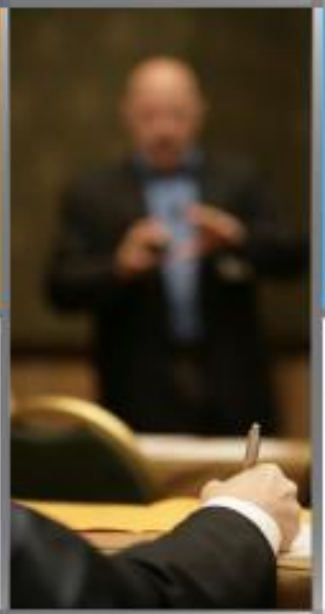
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Using Innovative Competition to Improve Application Security

Richard Menta

Lead IT Security Specialist

Quest Diagnostics

CSO 50 CONFERENCE +AWARDS

We trained developers for two days on secure Coding techniques. Improvement was minimal.

10%
Education

Development is most successful with a ‘blended’ learning approach

70% Experiences

- Formal Rotational Assignments (short & long term)
- Job Shadowing
- Special Assignments / Project Leadership
- Action Learning Teams
- Immersive eLearning
- Gaming
- Engaging webinars
- Business Simulation
- Skill demonstration

20% Relationships

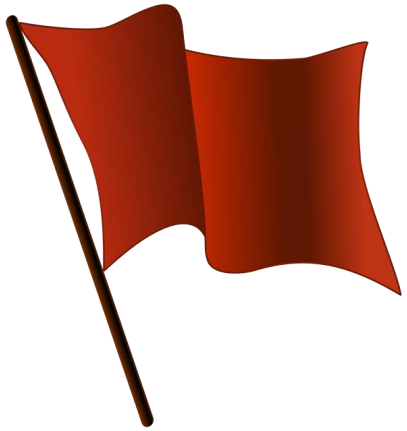
- Mentoring
- Coaching
- 360 Feedback
- Assessments & Feedback
- Observation
- Peer Interaction / Networks
- External Networks
- Communities of Practice
- Exposure to Sr. Leadership

10% Education

- Skill Development Programs
- Knowledge checks
- Internal & External Leadership Program course work
- Seminars
- Certifications

So we tried a ‘blended’ approach next

70% Experiences



Capture the Flag (CTF)

20% Relationships

- Skilled CTF participants code-review peers
- Event promoted to Sr. Leadership
- Promote a community of practice within the organization

