RiskBased SECURITY

Screw Being A Pentester - When I Grow Up I Want To Be A Bug Bounty Hunter

Jake Kouns
@jkouns
Chief Information Security Officer (CISO)
Risk Based Security

Carsten Eiram
@CarstenEiram
Chief Research Officer (CRO)
Risk Based Security

Community offerings:

OSVDB

SECore beta .info

DATALOSS db open security foundation

MY PRIVACY AUDIT

Commercial offerings:

VulnDB Risk Based Security

Cyber Risk Analytics

YOUR CISO Risk Based Security

Information Security: Career Decisions

IT Security Career Choices!

IT Security Career Choices – Blue vs. Red!

IT Security Career Choices – Red Team!

Pentester – Good Things About Red Teams

RiskBased SECURITY

- Constant learning opportunities
- Get to play and break things
- Generally well-paid
- Sometimes all options are open (e.g. Social Engineering)
- Getting root feels amazing; nothing better than winning!

Red Teams = Pentester

RiskBased SECURITY

- Red teams are typically thought of as pentesters
- Seems like security companies are constantly looking for pentesters!
  - Searching Indeed.com only shows 17 jobs for "pentesting" currently.

Pentester - Painful At Times?

RiskBased SECURITY

- Usually work for a company i.e. deal with company politics.
- Test during specific hours
- Write long reports no one reads to ensure they're seen as "valuable"
- Deal with clients (SOW, present findings, conference calls, etc.)

RiskBased SECURITY

Also the option of becoming an independent pentester!

Don't have to work for "the man", but work time breakdown is roughly:

- 1/3 actual pentesting (fun)
- 1/3 administrative tasks and documentation
- 1/3 being a sales weazel (finding clients!)

Is There A Better Career Choice?

Bounty Hunters

Bounty Hunters

Quick Overview To Set The Bug Bounty Stage

Research Motivation – Old Skool

- **Reporting vulns to vendors looked good on CV and got you credited in vendor advisories.**
- **Unemployed researchers could get jobs in the industry, turning a hobby into a (profitable) professional gig.**
- **Employed ones could get better jobs / higher salary. This still applies today!**

Reporting vulnerabilities to vendors back in the day (and sometimes today) was often a hassle!

Researchers would instead find alternatives...

Research Motivation – Old Skool

- Just publish somewhere to get social recognition, fame, and glory
- Trade / give away for goodwill and respect
- Use offensively for fun – or profit
- Store in a digital box somewhere and move on
- Or.....

Research Motivation – Old Skool

Some Early Bounties

- Some vendors / security companies realize that rewarding discoveries is an incentive for researchers to report their findings.
- August 2002, iDefense creates VCP (Vulnerability Coordination Program)
- August 2004, Mozilla creates their bug bounty program, paying USD 500 for critical bugs

In what year was the first bug bounty program started?

October 1995

Who started the first bug bounty program started?

Netscape – October 1995

- Netscape actually launched the Netscape Bugs Bounty back in October 1995 to improve the security of their products.

- Interestingly, their approach was to offer cash for vulnerabilities reported in the latest beta
  - Wanted to incentive researchers to help secure it before going into stable release
  - Not unlike part of Microsoft's bounty program today.

Full Disclosure

- 2000 - 2008 disclosure was a huge battle ground between vendors and researchers
- Researchers still had problems getting vendors to respond...
- Perception (true or not) was that vendors only fixed bugs when dropped
- Researchers were hardcore Full Disclosure the ”right” way
  - Importance placed on getting bugs fixed / improving security

Pwn2Own – A Bug Bounty Contest

- Created in 2007 for CanSecWest
  - Chance to win x2 Macbook Pro and USD $10k from ZDI
- Big money on the line in 2010
  - Total cash prize pool of USD $100,000
- Competition brings lots of PR and growing cash incentives

No More Free Bugs

- In March 2009 at CanSecWest, researchers announce their new philosophy: ”No More Free Bugs”.
- It’s not really clear how much effect this had
- At least sparked a debate about the issue, and made (some) researchers’ expectations of monetary compensation more publicly known.


Bug Bounties become
all the rage!

Type Of Bugs Bounties & Awards

- Company run bug bounties
- 3rd party bug bounties
  - ZDI
  - iDefense VCP
- Competitions
  - pwn2own
- Crowd-sourced programs
  - Bugcrowd
  - HackerOne
  - CrowdCurity
  - Synack
  - More!?

- Cash
- Prizes
  - Tshirt
  - Mug
  - Conferences
- Fame and glory
- Appreciation

Company Run Bug Bounties

Company Run Bug Bounties

- Bounties that are run by the company owning the website or software.
  - Facebook
  - Yahoo!
  - Paypal
  - AT&T
  - Google
  - Mozilla
  - cPanel
  - Microsoft
- In almost all cases, reporting and coordination is directly with the company and not through intermediaries.

Company Run Bug Bounties

RiskBased SECURITY

- The number of bug bounty programs continues to grow!
- We maintain a list of bounty programs for our research:
  - ~300 documented programs
  - ~260 have some type of reward
  - ~165 provide recognition with a hall of fame
  - ~75 have some type of monetary reward
- BugCrowd has a nice crowd sourced public list:
  - https://bugcrowd.com/list-of-bug-bounty-programs

Company Run Bug Bounties - Google

- Google started providing bounties in 2010
- Continues to be one of the more serious vendor bounties
  - Big reason bounties took off (Pwnium 4 announced **USD 2.7M** in prizes)
  - In Aug 2013 Google had paid out >$2 million in rewards for >2,000 valid reports
  - Offer bounties for other software
- They also continue to push for bugs getting fixed and disclosed in a timely manner.

Company Run Bug Bounties - Facebook

This program rewards high quality security research from the community that helps make Facebook more secure.

TARGETS:

Anything that could compromise the integrity of people's data, circumvent the privacy protections of people's data, or enable access to a system within our infrastructure is fair game.

BOUNTIES:

Program Founded: July 2011

Over 1,500 bounties have been paid out.

RESEARCHERS:

600+ unique researchers paid USD

Paid researchers in 79 countries. The top countries by number of researchers are India (147), USA (109), and UK (30).

Company Run Bug Bounties - Facebook

- Average Bounty Amount: In the low thousands
- $500 is our minimum, and don't have maximum set.
- Largest bounty was $33,500. You can read more about that payout here: https://www.facebook.com/BugBounty/posts/778897822124446.
- More details: https://www.facebook.com/whitehat

Facebook $1.5M In 2013

Topic: Social Enterprise Discover Follow via:

Facebook doled out $1.5M in bug bounty rewards in 2013

Summary: *Facebook received 14,763 bug submissions in 2013, a whopping 246 increase in one year.*

Facebook received 14,763 bug submissions in 2013, a whopping 246% increase in one year.

Only 687 were deemed valid and eligible to receive financial compensation.

Only 4.65% valid!

The world's la
the security re
showed no sign of waned interest last year.

For starters, Facebook received 14,763 bug submissions in 2013, a whopping 246 increase in one year.

The Menlo Park, Calif.-based company first launched its bug bounty program back in 2011.

The guidelines for submission a
Facebook itself.

The minimum reward amount is $500, and there is no maximum reward or ceiling.

nfrastructure:

- Facebook details two years of work to turn on default HTTPS
- Facebook explains how 'TAO' es social workloads, data sts
- ook devs explain how it maps user connections to other 'entities'
- Facebook translates natural language interface under Graph

Hold Outs

Third Party Bounties

Third Party Bug Bounties

- Bounties that are run by the other companies that do not own the software.
  - Typically is not for site specific or websites.
- They use the information to share with their customers or include in their own security products.
- In almost all cases, reporting and coordination is directly with the company running the bounties and not with the software vendor.

Third-party Bug Bounty Providers - ZDI

Founded: August 15, 2005 (10th year!)
Located: Austin, TX

TARGETS:

The research is focused on critical vulnerabilities in programs widely used in global enterprises, critical infrastructure, and the general computing community.

BOUNTIES:

While the Zero Day Initiative does offer a bug bounty, and is, as such, a "bug bounty program," the focus of our program is to foster an extended security research organization focused on responsible disclosure of vulnerabilities to and with vendors.

RESEARCHERS:

There are 3,000+ independent researchers registered to contribute to the ZDI.

Nearly 100 countries. US, UK, India, Germany, and France are the top 5 countries.

Unknown unique researchers paid USD

- Number of bounties paid posted online (1,715 by July 18th 2014):
  - http://www.zerodayinitiative.com/advisories/published/
- Average Bounty Amount: Unknown
- The ZDI has paid bounties ranging from three figures to six figures for vulnerabilities/exploits in the past.
- Extra monetary rewards etc. for ”return business”.

Third Company Providers – iDefense

- Does iDefense VCP still exist?
- Nothing published since October 2013?
- Submission form is still available, but don't waste your time… they've become irrelevant

Third-party Bug Bounty Providers - EIP

Founded: June 2012
Located: Austin, TX

TARGETS:

Critical and actually exploitable vulnerabilities in most major/widely deployed software.

BOUNTIES:

Unknown. They do not disclose such information about their program.

RESEARCHERS:

Unknown. They do not disclose such information about their program.

Third-party Bug Bounty Providers - EIP

- Information about the program is available at:
  - https://www.exodusintel.com/eip
- “We intend to ensure our offers are more than competitive when compared to other such programs. “
- Yearly bonuses with top 4 researchers being awarded $20,000 USD each as well as invitations to collaborative hacking events.

