



Everyone Can Play! Building CTFs for Non-Security Folks

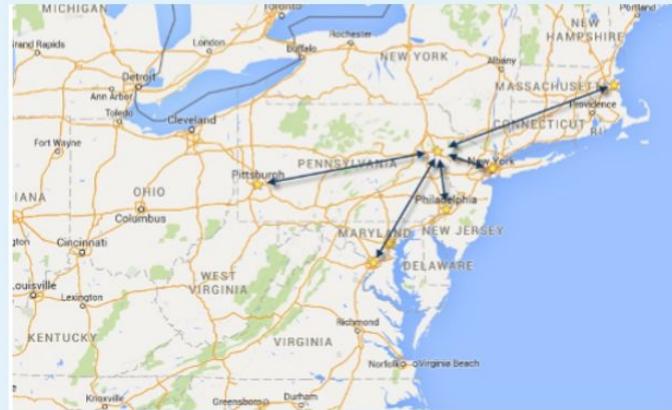
APRIL 2025

Joe Kuemerle

@jkuemerle@infosec.exchange

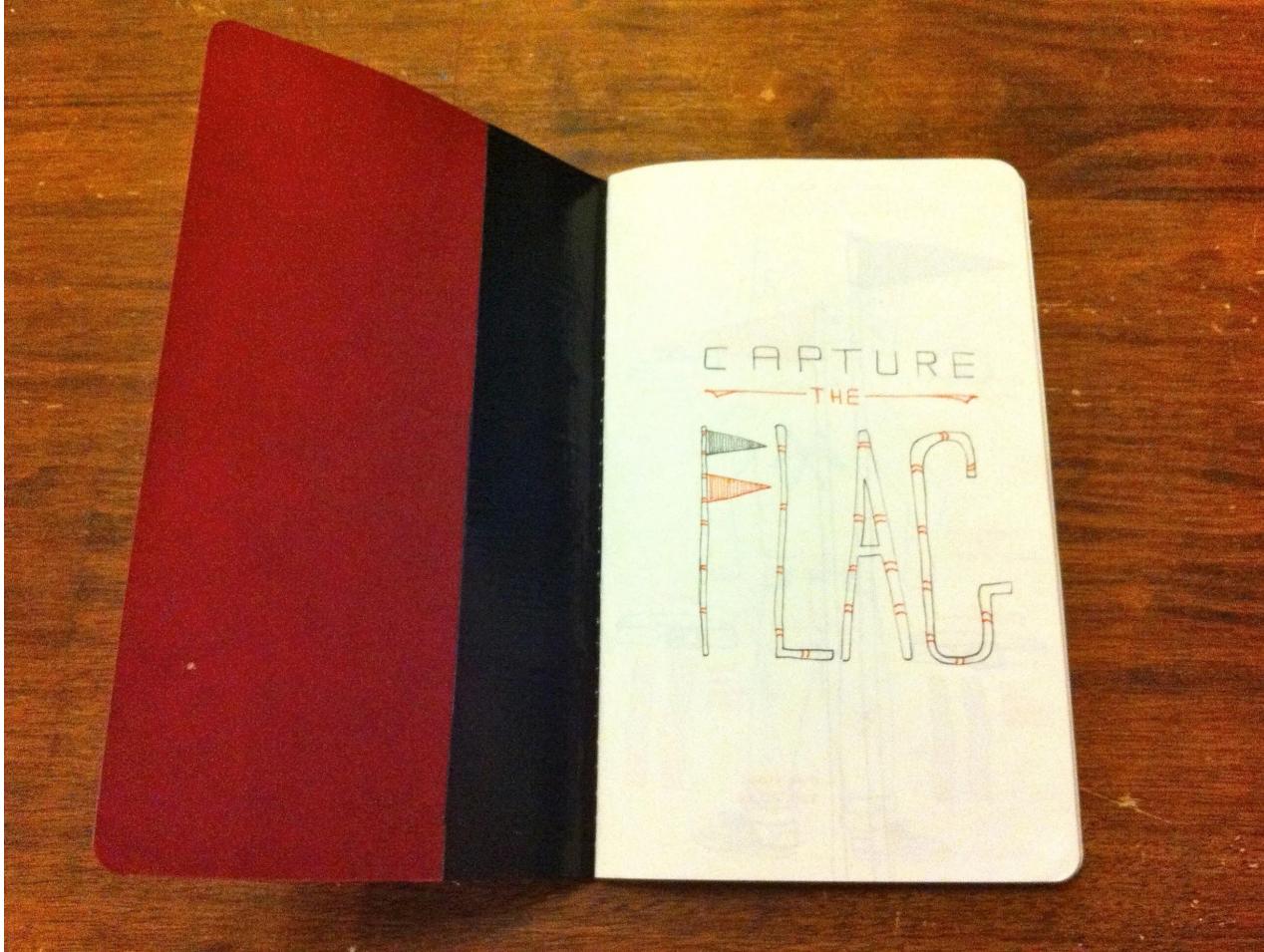
www.owasp.org

- Great speakers with top content
- A fraction of the cost of the more crowded conferences
 - 3-day conference plus lodging for ~\$1000
- Full-day deep dive preconference sessions available
- Easy travel from almost anywhere
- World-class keynotes
- In addition to the sessions, you get a great hallway Track, amazing food, attendee Welcome Reception, Game Night & more
- Family Day Friday - full day of kids' sessions, free for attendees' families
- Discounted Kalahari Resort rooms with water park access: stay, learn & play all week



Agenda

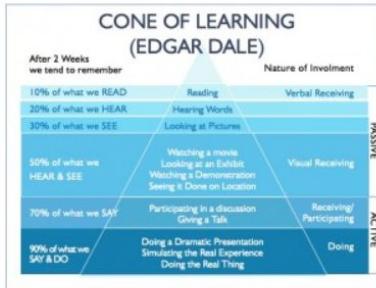
- **Why**
 - Learning studies
 - Proven success
- **What**
 - Building challenges
 - Easy to participate
 - Fun
- **How**
 - Easy to run
 - Measured





Source: National Training Laboratories, Bethel, Maine

Examples of what the Cone of Experience became. The links to the images above have been removed to protect the mistaken. They are just two examples of the hundreds found on a simple Web search.



<https://acrl.org/2014/01/13/tales-of-the-undead-learning-theories-the-learning-pyramid>



Multimodal Learning Through Media: What the Research Says



By Metiri Group – Commissioned by Cisco

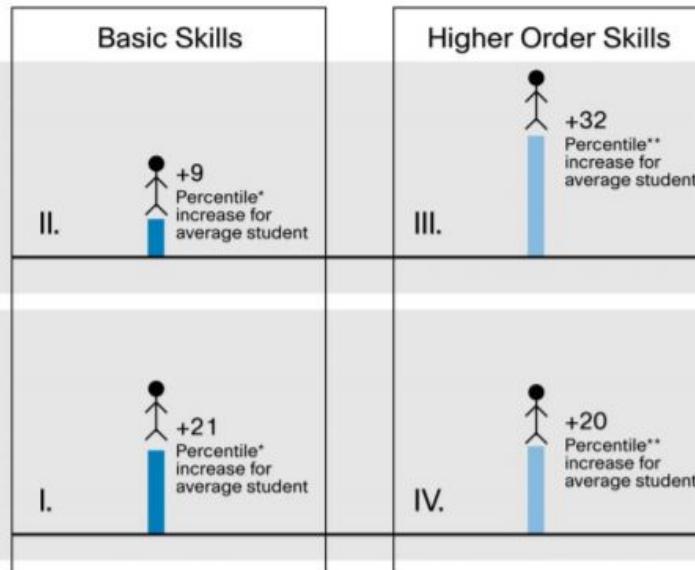
Contacts:

Charles Fadel, Global Lead, Education, Cisco Systems, Inc.: cfadel@cisco.com
Cheryl Lemke, CEO, Metiri Group: clemke@metiri.com

Multimodal Learning Through Media: What the Research Says

The Impact of Multimodal Learning in Comparison to Traditional, Unimodal Learning

Findings Reported Separately for Basic Skills and Higher Order Skills, and by the Inclusion or Absence of Interactivity



Interactive Multimodal Learning
Includes simulations, modeling, and real world experiences; typically includes collaboration with peers, but could be an individual interacting with resource

Non-Interactive Multimodal Learning
Includes using text with illustrations, watching and listening to animations, listening to lecture with graphics on devices such as whiteboards, etc.: typically involves individualized learning, or whole-group work that includes listening, observing, or reading, but little to no interaction



https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/Multimodal-Learning-Through-Media.pdf

1. Multimedia Principle: Retention is improved through words and pictures rather than through words alone.

2. Spatial Contiguity Principle: Students learn better when corresponding words and pictures are presented near each other rather than far from each other on the page or screen.

3. Temporal Contiguity Principle: Students learn better when corresponding words and pictures are presented simultaneously rather than successively.

