OWASP
Open Web Application
Security Project

If You Can’t Beat ‘Em Join ‘Em:

Practical Tips for Running a Successful Bug Bounty Program

Grant McCracken and Daniel Trauner
AppSecUSA 2016

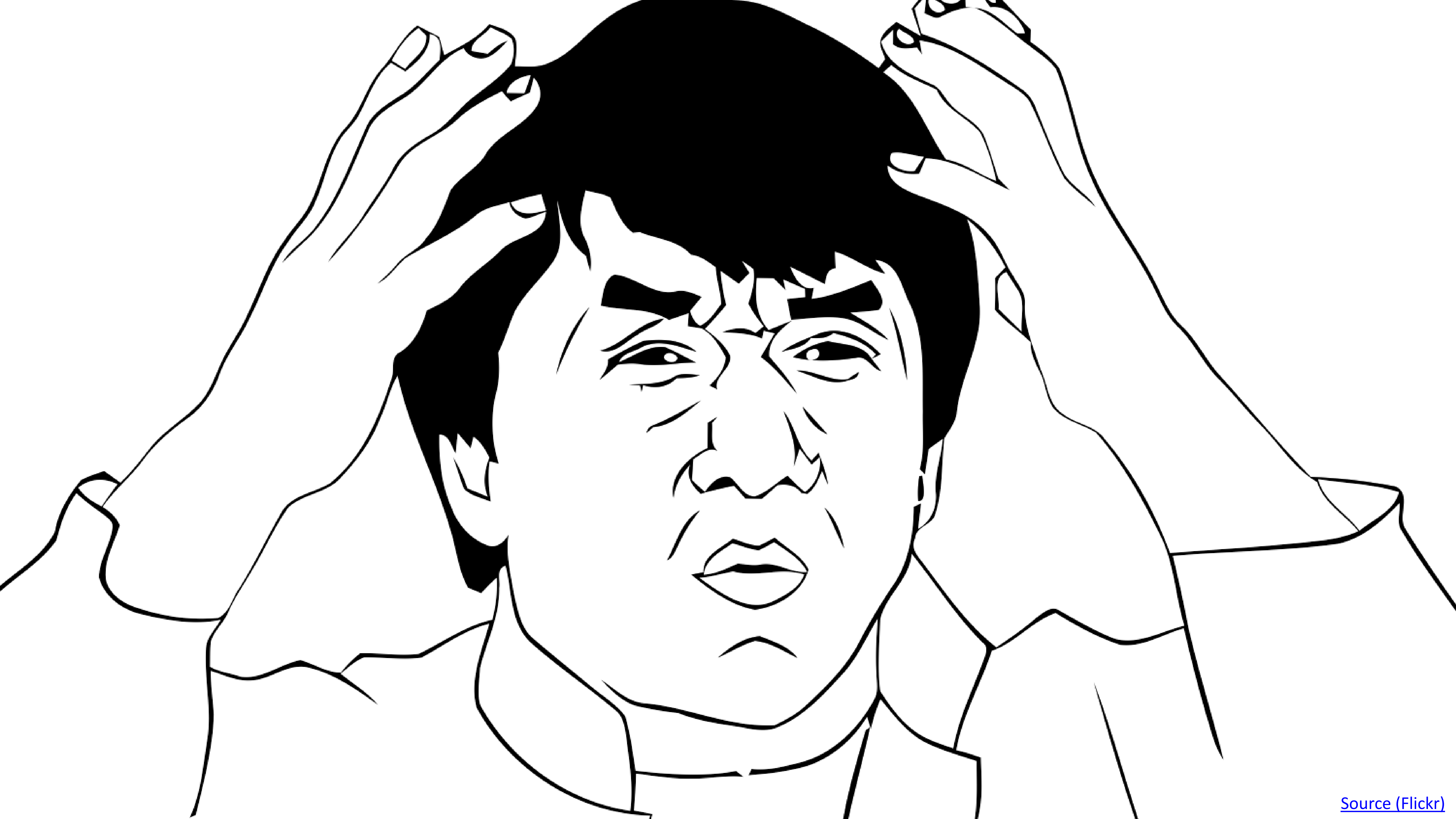
Grant

- Solutions Architect @Bugcrowd
  - Formerly an AppSec Engineer
- Before that, WhiteHat
- Traveling, music, stuff.

Dan

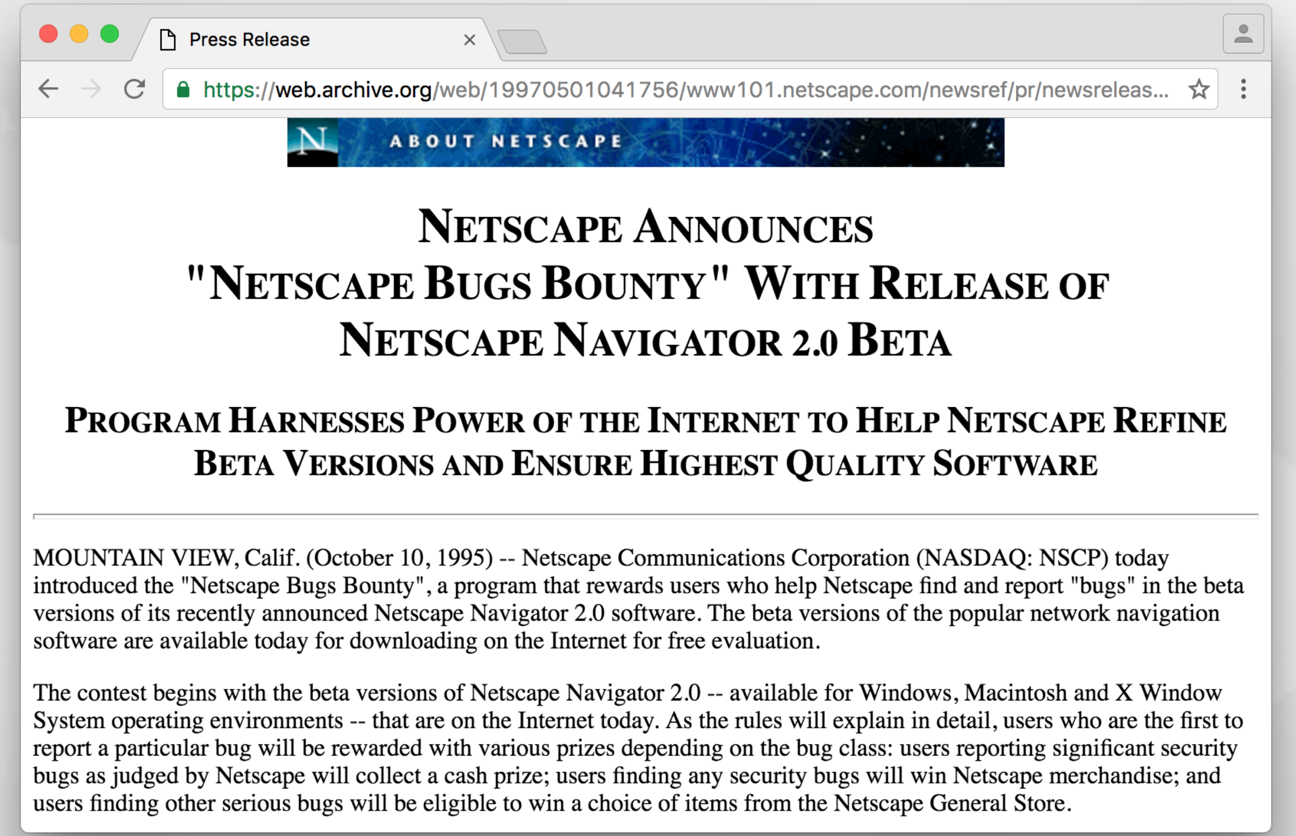
- Senior AppSec Engineer @Bugcrowd
- Before that, Software Security @HP
  - Static analysis – lots of languages
  - Focused on Apple iOS
- Art history and collecting