Third Company Providers – Pointers

- Make sure you're clear on what software they are likely to accept.
- Split each vulnerability (root cause – not attack vector) into a separate report.
- Include as many confirmed (no guesswork) details about the vulnerability as possible.
- Provide trimmed down PoCs and/or exploits.
- Clearly list tested software and versions as well as where to obtains trials etc.

Crowd-sourced Bounties

Crowd-Sourced Bounties

- Companies sign up with the service and they offer bounties through their platform
- Bounties are opened up to all researchers registered on the service's platform
- Validation of bug submission and bounty payments handled via the service
- Starting to see a blur between traditional bug bounties and pentesting / red team testing
  - Remove the sales aspect if you want to do independent pentesting

Bugcrowd Details

Founded: September 2012
Located: San Francisco, CA

TARGETS:

Web, mobile, client-side and embedded (IoT) applications.

Also introduced Flex, which is a crowd-sourced penetration test.

BOUNTIES:

23 public are currently active, and a number of private programs.

170 programs to various stages have been run.

57 companies since Oct ‘13.

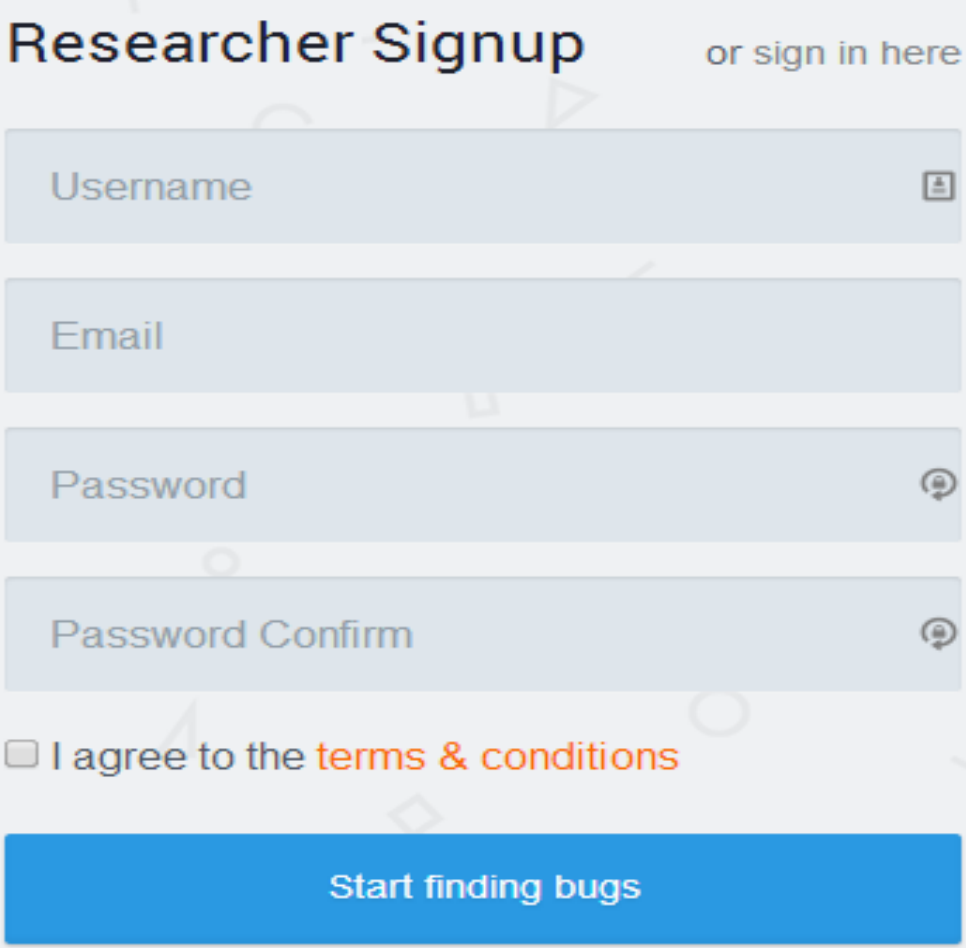
RESEARCHERS:

Over 10,000 researchers have signed up.

Researchers from around the world.

231 unique researchers paid USD

BugCrowd Sign-up Process

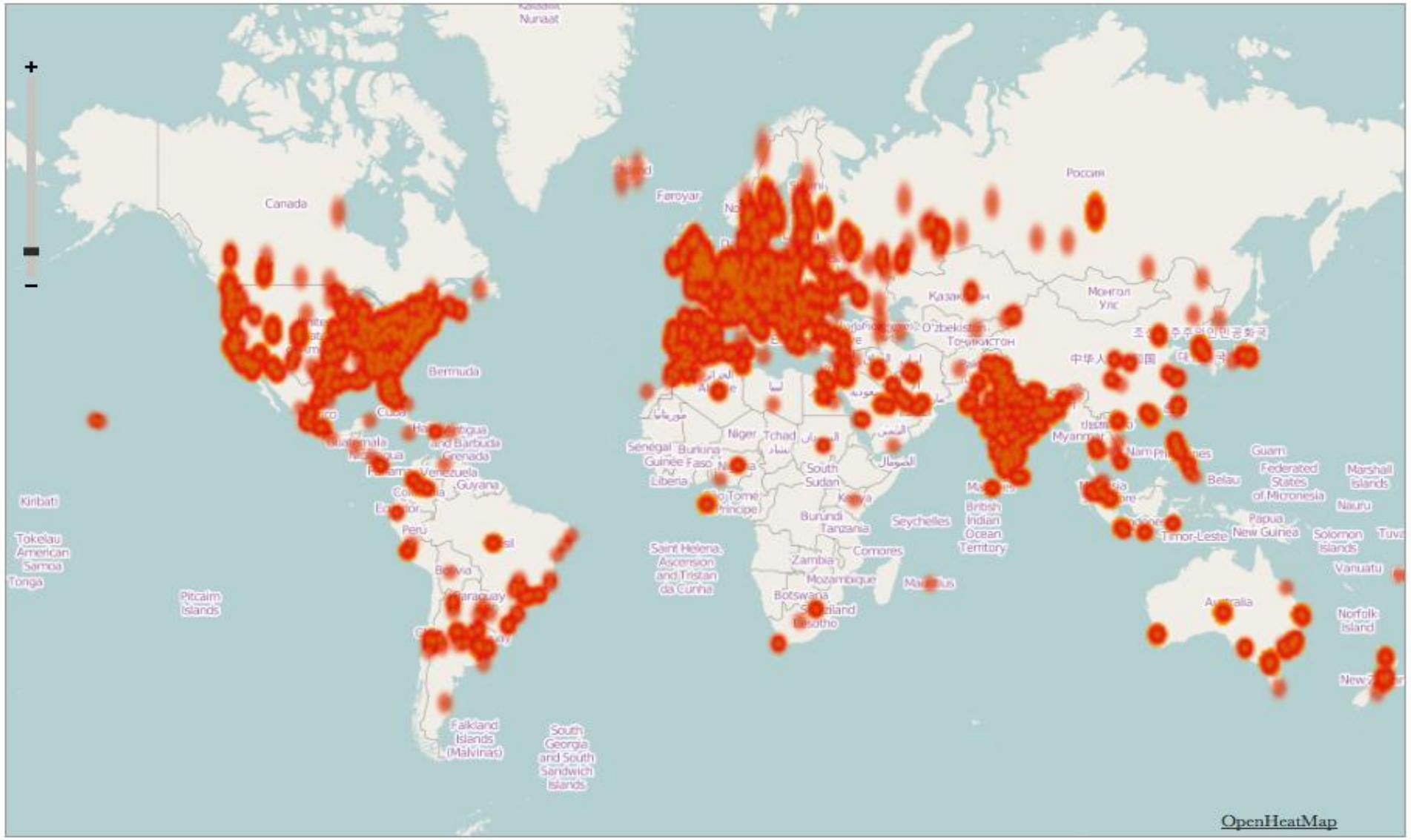


Bugcrowd Details

- 1,062 bugs since November 2012
- Average Bounty Amount: USD $241
  - Pay out primarily through PayPal, with rare exceptions made where with Western Union, wire transfer, and bitcoins.
  - Average time to process a submission (from submit to paid) is 2-6 weeks
- Largest single payout was USD $13,500.

Bounty Hunter Details

Bugcrowd Researcher Locations



Bugcrowd – Leaderboard & Kudos

RiskBased SECURITY

The Leaderboard

These guys kick ass and chew bubblegum. And they're all out of gum.

June / All Time

1st	sandeepv	150
2nd	mazen160	148
3rd	chmosama	136
4th	S_venkatesh	81
5th	karthickumar	77
6th	vineet	76
7th	Anonymous	72

Bugcrowd – Money vs. Kudos

OJ @TheColonial · 2h

Top 9 "bounties". Notice the "You are not participating" -- see if you can guess why. #nomorefreebugs /cc @Bugcrowd pic.twitter.com/FNdxJv3WCO

Details Reply Retweet Favorite More

Anshuman Bhartiya

@anshuman_bh

Follow

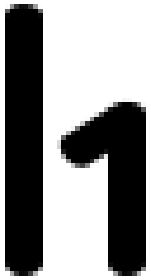
@TheColonial @justinsteven @Bugcrowd totally with you on that mate. Too many bounties with no bounty

Reply Retweet Favorite More

FAVORITE 1

6:19 PM - 21 May 2014

HackerOne Details



Founded: September 2013
Located: San Francisco, CA

TARGETS:

The bounties run by individual response teams can be focused on whatever software target the response team wants to be tested.