4. Coherence Principle: Students learn better when extraneous words, pictures, and sounds are excluded rather than included.

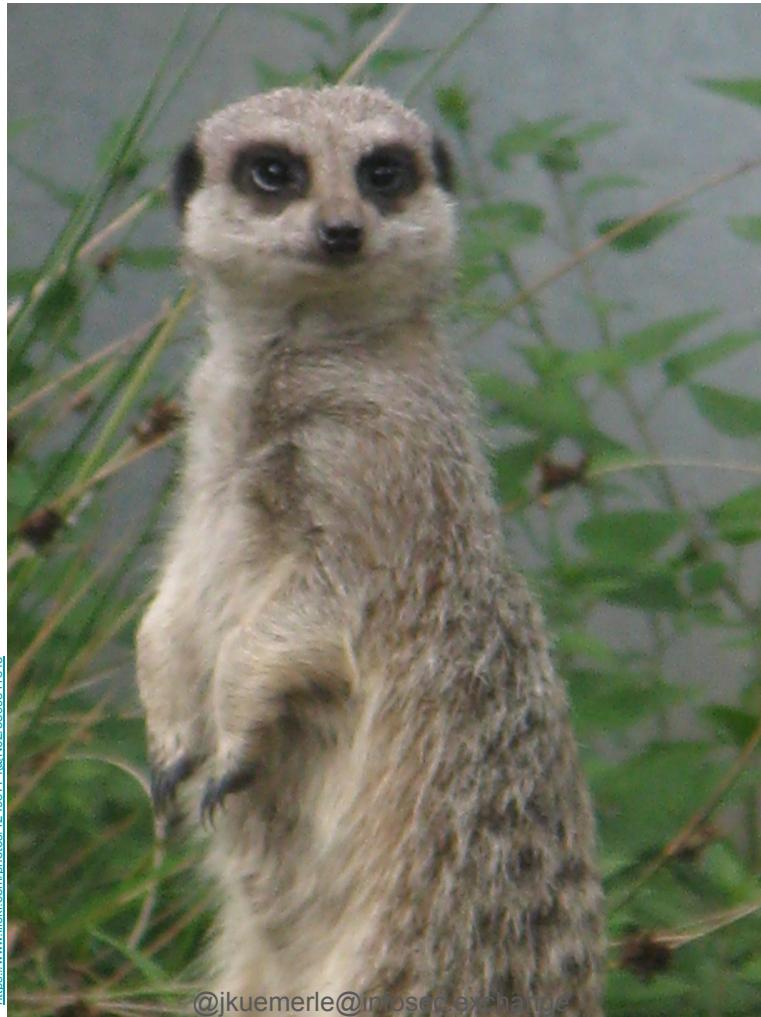
5. Modality Principle: Students learn better from animation and narration than from animation and on-screen text.

6. Redundancy Principle: Students learn better when information is not represented in more than one modality – redundancy interferes with learning.

7a. Individual Differences Principle: Design effects are higher for low-knowledge learners than for high-knowledge learners.

7b. Individual Differences Principle: Design effects are higher for high-spatial learners rather than for low-spatial learners.

8. Direct Manipulation Principle: As the complexity of the materials increase, the impact of direct manipulation of the learning materials (animation, pacing) on transfer also increases



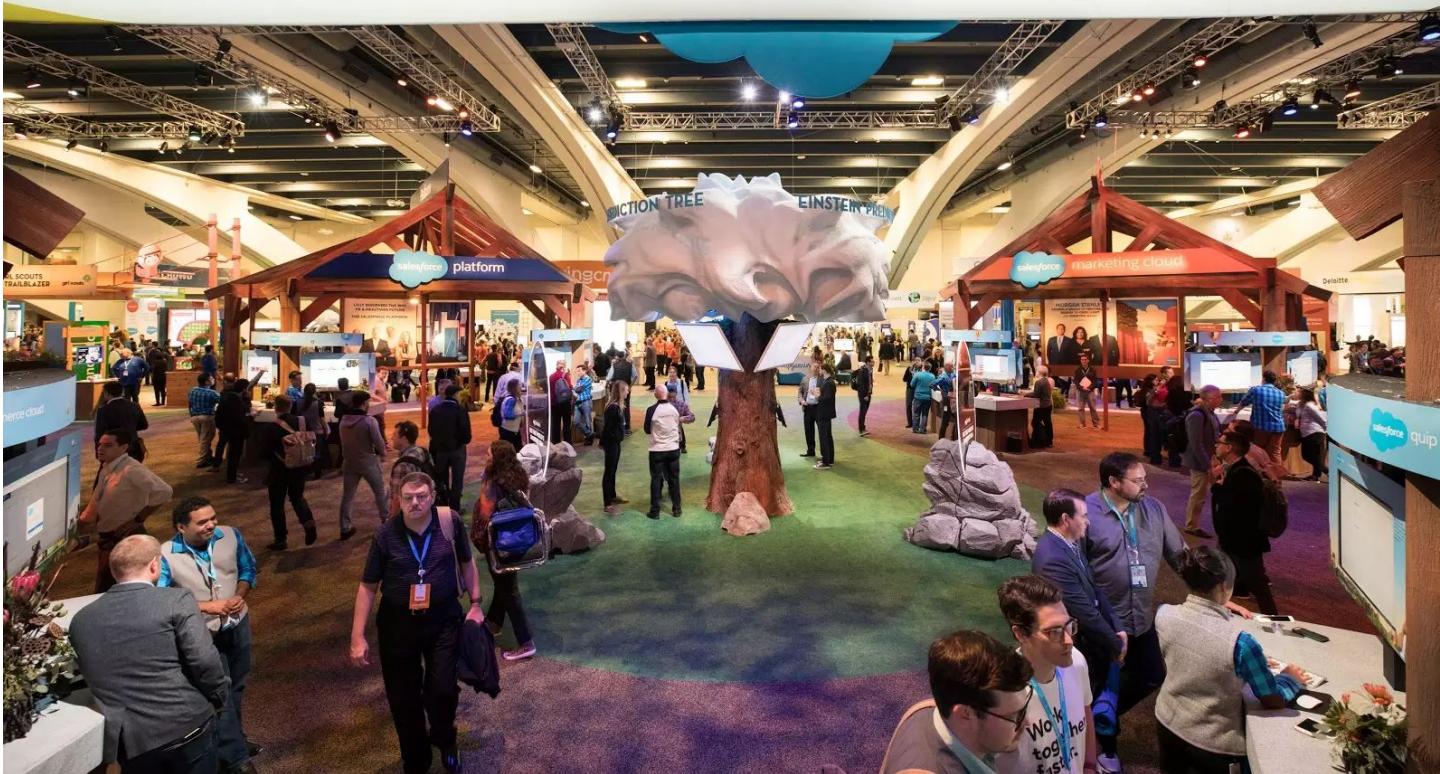
<https://www.flickr.com/photos/12495774@N02/3899511543>

@jkuemerle@infosec.exchange



@jkuemerle@infosec.exchange

CONNECT TO YOUR CUSTOMERS IN A WHOLE NEW WAY



https://trailhead.salesforce.com/pt-BR/content/learn/modules/get_ready_for_dreamforce_onsite/get_ready_for_dreamforce_onsite_get_to_know_the_campus

@jkuemerle@infosec.exchange



<https://www.flickr.com/photos/37984062@N03/3495248498>

1. Multimedia Principle: Retention is improved through words and pictures rather than through words alone.

2. Spatial Contiguity Principle: Students learn better when corresponding words and pictures are presented near each other rather than far from each other on the page or screen.

3. Temporal Contiguity Principle: Students learn better when corresponding words and pictures are presented simultaneously rather than successively.

4. Coherence Principle: Students learn better when extraneous words, pictures, and sounds are excluded rather than included.