10% Education

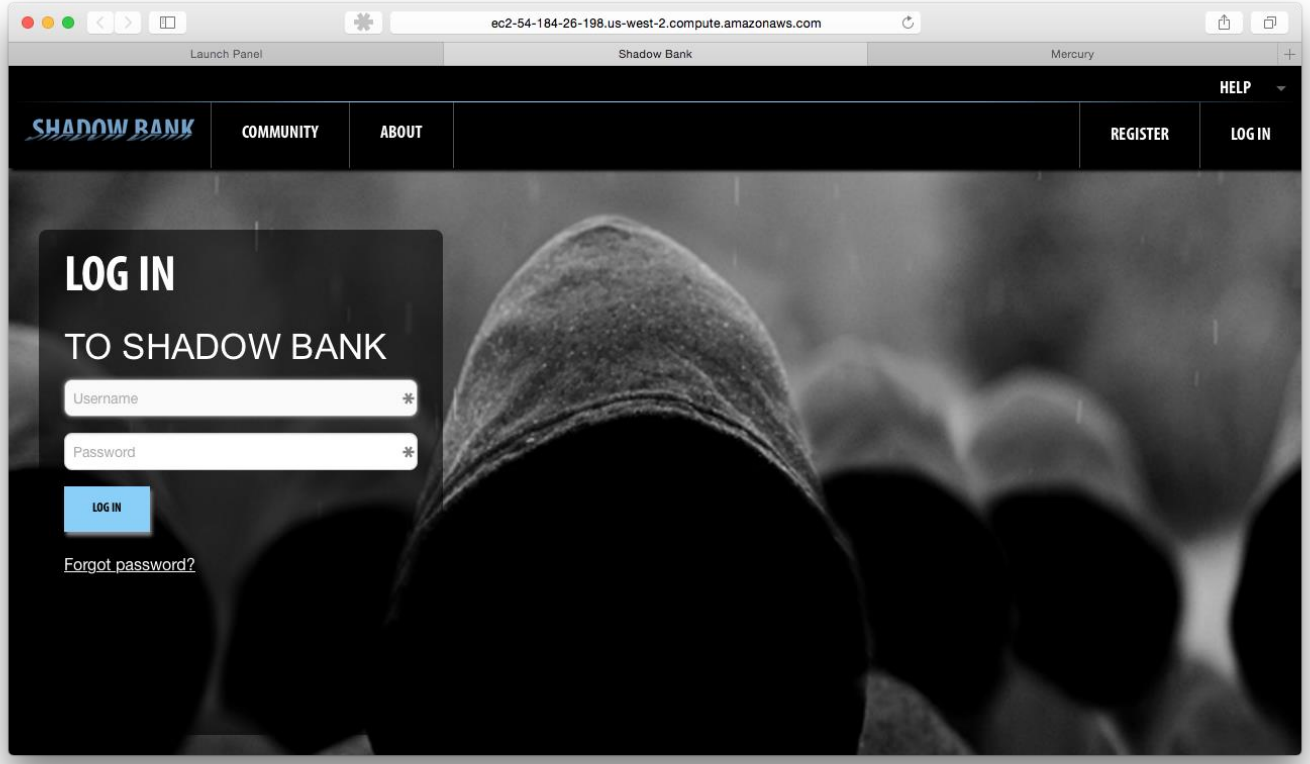
Monthly Lunch and Learns

- Hacking techniques delivered in small bites
- OWASP

Start with Lunch and Learns

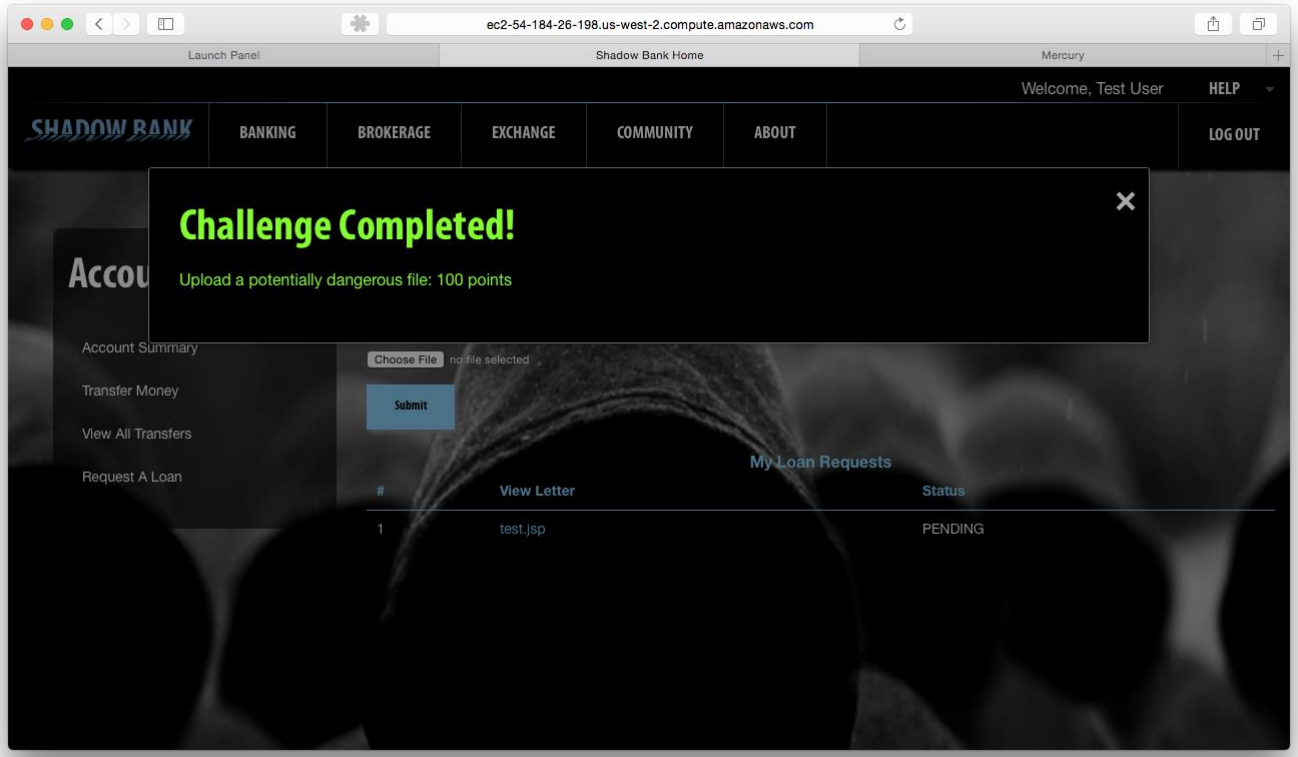
- 9 half-hour Lunch and Learns from January to September
- Each L&L focused on an attack technique in the OWASP Top 10
- Lunch and learns were recorded and placed on the Intranet as reference for the competition.
- Capture the Flag launched October 15th 2015

