

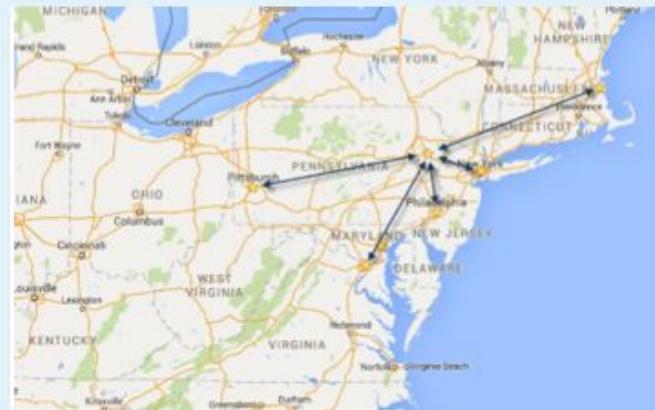
# Everyone Can Play!

## Building CTFs for Non-Security Folks

Joe Kuemerle / [joe@kuemerle.com](mailto:joe@kuemerle.com) / [@jkuemerle](https://twitter.com/jkuemerle)



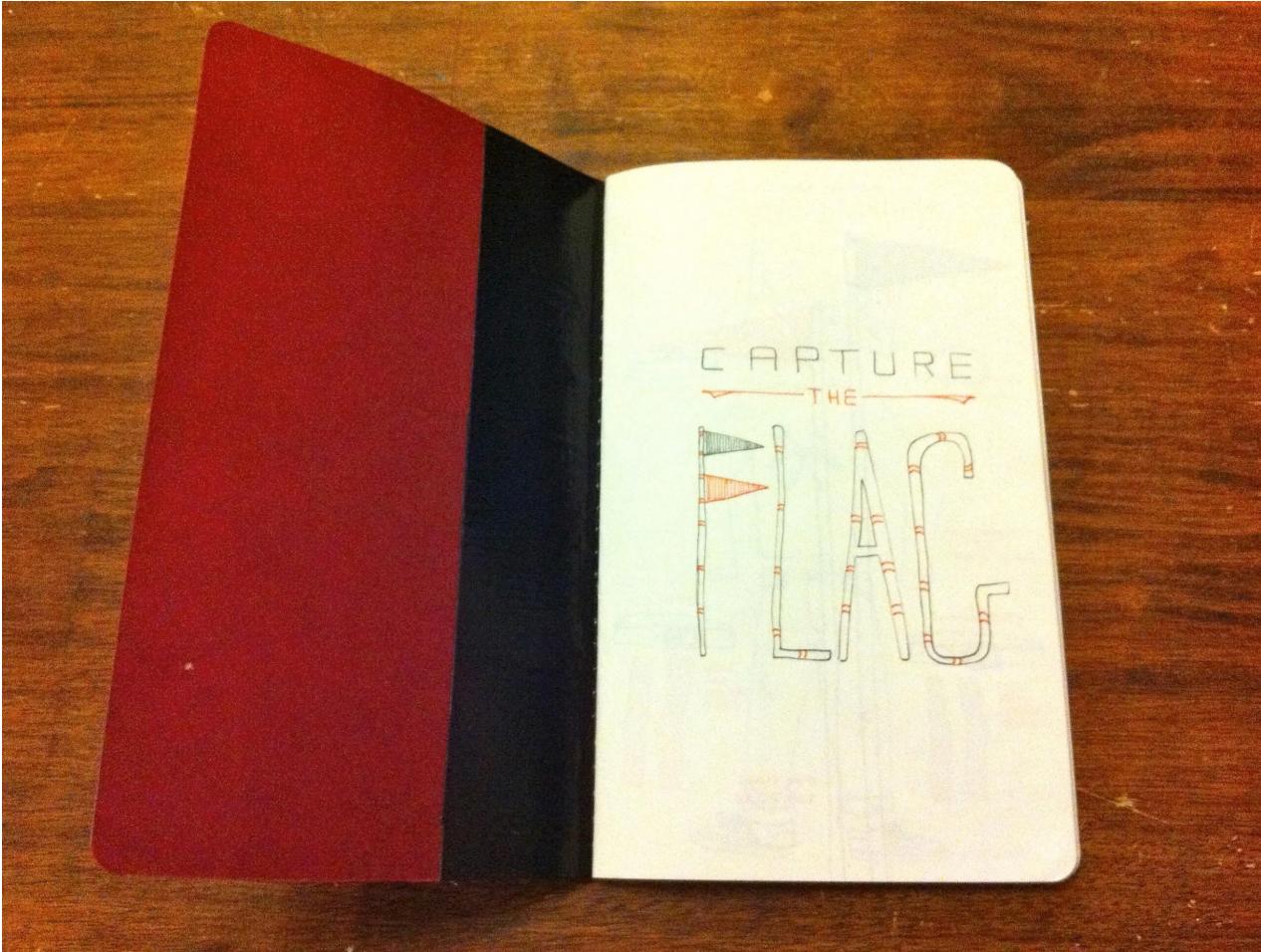
- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  - 3-day conference plus lodging for less than \$1000
- Full day deep dive preconference sessions available
- Easy to get to from almost anywhere
- In addition to the breakout sessions, you get a great hallway track, attendee reception, game night and more
- Full day of kids & family sessions on Friday, free for families of attendees
- Discounted Kalahari Waterpark room nights: stay, learn and play all in one place



<https://techbash.com> or @techbash

# Agenda

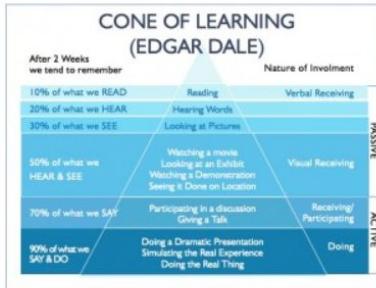
- **Why**
  - Learning studies
  - Proven success
- **What**
  - Building challenges
  - Easy to participate
  - Fun
- **How**
  - Easy to run
  - Measured





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

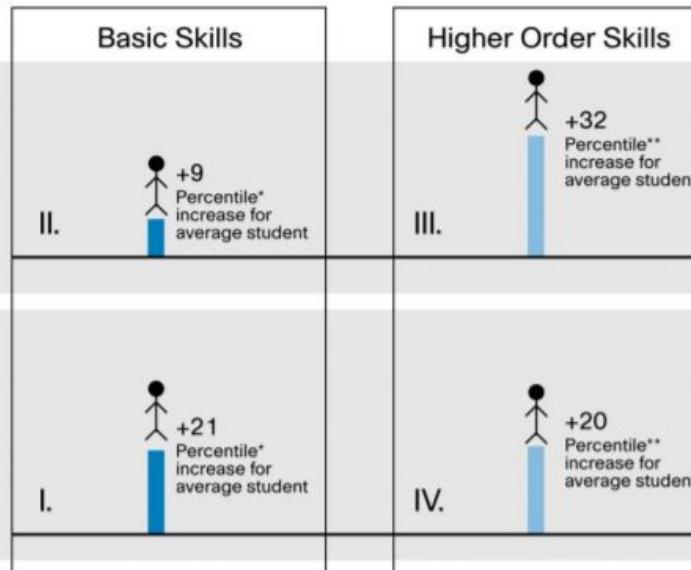
### Contacts:

Charles Fadel, Global Lead, Education, Cisco Systems, Inc.: [cfadel@cisco.com](mailto:cfadel@cisco.com)  
 Chevri Lemke, CEO, Metiri Group: [clemke@metiri.com](mailto: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](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.

