRYOFTESTING.COM

Stop


Bluetooth
Shodan
ip addresses, basic networking fire walls
Hidden
NAT
Zap & Vuln scanning
HTTP vs HTTPS
GET & POST Requests
HTTPOnly cookies & being able to hide them from the browser
Cookie Attributes
Key, Value Pairs
getting info from error pages
ISPs & handling traffic sink holes for DDos attacks
RSA encryption (two prime numbers
Tor
XXS Cross Site Scripting
MITM attacks
DDos Attacks
Sniffing packets
base 64 base 16 base 10 base 2
2FA
OSI Model
Security through obscurity
Salting & hashing
Phishing
Plain text
Pwned
The Cloud & Amazon aws & server farms
scrawlers
Patches
Fuzz Testing
special characters escape characters
Creating Risks Profiles
IOT
Websites make up - CSS - HTML - Javascript
& Variables
Binary vs Linear
Audits
Traffic
Encoding
one step at a time
Blue & Red teams in security
Auth Cookies
Parameter Tampering
default passwords (XKCD
HTTP headers
& Client side
engineering
different Security
Alpha nerds & contempt culture
Principle of least priviledge
IP Addresses
overlay skimmers never trust technology)
Sql Injections
Data types Integer (int) string boolean
TCP & UDP
Dictionary Attacks
Password manager
Skimmers
Server side
WHOIS
Verb tampering
Discovering Database Structure by using sql Injections
Explicit vs Explicit sql Injections
Ransom Attacks
queries & query string
Screen/ webpage
VPN
Application Posture
Hidden Fields on pages
Data Sanitisation white listing black listing
Cooki
ethical hacking
Domains
DNS
Priviledges Admin & Root
View Source on Chrome
nested statements loops
Properties
Attack Surface
Zero day
focused & Diffuse mode thinking
Interpreters compilers
& MAC Addresses
Disadvantages of
something you have
Incognito Mode in Chrome
User Agents
Reflected Data
Paths
different types of malware
Adware Spyware Viruses trojans worms Ransomware


Javascript
Traffic
Encoding
Auth Cookies
Parameter Tampering
default passwo (XKCD co
HTTP headers
Data types Integer (int) String boolean
TCP & UDP
& Client side
engineering
diff Secu
IP Addresses
overlay skimmers never trust technology)
Sql Injections
Password manager
Skimmers
Server side
WHOIS
Dictionary Attacks
Ransom Attacks
plicit vs Explicit sql Injections
Discovering Database Structure by using sql Injections
Data Sanitisation white listing black listing
Sessi Cooki
queries & query string
Screen/ webpage
VPN
Attack Surface
Zero da Od
Domains
DNS
tions
View Source on Chrome
nested Statements loops
Properties



Daily Review - Grace

How inspired do you feel to keep learning about security beyond this project?

This is a daily temperature check. How much are you loving security after today's session? Do you feel inspired to keep learning? Did it get you down?

	1	2	3	4	5	6	7	
yeah nah...	○	○	○	○	○	○	○	YEAH!!1!

What did you learn today?