BOUNTIES:

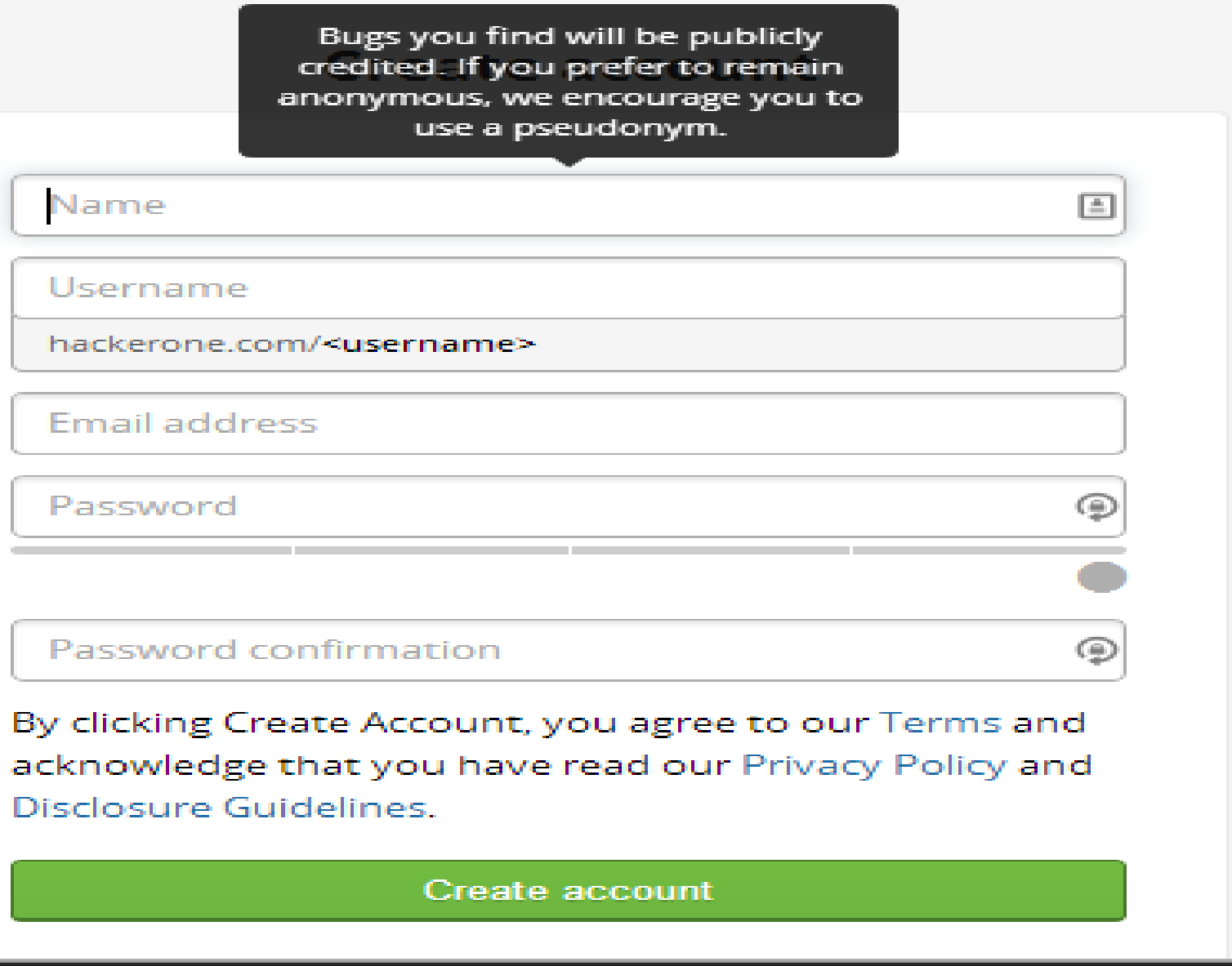
- 63 security teams currently run a public program on the HackerOne platform
- Many other teams currently running with a private soft launch program

RESEARCHERS:

Thousands of researchers have registered and over 800 researchers have submitted a valid finding leading to a bounty or recognition on a Hall of Fame.

Unknown # unique researchers paid USD

HackerOne Sign-up Process

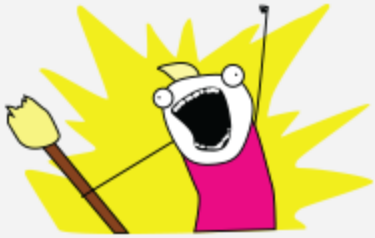


HackerOne Details

- 1,347 bugs have been paid.
- Average Bounty Amount: $677.67
- Largest single payout was $15,000.
- Multiple $15,000 bounties have been awarded through the platform.
  - One of these was the Internet Bug Bounty's $15,000 heartbleed reward, donated to charity by Neel Mehta.
  - Other $15,000 bounties were from Yahoo.

HackerOne – Internet Bug Bounty

RiskBased SECURITY

SANDBOX Sandbox Escapes	 The Internet	Flash Flash
 Python	 Ruby	php PHP
django Django	 Ruby on Rails	Perl Perl

HackerOne – Internet Bug Bounty

Some of the most critical vulnerabilities in the Internet's history have been resolved thanks to efforts of researchers fueled entirely by curiosity and altruism. We owe these individuals an enormous debt and believe it is our duty to do everything in our power to demonstrate how much this research is appreciated. To that end, the Internet Bug Bounty Panel will award public research into vulnerabilities with the potential for severe security implications to the public.

Simply put: hack all the things, send us the good stuff, and we'll do our best to reward you.

The Fine Print

To qualify, vulnerabilities should meet most of the following criteria:

- Be vendor agnostic: vulnerability is present in implementations from multiple vendors or a vendor with dominant market share. **Do not send us vulnerabilities that only impact a single website.**
- Be widespread: vulnerability manifests itself across a wide range of products, or impacts a large number of end users.
- Be severe: vulnerability has extreme negative consequences for the general public.
- Be novel: vulnerability is new or unusual in an interesting way.

The Panel will gladly assist with the coordinated disclosure of any potential vulnerabilities. However, we recognize that we may not be the most effective avenue in all circumstances. We will gladly consider rewards for vulnerabilities that have been publicly disclosed through some other means, provided they adhered to our disclosure guidelines.

It's important to keep in mind that not all submissions will qualify for a bounty. The decision to award

Report bug

$5,000
Minimum bounty

$9,500
Paid to hackers

3
Hackers thanked

3
Bugs closed

Top Hackers

markus
1 bug

Sandbox Escape

Bounties provided by IBB

The Internet Bug Bounty is issuing rewards for sandbox escapes - techniques that allow vulnerabilities to escape popular application sandboxes. The specifics of these techniques will differ between implementations but typically manifest as a kernel vulnerability, broker vulnerability, or logic error.

Qualifying Application Sandboxes

- Chrome (for any sandboxed process types including renderers, Pepper Flash and NaCl)
- Internet Explorer 10 EPM
- Adobe Reader (sandboxed in X and newer)
- Adobe Flash

Qualifying Operating Systems

- Windows 7+
- Linux, latest upstream version
- OSX, latest release

Additional Guidance

- Qualifying vulnerabilities must reliably demonstrate the ability, or likely ability, to escape one of the defined sandboxes. Demonstrating full exploitation is helpful but not necessarily required to qualify.
- Implementation bugs in these sandboxes themselves are not in scope and should be reported directly to the appropriate vendor. Your submission should include why you believe the bug is external to the application itself (e.g., a kernel bug).
- The Panel is a group of your peers serving as volunteers. They have limited amount of free time to

Report bug

$5,000
Minimum bounty

$23,000
Paid to hackers

4
Hackers thanked

6
Bugs closed

Top Hackers

datuzi
1 bug

CrowdCurity Details

CrowdCurity
Crowdsourced Security Testing

Founded: July 2013
Located: San Francisco, CA

TARGETS:

Web application security, with a focus on bitcoin.

BOUNTIES:

45 are currently active

90 programs have been run all time.

50 - 100 companies have used the platform.