BUG BOUNTY PROGRAMS



Source (Flickr)

Netscape "Bugs Bounty"


Press Release
https://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsreleas...
ABOUT NETSCAPE

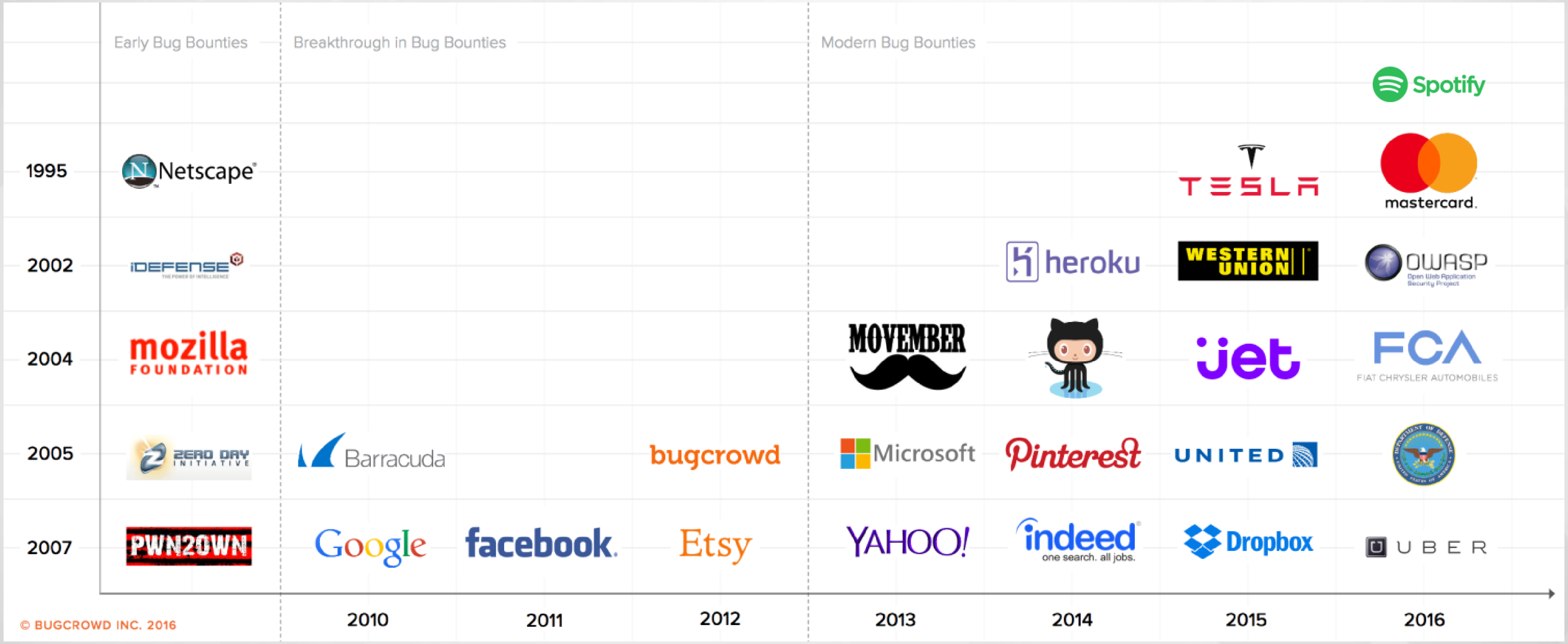
NETSCAPE ANNOUNCES "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA

PROGRAM HARNESSES POWER OF THE INTERNET TO HELP NETSCAPE REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE

MOUNTAIN VIEW, Calif. (October 10, 1995) -- Netscape Communications Corporation (NASDAQ: NSCP) today introduced the "Netscape Bugs Bounty", a program that rewards users who help Netscape find and report "bugs" in the beta versions of its recently announced Netscape Navigator 2.0 software. The beta versions of the popular network navigation software are available today for downloading on the Internet for free evaluation.

The contest begins with the beta versions of Netscape Navigator 2.0 -- available for Windows, Macintosh and X Window System operating environments -- that are on the Internet today. As the rules will explain in detail, users who are the first to report a particular bug will be rewarded with various prizes depending on the bug class: users reporting significant security bugs as judged by Netscape will collect a cash prize; users finding any security bugs will win Netscape merchandise; and users finding other serious bugs will be eligible to win a choice of items from the Netscape General Store.

An (Abbreviated) History of Bug Bounties Since 1995



WHY?