Summarise what you learned

Your answer

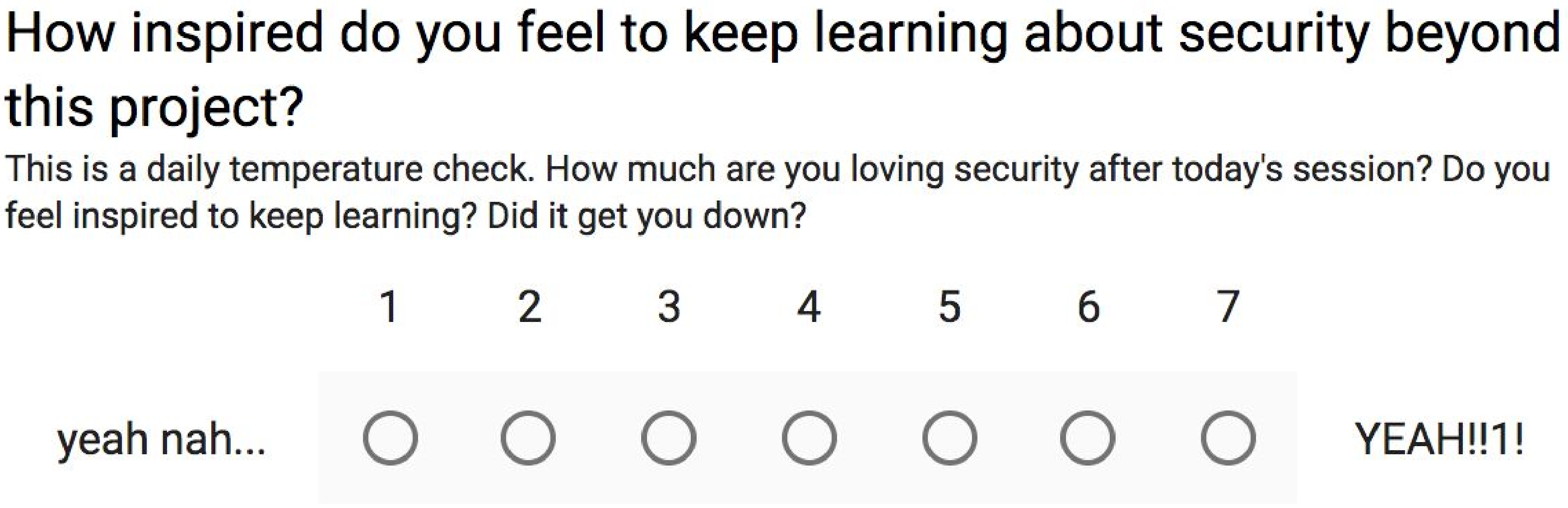
Feelings

A linear scale isn't always the best for capturing feelings, you can talk more about it here! Did you learn anything particularly cool? Did you find something challenging that knocked your confidence a bit?

Your answer

Paranoia

	1	2	3	4	5	6	7	
No worries, she'll be right	○	○	○	○	○	○	○	Everything is broken! No one is SAfe