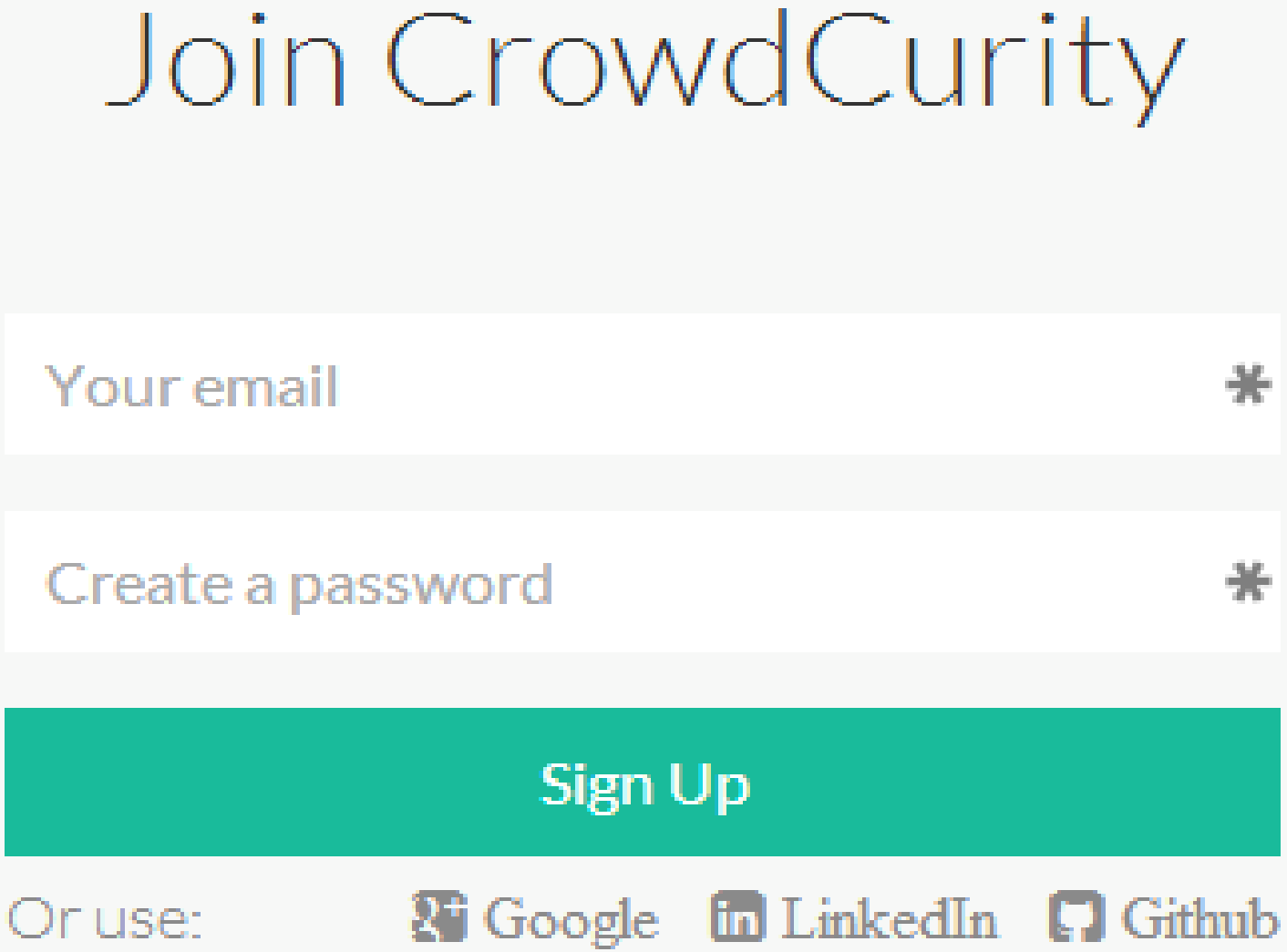
RESEARCHERS:

1,300 researchers have signed up with 300 – 400 being active.

Researchers from India, European countries (UK, Germany, Sweden), Malaysia, US.

~100 unique researchers paid USD

CrowdCurity – Sign-up Process



CrowdCurity Details

CrowdCurity
Crowdsourced Security Testing

- ~800 bugs have been paid
- Average Bounty Amount: $150
  - Standard package is $50, $300, $1,000 (low, medium, high)
  - Super package is $100, $500, $2,000 (low, medium, high)
- Largest single payout was $1,500.

CrowdCurity – Hall of Fame

jkouns

- Dashboard
- Payouts (0)
- Vulnerabilities
- Live Programs
- Tester Top 20
- Login Settings
- My Profile

Hall of Fame - CrowdCurity

		Score
1.	 bitquark	288
2.	 satishb3	252
3.	 cyberboy	138
4.	 reegun	137
5.	 igbuend	109

CrowdCurity – Tester of the Week

Mohit

From: India

I am a Security Researcher from India having curious mind in Cyber security and interested in Web Application Security and Programming
I love to play around security and breaking them too

15	4.2	51
Rank	Report Quality	Score

View original

Flag media

CrowdCurity @CrowdCurity 17s
This week, meet @amohitgupta1, our CrowdCurity Tester of the Week: j.mp/1z8iTIN #bugbounty pic.twitter.com/U1PxVL6J1X
Details

Synack Details

Founded: January 2013
Located: San Francisco, CA

TARGETS:

Synack is not a managed bug bounty provider.

Synack is focused on application vulnerabilities across web and mobile, along with host-based network infrastructure.

BOUNTIES:

Only runs paid engagements with customers and does not offer unpaid programs.

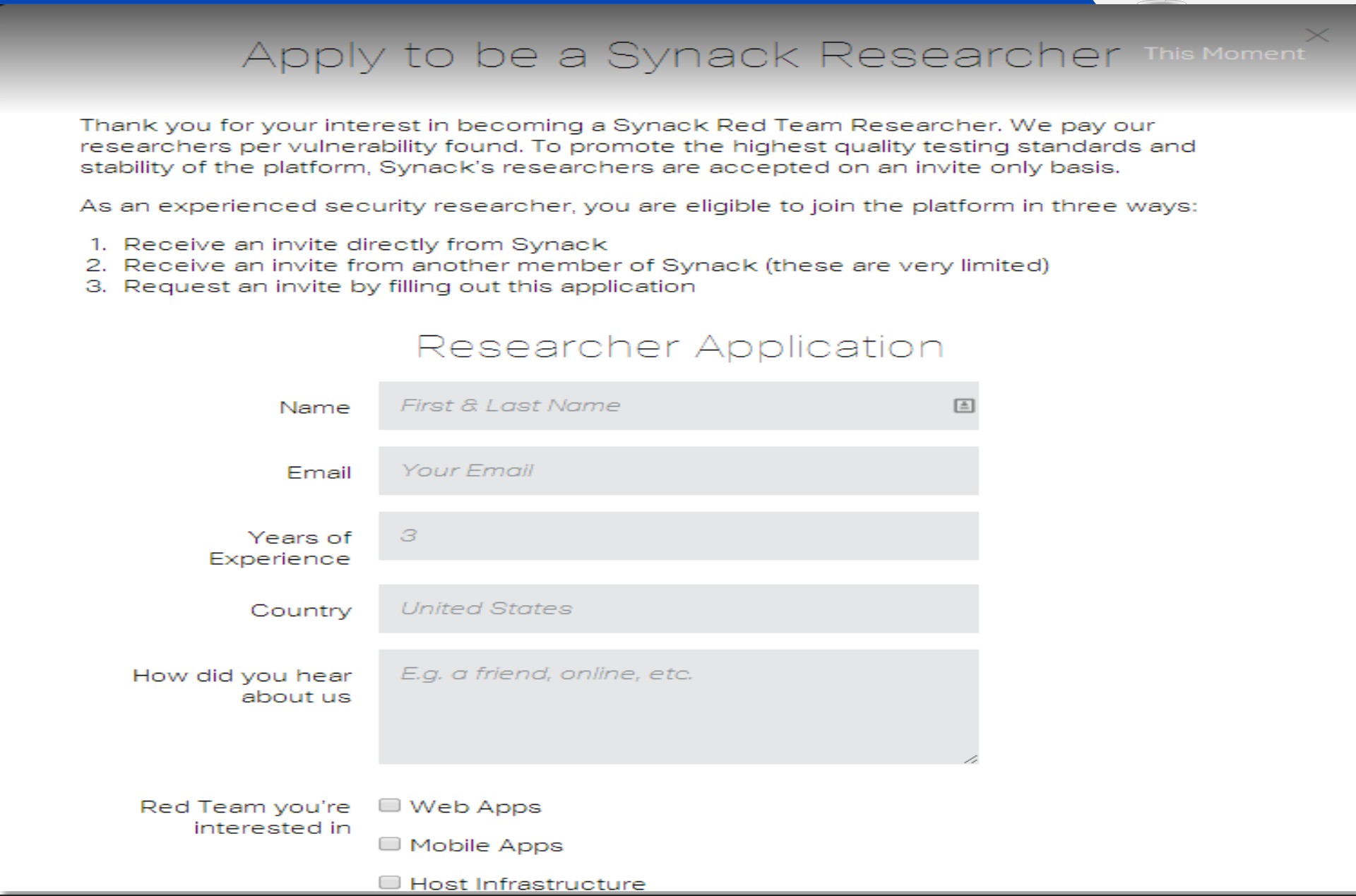
Unknown number of clients

RESEARCHERS:

Unknown number of researchers and how many unique paid USD

Approximately 40% of Synack researchers are US-based, with the remaining spread across 21 countries around the world, spanning 6 continents.

Synack Sign-up Process



Apply to be a Synack Researcher

This Moment

Thank you for your interest in becoming a Synack Red Team Researcher. We pay our researchers per vulnerability found. To promote the highest quality testing standards and stability of the platform, Synack's researchers are accepted on an invite only basis.

As an experienced security researcher, you are eligible to join the platform in three ways:

1. Receive an invite directly from Synack
2. Receive an invite from another member of Synack (these are very limited)
3. Request an invite by filling out this application

Researcher Application

Name — *First & Last Name*

Email — *Your Email*

Years of Experience — *3*

Country — *United States*

How did you hear about us — *E.g. a friend, online, etc.*

Red Team you're interested in

- ☐ Web Apps
- ☐ Mobile Apps
- ☐ Host Infrastructure

Synack Sign-up Process

Synack Details

- Number of payouts: Unknown
- Average Bounty Amount: Unknown
  - Bounties scale, given the severity and impact, and are normalized across customer base.
  - Most payouts range from USD $100 to $5,000 (no upper limit)
- Largest single payout: Unknown

Crowd-Sourced Bounties – Pointers

- Due to risk of duplicates, speed is more of a factor than other types of bug bounties to ensure decent ROI.
- Many provide a heads-up on when a new bounty starts – be ready to begin ASAP.
- When finding a vulnerability, quickly create a PoC, a short write-up, and then report it immediately.
  - Don't wait or you end up with kudos instead of cool cash!