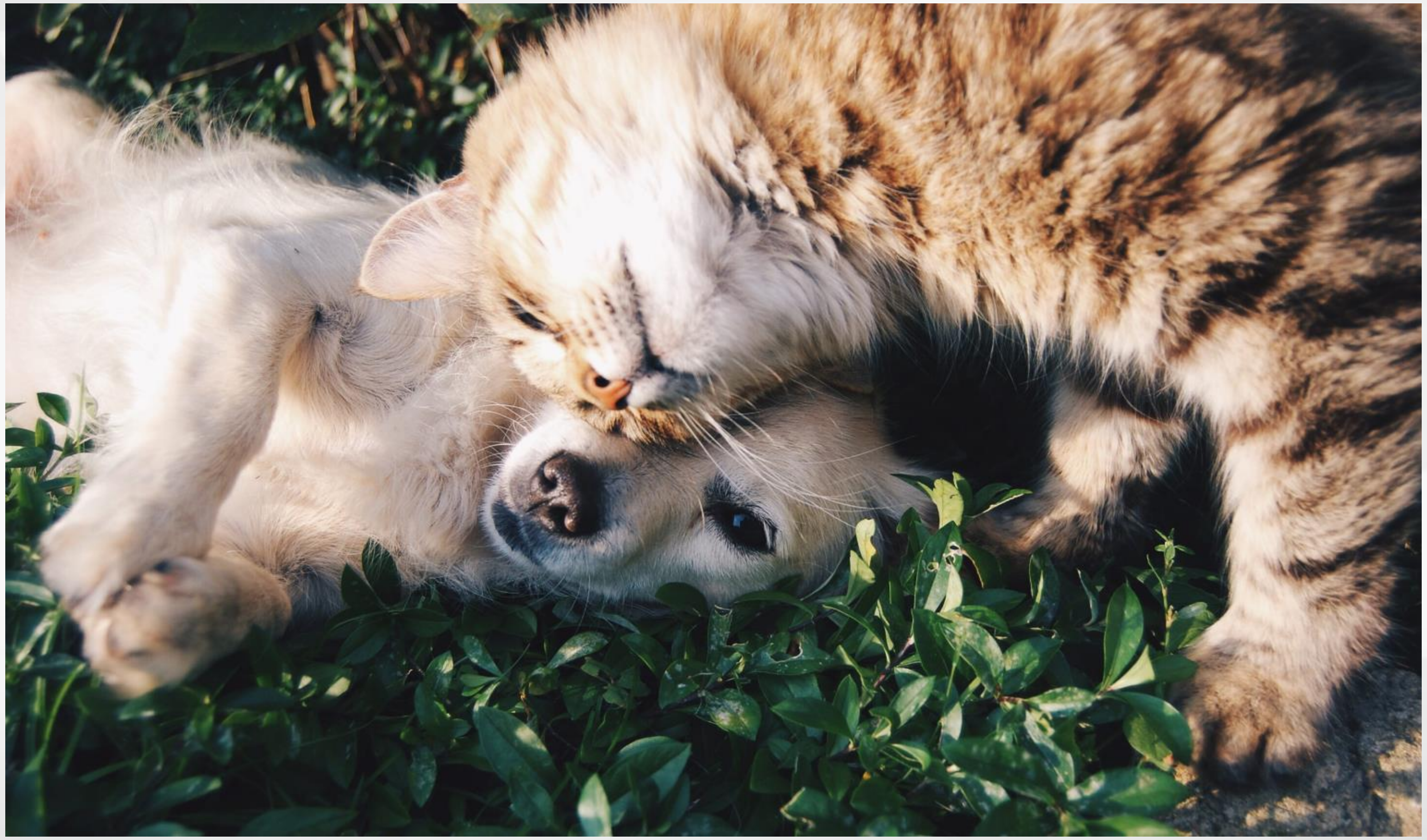
Do you really want to let people attack you?

Source (Hyperbole and a Half)

Yes! (They're doing it anyways...)

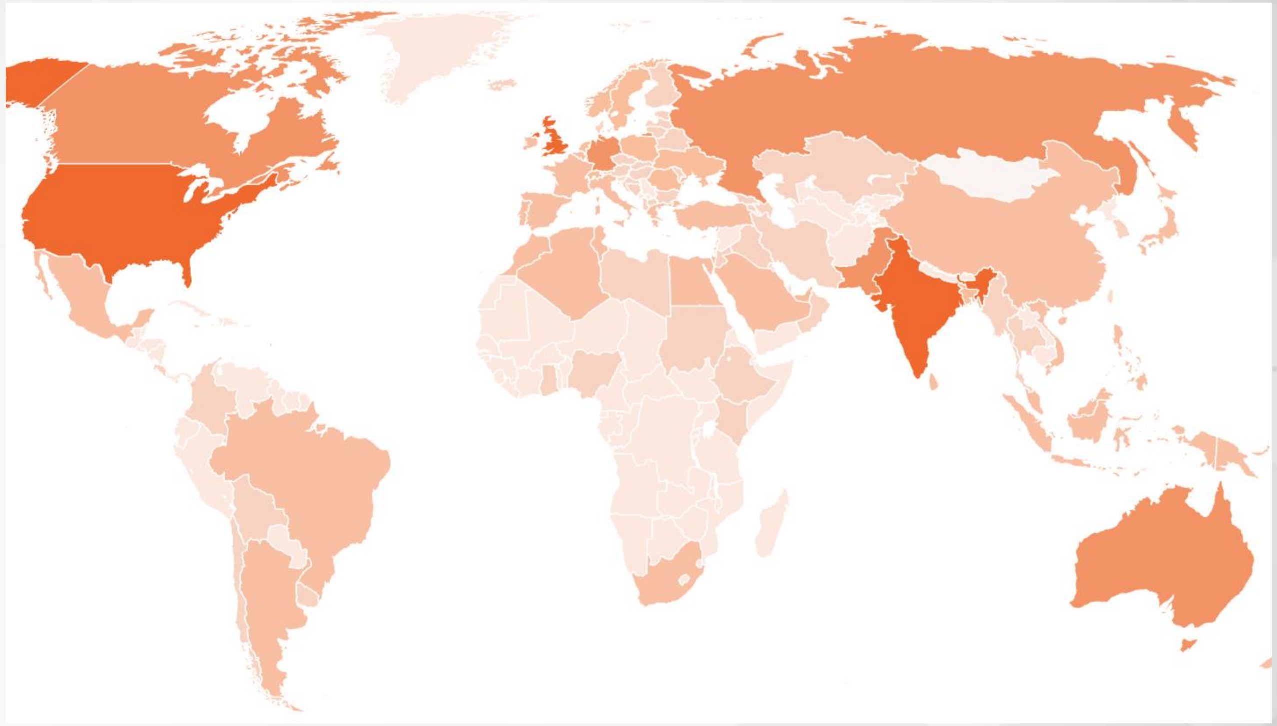
Source (Hyperbole and a Half)

You ~~vs.~~ and Them



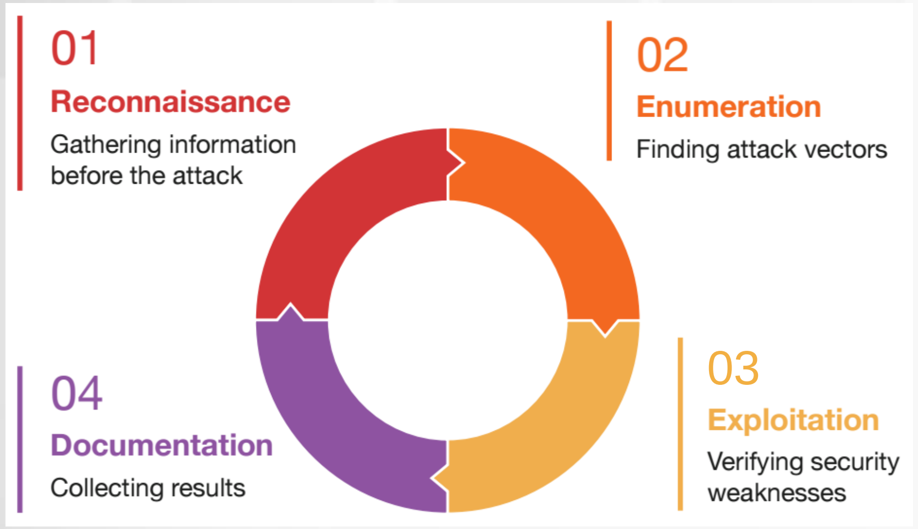
Who are these people?