Contestant objective: to compromise and manipulate a bank web site over a two week period



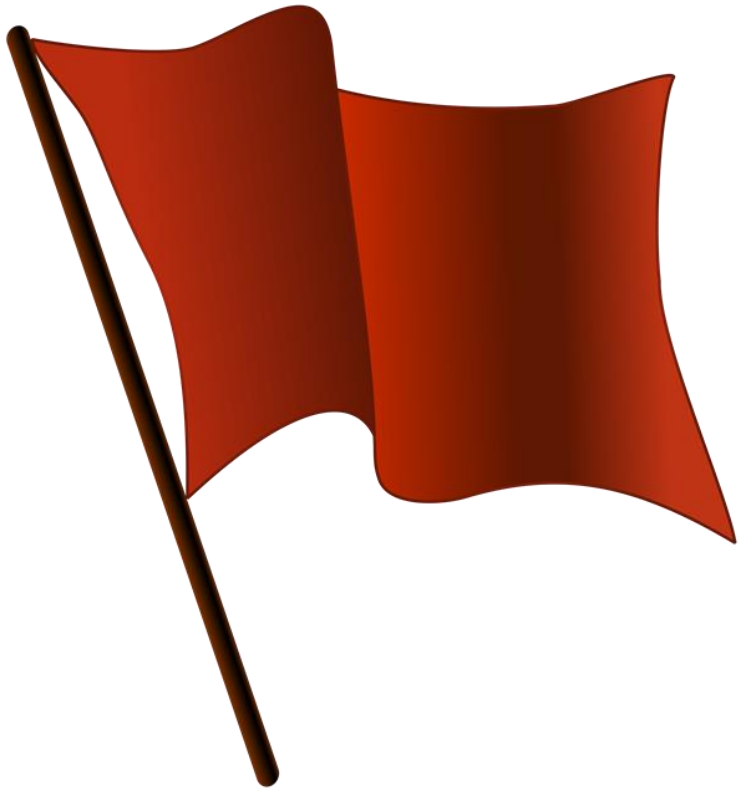
- Put the contestants into the shoes of a hacker and manipulate mistakes in coding. Flags ranged from 50 to 1,000 points based on difficulty.

The goal: get as many participants as possible to play as long as possible



- Be flexible: allow participants to play either as a team or individual
- Prizes for top three in Team and Individual divisions
- The more flags each person finds the more they learn

Participation was good. So how to we keep those who fall behind early to continue playing?



