Introduction to CTF

Traditional Course Practice

- More theory and basic concept, but less practice and lab
- Offensive Thinking
  - Think like a hacker

Real World Attack

- Overall attack life cycle
  - Reconnaissance
  - Gaining Access
  - Maintain Access
  - Clearing Tracks
- Need to cope with many fussy work
- Most security issue
  - Too simple to find
  - Too complex

The other way for security training

- CTF as the training for offensive security
  - Spread security techniques
  - Measure security skill
  - Practice, practice and more practice

- Emulate real world problems
  - Environment close to real environment
  - Eliminate the boring task and focus on advanced security skill

Capture the Flag

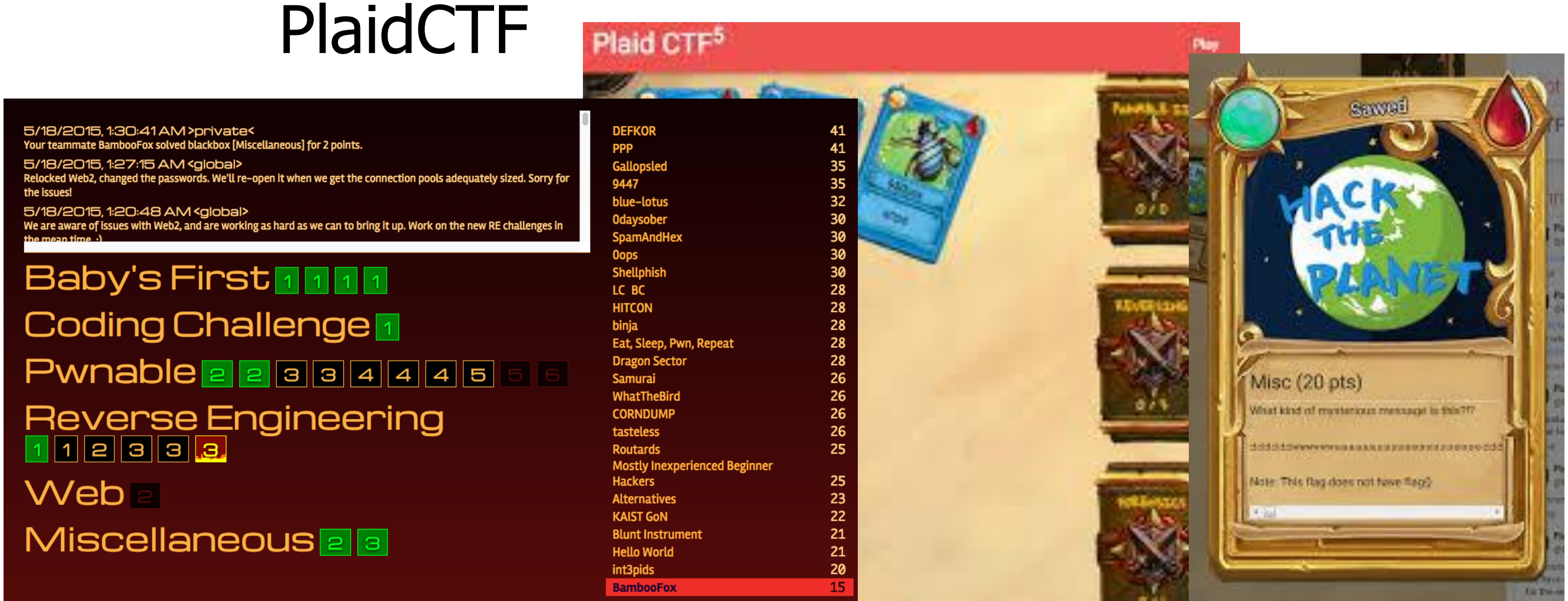
- The competition to steal data, a.k.a flag, from other computers
  - EX. Steal admin password from a web server
- Most problems are related to information security
- Good practice for students and even the experts

CTF

- Starting from Defcon 4 in 1996
  - Format is a mystery...
  - Held every year since 1996
  - The most important CTF now
- UCSB iCTF first held in 2001
  - The first CTF be held by academic organization

CTF around the world

- To enhance education of offensive security, CTFs are held in many country
  - U.S: DEFCON, Ghost In the Shellcode, PlaidCTF