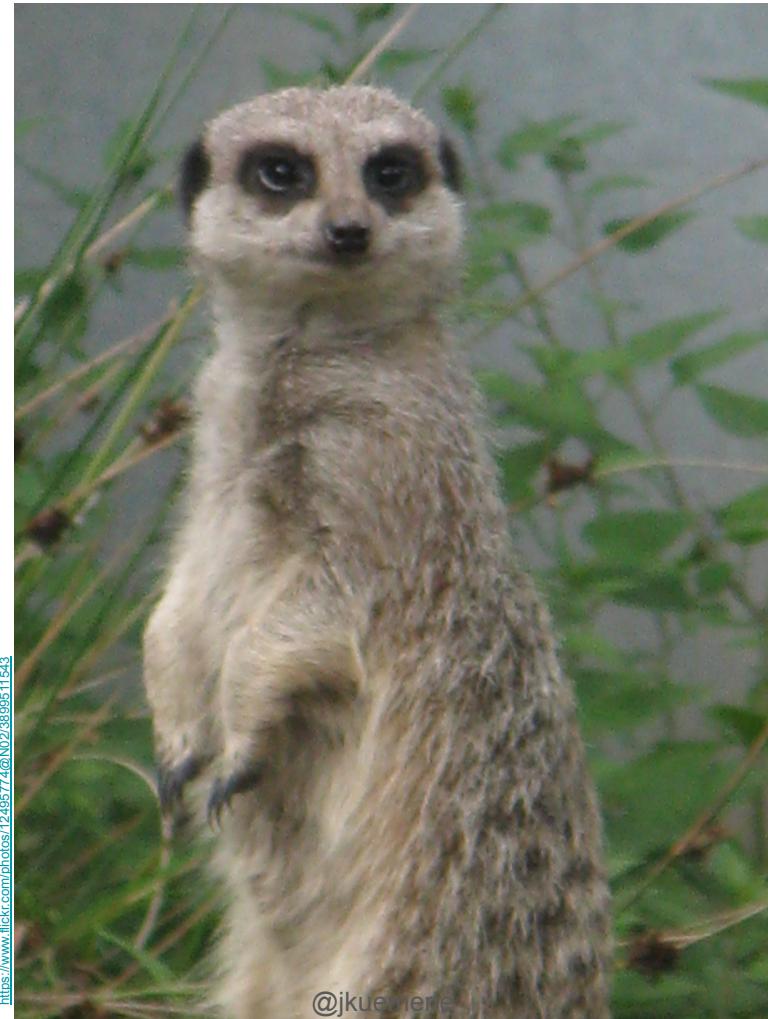
**5. Modality Principle:** Students learn better from animation and narration than from animation and on-screen text.

**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



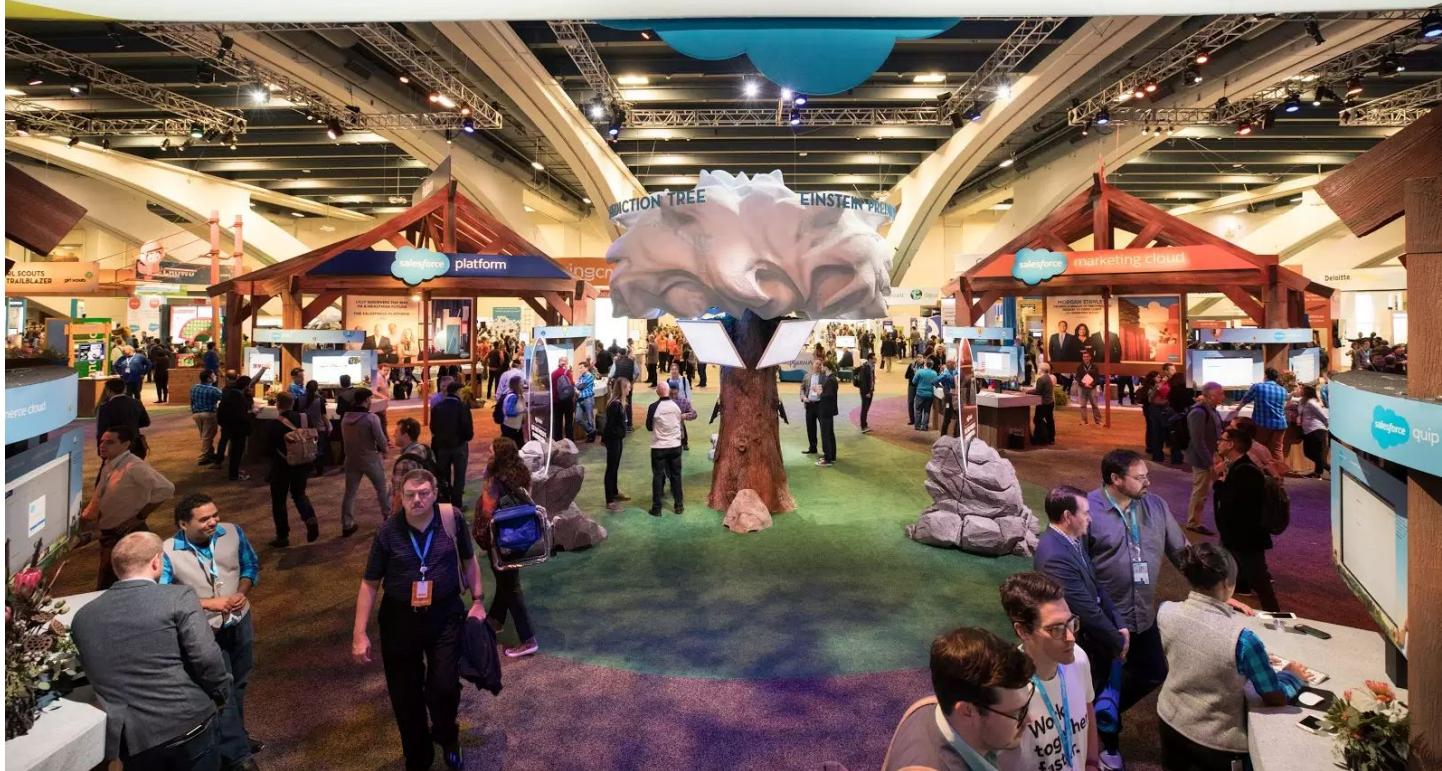
<https://www.flickr.com/photos/12495774@N02/3899511543>

@jkuemerle



@jkuemerle

# 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](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



<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.