- All ages
- All levels of experience
- All over the world
- Users and and non-users
- Passionate about security!



The Value of Crowdsourced Testing

Formal Methodologies



+

The Crowd's Creativity

HOW?

Overview

Pre-Launch

- Scope
- Focus
- Exclusions
- Environment
- Access

Post-Launch

- Managing Expectations
- Communicating Effectively
- Defining a Vulnerability Rating Taxonomy

But you never mentioned paying rewards!

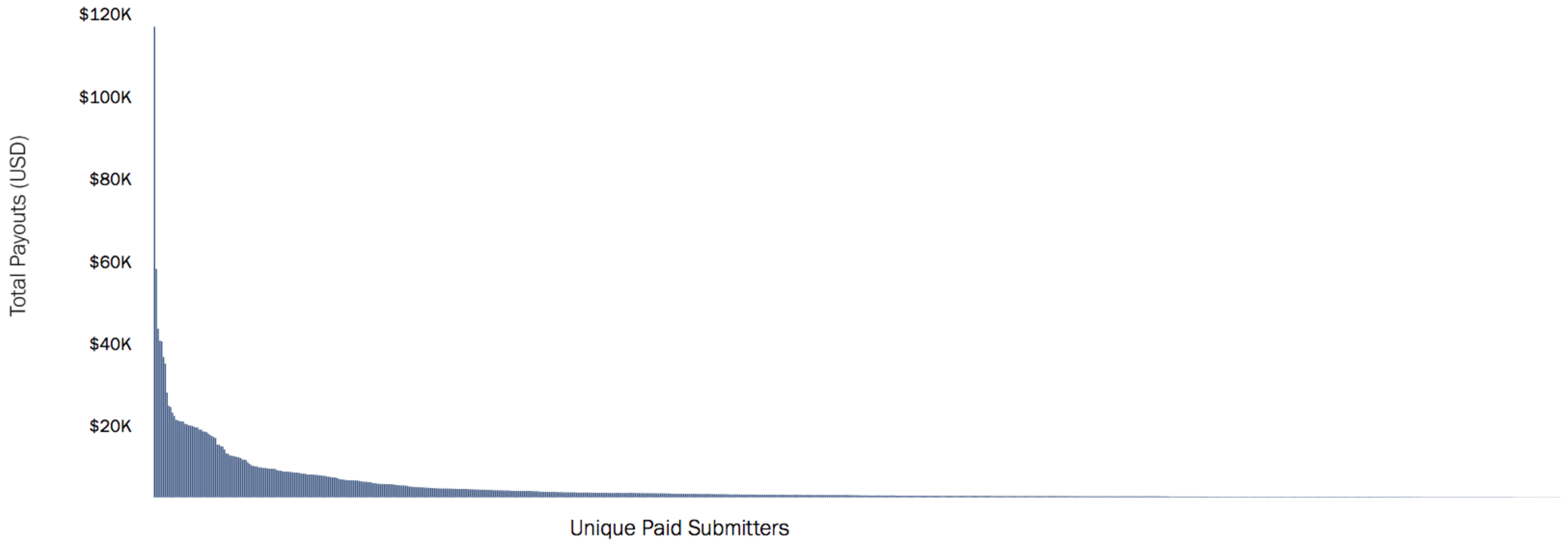


Figure 20: Distribution of cumulative payments cross individual paid submitters.

“Touch the code, pay the bug.”

PRE-LAUNCH

…but first, Step 0

- Basic resources and requirements
  - A full-time resource
  - Escalation policies
  - Organization-wide awareness

Find all of the dank memes for your slides

Scope

- Scope defines the researcher’s universe
  - Leave nothing open to interpretation
  - Understand your attack surface
  - Recognize the path of least resistance

Source (Flickr)

Focus

- You might care about specific:
  - Targets
  - Vulnerability Types
  - Functionality (e.g. payment processing)
- How?
  - Incentives

THE RUMORS ARE TRUE. GOOGLE WILL BE SHUTTING DOWN PLUS—
ALONG WITH HANGOUTS, PHOTOS, VOICE, DOCS, DRIVE, MAPS, GMAIL, CHROME, ANDROID, AND SEARCH—
TO FOCUS ON OUR CORE PROJECT:
THE 8.8.8.8 DNS SERVER.
Google

Source (xkcd)

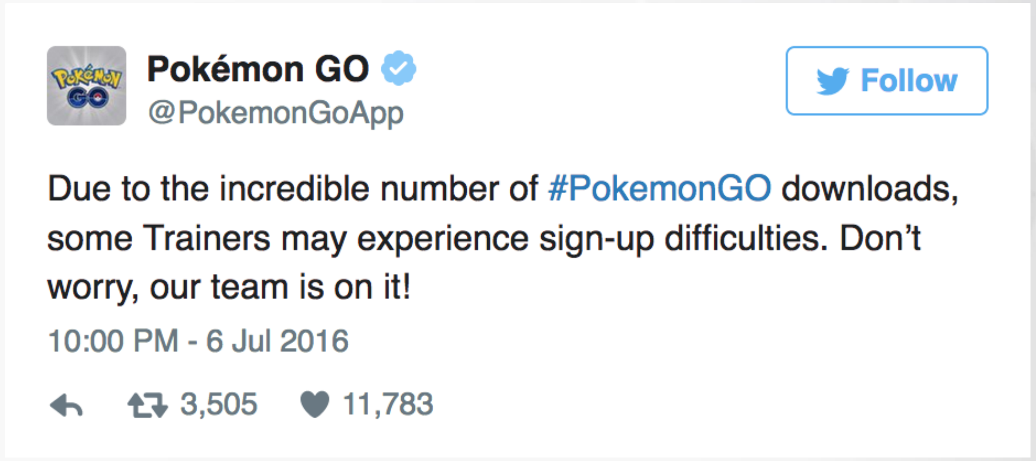
Exclusions

- You might *not* care about:
  - (Low-impact) “low hanging fruit”
  - Intended functionality
  - Known issues
  - Accepted risks
  - Issues based on pivoting

Source (Meme Generator)

Environment

- Production vs. staging
- Make sure it can stand up to testing!
  - Scanners
  - Contact forms
  - Pentesting requests
- Special bounty types
- Researcher environments