5/18/2015, 1:30:41 AM >private<
Your teammate BambooFox solved blackbox [Miscellaneous] for 2 points.
5/18/2015, 1:27:15 AM <global>
Relocked Web2, changed the passwords. We'll re-open it when we get the connection pools adequately sized. Sorry for the issues!
5/18/2015, 1:20:48 AM <global>
We are aware of issues with Web2, and are working as hard as we can to bring it up. Work on the new RE challenges in the mean time :)

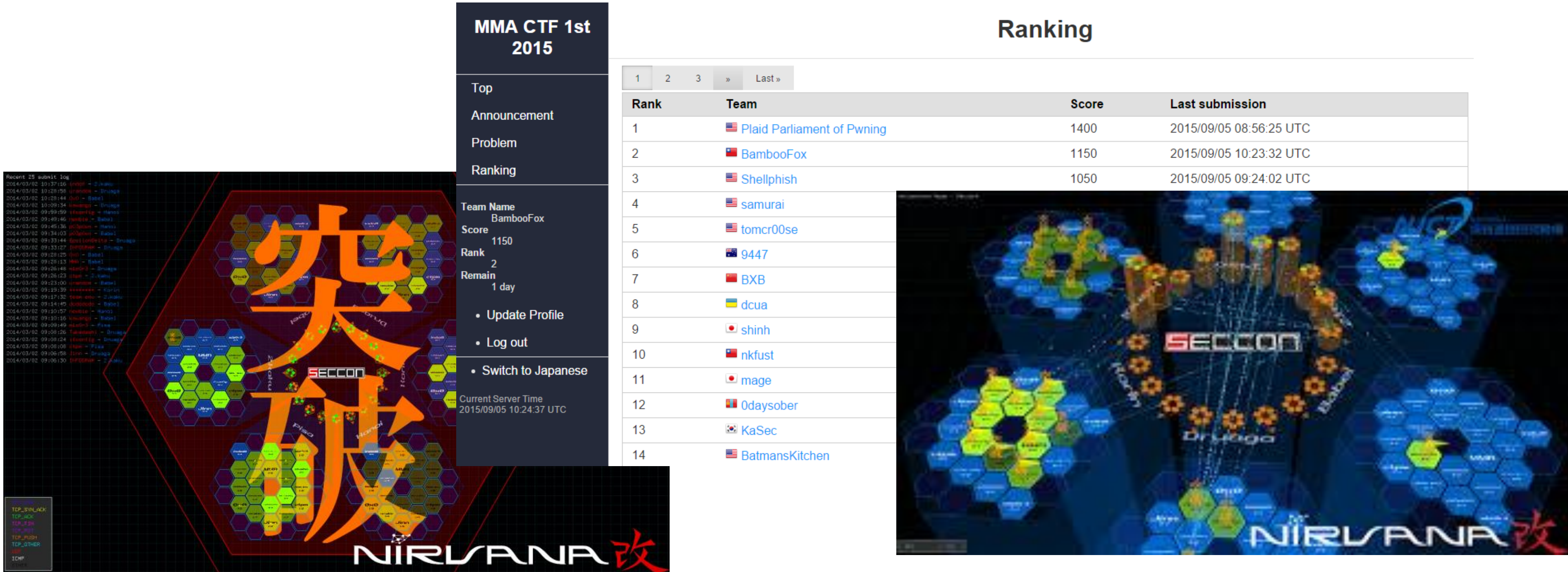
Baby's First 1 1 1 1
Coding Challenge 1
Pwnable 2 2 3 3 4 4 4 5 5 6
Reverse Engineering 1 1 2 3 3 3
Web 2
Miscellaneous 2 3

DEFKOR	41
PPP	41
Gallopsled	35
9447	35
blue-lotus	32
0daysober	30
SpamAndHex	30
Oops	30
Shellphish	30
LC BC	28
HITCON	28
binja	28
Eat, Sleep, Pwn, Repeat	28
Dragon Sector	28
Samurai	26
WhatTheBird	26
CORNDUMP	26
tasteless	26
Routards	25
Mostly Inexperienced Beginner Hackers	25
Alternatives	23
KAIST GoN	22
Blunt Instrument	21
Hello World	21
int3pids	20
BambooFox	15

Misc (20 pts)
What kind of mysterious message is this???
[illegible]
Note: This flag does not have flag{}