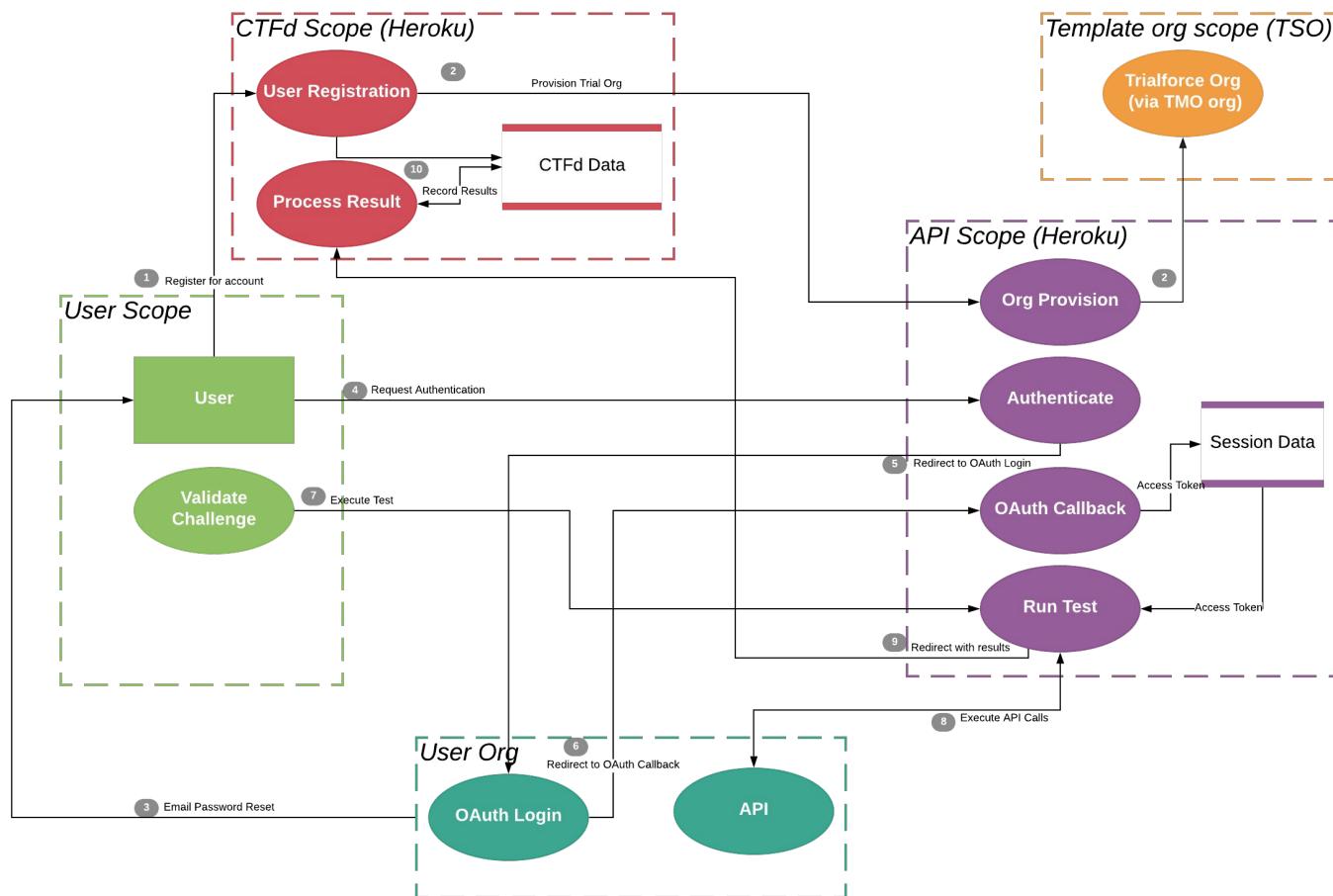
**5. Modality Principle:** Students learn better from animation and narration than from animation and on-screen text.