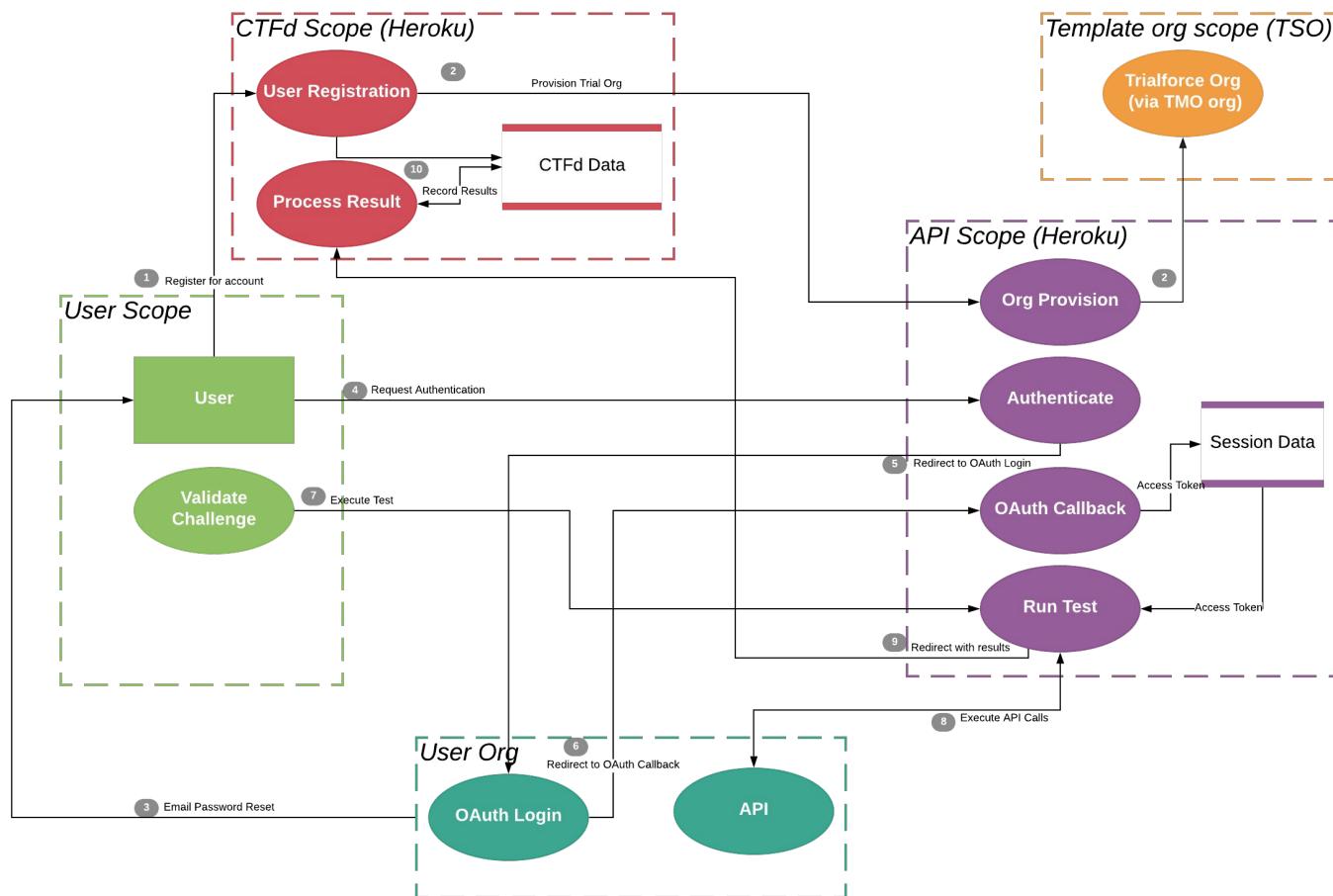
5. Modality Principle: Students learn better from animation and narration than from animation and on-screen text.

6. Redundancy Principle: Students learn better when information is not represented in more than one modality – redundancy interferes with learning.

7a. Individual Differences Principle: Design effects are higher for low-knowledge learners than for high-knowledge learners.

7b. Individual Differences Principle: Design effects are higher for high-spatial learners rather than for low-spatial learners.

8. Direct Manipulation Principle: As the complexity of the materials increase, the impact of direct manipulation of the learning materials (animation, pacing) on transfer also increases



<https://engineering.salesforce.com/capture-the-flag-secure-your-knowledge-37b43180e55a>

Register

First Name

Last Name

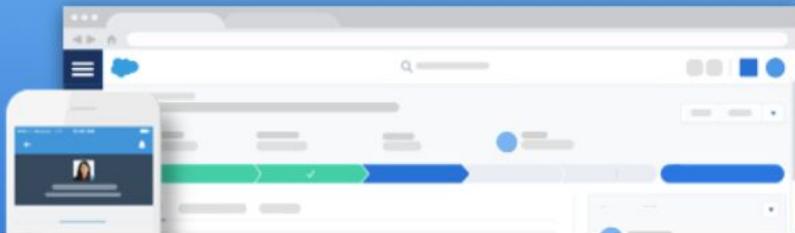
User Name

Email

Password

Submit

Thanks for signing up with Salesforce!



Click below to verify your account.

Verify Account

To easily log in later, save this URL:

[https://\[REDACTED\].my.salesforce.com](https://[REDACTED].my.salesforce.com)

Username:

[REDACTED]@[REDACTED].com.399495

Again, welcome to Salesforce!

@jkuemerle@infosec.exchange

Challenges

Initialization

Initialize
50

Trivia

Trivia012 100	Trivia013 100	Trivia014 100	Trivia015 100
Trivia016 100	Trivia017 100	Trivia018 100	Trivia019 100
Trivia020 100	Trivia021 100	Trivia028 100	Trivia029 100
Trivia030 100	Trivia031 100	Trivia032 100	Trivia033 100
Trivia034 100	Trivia035 100	Trivia036 100	Trivia037 100

Challenge

0 Solves



Cross Site Scripting Protection

500

Astro read the following snippet and wanted to secure their org in the same way: If a reflected cross-site scripting attack is detected, the browser renders a blank page with no content.

Help Astro secure their org so that if a reflected cross-site scripting (XSS) attack is detected, the browser renders a blank page with no content.

Validate



SETUP

Session Settings

Enable Stricter Content Security Policy [i](#)

Lightning Locker API Version

Use security enhancements in API version

47.0



Freeze JavaScript Prototypes

Freeze JavaScript Prototypes [i](#)