CTF around the world

- To enhance education of offensive security, CTFs are held in many country
  - Japan: SECCON, TMCTF, MMACTF



MMA CTF 1st 2015

- Top
- Announcement
- Problem
- Ranking

Team Name: BambooFox
Score: 1150
Rank: 2
Remain: 1 day

- Update Profile
- Log out
- Switch to Japanese

Current Server Time
2015/09/05 10:24:37 UTC

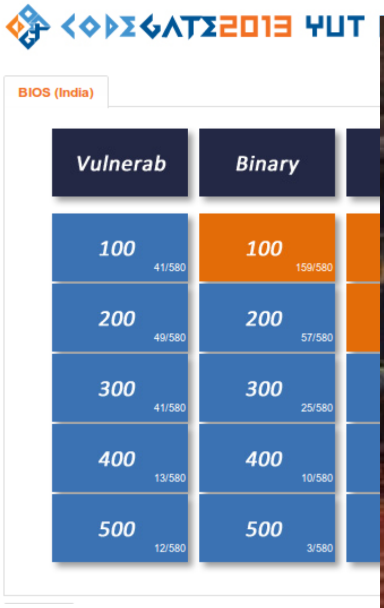
Ranking

1 2 3 » Last »

Rank	Team	Score	Last submission
1	Plaid Parliament of Pwning	1400	2015/09/05 08:56:25 UTC
2	BambooFox	1150	2015/09/05 10:23:32 UTC
3	Shellphish	1050	2015/09/05 09:24:02 UTC
4	samurai		
5	tomcr00se		
6	9447		
7	BXB		
8	dcua		
9	shinh		
10	nkfust		
11	mage		
12	0daysober		
13	KaSec		
14	BatmansKitchen		

CTF around the world

- To enhance education of offensive security, CTFs are held in many country
  - Korea: CodeGate, SECUINSIDE



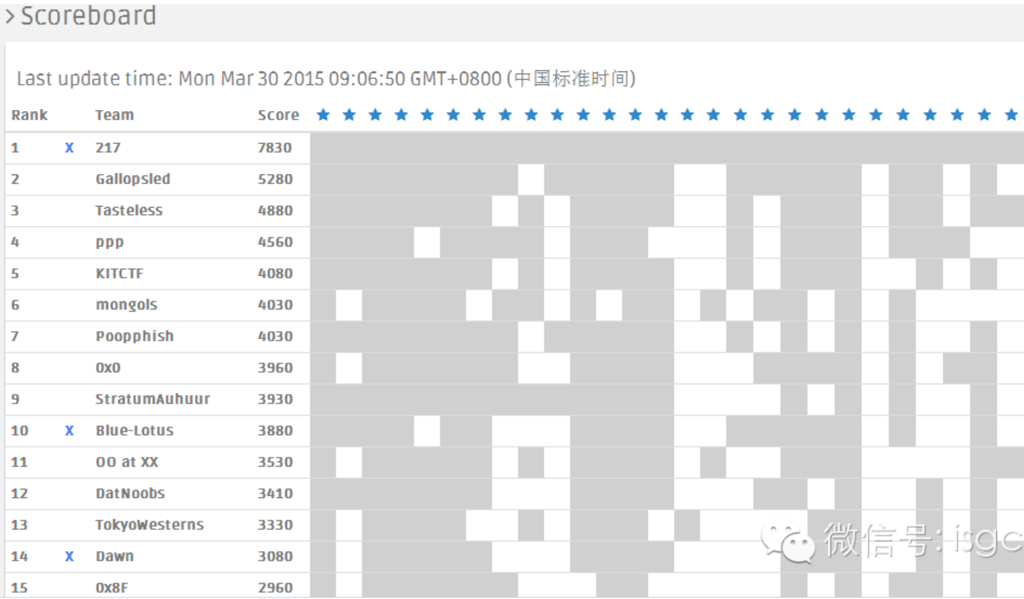
CODEGATE2013 YUT

BIOS (India)

Vulnerab	Binary
100 41/580	100 159/580
200 49/580	200 57/580
300 41/580	300 25/580
400 13/580	400 10/580
500 12/580	500 3/580