**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

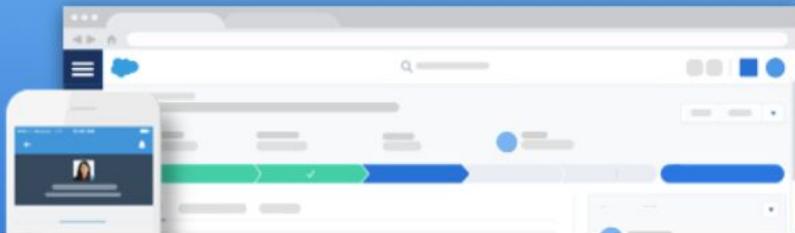
User Name

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

# 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

X

# Cross Site Scripting Protection

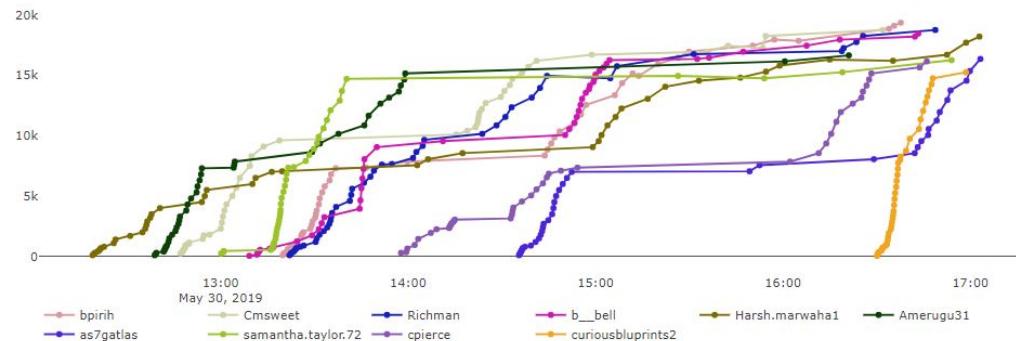
500

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

@jkuemerle

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

Total Participants

486

Participants

200

150

100

50

0

189

135

116

46

19 November

20 November

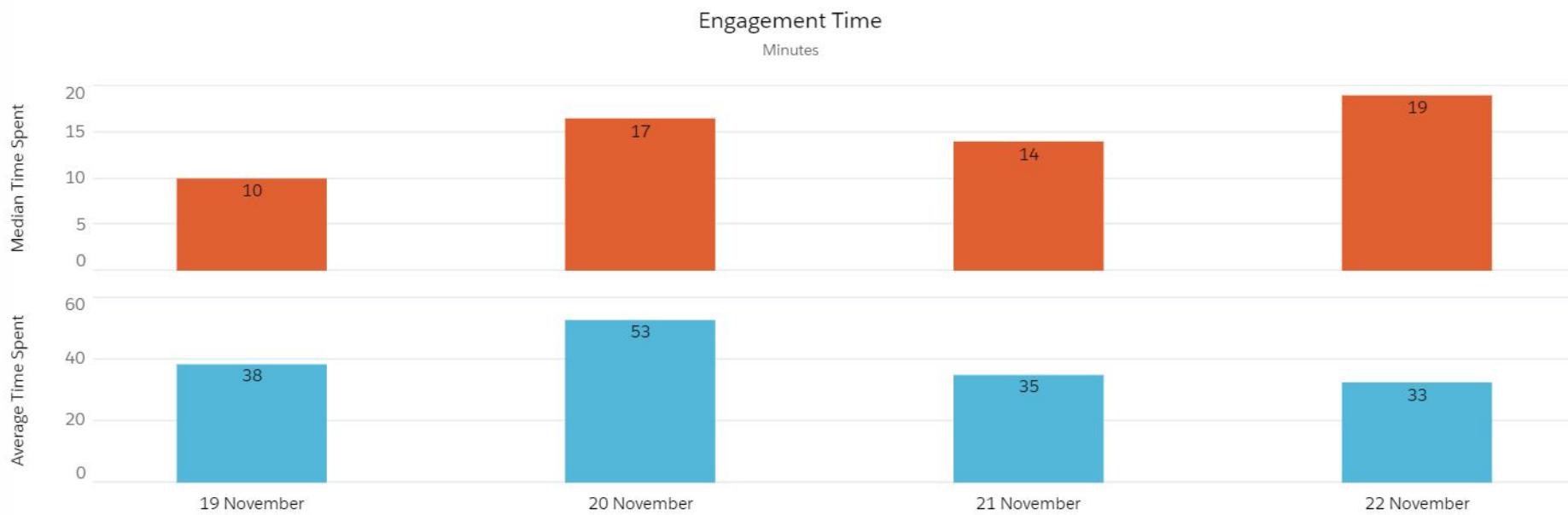
21 November

22 November

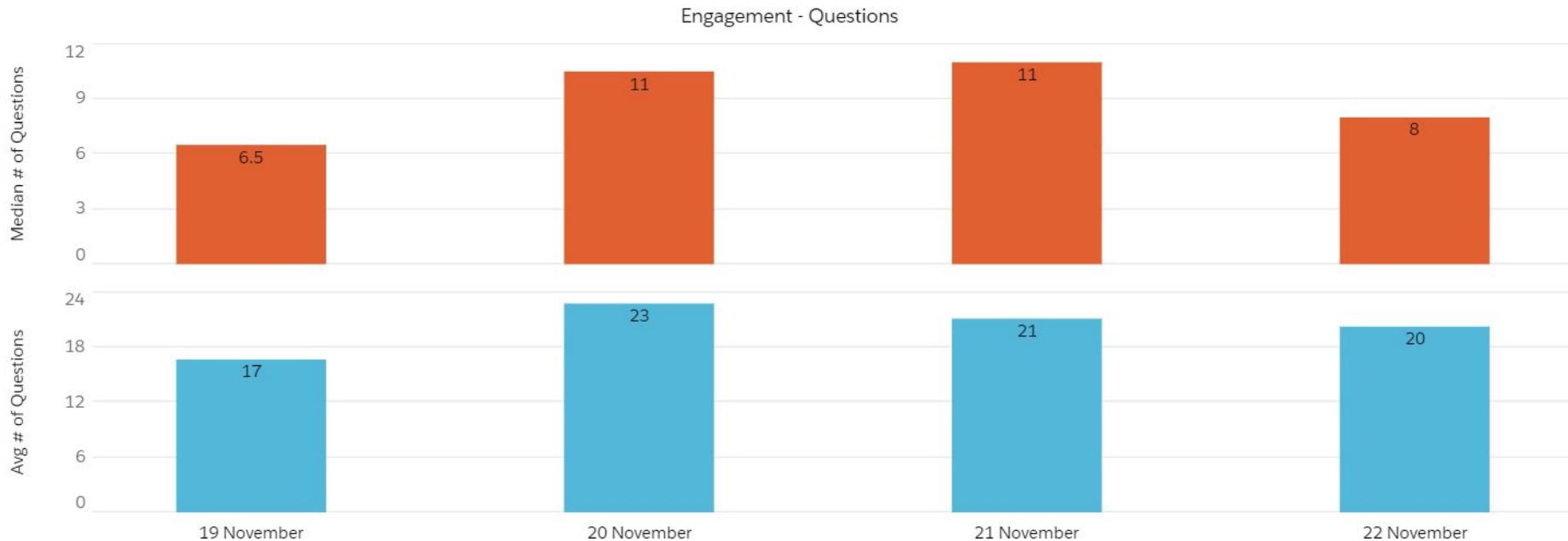
date

@jkuemerle

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

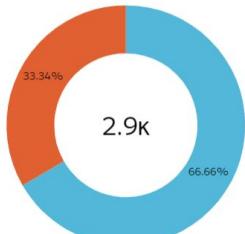


<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>

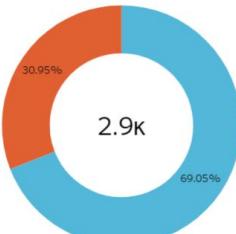


<https://engineering.salesforce.com/play-games-learn-better-fc782757c884>

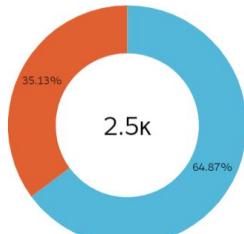
Answers - 19 November



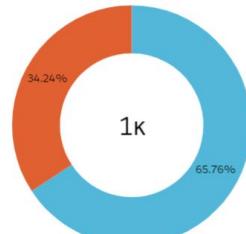
Answers - 20 November



Answers - 21 November

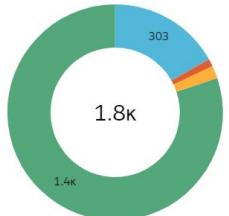


Answers - 22 November



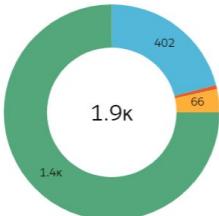
Solves By Category

19 November



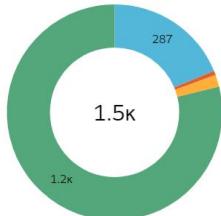
Solves By Category

20 November



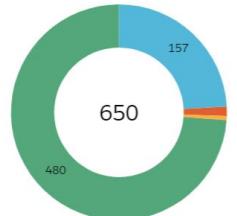
Solves By Category

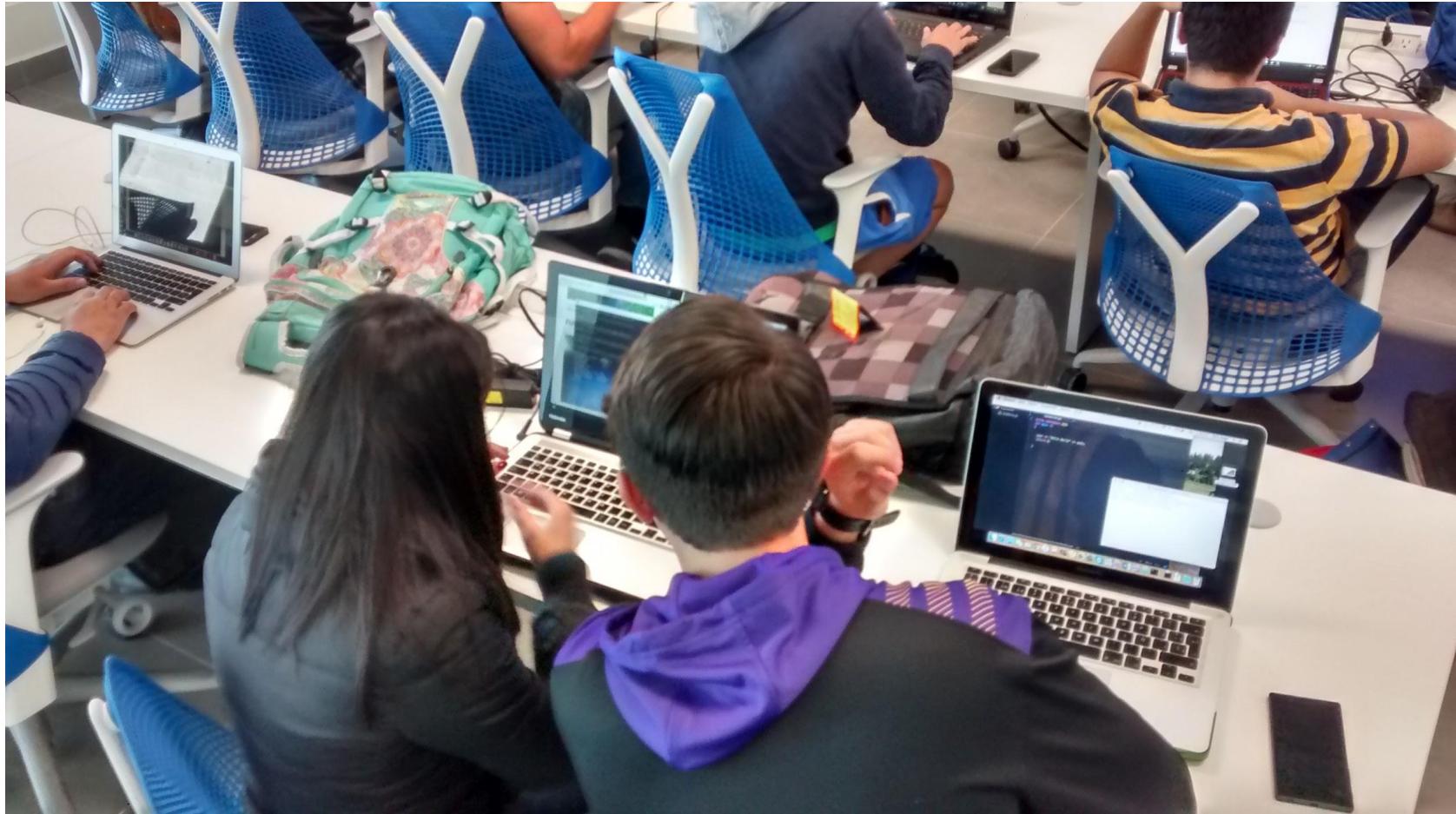
21 November



Solves By Category

22 November







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

@jkuemerle



### CROSSWORD 78

**ACROSS**

- 1. Scraps
- 2. Bulwarks'
- 3. Kill
- 4. Troublesome water bird
- 5. Voice range
- 6. Little story for a novel
- 7. Butter
- 8. Snore, e.g.
- 9. Cut or break
- 10. Mild south
- 11. Curved
- 12. Tavern drink
- 13. Sips
- 14. Seeds, or beans
- 15. Mischievous tyke

**DOWN**

- 20. Made a cluster
- 21. Glutton
- 22. Hunter's humor
- 23. —— n.
- 24. —— of luxury
- 25. —— features
- 26. —— food
- 27. —— pasty
- 28. —— forward
- 29. —— for a great deal
- 30. —— & port
- 31. Move with elegance
- 32. Stand ——
- 33. Wriggling