Pokémon GO
@PokemonGoApp

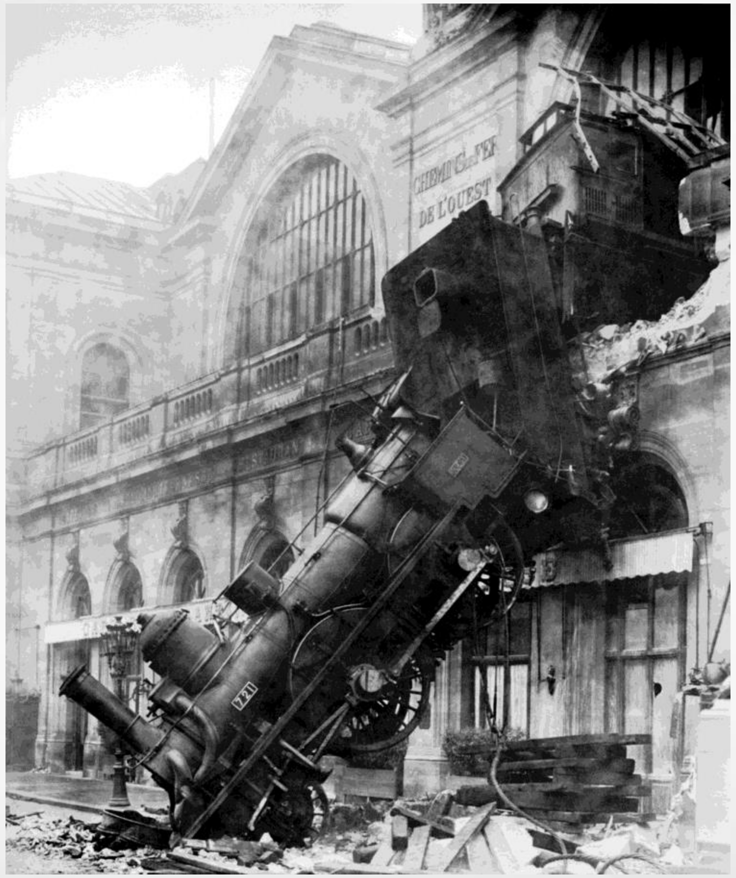
Due to the incredible number of #PokemonGO downloads, some Trainers may experience sign-up difficulties. Don't worry, our team is on it!

10:00 PM - 6 Jul 2016

3,505 11,783

Source (Twitter @PokemonGoApp)

This is what a shared environment looks like…



Access

- Easier = better
- Provide adequate resources for success
  - E.g. sandbox credit cards
- No shared credentials

Source (Demotivation)

Remember…

POST-LAUNCH

Manage Expectations

Source (Jane Donald)

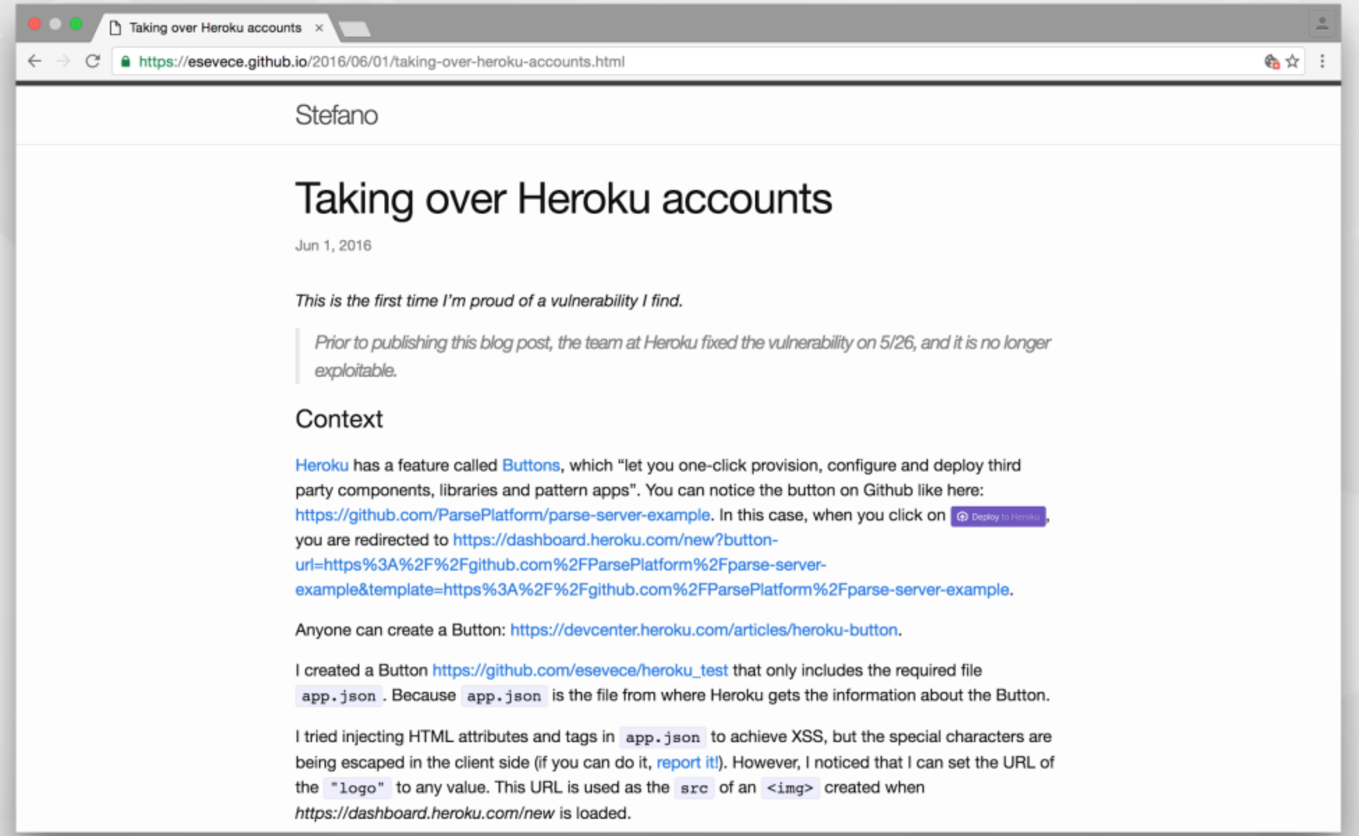
Manage Expectations

Source (SoJo 104.9)

Communication is Key

- Researchers like:
  - Concise, unambiguous responses
    - ESL
  - Short response time
  - Predictable reward time
- Stay on top of these issues!
- Public disclosure?

Coordinated Disclosure



Taking over Heroku accounts

https://esevece.github.io/2016/06/01/taking-over-heroku-accounts.html

Stefano

Taking over Heroku accounts

Jun 1, 2016

This is the first time I'm proud of a vulnerability I find.

> *Prior to publishing this blog post, the team at Heroku fixed the vulnerability on 5/26, and it is no longer exploitable.*

Context

Heroku has a feature called Buttons, which "let you one-click provision, configure and deploy third party components, libraries and pattern apps". You can notice the button on Github like here: https://github.com/ParsePlatform/parse-server-example. In this case, when you click on Deploy to Heroku, you are redirected to https://dashboard.heroku.com/new?button-url=https%3A%2F%2Fgithub.com%2FParsePlatform%2Fparse-server-example&template=https%3A%2F%2Fgithub.com%2FParsePlatform%2Fparse-server-example.