CTF around the world

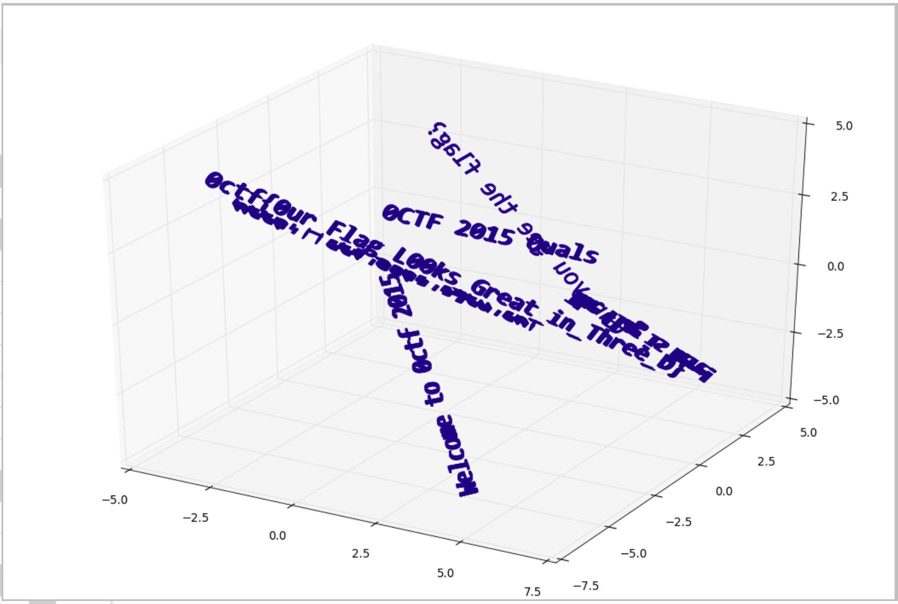
- To enhance education of offensive security, CTFs are held in many country
  - China: XCTF, BCTF, 0CTF, …..



> Scoreboard

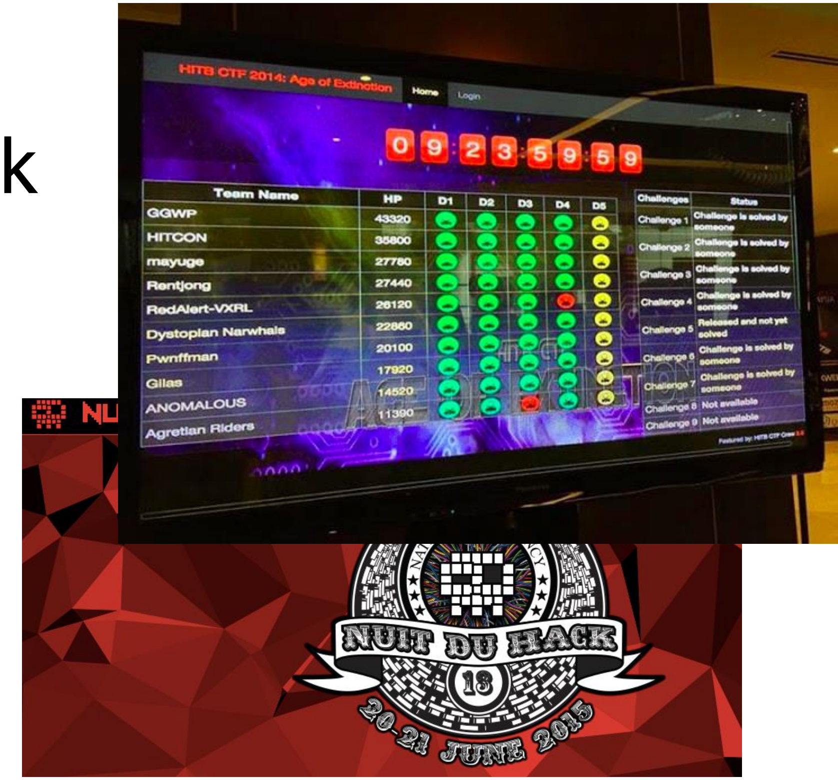
Last update time: Mon Mar 30 2015 09:06:50 GMT+0800 (中国标准时间)