- 34. Amusement
- 35. Animal
- 36. Duds
- 37. Wiener dog
- 38. —— for all
- 39. —— lesson
- 40. —— of art
- 41. —— of the year
- 42. —— of the year
- 43. —— of the year
- 44. —— of the year
- 45. —— of the year
- 46. —— of the year
- 47. —— of the year
- 48. —— of the year
- 49. —— of the year
- 50. —— of the year
- 51. —— of the year
- 52. —— of the year
- 53. —— of the year
- 54. —— of the year
- 55. —— of the year
- 56. —— of the year
- 57. —— of the year
- 58. —— of the year
- 59. —— of the year
- 60. —— of the year
- 61. —— of the year
- 62. —— of the year
- 63. —— of the year
- 64. —— of the year
- 65. —— of the year
- 66. —— of the year
- 67. —— of the year
- 68. —— of the year
- 69. —— of the year
- 70. —— of the year
- 71. —— of the year
- 72. —— of the year
- 73. —— of the year
- 74. —— of the year
- 75. —— of the year
- 76. —— of the year
- 77. —— of the year
- 78. —— of the year
- 79. —— of the year
- 80. —— of the year
- 81. —— of the year
- 82. —— of the year
- 83. —— of the year
- 84. —— of the year
- 85. —— of the year
- 86. —— of the year
- 87. —— of the year
- 88. —— of the year
- 89. —— of the year
- 90. —— of the year
- 91. —— of the year
- 92. —— of the year
- 93. —— of the year
- 94. —— of the year
- 95. —— of the year
- 96. —— of the year
- 97. —— of the year
- 98. —— of the year
- 99. —— of the year
- 100. —— of the year

### CROSSWORD

**DOWN**

- 1. Leading lady
- 2. Airborne toy
- 3. Maxime
- 4. Acidine
- 5. Plastic
- 6. Wood collector
- 7. Chalkings
- 8. Large segment
- 9. Stone layer
- 10. Horse's kin
- 11. Vote in favor
- 12. Pin's kin
- 13. In the back
- 14. Carving
- 15. City vehicle
- 16. Frosted
- 17. Liquid rock
- 18. To any way
- 19. Auto imperfection
- 20. More than should be
- 21. Outrageous
- 22. Band by the band
- 23. Girls\*

- **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

## 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

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>

[https://github.com/salesforce/integrated\\_challenge](https://github.com/salesforce/integrated_challenge)