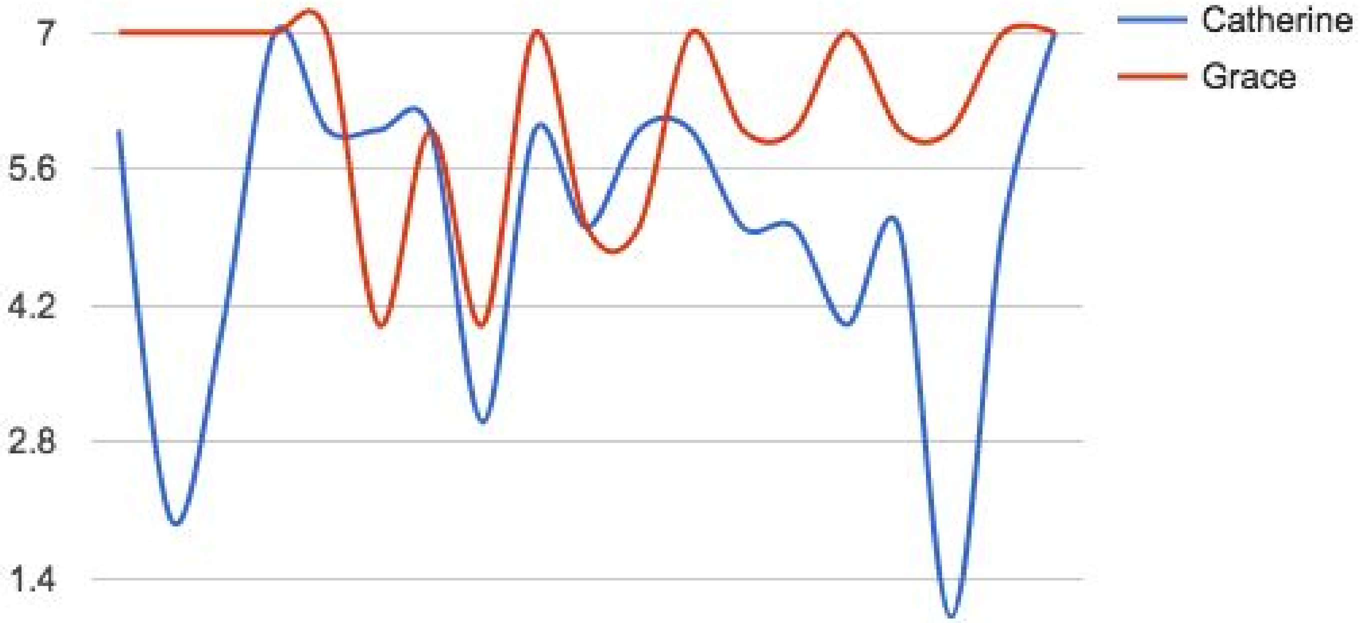


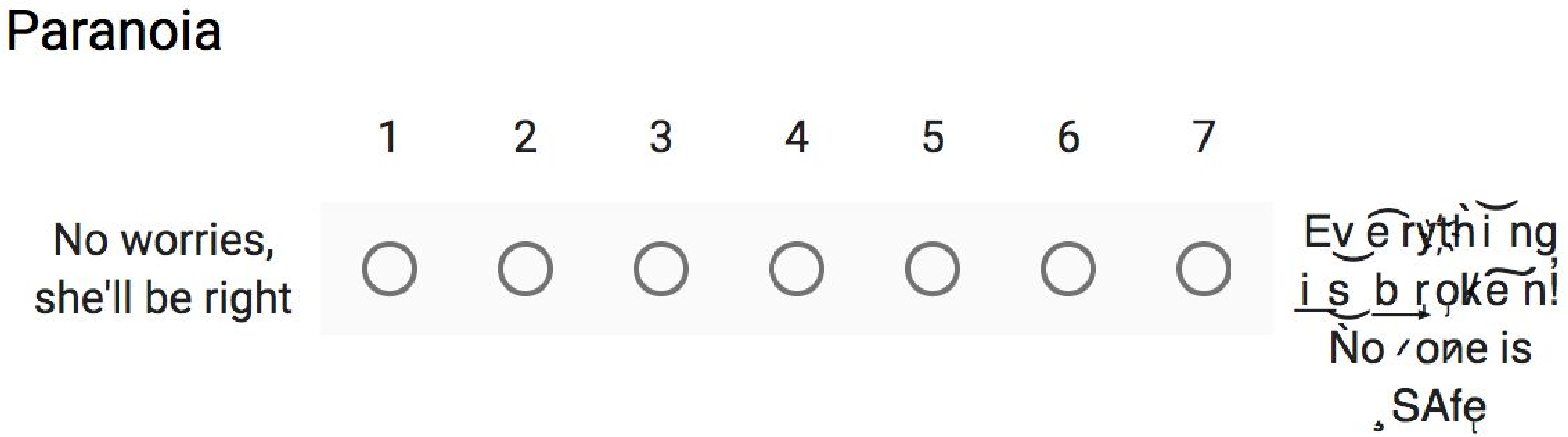
How inspired do you feel to keep learning about security beyond this project?

This is a daily temperature check. How much are you loving security after today's session? Do you feel inspired to keep learning? Did it get you down?

	1	2	3	4	5	6	7	
yeah nah...	○	○	○	○	○	○	○	YEAH!!1!

How inspired do you feel to keep learning about security beyond this project?