- 12 teams (46 members) competed in the Team Division
- 17 competed as individuals
- Total of 63 participants
- 52 flags and 1,295 total points
- “Flag of the Day” prizes so middle-of-the-pack entries have another opportunity to win
- Lots of fun with the team names and aliases (Sombrero Blanco, Questonymous, etc.)

Put them in the Spotlight! Daily Sports Updates were emailed to everyone in IT.

Quest Diagnostics | ITSecurity

Capture the Flag Update 9

BREAKING NEWS.....Big Buck Stalker just took the overall lead, passing everyone including Sombrero Blanco and Dud and taking over first in the Individual Division!

It gets better. The Landsharks and Booyah have both come back! The Landsharks are now in a tie with Sombrero Blanco for first place in the Team Division, while Booyah has moved to just 25 points behind them!

It's a street fight folks! Don't think for a moment The Mightly Morphin, DTeam1, The RESPONDERS and TEAM IDW are going to let these moves go unchallenged....

Contestant Note: Scoring will stop at 1:00 Eastern Time, 12:00 Central Time sharp on Wednesday the 28th!

Below is the overall scoreboard as of 4:13 today:

Scoreboard	
Player	**Score**
BigBuckStalker	9870
Sombreroblanco	9520

Objectives of the Sports Updates:

- To recognize the leaders
- Teams and individuals who start out slow tend to give up. Updates specifically targeted them.
- Generate excitement for participants
- Generate excitement for those who didn't participate, in hopes it drives them to take part in the future

The RESPONDERS and TeamIDW gave up early and told us so. Sports Update coaxed them back!

Below is the overall scoreboard as of 10:00 am this morning:

Sombreroblanco	9095
TheMightyMorphin	8295
booyah	8170
DTeam1	7845
Questonymous	6970
Landsharks	6720
dud	5770
0wnr0p3r4tr	4570
K10	3795
Brill	3520
BigBuckStalker	3170
TheBlitz	3020
ApArchitectsB	1870
RESPONDERS	1645
Knocker	1420
TeamIDW	1370
FireBlaster	920
YouDontNeedToSeeMyIdentification	720