<https://www.flickr.com/photos/5031888@N00/304887602>

@jkuemerle

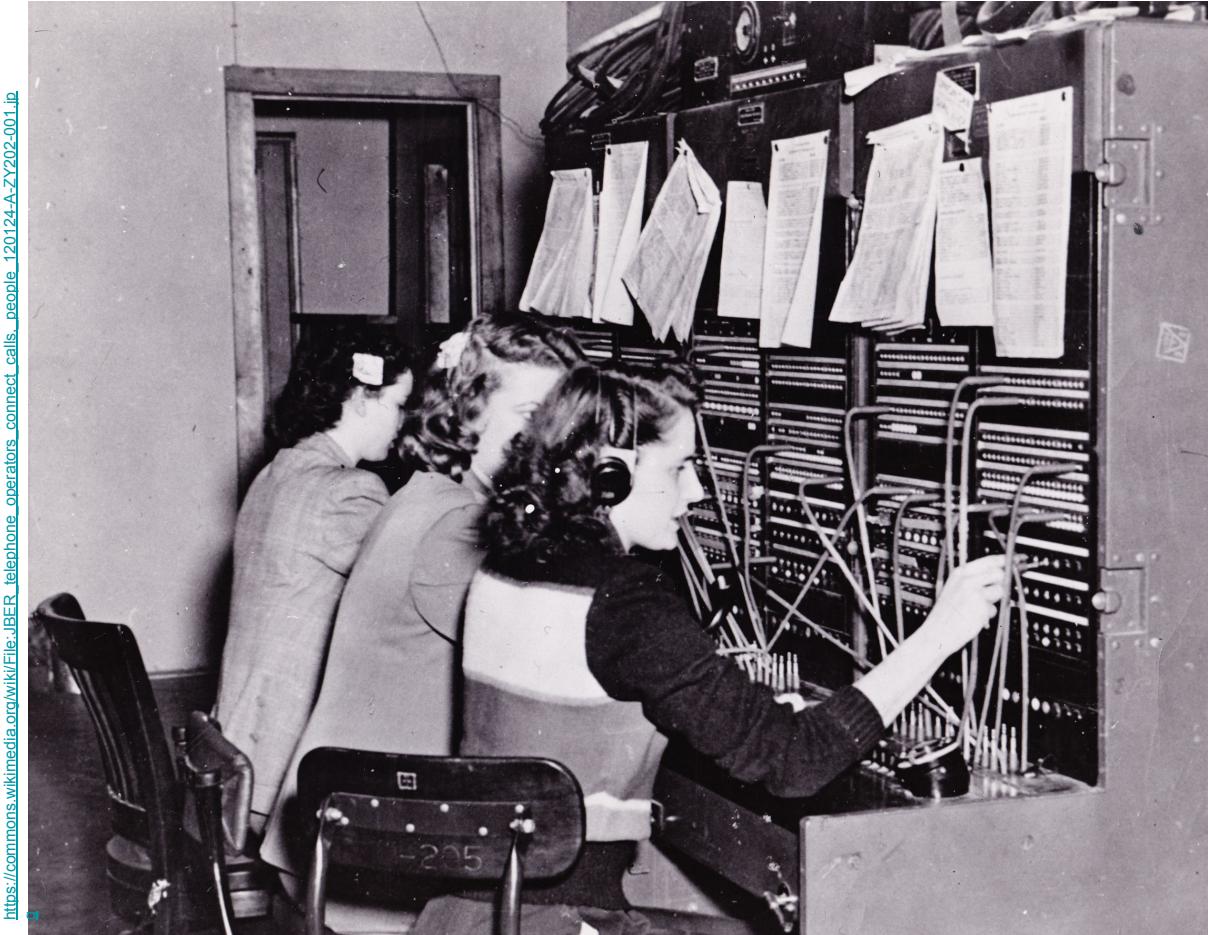
[https://commons.wikimedia.org/wiki/File:Judges\\_hold\\_up\\_their\\_respective\\_scores.jpg](https://commons.wikimedia.org/wiki/File:Judges_hold_up_their_respective_scores.jpg)



@jkueemerle



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



[https://commons.wikimedia.org/w/index.php?title=File:IBER\\_telephone\\_operators\\_connect\\_calls\\_120124-A-ZY202-001.jp](https://commons.wikimedia.org/w/index.php?title=File:IBER_telephone_operators_connect_calls_120124-A-ZY202-001.jp)

@jkuemerle



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

@jkuemerle

[http://www.bertiesinn.com/beltsander\\_races/2017\\_beltsander\\_race.html](http://www.bertiesinn.com/beltsander_races/2017_beltsander_race.html)



@jkuemerle



Confidential Document - Sensitive	Zero Stars	Login Admin	Weird Crypto
100	100	250	250
Bjoern's Favorite Pet - Broker	Forged Review	Login Amy	Login Jim
450	450	450	450
Payback Time	Product Tampering	Access Log - Sensitive Data Exposure	Misplaced Signature File
450	450	700	700
Server-side XSS Protection	User Credentials	Change Bender's Password - Emergency	Email Leak - Sensitive Data Exposure
700	700	1000	1000
Extra Language - Broken Anti-CSRF	Frontend Typosquatting	NoSQL Exfiltration	Reset Bjoern's Password
1000	1000	1000	1000
Two Factor Authentication	Imaginary Challenge	SSRF	
1000	1350	1350	





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

@jkuemerle

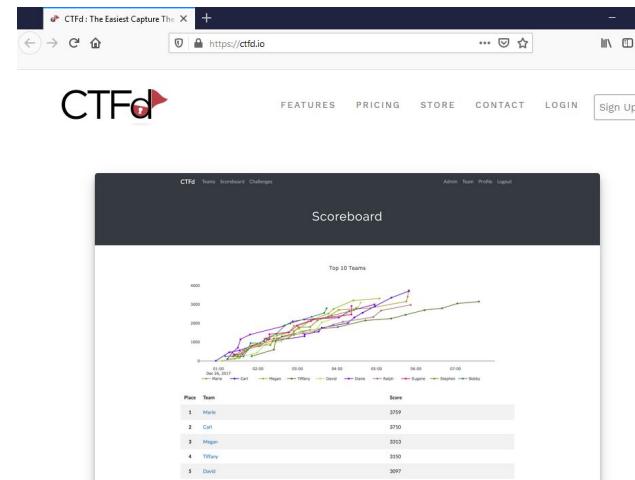


# Platforms

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.

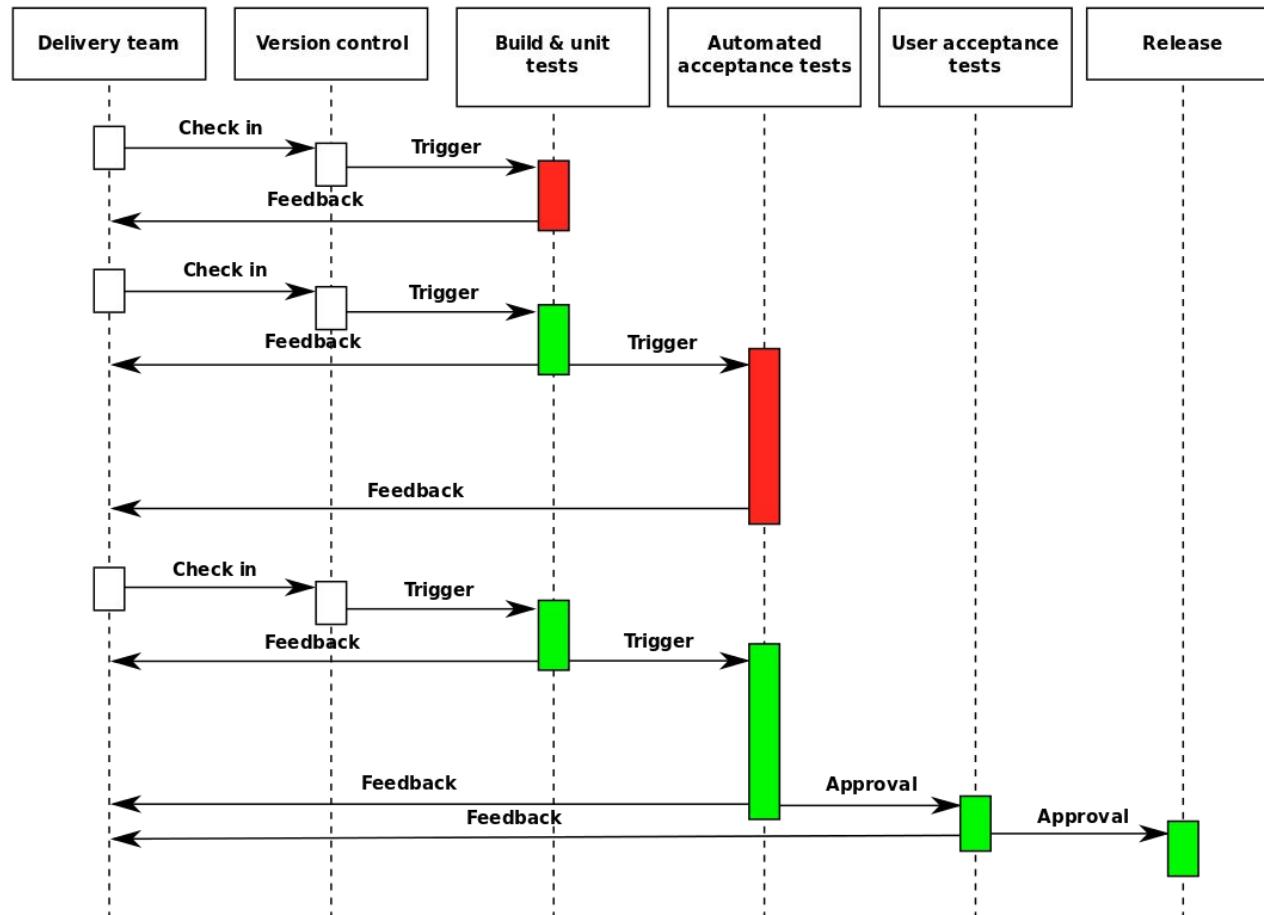
<https://github.com/apsdehal/awesome-ctf>