XSS protection

Enable XSS protection

Content Sniffing protection

Enable Content Sniffing protection

Challenge

0 Solves



Cross Site Scripting Protection

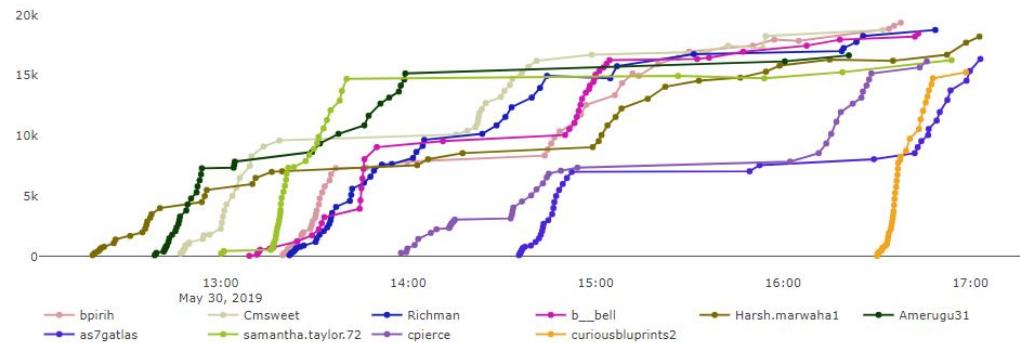
500

Congratulations! Your flag value is: JhdHVs

Submit Flag

Scoreboard

Top 10 Teams



Place	Team	Score
1	bpirih	19350
2	Cmsweet	18750
3	Richman	18750
4	b__bell	18450

<https://flickr.com/photos/codepo8/5790470307/>



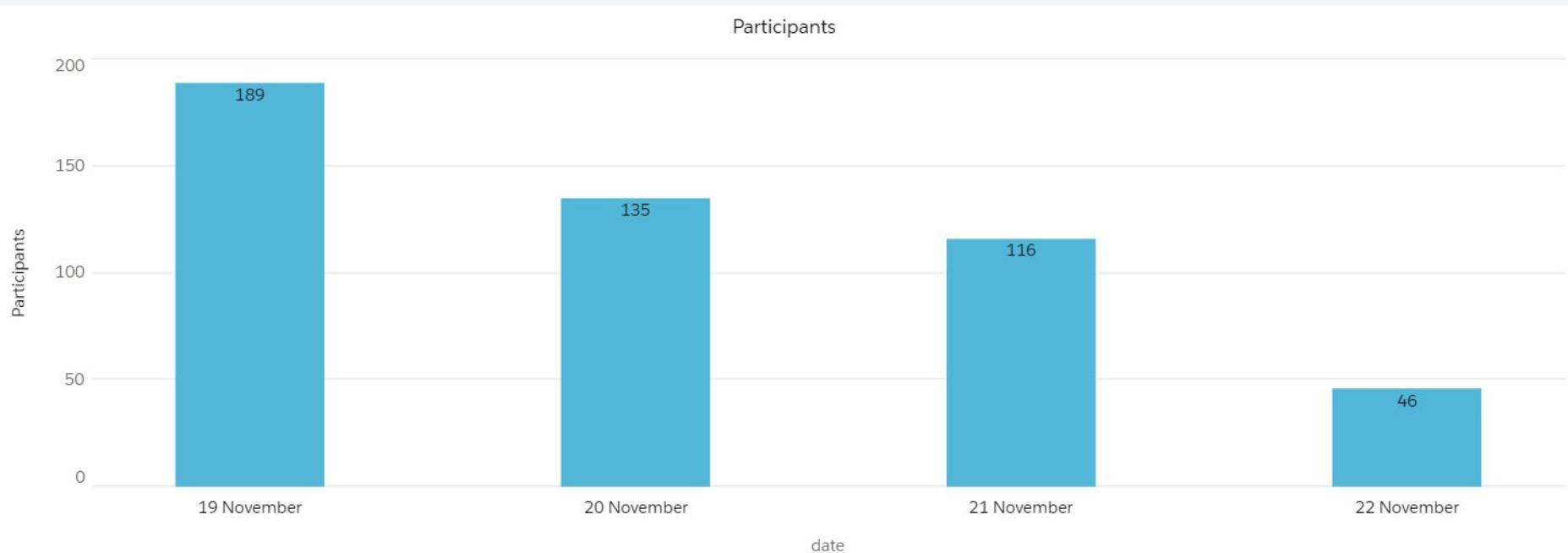
@jkuemerle@infosec.exchange

<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>

Total Participants

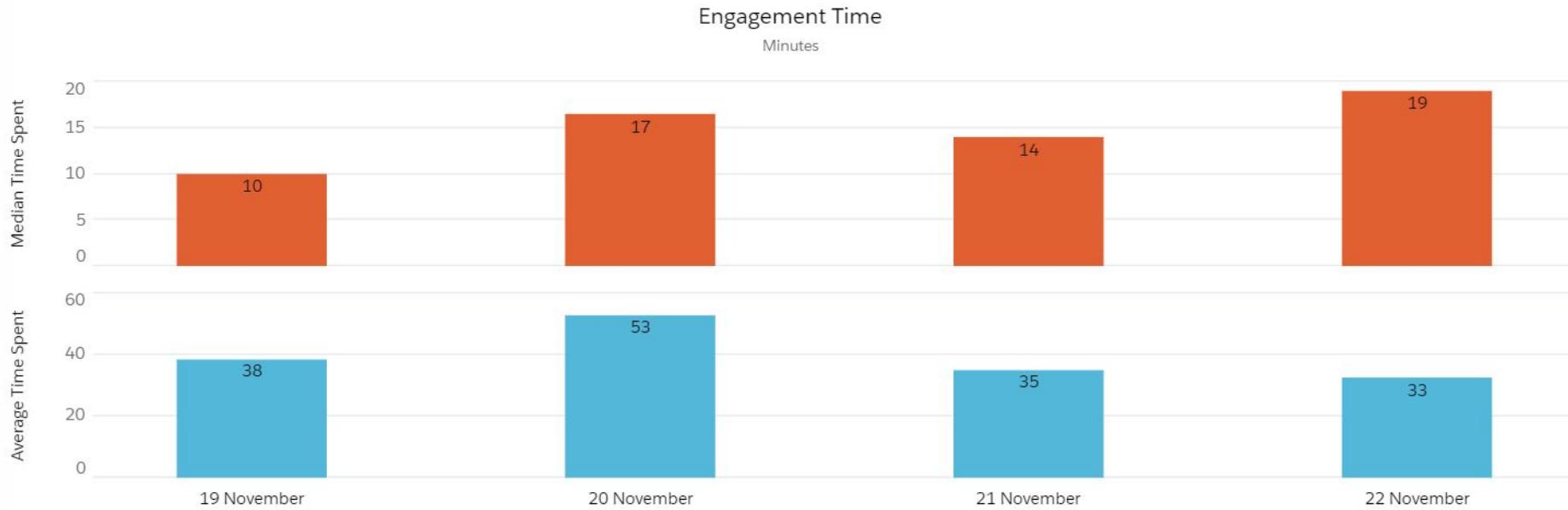
486

Participants

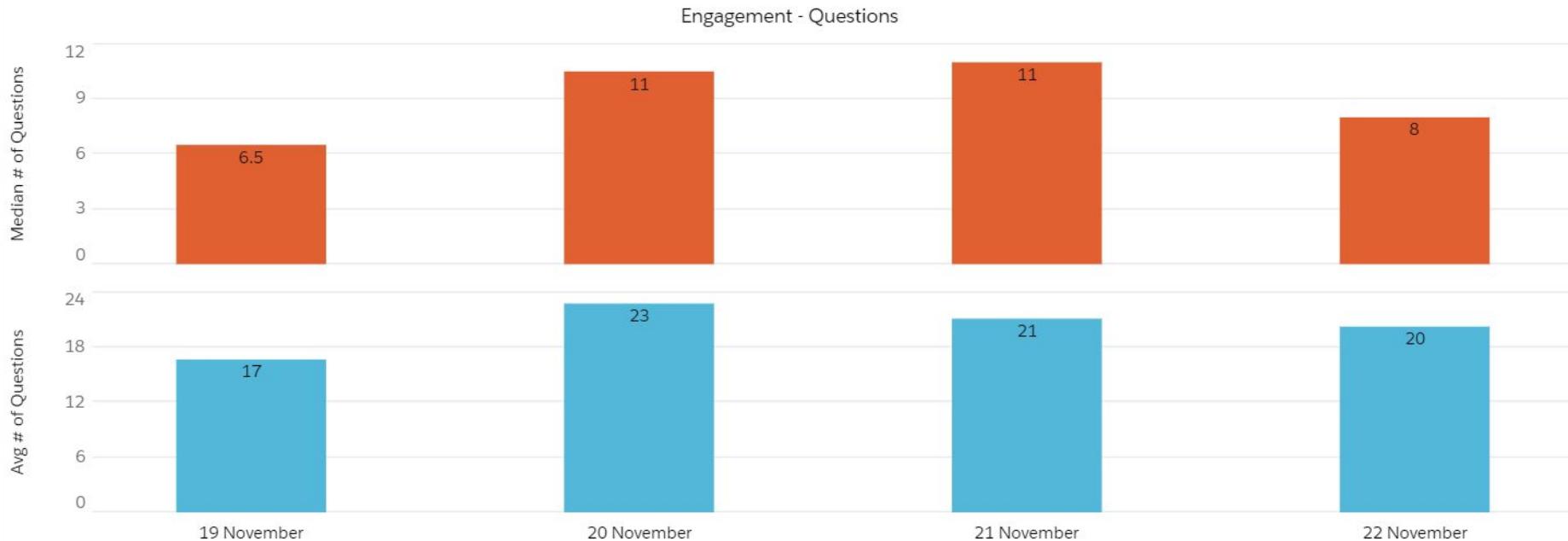


@jkuemerle@infosec.exchange

<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>

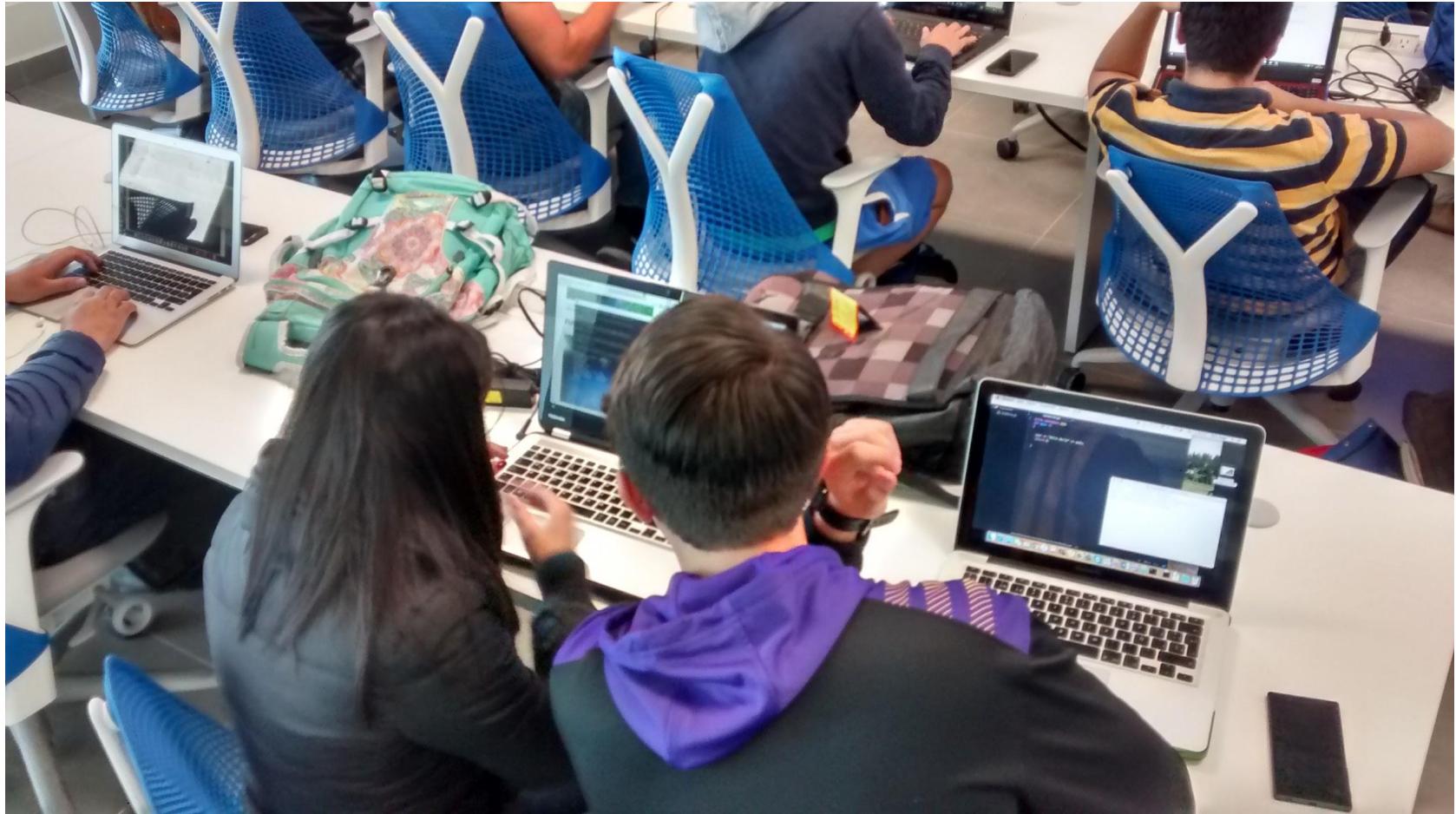


<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>



<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>







<https://www.flickr.com/photos/79673928@N08/10519784515>

@jkuemerle@infosec.exchange



CROSSWORD 78

ACROSS
1. Scraps
6. Bulwarks'
9. Kill
10. Troubles
12. Voice range
13. Little story
15. Little story
16. Story
18. Novel, e.g.
19. Cut or break
20. Mild south
21. Curved
22. Tavern drink
23. Sip
24. Words or lines
25. Mischievous
26. Tyke

20. Made a
choice
30. Glutton
32. Owner's
name
33. Necessity
34. —
35. Wonderful
Life
36. — & port
37. More with
less
38. Blood
39. Wriggling
41. Assumption
43. Duds
45. Wiener dog
46. Duds
47. Friend of
good fortune

49. Diesel (1)
air system
51. Gun game
52. — of
luxury
53. Royal
feature
54. —
55. Fool poorly
56. Forwarded
57. Dismayed
58. Tame
59. Shape

DOWNS

1. Lading lode
2. Airborne toy
3. Maxine
4. Headliner
5. Audited tape
6. Fleet
7. Wood collector
8. Chalkings
9. Large segment
10. Stone layer

11. Auto

12. Imperfection
13. Soft drink
14. Hawaiian
15. That by the
hand by the
hand — Girls'

87. Offset
88. Very fine
rain
89. Game missile

90. Tires
91. Miss
92. In the back
93. Dog
94. Classification
95. City van
96. Frosted
97. Liquid rock
98. In any way
99. Raisin
100. Pounding
tires
101. Arctic
transport
102. Soft drink
103. Hawaiian
104. More than
should be
105. Outrageous
106. That by the
hand by the
hand — Girls'

107. Horse's kin
108. Pin's kin
109. In the back
110. Carving
111. Auto
112. Headline
113. Auto
114. Auto
115. Auto
116. Auto
117. Auto
118. Auto
119. Auto
120. Auto
121. Auto
122. Auto
123. Auto
124. Auto
125. Auto
126. Auto
127. Auto
128. Auto
129. Auto
130. Auto
131. Auto
132. Auto
133. Auto
134. Auto
135. Auto
136. Auto
137. Auto
138. Auto
139. Auto
140. Auto
141. Auto
142. Auto
143. Auto
144. Auto
145. Auto
146. Auto
147. Auto
148. Auto
149. Auto
150. Auto
151. Auto
152. Auto
153. Auto
154. Auto
155. Auto
156. Auto
157. Auto
158. Auto
159. Auto
160. Auto
161. Auto
162. Auto
163. Auto
164. Auto
165. Auto
166. Auto
167. Auto
168. Auto
169. Auto
170. Auto
171. Auto
172. Auto
173. Auto
174. Auto
175. Auto
176. Auto
177. Auto
178. Auto
179. Auto
180. Auto
181. Auto
182. Auto
183. Auto
184. Auto
185. Auto
186. Auto
187. Auto
188. Auto
189. Auto
190. Auto
191. Auto
192. Auto