Brokers – Better Approach?

Bug Brokers

- Researchers who find vulnerabilities, work with a broker to find the best market and price to sell the information.
- Could be a number of avenues, including Gray and Black Markets.
- Generally thought to be the way to get the most money possible for your research.
- In almost all cases, reporting and coordination is directly with the broker only who handles the who transaction.
- Details of the vulnerabilty are never to be published.

Brokers - SSD

Founded: 2010 (Beyond Security)
Located: Cupertino, CA

TARGETS:

Purchasing program isn't focused on specific vulnerabilities or vendors, rather on things of interest.

BOUNTIES:

"SecuriTeam Secure Disclosure" is a researcher-oriented program where security researchers can get paid for vulnerabilities they discover, according to the severity/interest of the specific vulnerability.

RESEARCHERS:

Unknown number of researchers

We have researchers from all continents except Africa., with most of them are from the US and Europe.

Unknown unique researchers paid USD

Brokers - SSD

- Over 100 bounties paid in the last year
- Average Bounty Amount: USD $5,000 to $100,000
- Largest single payout: Above USD $1,000,000

Secunia SVCRP

NEWS

Secunia Offers to Coordinate Vulnerability Disclosure on Behalf of Researchers

New vulnerability coordina
researchers and make thei

CLOSED FOR BUSINESS

By Lucian Constantin | Follow
IDG News Service | Nov 2, 2011 8:00 AM

RIP August 2013

Danish vulnerability management company Secunia aims to make the task of reporting software vulnerabilities easier for security researchers by offering to coordinate disclosure with

..”the decision to end SVCRP is based on the conclusion that the amount of time and effort”.. “outweighs the benefits to our own organizations”..

FEA

PRESENTED BY NETSKOPE

10 Alternatives to Heavy-Handed Cloud App Control

Blocking any useful cloud

However, accordin
specialist, SVCRP d
programs, but to complement them.

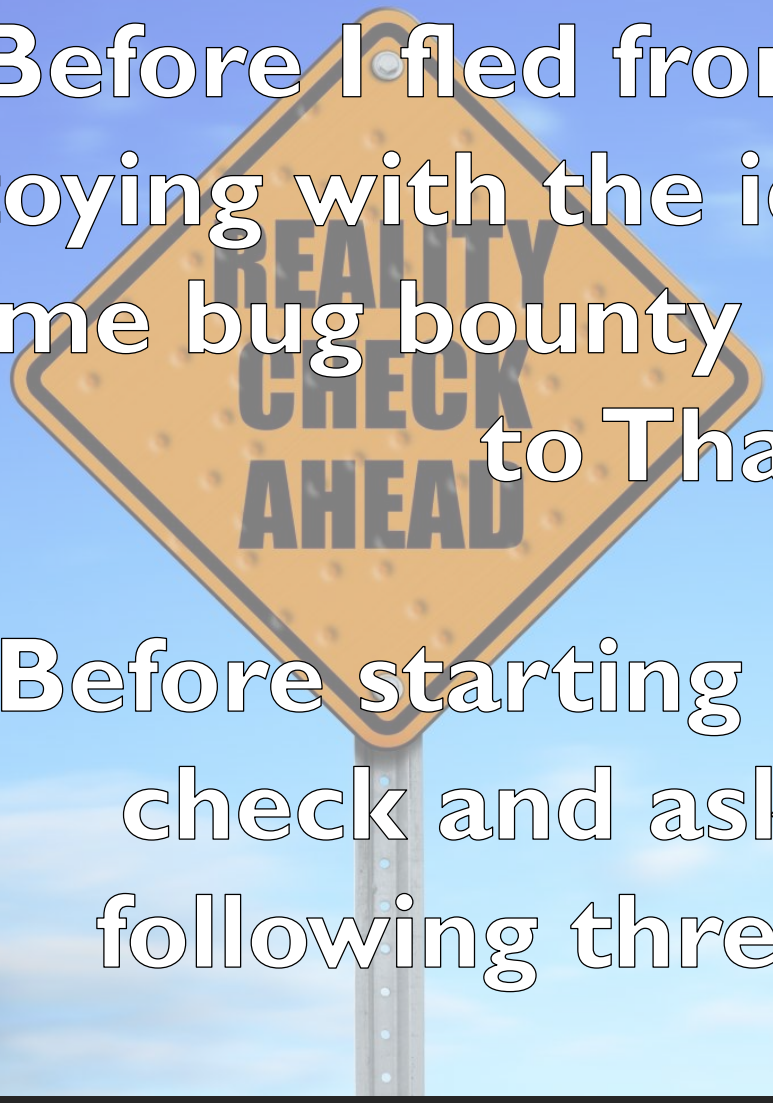
"Other major vulnerability coordination offerings exist but

Researcher Finds Over 20 Vulnerabilities in SCADA Software

the grugq

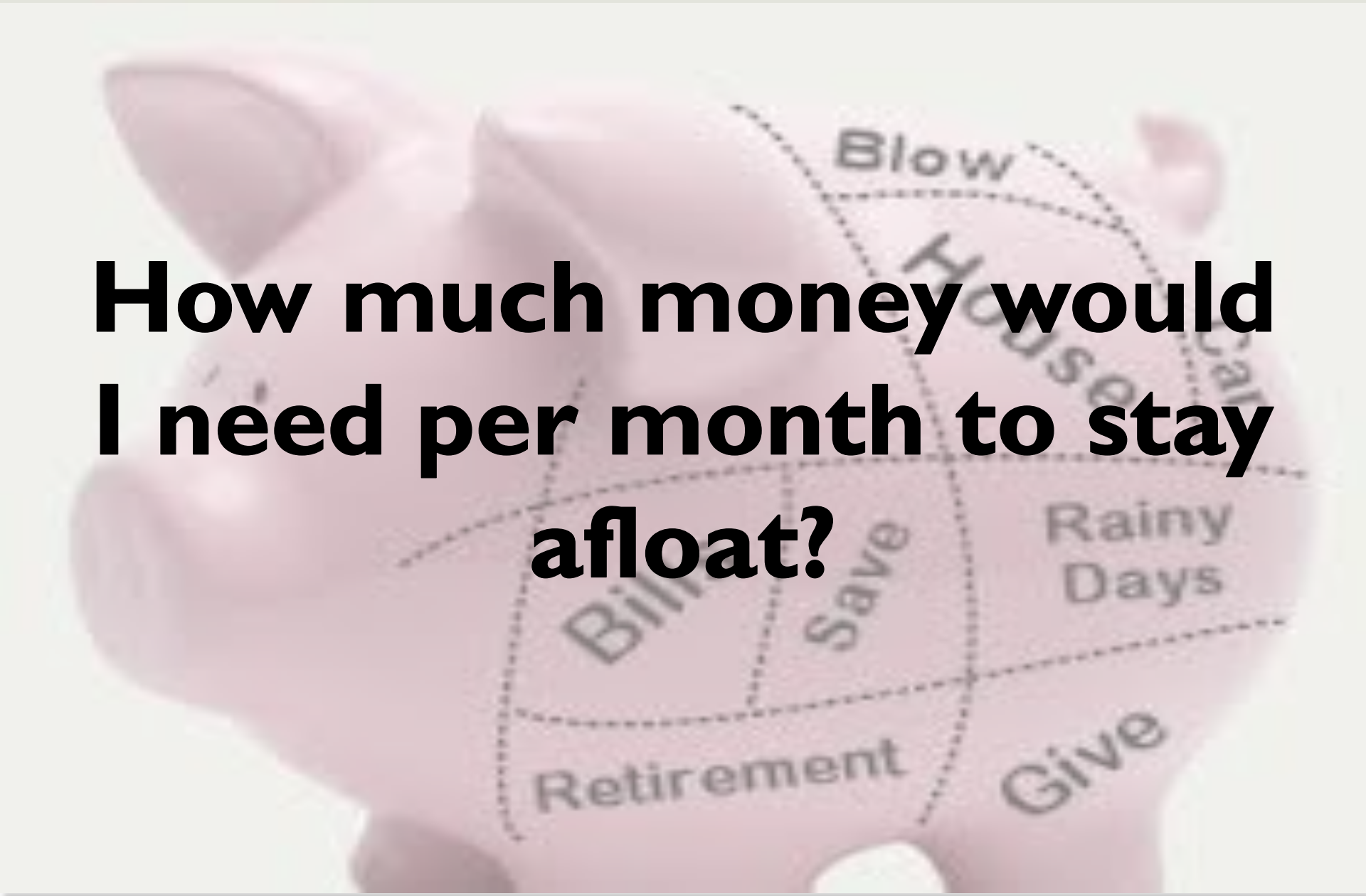
Bug Bounties – Is It Worth Your Time?