Rank		Team	Score
1	X	217	7830
2		Gallopsled	5280
3		Tasteless	4880
4		ppp	4560
5		KITCTF	4080
6		mongols	4030
7		Poopphish	4030
8		0x0	3960
9		StratumAuhuur	3930
10	X	Blue-Lotus	3880
11		00 at XX	3530
12		DatNoobs	3410
13		TokyoWesterns	3330
14	X	Dawn	3080
15		0x8F	2960



CTF around the world

- To enhance education of offensive security, CTFs are held in many country
  - Russia: RuCTF
  - France: Nuit du Hack CTF
  - Malaysia: HITB CTF
  - Colombia: Backdoor CTF



HITB CTF 2014: Age of Extinction

Team Name	HP	D1	D2	D3	D4	D5
GGWP	43320	🟢	🟢	🟢	🟢	🟡
HITCON	35800	🟢	🟢	🟢	🟢	🟡
mayuge	27780	🟢	🟢	🟢	🟢	🟡
Rentjong	27440	🟢	🟢	🟢	🟢	🟡
RedAlert-VXRL	26120	🟢	🟢	🟢	🔴	🟡
Dystopian Narwhals	22860	🟢	🟢	🟢	🟢	🟡
Pwnffman	20100	🟢	🟢	🟢	🟢	🟡
Gilas	17920	🟢	🟢	🟢	🟢	🟡
ANOMALOUS	14520	🟢	🟢	🟢	🟢	🟡
Agretian Riders	11390	🟢	🟢	🔴	🟢	🟡

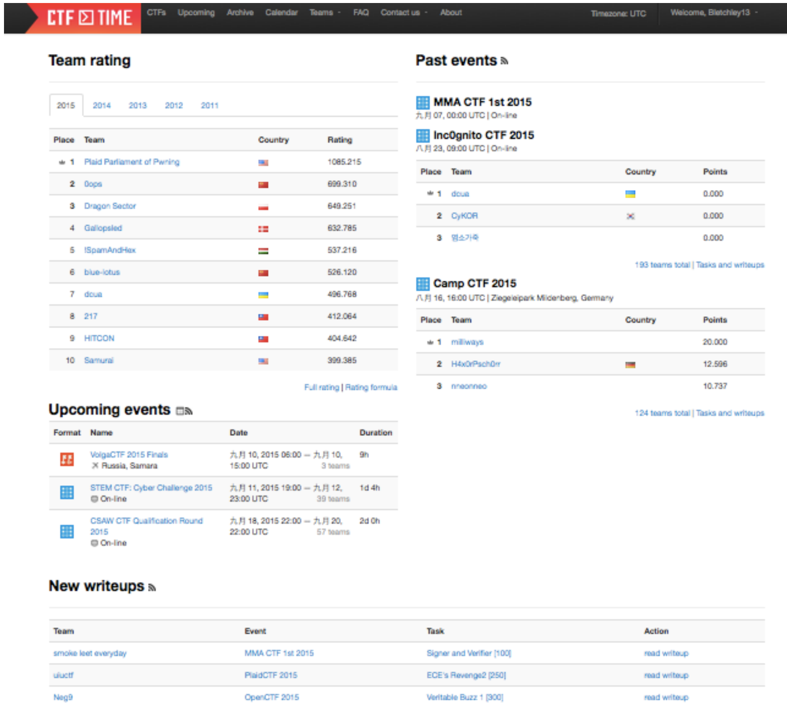
Challenges	Status
Challenge 1	Challenge is solved by someone
Challenge 2	Challenge is solved by someone
Challenge 3	Challenge is solved by someone
Challenge 4	Challenge is solved by someone
Challenge 5	Released and not yet solved
Challenge 6	Challenge is solved by someone
Challenge 7	Challenge is solved by someone
Challenge 8	Not available
Challenge 9	Not available

Featured by: HITB CTF Crew

CTFTime

- Created by kyprizel (MSLC) in 2010

- Centralize ranking and statistic website



Team rating

2015 2014 2013 2012 2011

Place	Team	Country	Rating
1	Plaid Parliament of Pwning	🇺🇸	1085.215
2	0ops	🇨🇳	699.310
3	Dragon Sector	🇵🇱	649.251
4	Gallopsled	🇩🇰	632.785
5	!SpamAndHex	🇭🇺	537.216
6	blue-lotus	🇨🇳	526.120
7	dcua	🇺🇦	496.768
8	217	🇹🇼	412.064
9	HITCON	🇹🇼	404.642
10	Samurai	🇺🇸	399.385