193. Auto
194. Auto
195. Auto
196. Auto
197. Auto
198. Auto
199. Auto
200. Auto
201. Auto
202. Auto
203. Auto
204. Auto
205. Auto
206. Auto
207. Auto
208. Auto
209. Auto
210. Auto
211. Auto
212. Auto
213. Auto
214. Auto
215. Auto
216. Auto
217. Auto
218. Auto
219. Auto
220. Auto
221. Auto
222. Auto
223. Auto
224. Auto
225. Auto
226. Auto
227. Auto
228. Auto
229. Auto
230. Auto
231. Auto
232. Auto
233. Auto
234. Auto
235. Auto
236. Auto
237. Auto
238. Auto
239. Auto
240. Auto
241. Auto
242. Auto
243. Auto
244. Auto
245. Auto
246. Auto
247. Auto
248. Auto
249. Auto
250. Auto
251. Auto
252. Auto
253. Auto
254. Auto
255. Auto
256. Auto
257. Auto
258. Auto
259. Auto
260. Auto
261. Auto
262. Auto
263. Auto
264. Auto
265. Auto
266. Auto
267. Auto
268. Auto
269. Auto
270. Auto
271. Auto
272. Auto
273. Auto
274. Auto
275. Auto
276. Auto
277. Auto
278. Auto
279. Auto
280. Auto
281. Auto
282. Auto
283. Auto
284. Auto
285. Auto
286. Auto
287. Auto
288. Auto
289. Auto
290. Auto
291. Auto
292. Auto
293. Auto
294. Auto
295. Auto
296. Auto
297. Auto
298. Auto
299. Auto
300. Auto

<https://www.flickr.com/photos/78814955@N00/46868044302>

@jkuemerle@infosec.exchange

- **Relevancy** - challenges should use the same technologies and platforms that the participants work in
- **Appropriateness** - challenges should cover vulnerability categories that are known to exist in the participants codebases
- **Interesting/Engaging** - challenges should draw the participants attention and encourage them to find solutions
- **Solvable** - challenges should have a clear and accurate solution
- **Reflective** - challenges should reinforce targeted concepts

<https://www.flickr.com/photos/93416311@N00/2195946360>



@jkuemerle@infosec.exchange

Red Flags - Avoid

- **Excessive Obscurity** - solutions should be discoverable (with a reasonable amount of effort)
- **Non-Relevant** - work to solve challenges should not be far outside of the participants skill set and work requirements
- **Open Ended** - challenges should have enough guidance to allow the participant to find an agreed upon “good” solution



<https://www.flickr.com/photos/21597369@N06/2091577071>

@jkuemerle@infosec.exchange

TO DO:

- Hang Whiteboard
- Buy Different Color
Markers

- **Relevancy** - challenges should use the same technologies and platforms that the participants work in
- **Appropriateness** - challenges should cover vulnerability categories that are known to exist in the participants codebases
- **Interesting/Engaging** - challenges should draw the participants attention and encourage them to find solutions
- **Solvable** - challenges should have a clear and accurate solution
- **Reflective** - challenges should reinforce targeted concepts

Red Flags - Avoid

- **Excessive Obscurity** - solutions should be discoverable (with a reasonable amount of effort)
- **Non-Relevant** - work to solve challenges should not be far outside of the participants skill set and work requirements
- **Open Ended** - challenges should be have enough guidance to allow the participant to find an agreed upon “good” solution