Reality Check Before Starting Out



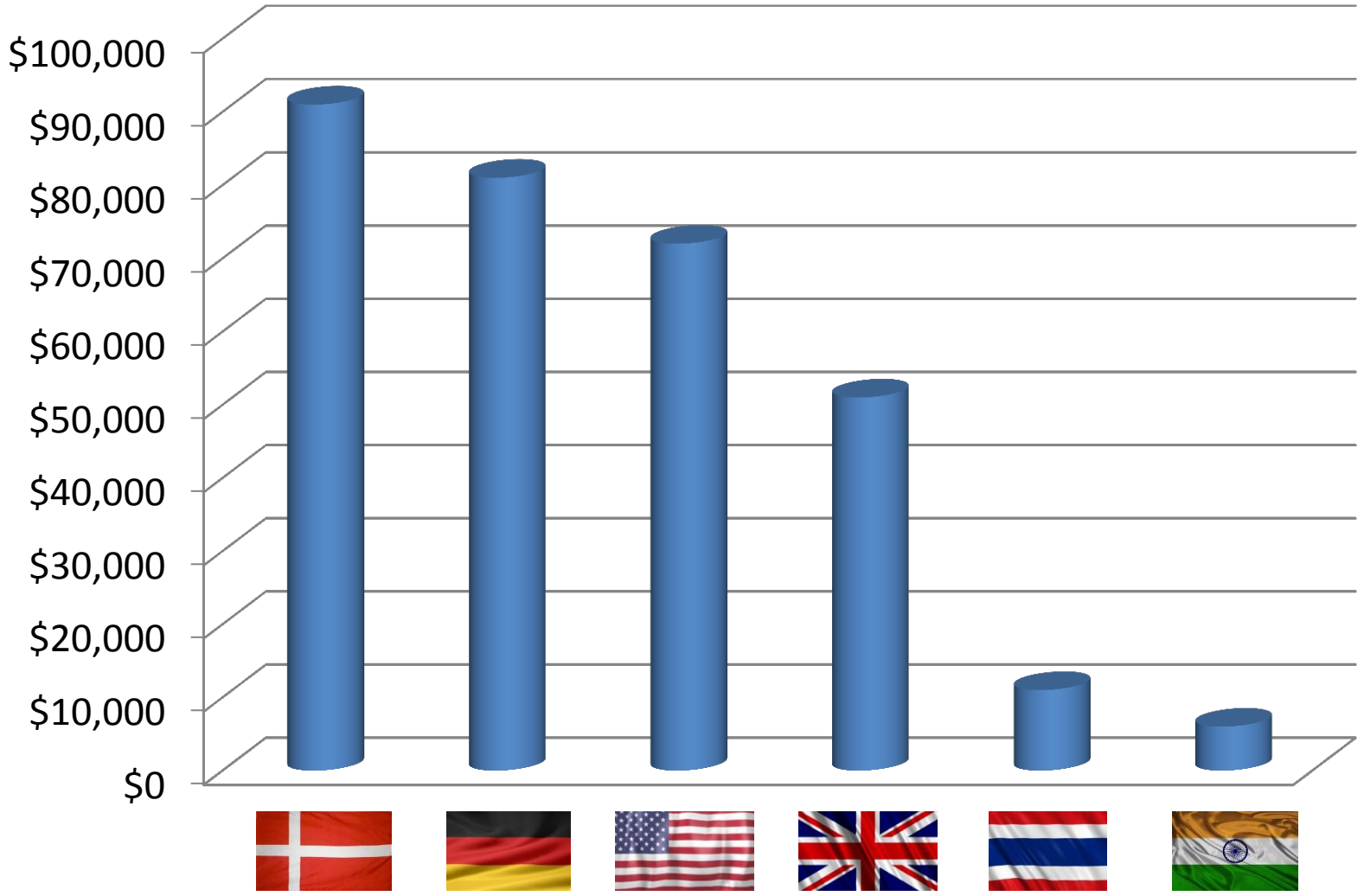
Before I fled from Secunia, I was toying with the idea of going full-time bug bounty hunter and move to Thailand.

Before starting out, do a reality check and ask yourself the following three questions…



How much money would I need per month to stay afloat?

Location Matters - Pentester Average Annual Salaries



*All amounts in USD

RiskBased SECURITY

What does the combination of products, vulnerability types, and numbers look like to make that happen?

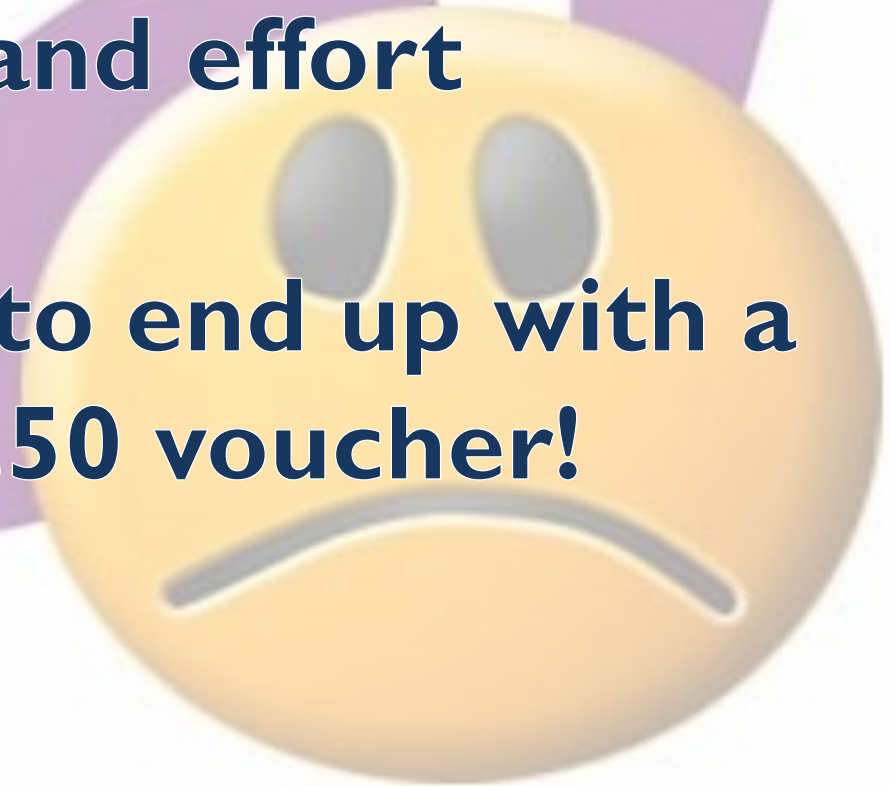
HELIX-DESIGNS

Due Diligence Before Putting in Work

RiskBased SECURITY

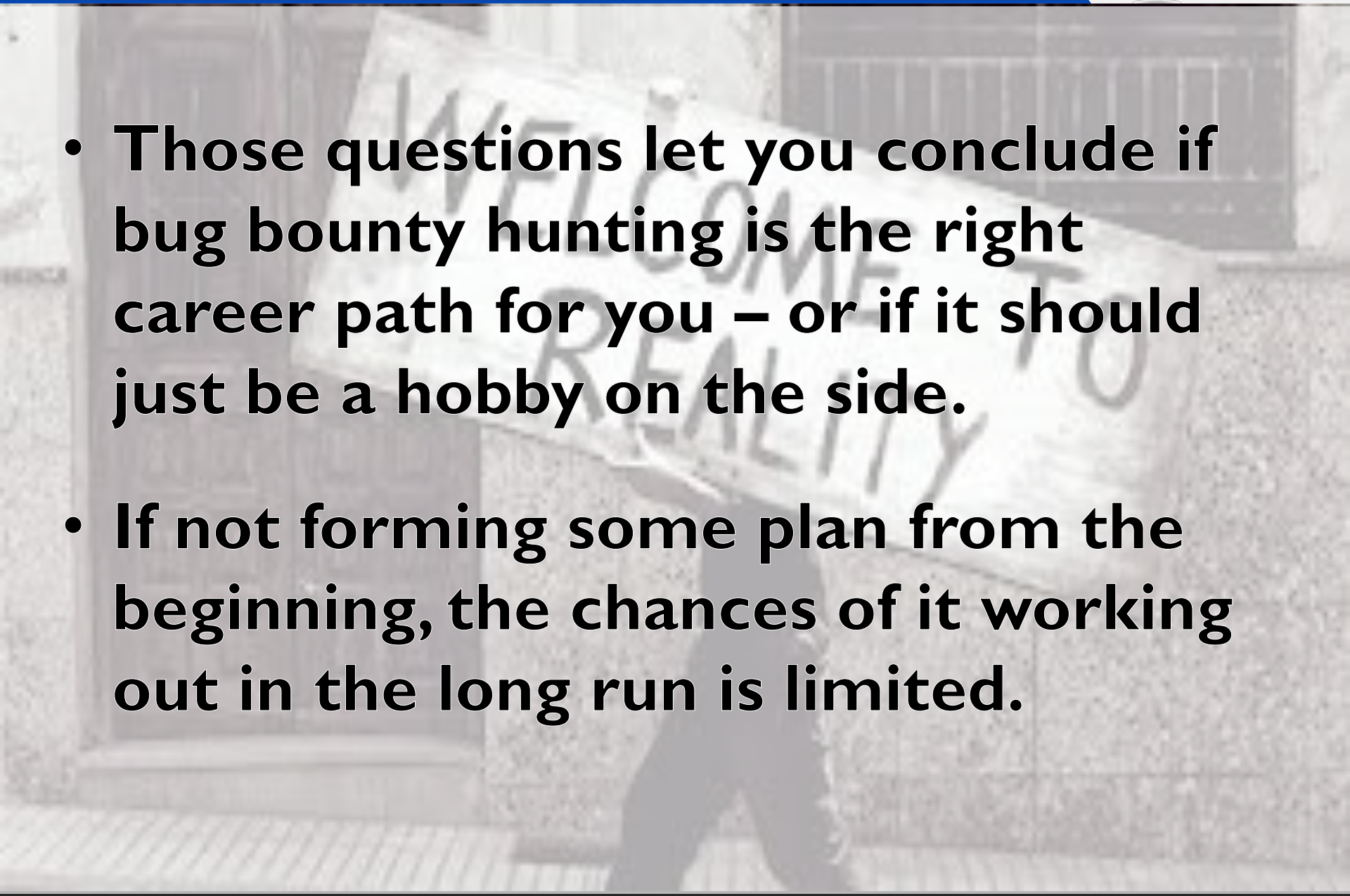
Figure out the reward types and sizes before investing a lot of time and effort

Would suck to end up with a USD 12.50 voucher!