Anyone can create a Button: https://devcenter.heroku.com/articles/heroku-button.

I created a Button https://github.com/esevece/heroku_test that only includes the required file `app.json`. Because `app.json` is the file from where Heroku gets the information about the Button.

I tried injecting HTML attributes and tags in `app.json` to achieve XSS, but the special characters are being escaped in the client side (if you can do it, report it!). However, I noticed that I can set the URL of the `"logo"` to any value. This URL is used as the `src` of an `<img>` created when *https://dashboard.heroku.com/new* is loaded.

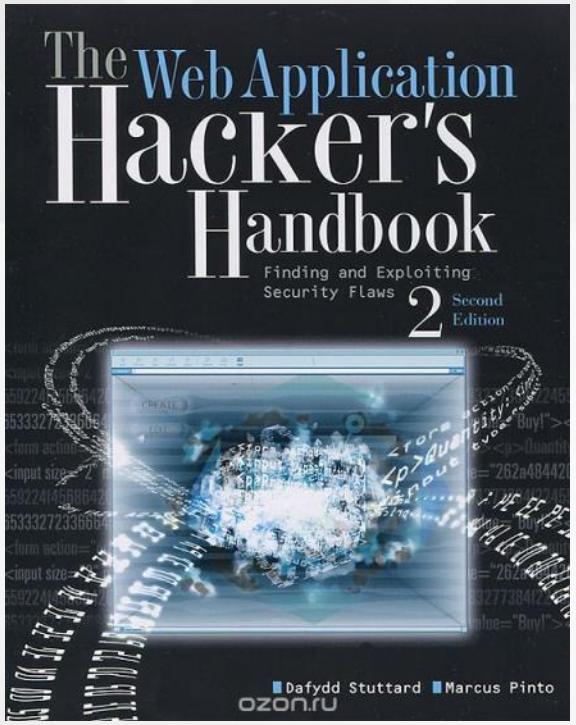
Source (Stefano Vettorazzi)

Define a Vulnerability Rating Taxonomy (VRT)

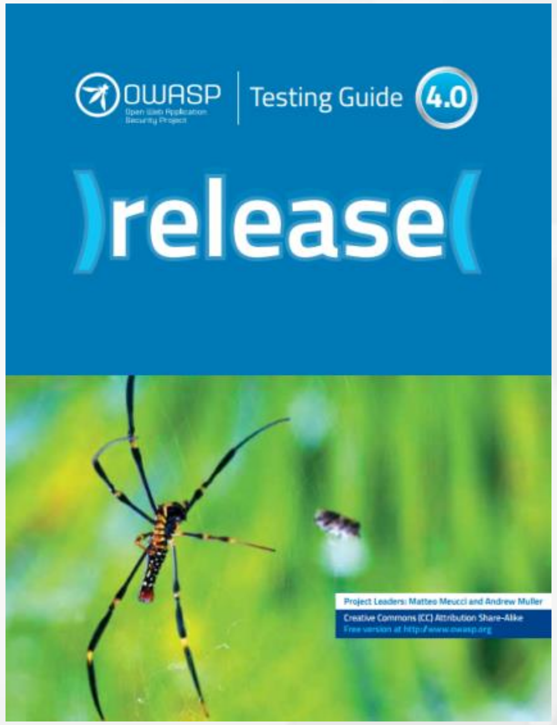
- For program owners:
  - Speeds up triage process
  - Track your organization's security posture
  - Arrive at a reward amount more quickly
- For researchers:
  - Focus on high-value bugs
  - Avoid wasting time on non-rewardable bugs
  - Alongside brief, helps build trust

THINK LIKE A RESEARCHER

The Regular Methodologies


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto
ozon.ru

Source (Amazon)


OWASP
Testing Guide 4.0
)release(
Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike

Source (OWASP)