**Click to
Enter the
Course**

<https://www.flickr.com/photos/95380334@N04/8704970501>

@jkuemerle@infosec.exchange

https://github.com/salesforce/integrated_challenge



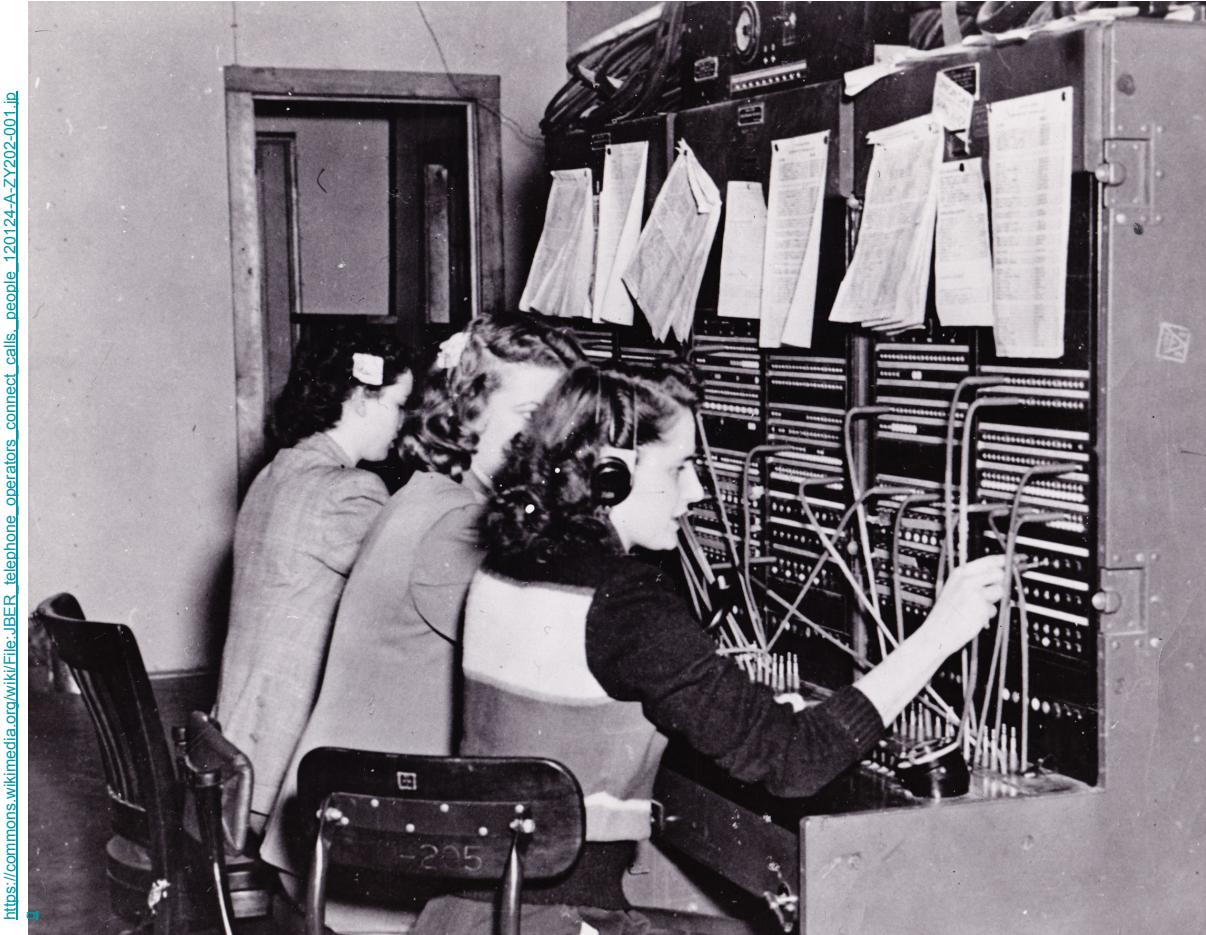
<https://www.flickr.com/photos/5031888@N00/304867602>

@jkuemerle@infosec.exchange





<https://www.flickr.com/photos/144008357@N08/3294365784>



https://commons.wikimedia.org/w/index.php?title=File:IBER_telephone_operators_connect_calls_1940s.jpg

@jkuemerle@infosec.exchange



<https://www.flickr.com/photos/23299838@N08/3350934724>

@jkuemerle@infosec.exchange

http://www.bertiesinn.com/beltsander_races/2017_beltsander_race.html



@jkuemerle@infosec.exchange



Confidential Document - Sensitive
100

Zero Stars
100

Login Admin
250

Weird Crypto
250

Bjoern's Favorite Pet - Broker
450

Forged Review
450

Login Amy
450

Login Jim
450

Payback Time
450

Product Tampering
450

Access Log - Sensitive Data Exposure
700

Misplaced Signature File
700

Server-side XSS Protection
700

User Credentials
700

Change Bender's Password - Emergency
1000

Email Leak - Sensitive Data Exposure
1000

Extra Language - Broken Anti-CSRF
1000

Frontend Typosquatting
1000

NoSQL Exfiltration
1000

Reset Bjoern's Password
1000

Two Factor Authentication
1000

Imaginary Challenge
1350

SSRF
1350





<https://www.flickr.com/photos/jheezzy/3769080979/>

@jkueemerle@infosec.exchange



<https://www.wikipedia.org/w/index.php?title=Integration&oldid=9100000>

Platforms

Projects that can be used to host a CTF

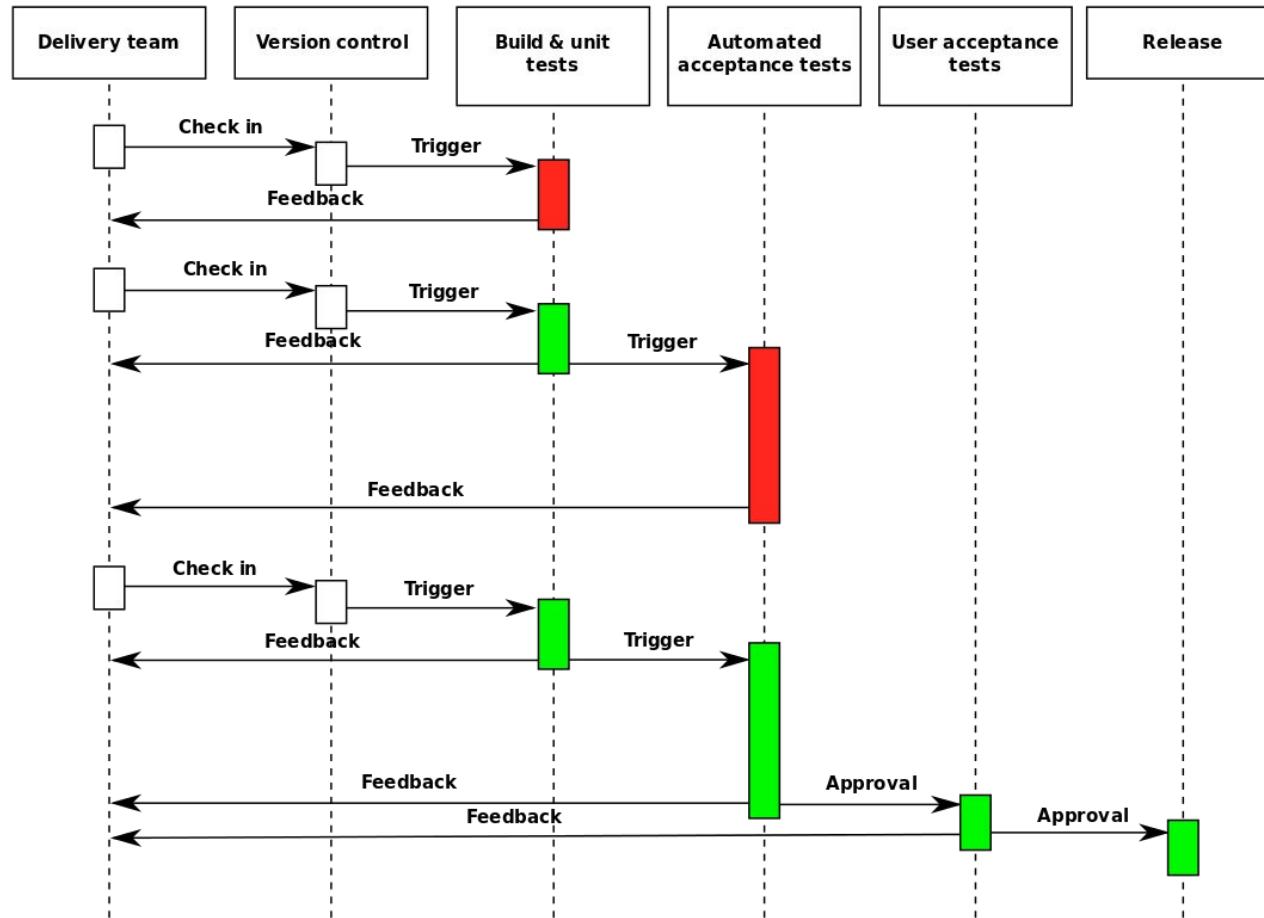
- [CTFd](#) - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon.
- [FBCTF](#) - Platform to host Capture the Flag competitions from Facebook.
- [Haaukins](#)- A Highly Accessible and Automated Virtualization Platform for Security Education.
- [HackTheArch](#) - CTF scoring platform.
- [Mellivora](#) - A CTF engine written in PHP.
- [NightShade](#) - A simple security CTF framework.
- [OpenCTF](#) - CTF in a box. Minimal setup required.
- [PicoCTF](#) - The platform used to run picoCTF. A great framework to host any CTF.
- [PyChallFactory](#) - Small framework to create/manage/package jeopardy CTF challenges.
- [RootTheBox](#) - A Game of Hackers (CTF Scoreboard & Game Manager).
- [Scorebot](#) - Platform for CTFs by Legitbs (Defcon).
- [SecGen](#) - Security Scenario Generator. Creates randomly vulnerable virtual machines.