Reality Check Before Starting Out

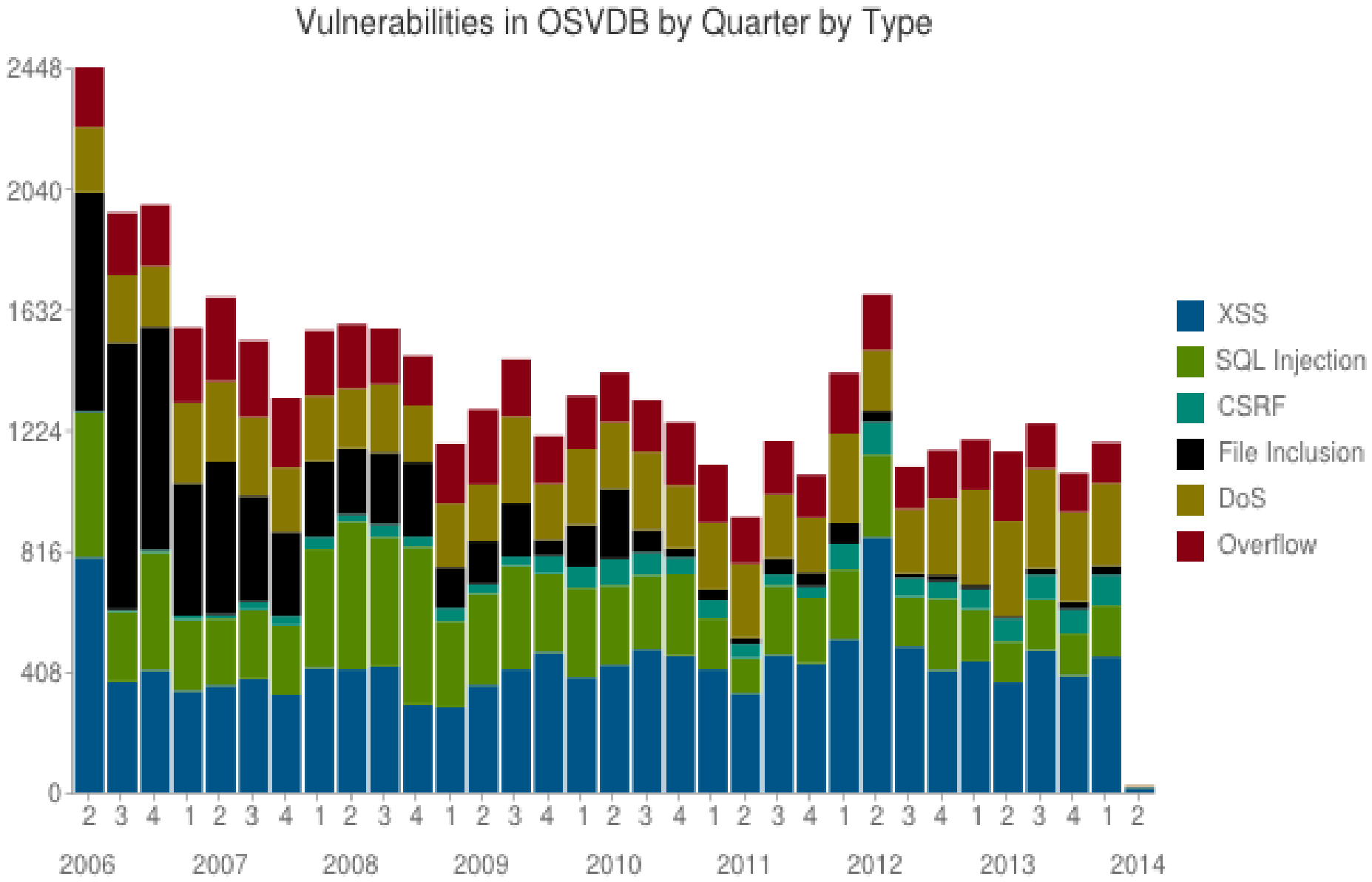
Reality Check Before Starting Out



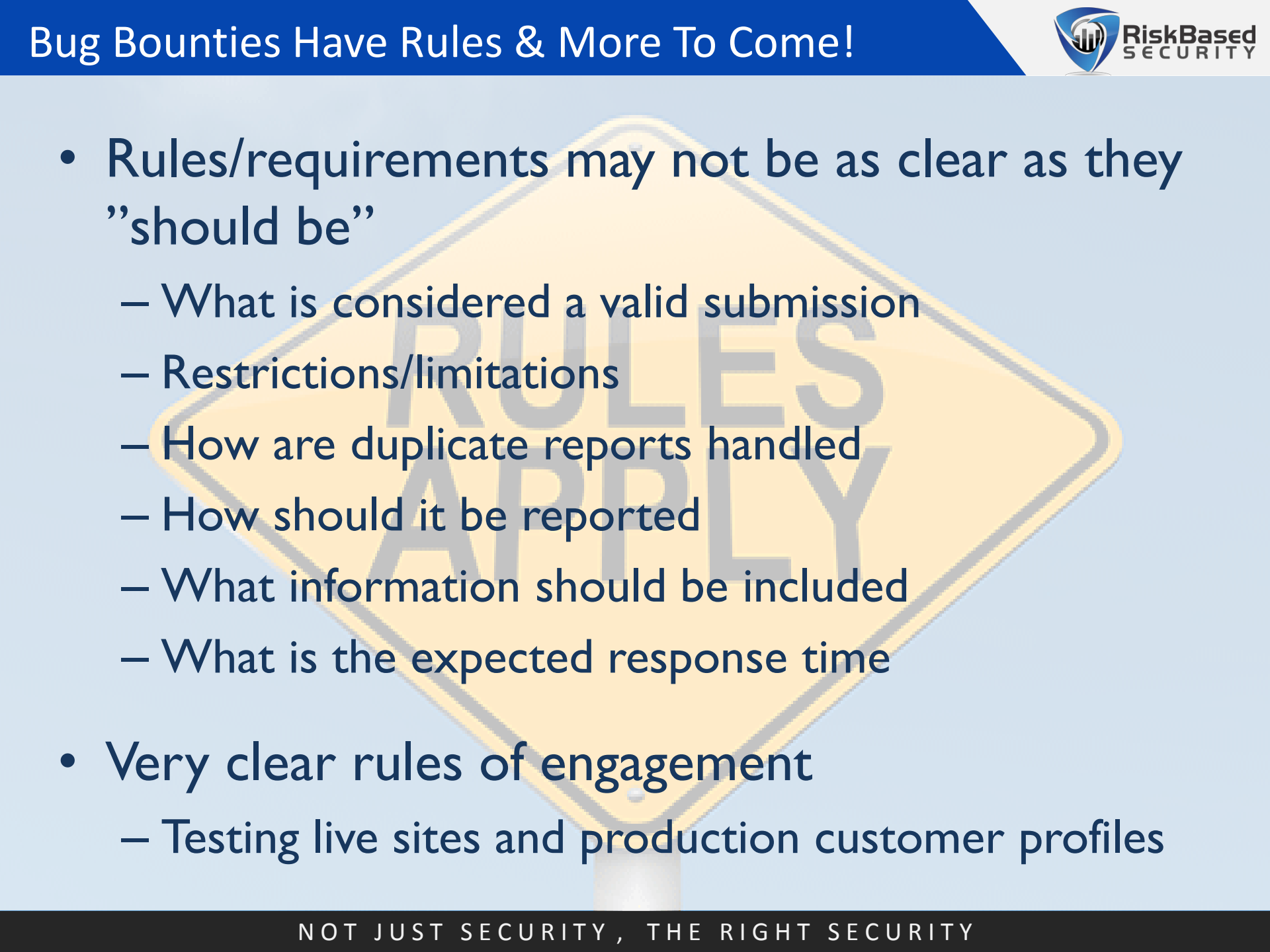
- **Those questions let you conclude if bug bounty hunting is the right career path for you – or if it should just be a hobby on the side.**
- **If not forming some plan from the beginning, the chances of it working out in the long run is limited.**

Bug Bounties – What Is To Come?

Software Is Still Awful



Bug Bounties Have Rules & More To Come!