Cyber Security Training made simple

With the best Capture The Flag platform

What's a Capture The Flag?



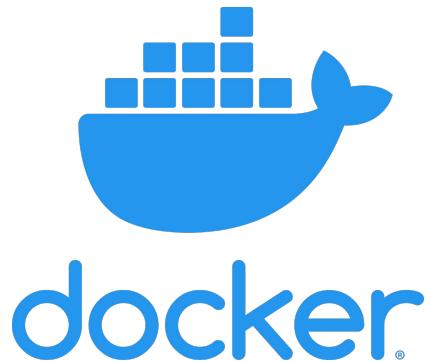
[https://commons.wikimedia.org/wiki/File:Continuous\\_Delivery\\_process\\_diagram.svg](https://commons.wikimedia.org/wiki/File:Continuous_Delivery_process_diagram.svg)

@jkuemerle



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

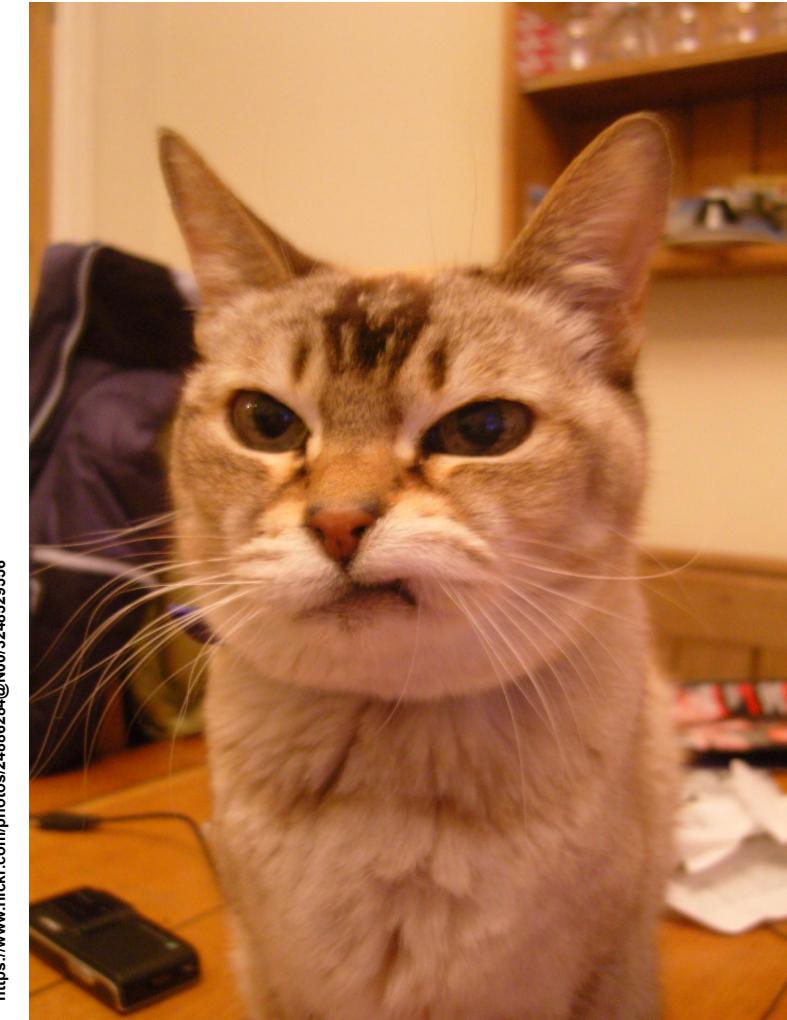
@jkuemerle



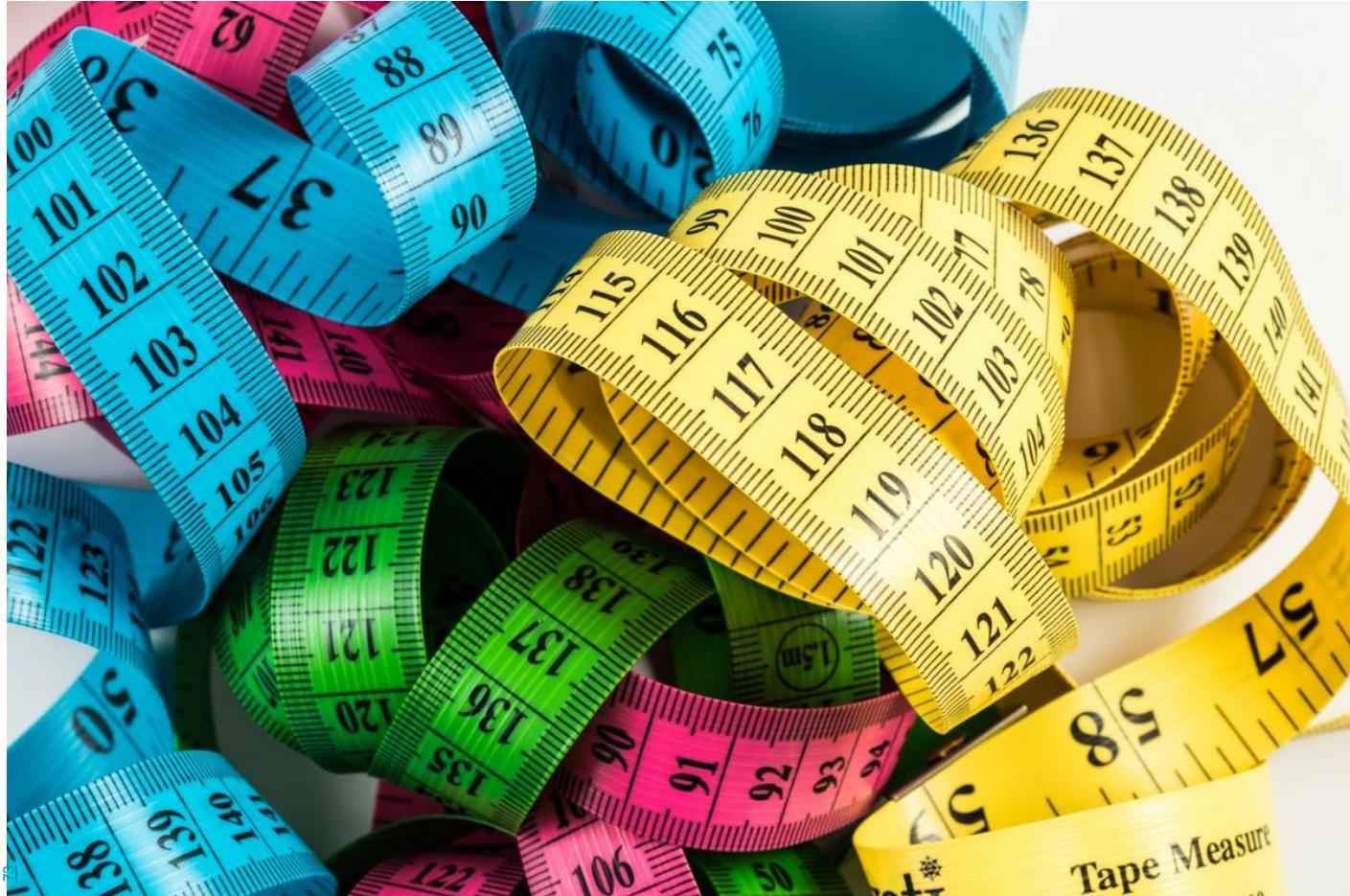
<https://github.com/jkuemerle/blueteam-2022-ctf>

The screenshot shows a GitHub repository page for 'blueteam-2022-ctf'. The title of the file is 'README.md'. The content of the file is as follows:

```
谁都能够玩！为非安全人员构建伟大的CTFs  
##Blue Team Con 2022 by @jkuemerle ##  
Materials and references for "Everyone Can Play! Building Great CTFs for Non-Security Folks" presented at Blue Team Con 2022  
Hands on activites require local Docker and/or free Heroku account. Local execution of utility scripts requires Node.JS.  