<https://github.com/apsdehal/awesome-ctf>

The screenshot shows the CTFd platform's scoreboard page. At the top, there is a navigation bar with links for FEATURES, PRICING, STORE, CONTACT, LOGIN, and SIGN UP. Below the navigation is a logo for CTFd and a "Scoreboard" heading. The main area features a line graph titled "Top 10 Teams" showing scores over time. The x-axis represents time from 01:00 to 07:00, and the y-axis represents score from 0 to 4000. Multiple colored lines represent different teams, all showing a general upward trend. Below the graph is a table listing the top 10 teams with their names and scores:

Rank	Team	Score
1	Mari	3759
2	Carl	3750
3	Megan	3513
4	Tiffany	3500
5	David	3097
6	Dave	3000

At the bottom of the page, there is a tagline: "Cyber Security Training made simple" followed by "With the best Capture The Flag platform". A blue button at the bottom right says "What's a Capture The Flag?".



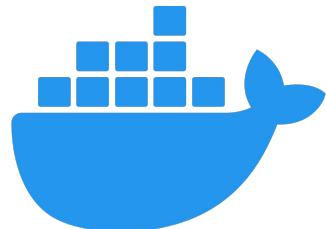
https://commons.wikimedia.org/wiki/File:Continuous_Delivery_process_diagram.svg

@jkuemerle@infosec.exchange



<https://www.flickr.com/photos/mknowles/5358317992>

@jkuemerle@infosec.exchange



docker®



<https://github.com/jkuemerle/basc2025>

Everyone Can Play! Building Great CTFs for Non-Security Folks

BASC 2025 by @jkuemerle@infosec.exchange

Materials and references for "Everyone Can Play! Building Great CTFs for Non-Security Folks" presented at BASC 2025

Hands on activites are optimized for running in Docker Compose. Local execution of utility scripts requires [Node.js](#).

To participate in the hands on activities, clone the this repository then `docker compose build` to spin up all of the components locally.

For the report building any reporting tool will work. The workshop will use [Tableau Public](#)

Components

CTFd

Lightly customized version of [CTFd](#)

OWASP Juice Shop

Lightly customized version of [OWASP Juice Shop](#)

LLM CTF

Custom LLM based CTF challenges.

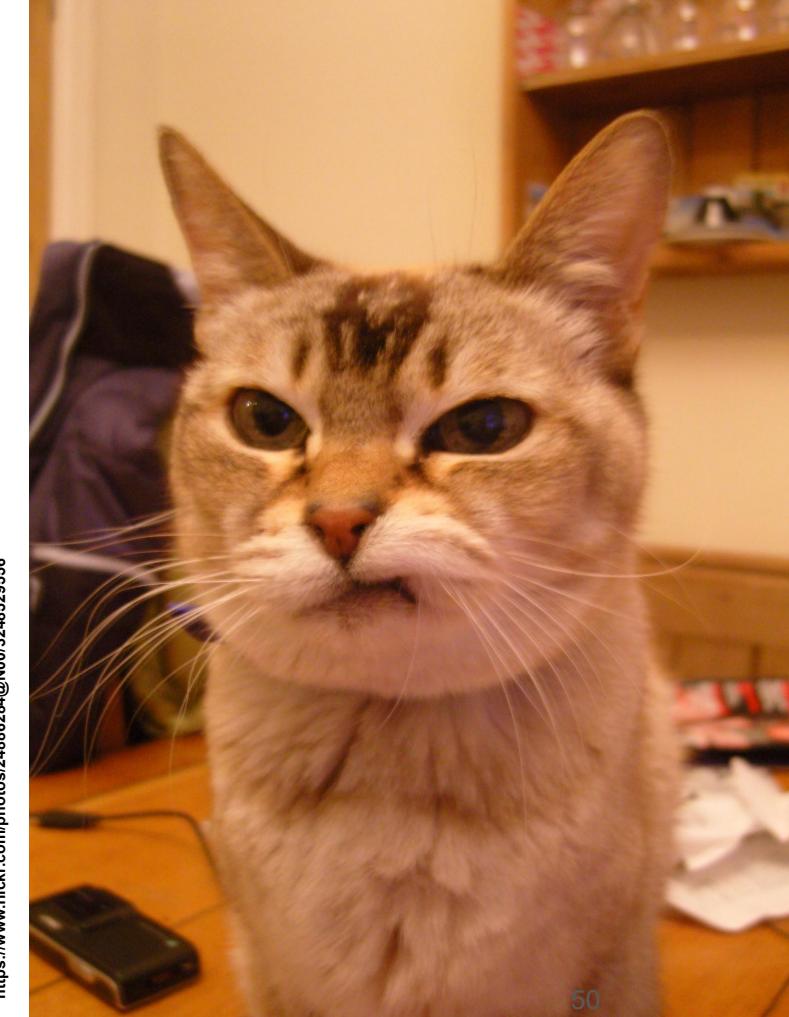
Reporting

[Tableau Public](#)

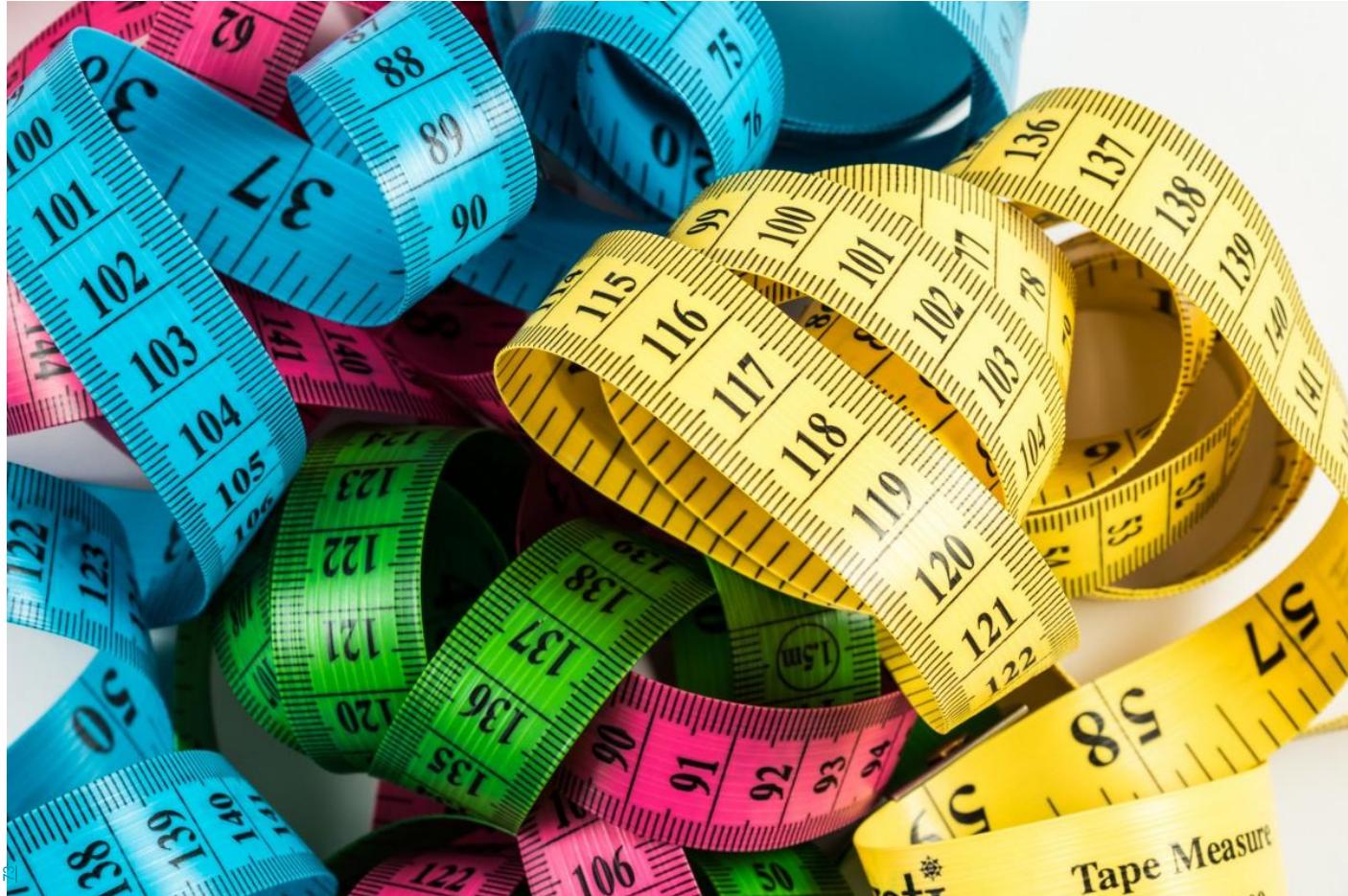
Utility Scripts

Are located in the [scripts](#) folder.