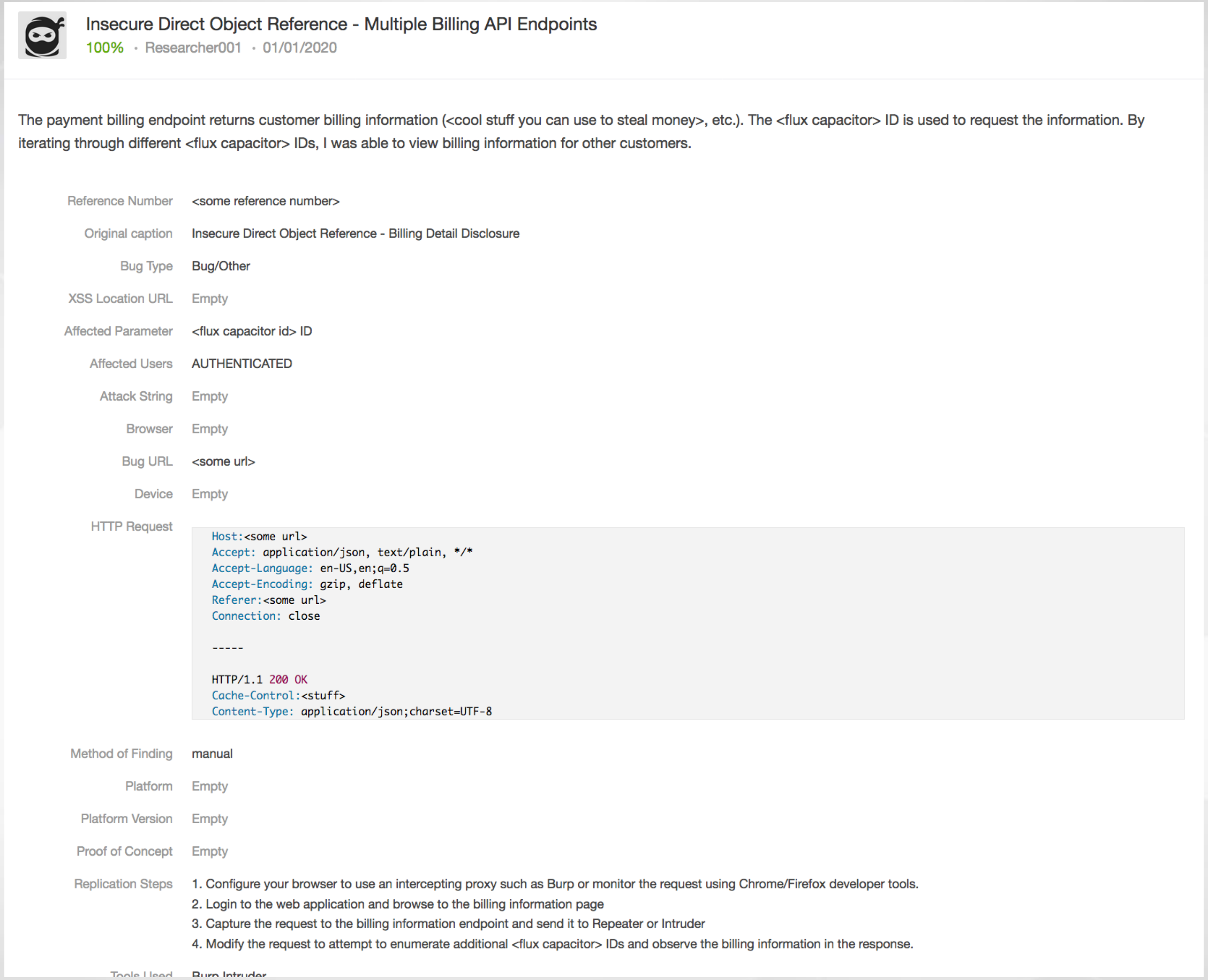
The Bughunter's Methodology

- Identify roads less traveled
  - Acquisitions (define the rules)
  - Functionality changes or redesigns
  - Mobile websites or apps
- Think like a researcher
  - Wikipedia (acquisitions)
  - Google dorks, recon-ng, altdns, etc.
    - jhaddix/domain (enumall)
    - ChrisTruncer/EyeWitness
  - Researchers' Blogs
  - And many more we can't fit into this talk!

I DON'T ALWAYS TAKE THE ROAD LESS TRAVELED
BUT WHEN I DO, IT'S BECAUSE I USED APPLE MAPS

Source (Meme Generator)

A GOOD REPORT



Insecure Direct Object Reference - Multiple Billing API Endpoints

100% · Researcher001 · 01/01/2020

The payment billing endpoint returns customer billing information (<cool stuff you can use to steal money>, etc.). The <flux capacitor> ID is used to request the information. By iterating through different <flux capacitor> IDs, I was able to view billing information for other customers.

Reference Number	<some reference number>
Original caption	Insecure Direct Object Reference - Billing Detail Disclosure
Bug Type	Bug/Other
XSS Location URL	Empty
Affected Parameter	<flux capacitor id> ID
Affected Users	AUTHENTICATED
Attack String	Empty
Browser	Empty
Bug URL	<some url>
Device	Empty

HTTP Request

```
Host:<some url>
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:<some url>
Connection: close

-----

HTTP/1.1 200 OK
Cache-Control:<stuff>
Content-Type: application/json;charset=UTF-8
```

Method of Finding	manual
Platform	Empty
Platform Version	Empty
Proof of Concept	Empty

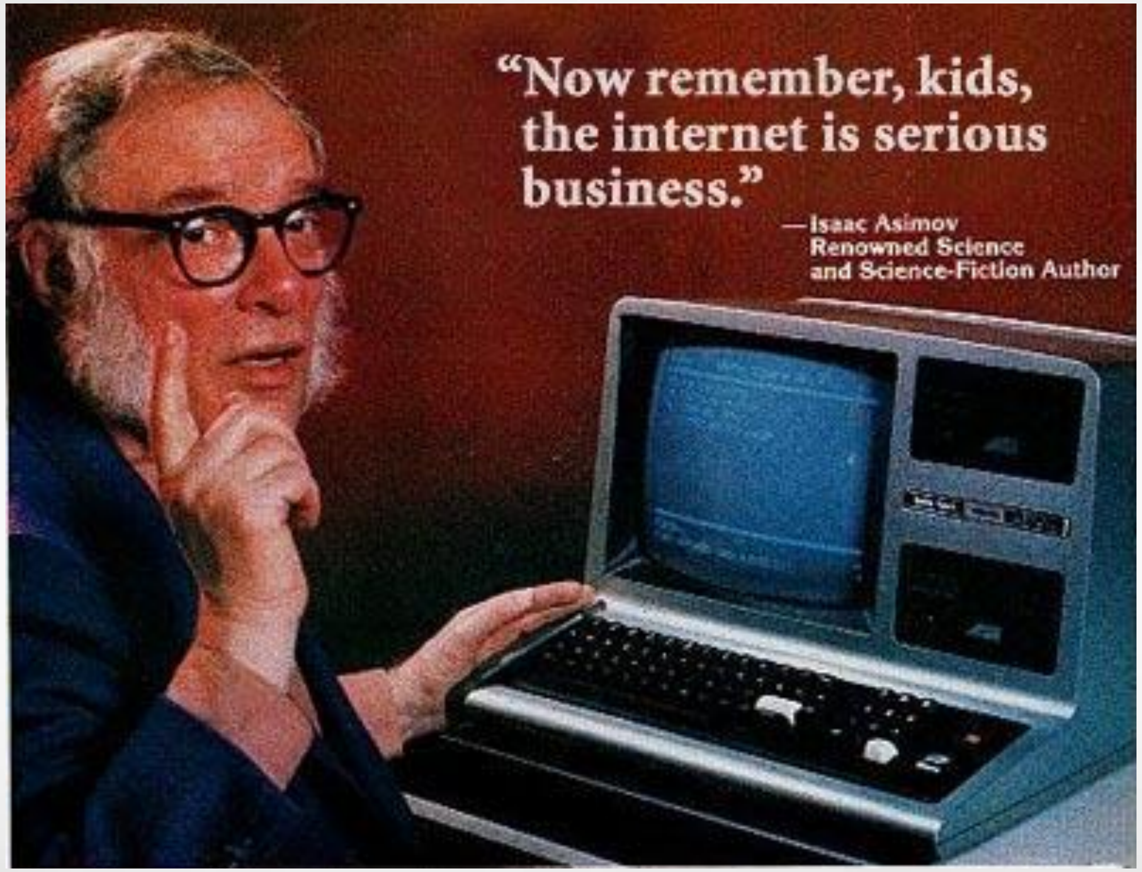
Replication Steps

1. Configure your browser to use an intercepting proxy such as Burp or monitor the request using Chrome/Firefox developer tools.
2. Login to the web application and browse to the billing information page
3. Capture the request to the billing information endpoint and send it to Repeater or Intruder
4. Modify the request to attempt to enumerate additional <flux capacitor> IDs and observe the billing information in the response.