Full rating | Rating formula

Upcoming events

Format	Name	Date	Duration
	VolgaCTF 2015 Finals Russia, Samara	九月 10, 2015 06:00 — 九月 10, 15:00 UTC 3 teams	9h
	STEM CTF: Cyber Challenge 2015 On-line	九月 11, 2015 19:00 — 九月 12, 23:00 UTC 39 teams	1d 4h
	CSAW CTF Qualification Round 2015 On-line	九月 18, 2015 22:00 — 九月 20, 22:00 UTC 57 teams	2d 0h

New writeups

Team	Event	Task	Action
smoke leet everyday	MMA CTF 1st 2015	Signer and Verifier [100]	read writeup
uiuctf	PlaidCTF 2015	ECE's Revenge2 [250]	read writeup
Neg9	OpenCTF 2015	Veritable Buzz 1 [300]	read writeup

Past events

MMA CTF 1st 2015

九月 07, 00:00 UTC | On-line

Inc0gnito CTF 2015

八月 23, 09:00 UTC | On-line

Place	Team	Country	Points
1	dcua	🇺🇦	0.000
2	CyKOR	🇰🇷	0.000
3	멍소가락		0.000

193 teams total | Tasks and writeups

Camp CTF 2015

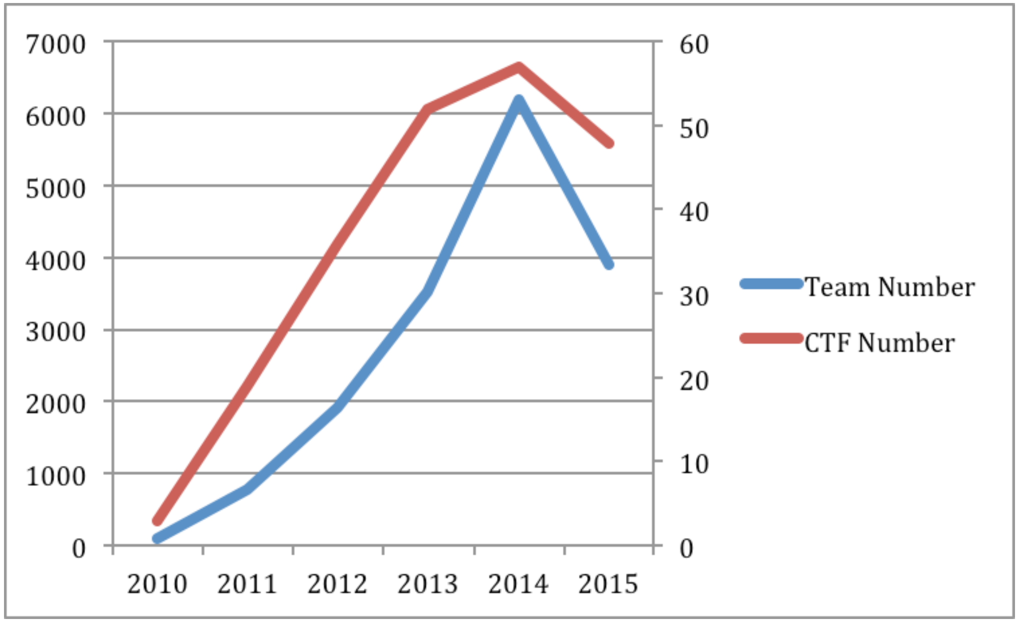
八月 16, 16:00 UTC | Ziegeleipark Mildenberg, Germany

Place	Team	Country	Points
1	milliways		20.000
2	H4x0rPsch0rr	🇩🇪	12.596
3	nneonneo		10.737