@jkuemerle@infosec.exchange



<https://www.flickr.com/photos/24886284@N00/3248529556>





<https://www.flickr.com/photos/andrewwhurley/6254409229>

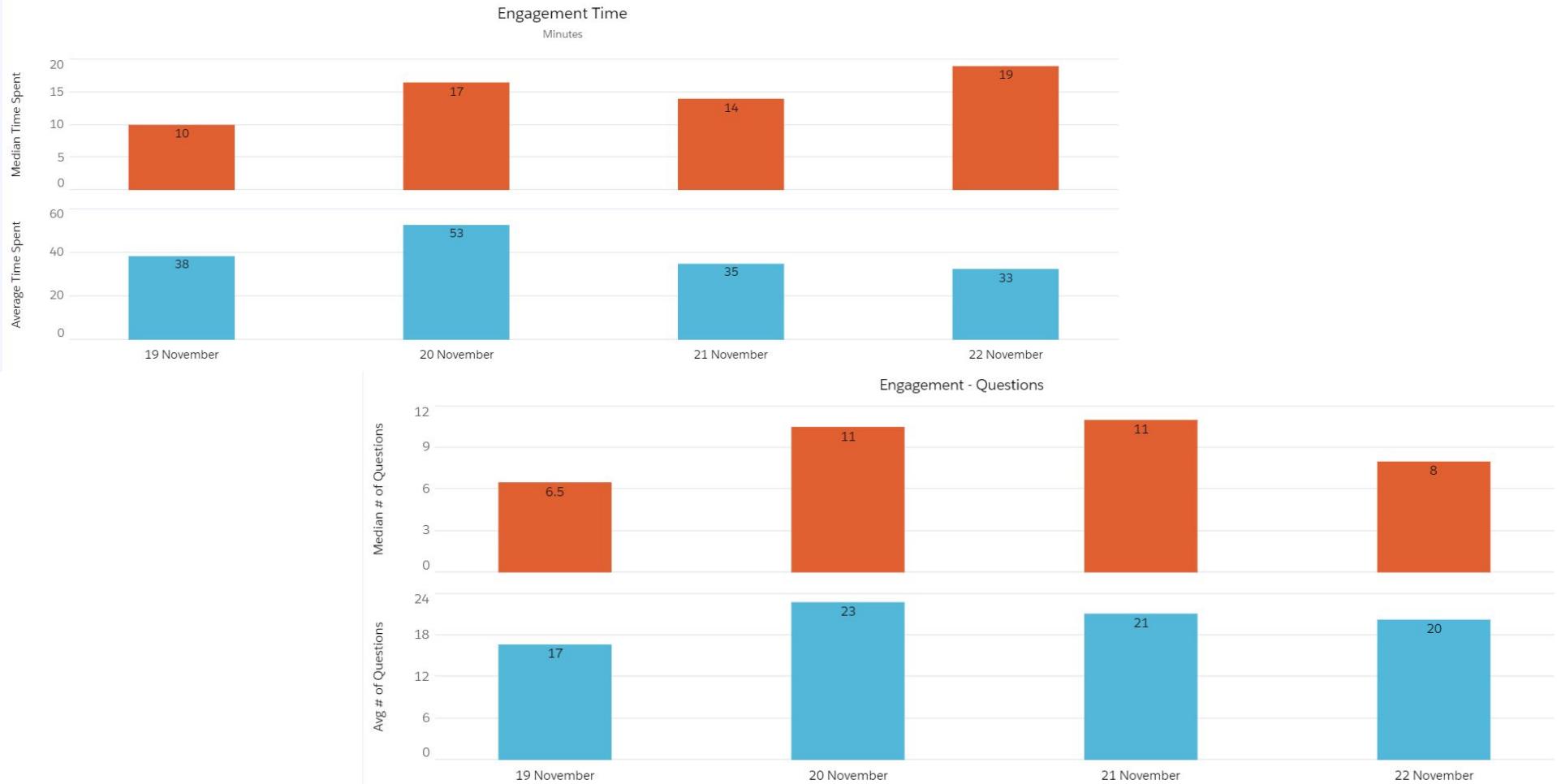
@jkuemerle@infosec.exchange



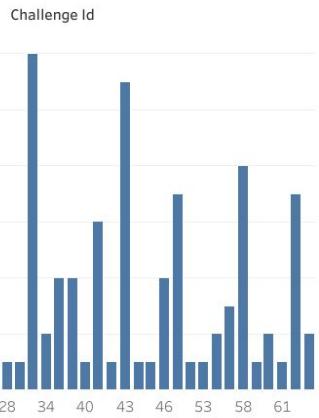
<https://www.flickr.com/photos/70267096@N00/8234628909>

@jkuemerle@infosec.exchange

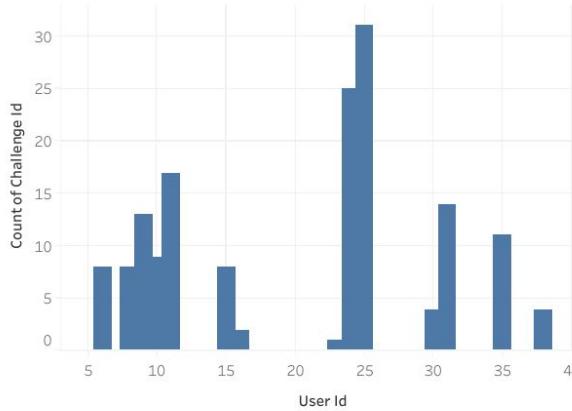
<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>



Challenge Solves



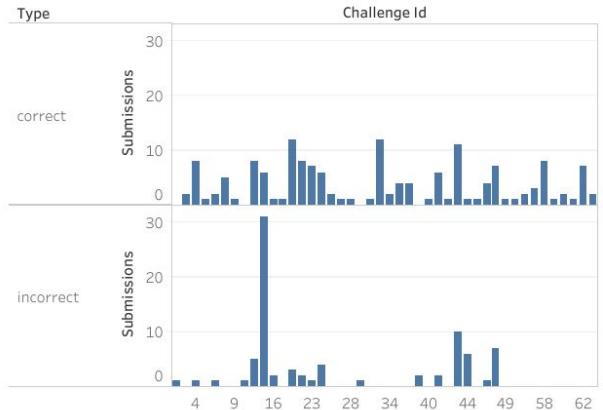
Solves By User



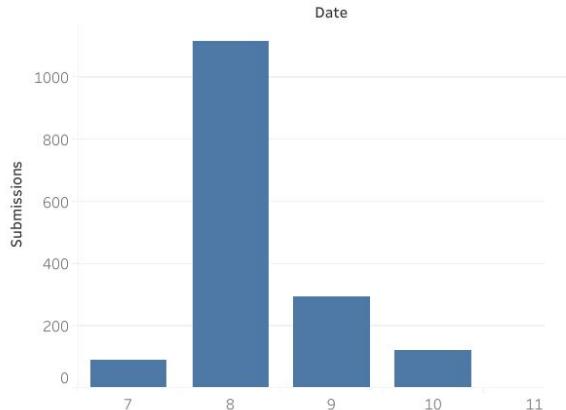
ctf/CTF_Data/results

- CTF-Challenges.csv
- CTF-solves.csv
- CTF-submissions.csv
- CTF-users.csv

Challenge Attempts



Daily Activity



<https://bit.ly/BASC-CTF-Dashboard>



Other Vulnerable Things

- <https://yieldcat.com> - Vulnerable web app
- <https://github.com/step-security/github-actions-goat> - Deliberately Vulnerable GitHub Actions CI/CD Environment
- <https://github.com/RhinoSecurityLabs/cloudgoat> - "Vulnerable by Design" AWS deployment tool.
- <https://github.com/ine-labs/AzureGoat> - A Damn Vulnerable Azure Infrastructure
- <https://github.com/ine-labs/AWSGoat> - A Damn Vulnerable AWS Infrastructure
- <https://github.com/vavkamil/awesome-vulnerable-apps>

Conclusion

- **Why**
- **What**
- **How**

Next Steps

- Next week you should:
 - Identify teams that will benefit from CTF style training
 - Identify SMEs to build a pilot CTF
- In the first three months following this presentation you should:
 - Have run a CTF and iterated on the design, challenges and goals
 - Run retrospectives of both CTF builders and CTF players
 - Gathered usage data into a repository
- Within six months you should:
 - Have an active, ongoing CTF based training program
 - Run regular retrospectives and incorporate feedback
 - Report KPIs and regularly survey program effectiveness

Resources

- https://github.com/salesforce/integrated_challenge
- <https://github.com/apsdehal/awesome-ctf>
- https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/Multi-modal-Learning-Through-Media.pdf
- <https://engineering.salesforce.com/capture-the-flag-secure-your-knowledge-37b43180e55a>
- <https://engineering.salesforce.com/play-games-learn-better-fc782757c884>
- <https://github.com/CTFd/CTFd>
- <https://github.com/jkuemerle/basc2025>
- <https://github.com/SamuraiWTF/samuraiwtf>





THANK YOU

FOR YOUR ATTENTION



ADDRESS

401 Edgewater Place, Suite 600
Wakefield, MA 01880



PHONE

+1 951-692-7703



E-MAIL

contact@owasp.org