Tools Used Burp Intruder

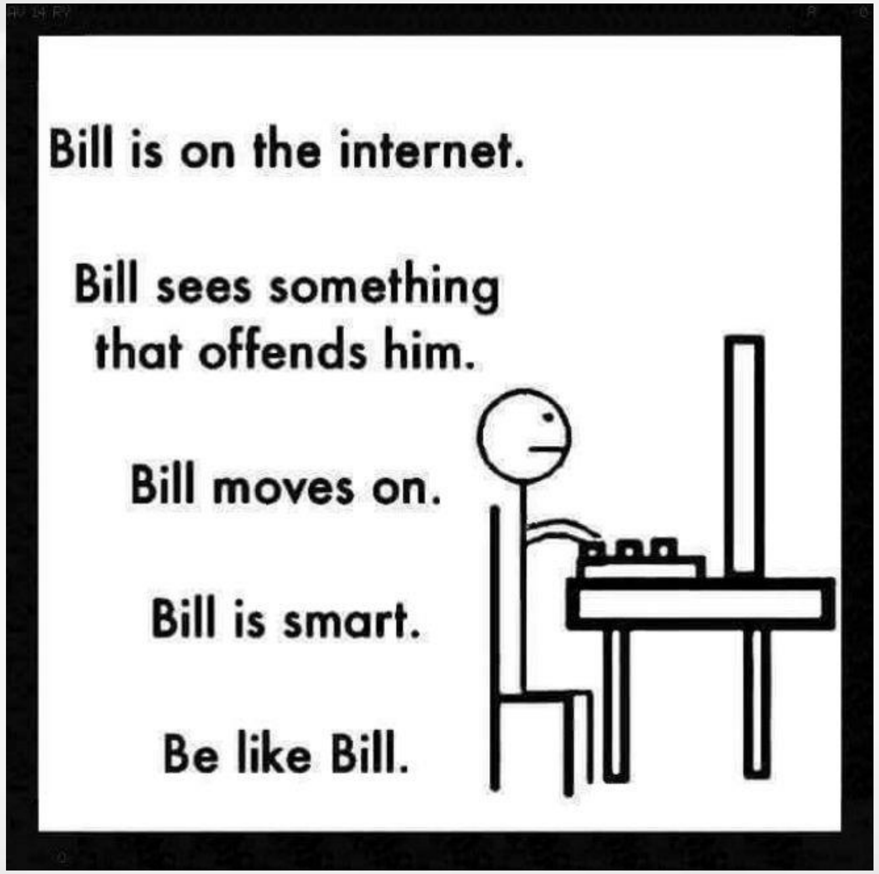
FINAL TIPS

Consider the business impact!


"Now remember, kids, the internet is serious business."
—Isaac Asimov
Renowned Science and Science-Fiction Author

[Source (Know Your Meme)]

Remember what it's all about.



Source (BBC)

Case Study: Instructure

	2013 (Pentest)	2014 (Bug Bounty)	2015 (Bug Bounty)
Critical	0	0	0
High	1	25	3
Medium	1	8	2
Low	2	16	5

Source (Instructure)

It's super
effective!

Source (Stack Exchange)

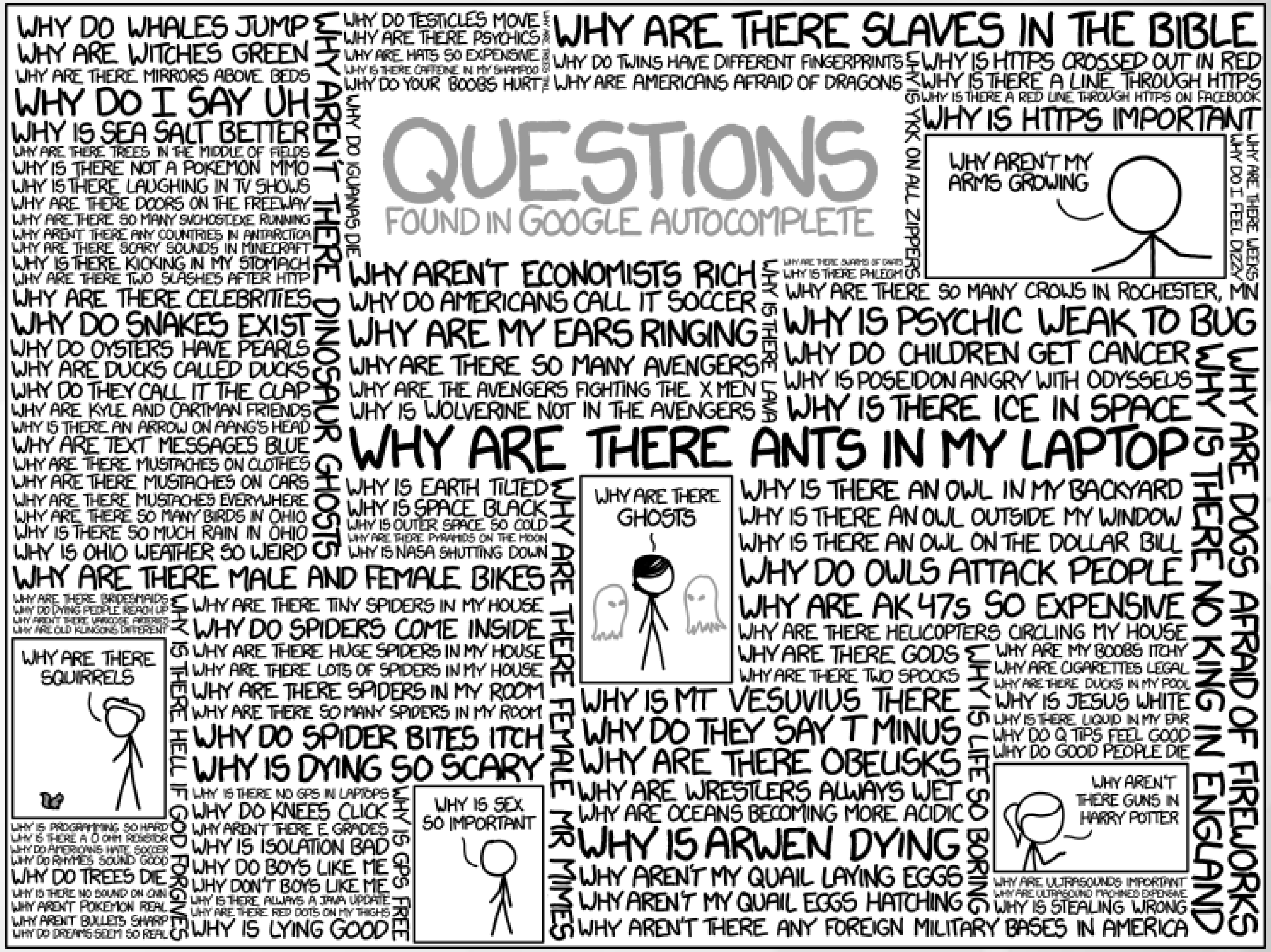
Thanks!

Grant McCracken

grant@bugcrowd.com

Daniel Trauner

dan@bugcrowd.com


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY IS YKK ON ALL ZIPPERS
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS THERE NO KING IN ENGLAND
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47S SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KLINGONS DIFFERENT
WHY ARE THERE SQUIRRELS
WHY IS THERE HELL IF GOD FORGIVES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY ARE THERE FEMALE MR MIMES
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY IS LIFE SO BORING
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT

Source (xkcd)