To perform command line configuration of Heroku install the Heroku CLI.  
To use the activities, clone the this repository and the below repositories. If you will be working using local Docker you can build both the CTFd Docker Compose definition and the OWASP Juice Shop Docker image.  
For the report building any basic reporting tool will work. The workshop will use a custom version of the Elasticsearch, Logstash, Kibana (ELK) Docker Image.
```



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





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

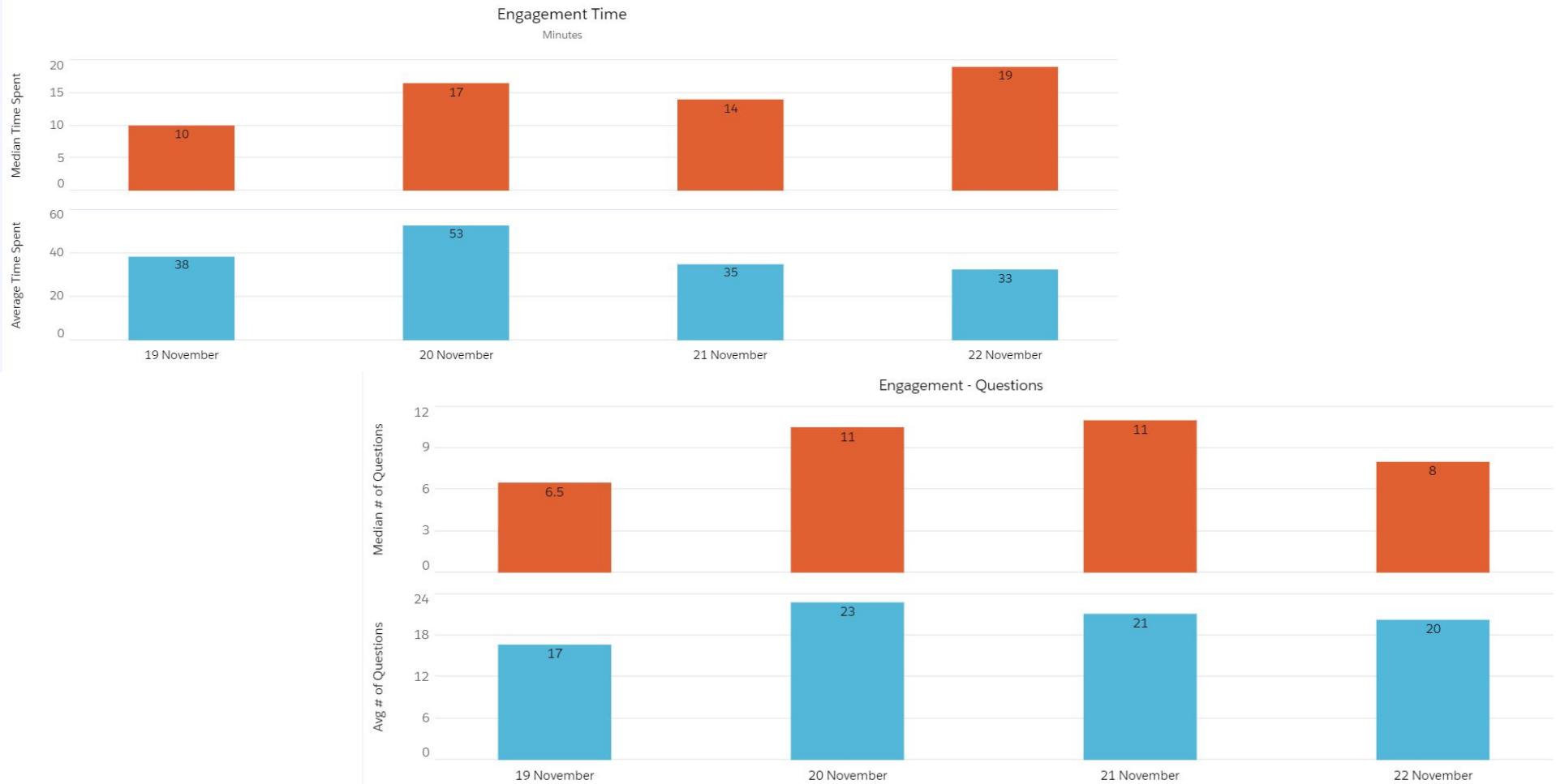
@jkuemerle

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



@jkuemerle

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



# Conclusion

- Why
- What
- How

- 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/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://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/blueteam-2022-ctf>

<https://www.flickr.com/photos/88547796@N00/5716815256>



@jkuemerle