124 teams total | Tasks and writeups

Trend of CTFs

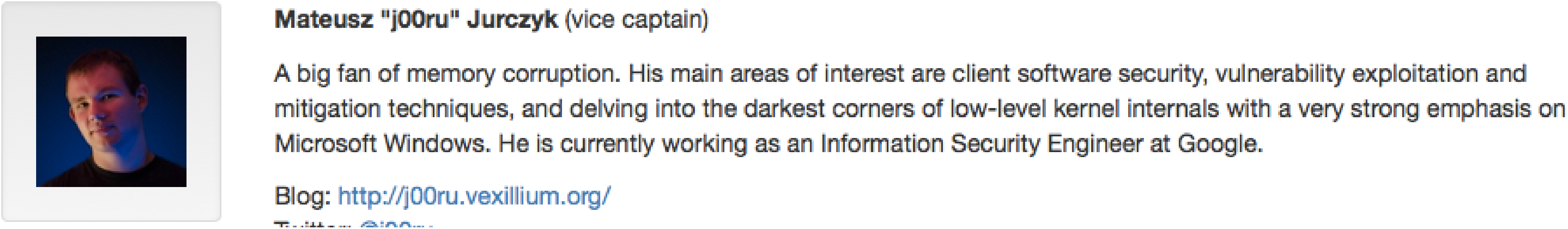
- CTF contest
  - Less than 10 in 2010
  - More than 50 CTFs in 2014
- CTF teams
  - More than 6000 teams in 2014
  - Many famous teams



Famous CTF teams

- PPP(US, CMU)
- HITCON(TW)
- 217(TW, NTU)
- 0ops(China, Shanghai Jiao Tong University)
- Blue-Lotus(China, Tsinghua University)
- Dragon Sector(Poland)
- Gallopsled(Danmark)
- Shellphish(US, UCSB)
- DEFKOR(Korea)

Dragon Sector



Mateusz "j00ru" Jurczyk (vice captain)

A big fan of memory corruption. His main areas of interest are client software security, vulnerability exploitation and mitigation techniques, and delving into the darkest corners of low-level kernel internals with a very strong emphasis on Microsoft Windows. He is currently working as an Information Security Engineer at Google.

Blog: http://j00ru.vexillium.org/

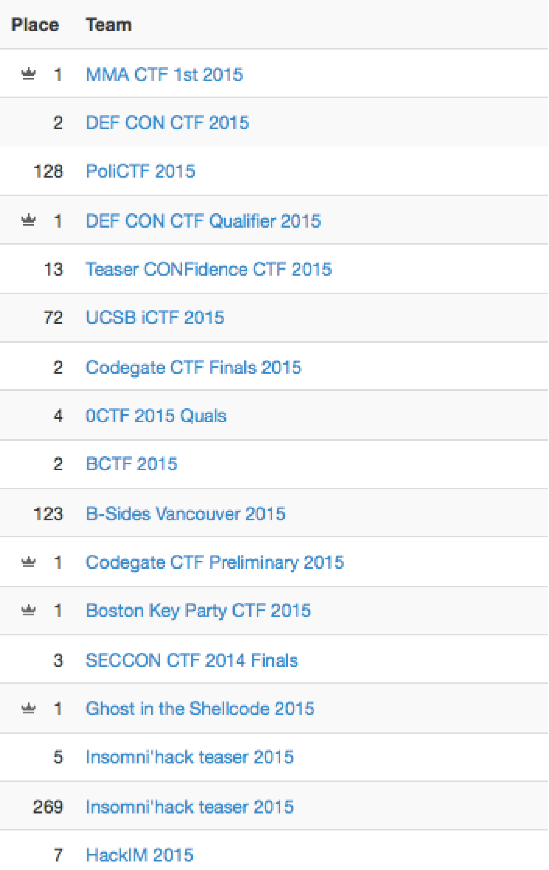
Twitter: @j00ru

0ops

- Students from Shanghai Jiao Tong University and Keen Team
  - Winner of Pwn2Own 2014

PPP

- CMU CYLAB



Place	Team
♛ 1	MMA CTF 1st 2015
2	DEF CON CTF 2015
128	PoliCTF 2015
♛ 1	DEF CON CTF Qualifier 2015
13	Teaser CONFidence CTF 2015
72	UCSB iCTF 2015
2	Codegate CTF Finals 2015
4	0CTF 2015 Quals
2	BCTF 2015
123	B-Sides Vancouver 2015
♛ 1	Codegate CTF Preliminary 2015
♛ 1	Boston Key Party CTF 2015
3	SECCON CTF 2014 Finals
♛ 1	Ghost in the Shellcode 2015
5	Insomni'hack teaser 2015
269	Insomni'hack teaser 2015
7	HackIM 2015

