Facebook CTF Platform

github.com/facebook/fbctf

Paul Marinescu
Capture The Flag

reverse engineering, forensics, web application security, cryptography, binary exploitation
Facebook opens up its anti-hacker training tool

Anyone can see how Capture the Flag teaches the value of strong security.

Jon Fingas 05.11.16 in Security

Companies frequently like to teach the virtues of online security through Capture the Flag competitions, where you're encouraged to both create hacks and protect against them. Developing those competitions isn't always easy. However, Facebook is giving trainers an upper hand by open sourcing the code for its own Capture the Flag platform, letting anyone host a similar cybersecurity challenge or build on what Facebook has learned. The move should be particularly useful for companies and

Facebook's plan to train a new generation of cybersecurity pros

Alexandra Samuel 13 May 2016

Facebook likes hackers. Not the kind that break into its accounts, but the ethical kind that can find and fix software vulnerabilities that plague massive tech companies.

In fact, it is so committed to educating and encouraging this kind of bug hunting that it's sharing its internal Capture the Flag (CTF) security training platform with high schoolers, college students, and anyone who wants to learn how to think more like a hacker.

You Can Now Play Capture the Flag Through Facebook

by Robert Hackett @rhhackett

MAY 11, 2016, 6:00 AM EDT

Motivation

Demand for Infosec professions is growing 3.5x faster than the overall IT job market (12x faster than total labor market)
Motivation

The U.S. Bureau of Labor Statistics predicts more than two thirds of the 1.4 million security jobs needed by 2020 will go unfilled.
Infosec at Facebook

Security Engineers

Whitehat Program
Educational Tools

- Scarce for schools, students and non-profits
- CTFs can teach more technical skills than an average computer science program
History
We Organized CTFs

• From middle schools to Girl Scouts of America to University of Cambridge to Security Conferences

• ...and dozens of places in-between
Open Source@FB Gained Momentum

• HHVM
• Flow
• osquery
• React
• ... and a lot more
We have snacks downstairs if you need a break!

Hint: The biggest flag has 256 bits.

Egypt is open again.

Angola just got easier (32 bits all the way!)

Belarus Crypto challenge is open.

Egypt challenge will be reopened later. Work on something else for now.

[ 11:14:51 ] oxford captured United Kingdom
[ 11:15:16 ] oxford captured Austria
[ 11:17:25 ] Cambridge captured Austria
[ 11:17:25 ] phishnchips captured Austria
[ 11:17:33 ] phishnchips captured Yemen
[ 11:17:42 ] Cambridge captured United Kingdom
[ 11:17:54 ] Cambridge captured Yemen
TEAM REGISTRATION

Register to play Capture The Flag here. Once you have registered, you will be logged in.

NAME: Derp
EMAIL: derp@facebook.com
TEAM NAME: 0xFEEDFACE
PASSWORD: ****

CHOOSE AN EMBLEM
tutorial_Captures

Countries marked with an ▲ are captured by you.
Countries marked with an △ are owned by others.

NEXT

SKIP TO PLAY

Flag challenge is open!
The game has started!
What protocol is described in RFC 2324?

Hyper Text Coffee Pot Control Protocol

NO HINT SUBMIT

10 PTS
type quiz
category Quiz
first_capture Uncaptured
You've recovered 3 encrypted files and an RSA public key. Since the files are RSA encrypted and RSA hasn't been broken yet, I guess you should just give up now.

[ tooSmall_b641b3a6f87b8f2b495b358be80197.tar.gz ]

flag[rsa_i5_n00b]

REQUEST HINT

**100**

flag

category

None

first_capture

Uncaptured

completed_by >
$ git clone https://github.com/facebook/fbctf
$ cd fbctf
$ vagrant up
Challenge library available on demand

reverse engineering, forensics, web application security, cryptography, binary exploitation
Two Weeks Later

> 4,000 stars

> 650 forks

3rd party contributions
Under the Hood

- Hack/HHVM
- XHP
- Flow
Bug Bounty

Report through the bug bounty system before sending a pull request
Cambridge CTF
April 2016
• Organized by Cambridge University and Facebook
• 10 participating UK universities
• Two parallel CTFs (on-site and online)
• 5 hours
Challenges

• 30 challenges
• Equal number of quizzes and flags
• One *base* (king of the hill)
• Guest challenges
• 2 left unsolved
3 Amazon EC2 instances per CTF
<table>
<thead>
<tr>
<th>filter_</th>
<th>rank</th>
<th>team_name_</th>
<th>quiz_pts_</th>
<th>flag_pts_</th>
<th>base_pts_</th>
<th>total_pts_</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CAMBRIDGE</td>
<td>330</td>
<td>2425</td>
<td>741</td>
<td>3476</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>IMPERIAL COLLEGE</td>
<td>330</td>
<td>2020</td>
<td>0</td>
<td>2330</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>SUCSS_2_BU</td>
<td>330</td>
<td>1010</td>
<td>967</td>
<td>2307</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>PHISHNCHIPS</td>
<td>330</td>
<td>1485</td>
<td>0</td>
<td>1815</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>OXFORD</td>
<td>330</td>
<td>980</td>
<td>0</td>
<td>1270</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>AFNOM</td>
<td>330</td>
<td>750</td>
<td>0</td>
<td>1080</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>QUB</td>
<td>330</td>
<td>400</td>
<td>0</td>
<td>730</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>4DUMBKENTS</td>
<td>330</td>
<td>290</td>
<td>0</td>
<td>620</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>SURREY</td>
<td>330</td>
<td>220</td>
<td>0</td>
<td>550</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>UCL-THOR</td>
<td>330</td>
<td>205</td>
<td>0</td>
<td>480</td>
</tr>
</tbody>
</table>
Happy Hacking!

github.com/facebook/fbctf