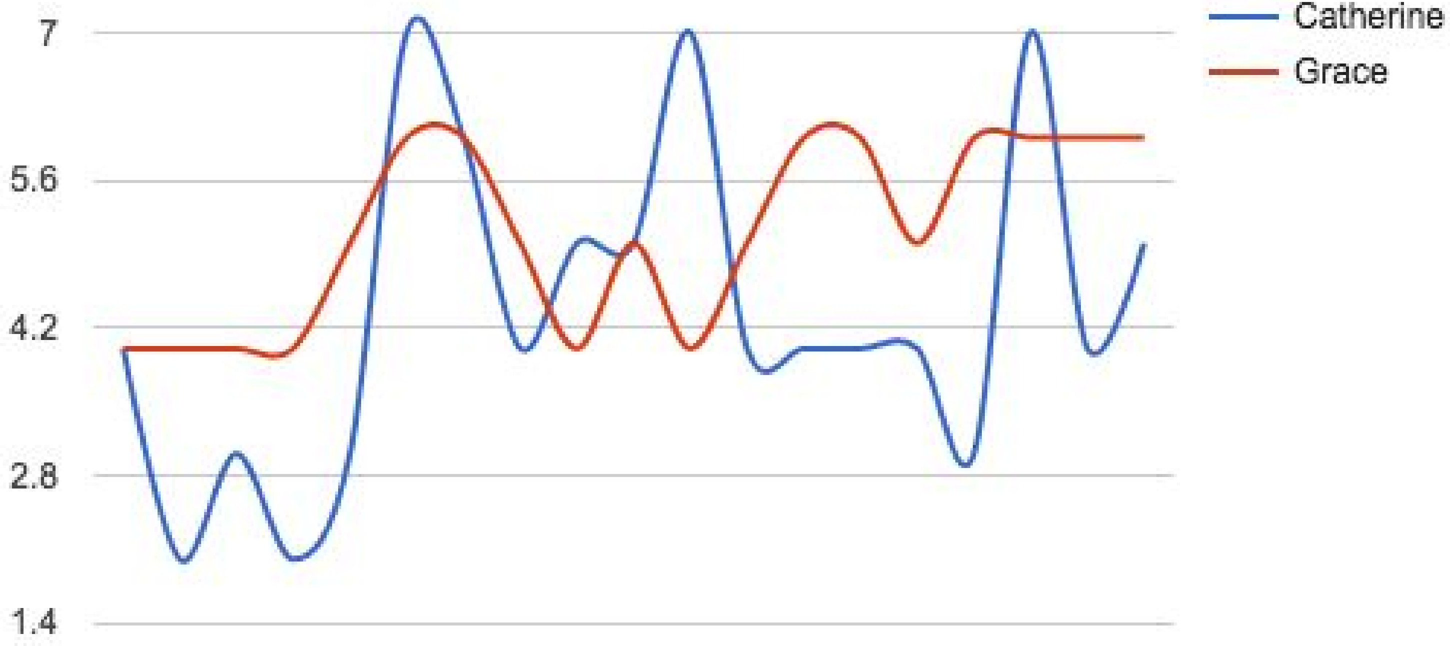




Paranoia

	1	2	3	4	5	6	7	
No worries, she'll be right	○	○	○	○	○	○	○	Everything is broken! No one is SAfe

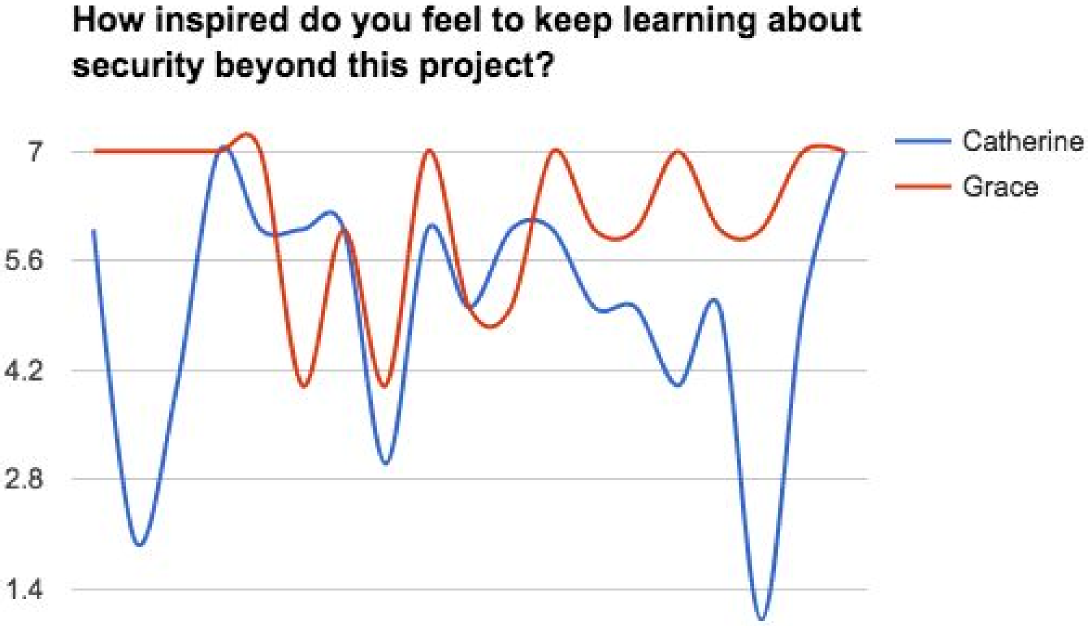
Paranoia



Advice for Mentees

It’s okay to feel embarrassed

Expect dips in interest, it’s normal



Seek real life success stories

Communicating with mentor about things that are too complicated

Don’t be put off by the haters

Advice for Mentors

Set expectations
# (#1 reason why people get mad)

Be flexible, allow for tangents and to pursue curiosity

If you don’t know the answer to a question, or you’re a little fuzzy, then look it up together

Don’t assume anything about what your mentee knows or has learned

Don’t jump in to save the day

Celebrate learnings!

Think about the cultural context of your mentee

tl;dr:

- ✌ □ 30 Days of Security Testing
- 👌 Hack Yourself First by Troy Hunt
- 👍 Interviews
- 💪 News articles

✨THANK YOU✨

Catherine.McIlvride@assurity.co.nz
hello@gracenolan.me

@GracieNoLag

Thank you to:

⭐ Pipes ⭐ Lily ⭐ Erica ⭐ @nzkarit ⭐ Kirk / Kim / OWASP ⭐ Assurity ⭐ Enable ⭐