- Rules/requirements may not be as clear as they ”should be”
  - What is considered a valid submission
  - Restrictions/limitations
  - How are duplicate reports handled
  - How should it be reported
  - What information should be included
  - What is the expected response time
- Very clear rules of engagement
  - Testing live sites and production customer profiles

Legal Threats – They Still Happen!

- Cisco vs Mike Lynn (2005)

2005-07-29	Cisco Systems, Inc.	Mike Lynn / ISS	Cisco router vulnerabilities	X Resigned from ISS before settlement, gave BH presentation, future disclosure injunction agreed on

- Still happens today... And unfortunately with some success!

When	Company making threat	Researchers	Research Topic	Resolution/Status
2014-01-15	Covered California	Kristian Erik Hermansen and Matt Ploessel	Security flaws in Covered California website	X Video taken down from Youtube and the researchers were visited by the FBI and asked to stop discussing the issues.
2014-01-08	Public Transport Victoria	Joshua Rogers	Security flaws in PTV website	X Company referred incident to Victoria Police
2013-12-16	ZippyYum	Daniel Wood	Insecure Data Storage in iOS Subway ordering app	X Researcher says no NDA was signed and has retained an attorney to handle any potential legal action [Mailing List Thread]

Source: http://attrition.org/errata/legal_threats/

Bounty vs Extortion

12 Teen Arrested for 30+ Swattings, Bomb Threats

MAY 14

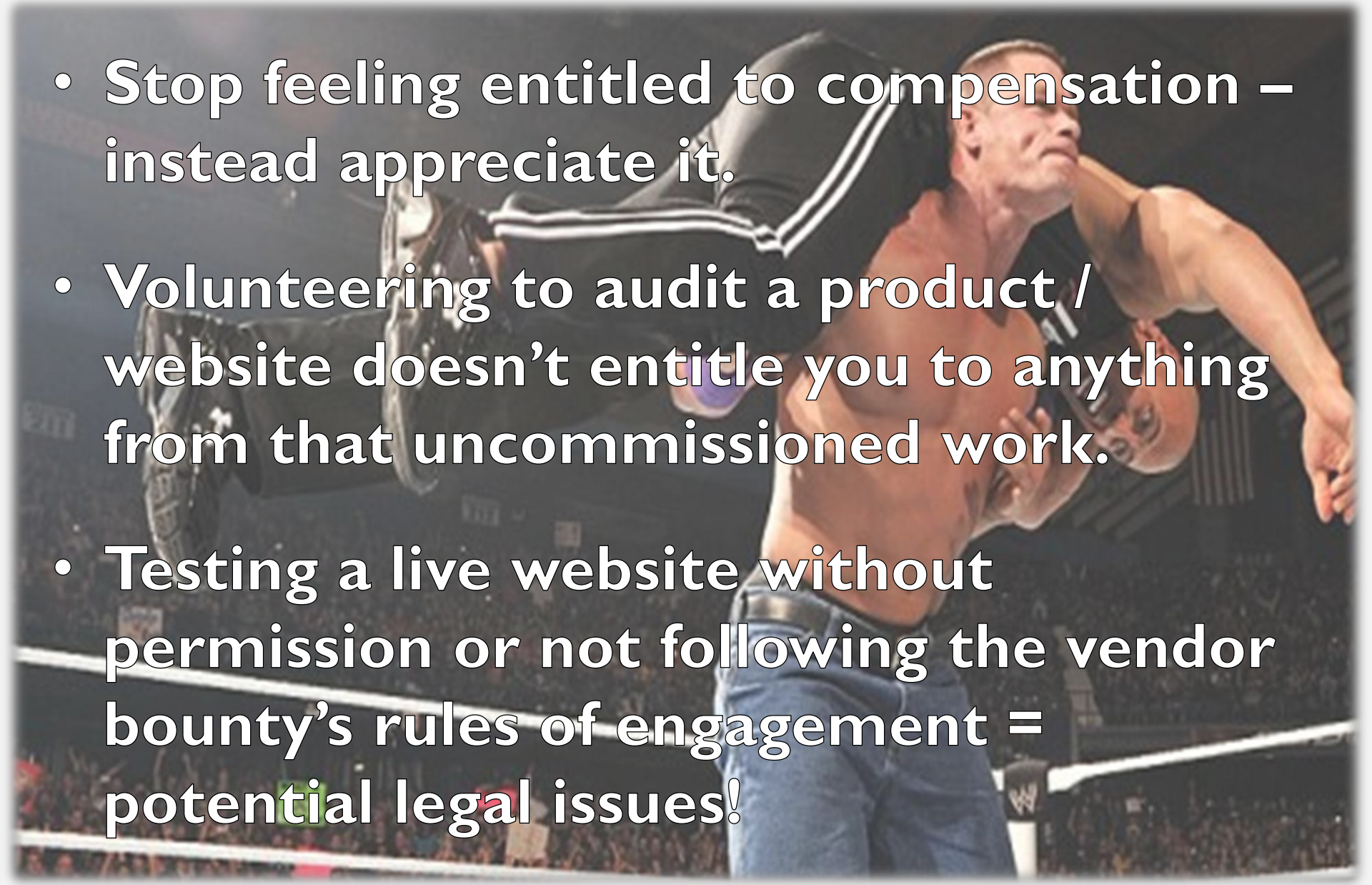
A 16-year-old male from Ottawa, Canada has been arrested for allegedly making at least 30 fraudulent calls to emergency services across North America over the past few months. The false alarms — *two of which targeted this reporter* — involved calling in phony bomb threats and multiple attempts at "swatting" — a hoax in which the perpetrator spoofs a call about a hostage situation or other violent crime in progress in the hopes of tricking police into responding at a particular address with deadly force.

On March 9, a user on Twitter named @ProbablyOnion (possibly NSFW) started sending me rude and annoying messages. A month later (and several weeks after blocking him on Twitter), I received a phone call from the local police department. It was early in the morning on Apr. 10, and the cops wanted to know if everything was okay at our address.

Since this was not the first time someone had called in a fake hostage situation at my home, the call I received came from the police department's non-emergency number, and they were unsurprised when I told them that the Krebs manor and all of its inhabitants were just fine.

Minutes after my local police department received that fake notification, @ProbablyOnion was bragging on Twitter about swatting me, including me on his public messages: "You have 5 hostages? And you will kill 1 hostage every 6 times and the police have 25 minutes to get you $100k in clear plastic." Another message read: "Good morning! Just dispatched a swat team to your house, they didn't even call you this time, hahaha."

Attitude Adjustment (Researchers)

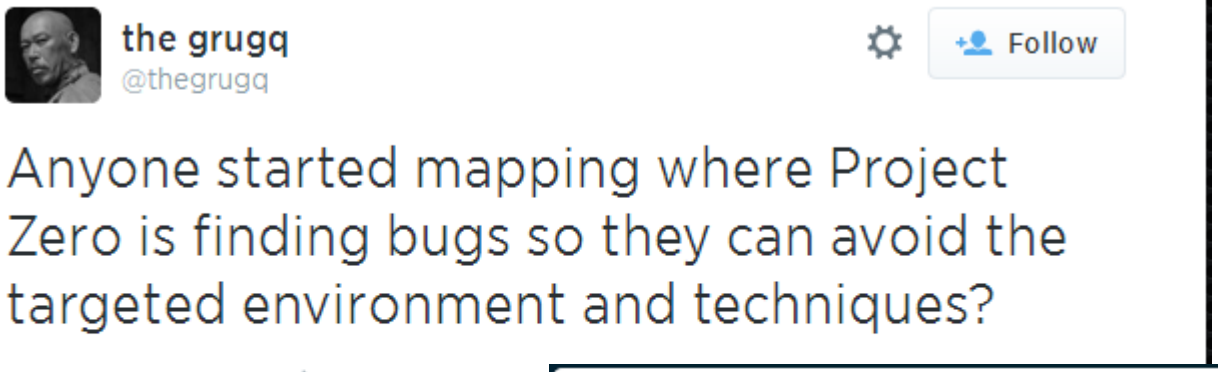


- Stop feeling entitled to compensation – instead appreciate it.
- Volunteering to audit a product / website doesn't entitle you to anything from that uncommissioned work.
- Testing a live website without permission or not following the vendor bounty's rules of engagement = potential legal issues!

Impact of Google Project Zero

- New initiative by Google. "Dream team" of researchers to hunt for and weed out bugs is popular software.
- While no impact to web bug bounty hunters, it may affect software bounty hunters.
- What happens when popular software is exposed to bad ass researchers and an immense cluster of fuzzing power?

Impact of Google Project Zero



Future of Bug Bounties

- More and more companies jump on board!
- Karma and kudos points become irrelevant
- Researchers will follow the money!
  - They work with whoever pays the most including grey/black markets
- Fad has potential to wear off
  - While bounties will continue to exist, companies spend more resources on SDL processes

Thank you!

This presentation would not have been possible without the support and data from several individuals and companies!

We want to thank the following!

- Brian Martin
- Katie Mo / HackerOne
- Nate Jones / Facebook
- HP / ZDI
- CrowdCurity
- SecuriTeam
- Marisa & Casey / BugCrowd
- Bug Bounty Hunters!

Discussion!

RiskBased SECURITY

Screw Being A Pentester - When I Grow Up I Want To Be A Bug Bounty Hunter

Jake Kouns
@jkouns
Chief Information Security Officer (CISO)
Risk Based Security

Carsten Eiram
@CarstenEiram
Chief Research Officer (CRO)
Risk Based Security