OWASP
AppSec Europe
London 2nd-6th June 2018

Capture the Flags

Gamifying Security Education

Max and John


wikiHow to Play Capture the Flag

Introduction

Max Feldman

Product Security

@MrsBufferworths

John Sonnenschein

Red Team

@johnnysunshine

Capture the Flags

Max and John

Let's Talk About

- Our SDL Process
- Security Education
- CTFs
- Planning
- The Flags
- Execution
- Lessons Learned

Our SDL Process

Capture the Flags

Max and John

Development at Slack

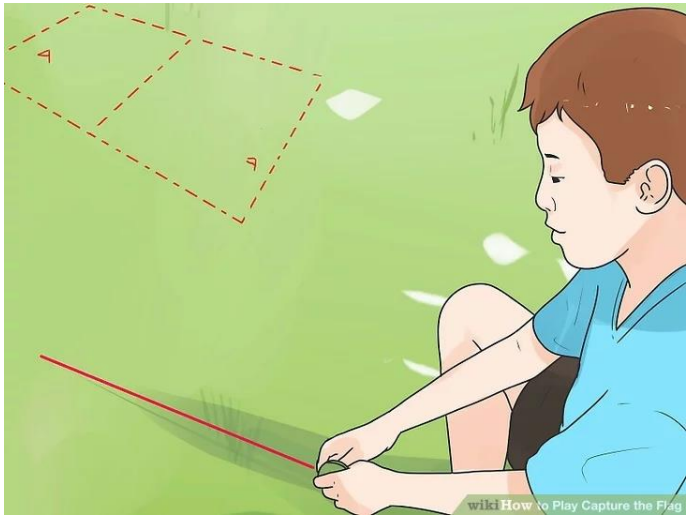
- We have a CI/CD pipeline
- Easy to push code
- 100 deploys to production daily

Capture the Flags

Max and John

Development at Slack

- SDL process/tool (just open-sourced!)
- Self-service checklists for security concerns, transparent communication
- Culture of trusting our developers



Security Education

Security Education

- Developers aren't always security experts
- Slideshows, text, etc. can be informative but boring
- Different employees, different backgrounds
- Goal: learn as a team, leverage everyone's unique skills

Capture the Flags

Max and John

Security Education

- Security training and classes can be expensive/overkill
- Security conferences may not be relevant enough
- Are also full of degenerates
- Can we improve our education techniques?

YES

CTFs

Capture the Flags

Max and John

CTFs

- Started/formalized at DEFCON 4, grown in popularity
  - More formalization, automation
- Two main types: jeopardy, attack/defense
- There is almost never a weekend without a CTF

Capture the Flags

Max and John

CTFs

- DEFCON 4: First formal CTF, contestants provided & then hacked others, points judged
- Organized by various groups, mostly winning CTF teams
- DEFCON, Black Hat, conferences
- SANS Netwars - CTF as training

Capture the Flags

Max and John

Recent/Noteworthy CTFs

- DEF CON 24 - Cyber Grand Challenge
  - First fully automated machine learning CTF
- DEF CON 25 - cLEMENcy
  - middle-endian, 9-bit byte length machine

Capture the Flags

Max and John

Pros

- Great puzzles
- Great rewards/incentives
- Great memes
- ctfd/fbctf/custom platforms have evolved

Cons

- Not always work-appropriate (e.g. Blaze CTF - The weed CTF)
- Tailored to a different level of security skill

Planning

Capture the Flags

Max and John

CTF Goals

- Raise security awareness and skills
- Engage a broad audience
  - Most of our employees are *not* hackers
- Measure our impact