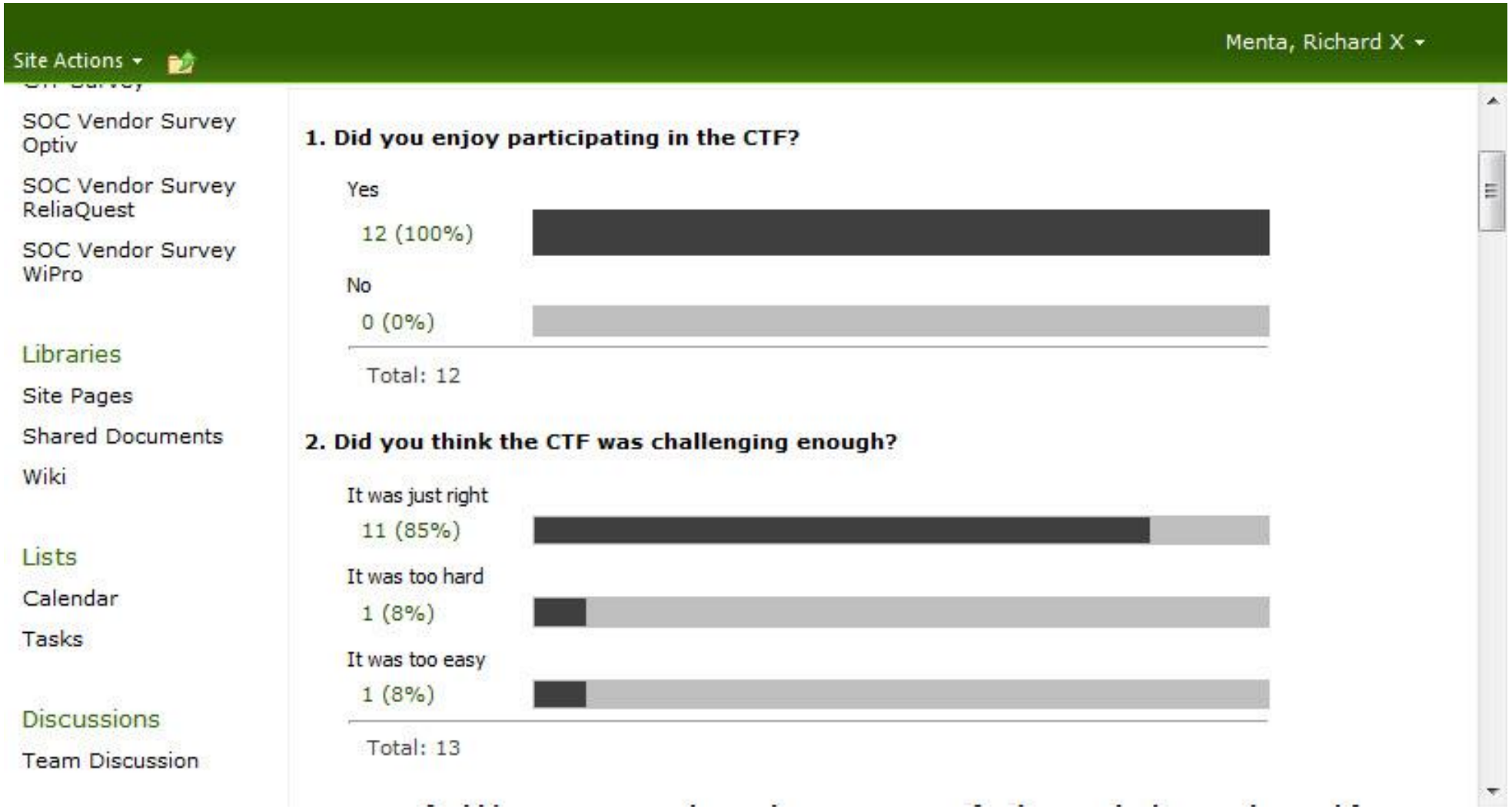
Oct 20 2015

Scoreboard

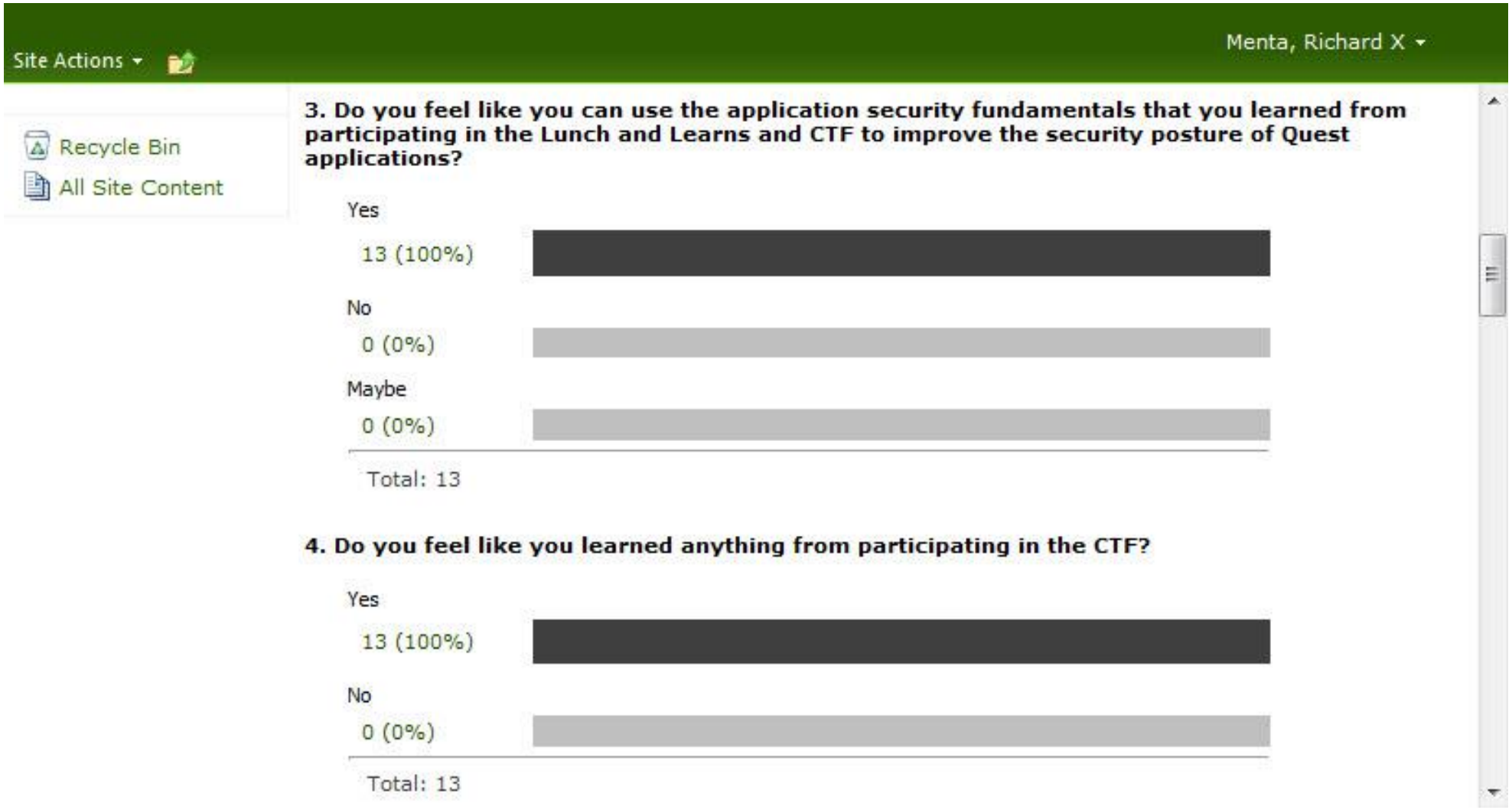
Player	Score
Sombreroblanco	10820
TheMightyMorphin	10670
RESPONDERS	10670
dud	10245
BigBuckStalker	10220
Landsharks	9620
booyah	9395
TeamIDW	9245
DTeam1	9020
Questonymous	8895
Knocker	8370
TheBlitz	7945
K10	7070
Brill	6345
0wnr0p3r4tr	4695
MrR0b07	3160
FireBlaster	2720
yantherunner	2420
ApArchitectsB	1870
WileECoyote	1175
YouDontNeedToSeeMyIdentification	745