Capture the Flags

Max and John

CTF Communication

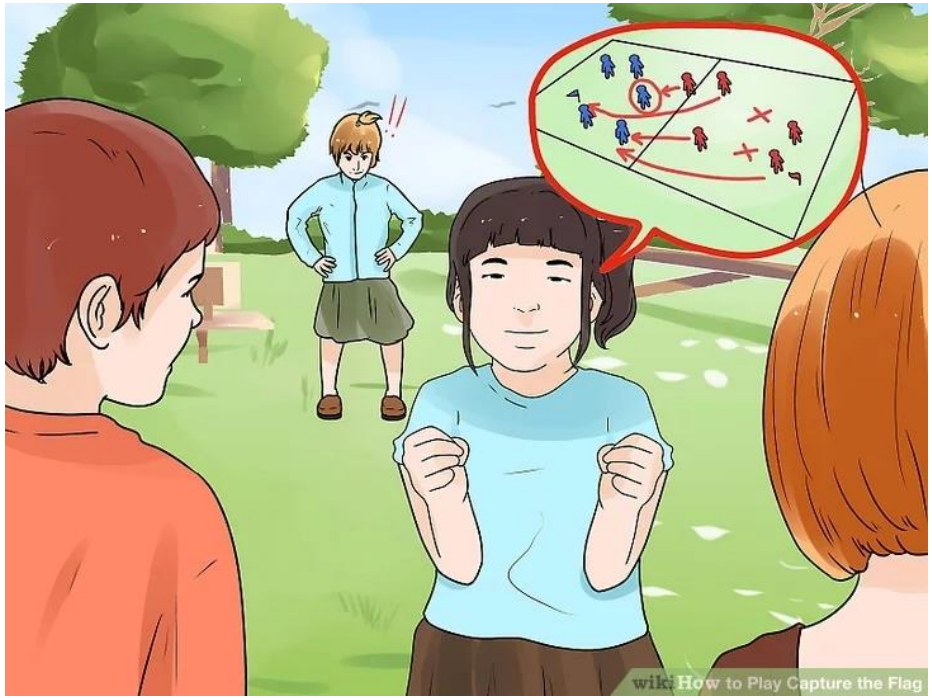
- Started planning for October (Hacktober) in August
- Plan with the internal events & comms departments
  - Also organized live lockpicking village
- Channels for CTF organizers and for CTF participants, office hours
- Avoiding disruption: length of time for the challenges to run
- PRIZES!!!

Capture the Flags

Max and John

CTF Planning

- Security trivia
- Webapp
- Crypto
- Forensics
- OSINT
- Slack-specific challenges



Capture the Flags

Max and John

CTF Infrastructure

- Chose fbctf (Thanks Facebook!) because it was prettier
  - fidgetspinning.life domain
  - Also a spreadsheet offering accessible version
- DigitalOcean
- Slack for collaboration
- Slack is Where CTFs Happen™

{the_flags}

Capture the Flags

Max and John

CTF Flags

- Meme-based, avocado toast?
- Heavy integration of puns
- Split the work between relevant teams

Capture the Flags

Max and John

Trivia and Sleuthing

- *If you WannaCry my lover, All your base are belong to us*
- Show some security pop culture
- OSINT and Slack-specific challenges
- Made to be accessible to anyone, regardless of technical level

Capture the Flags

Max and John

Trivia and Sleuthing

- *It's all Latin to me*
  - Simple ROT13, intro to Caesar ciphers
- *hash me outside how bow dah* (this was topical at the time)
  - Hashkiller MD5, showed ease of cracking

Capture the Flags

Max and John

Forensics

- IR Team put together a PCAP with an attack scenario
- Covered Wireshark basics, traffic analysis, .doc properties, EXIF

Capture the Flags

Max and John

Forensics

- A range of web application flags
  - HTML comments to PHP deserialization
- Covered many of OWASP Top 10
- XSS exploitation (including PhantomJS for automated verification of working exploit payload)

Execution

Capture the Flags

Max and John

CTF Execution

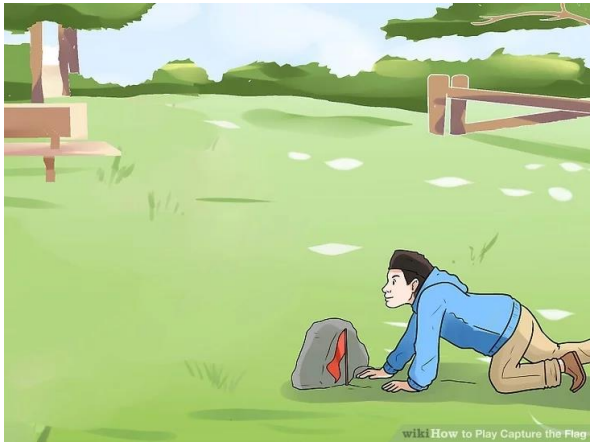
- Company-wide announcements, preparation, coordination with internal events
- By the end of day one, one team of 5 had most of the challenges
- Ran out of challenges
    - Had to make (/borrow) more challenges

Capture the Flags

Max and John

What Worked

- People participated, globally, diverse departments
- More interactions with the company (as a team, us as individuals)
- People asking about challenges, commenting/complimenting
- Teams were formed!
    - Teamwork makes the dream possible



Capture the Flags

Max and John

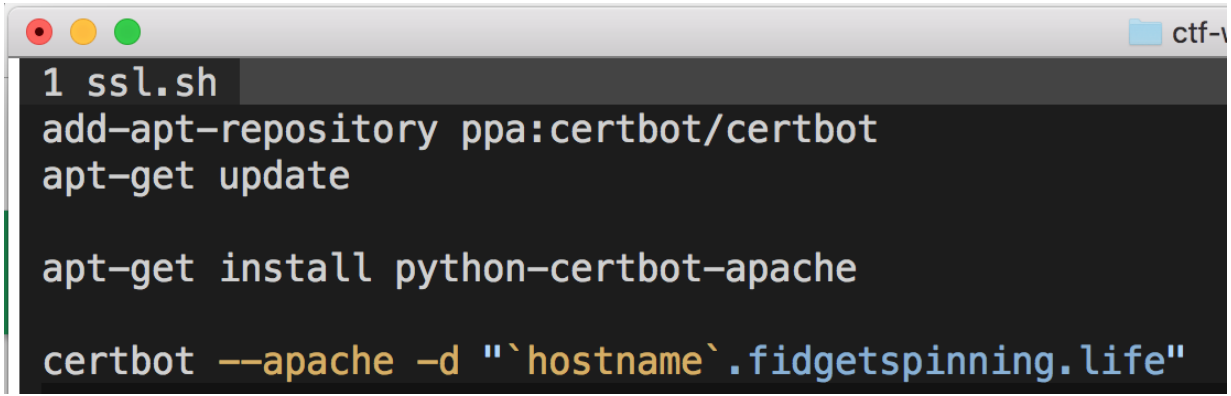
What Worked

- The servers stayed up*
  - *for the most part (five eights of availability, a B+)
- fbctf is flashy and fun
- Four individuals completed all challenges


redacted
Certificate of Hacking
presented to
redacted
for
Doing Good Hacking at the CTF
Security People
10/18/2017

What Didn't

- Fbctf
  - HHVM caching issues
  - Hard to pull a list of challenges, forces you to use the map
- Max not a sysadmin (lots of copy-pasting scripts)



Capture the Flags

Max and John

What Didn't

- Occasional flubs of challenges (in haste to make new ones)
- DigitalOcean
  - Probably a better way to utilize this
  - Manual fixes

Capture the Flags

Max and John

Surprises

- Pleasant surprises:
  - Higher than expected level of participation (good engagement, good discussions)
  - Attention from higher levels, engagement from ICs to execs
- Less pleasant:
  - Really smart people doing it (ran out of challenges)
  - Lol lost productivity from everyone involved

Lessons Learned

Capture the Flags

Max and John

Feedback

- Favorite challenge:
  - SQLi
  - SSRF, Python
- Least favorite:
  - XSS
  - Padding Oracle

Capture the Flags

Max and John

Feedback

- Positive aspects:
  - Collaboration
  - Education
- Areas to improve:
  - Sandboxing, more difficult challenges
  - “more pr, buildup!”

Capture the Flags

Max and John

Lessons Learned

- Have a cool domain name
  - Tidepods.life next
- Market better ahead of time
- Don’t underestimate people
- Incorporate more teams

Future Work

Capture the Flags

Max and John

Future Work

- Next October!
- More participation
- Communication++
- Tiers/prizes for different levels

Thank you!