Oct 28 2015 Final

Post Capture the Flag Survey



Post Capture the Flag Survey

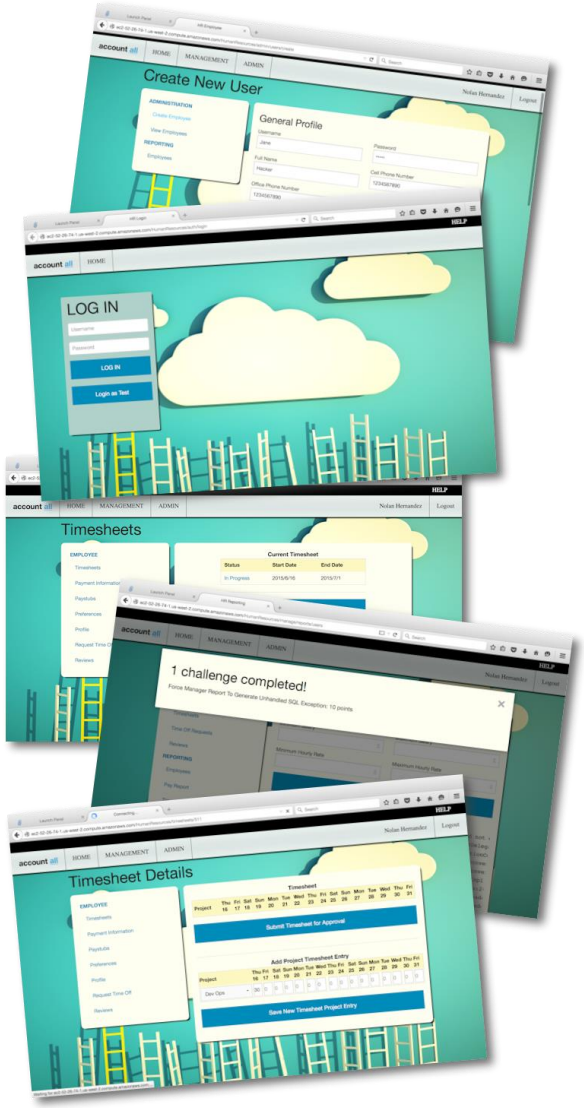


Post Capture the Flag Survey

Post Capture the Flag Quotes

- *"It became so addictive. Playing this game until midnight last few days."*
- *"This is an awesome idea. This event gave a better understanding about the vulnerability as we try to exploit it. Further reading about the vulnerability and other vulnerabilities were priceless."*
- *"It was a great experience. There will be a lot more people joining if you guys do another CTF event."*
- *"This was a great idea and it went very well. It seemed to get good management support and I think everyone seemed to see the value in it which was great. Developers know how to protect sites but turning that around to attacking them is a very different set of muscles. It was nice being able to exercise those muscles in a safe environment."*
- *"I love the play-by-play. Maybe you should have been a sports commentator."*

We ran our 2nd annual event in October 2016



- 2016 drew 104 participants, up from 63 in 2015
- In this year's event all teams and individuals who placed in the top 10 of the rankings found over 90% of the flag, some quite difficult.
- Between the two events we saw a sharp reduction in common coding flaws
- Anecdotal evidence: Some participants not only fixed their own flaws, if they spotted someone else's flaws they told them and instructed them how to fix it.

Sports Update again motivated participants

Quest Diagnostics | ITSecurity

CTF Sport Update Final: Crashers Crash third Place

Wow, did that one go down to the wire! The big story of the entire Capture the Flag competition belongs to Inder Kunchakurti's team the **Crashers** who almost pulled off a surprise upset in this year's RED Flag event. This morning at 9:15 am the **Crashers** were sitting in 9th place and thousands of points behind the leaders. Less than four hours later they were just a hair away from the top spot and staring at the kill when time ran out.

9:15 AM 10/31/16

PLACE	SCORE	PLAYER HANDLE
1	12750	1=1
2	12500	WildThing
3	11925	AlUrPHIrBelong2Us
4	11875	Weisser Hut
5	11875	Figgis Agency
6	11525	Mr. Big Byte
7	11105	dud
8	10775	redhiro
9	10175	Crashers

Noon 10/31/16

PLACE	SCORE	PLAYER HANDLE
1	12750	1=1
2	12500	WildThing
3	12225	Crashers
4	11925	AlUrPHIrBelong2Us
5	11875	Weisser Hut
6	11875	Figgis Agency

Facebook Releases Free CTF Platform

Facebook encourages wannabe hackers by making Capture The Flag open source
http://betanews.com/2016/05/11/facebook-capture-the-flag-open-source/

Facebook CTF is Now Open Source! (download platform)
https://m.facebook.com/notes/facebook-ctf/facebook-ctf-is-now-open-source/525464774322241

Takeaways

- *Don’t let participants feel they are playing in isolation.*
- *Generate excitement beyond those participating.*
- *Competition drove contestants to find that extra edge. Most did additional research online.*
- *Capture the Flag was less expensive than classroom teaching and more effective.*
- *Residual mentoring and coaching appeared organically after the event.*
- *Common coding errors dropped significantly.*