Why CTF

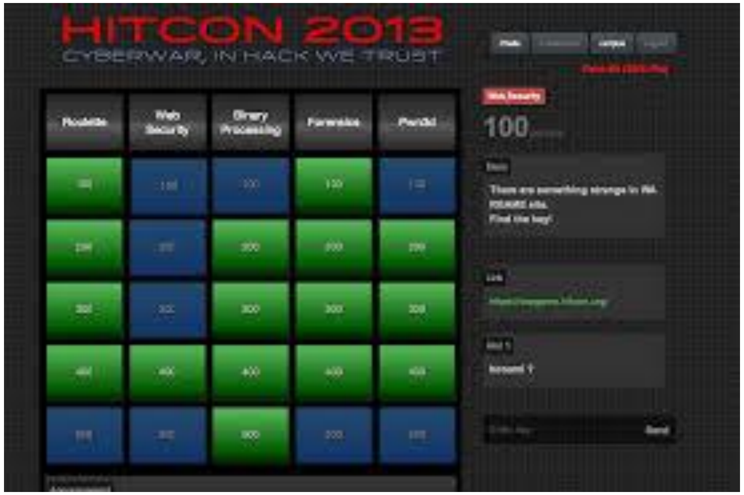
- Practice your hacking skills

- Compete with top hackers among the world

CTF TYPES

JeoPardy

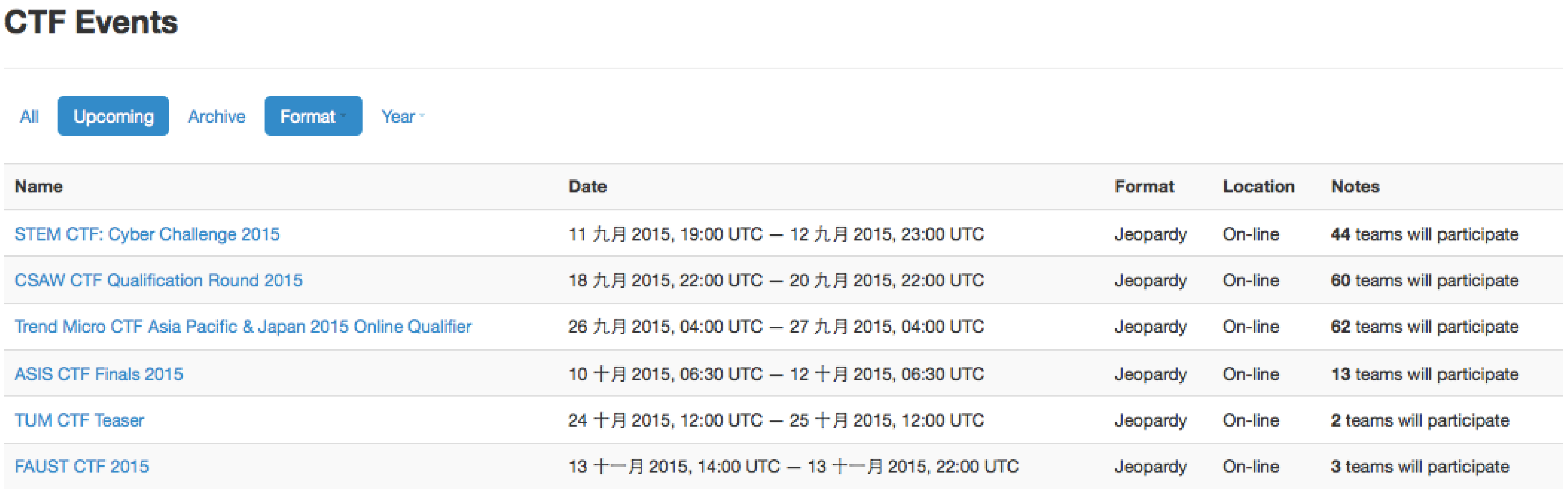
- Problems are classified into different disciplines
  - Most JeoPardy CTF contain 20~30 problems
  - Pwn, Reverse Engineering, Web security, Forensics and Cryptography
  - More difficult problem worth more score
- About 90% CTFs are in JeoPardy style
  - Can be held online and hundred of teams can involve



Search
Boston Key Party 2015 › Pwning Reversing Crypto "School Bus"

JeoPardy

- JeoPardy CTF in this years



CTF Events

Name	Date	Format	Location	Notes
STEM CTF: Cyber Challenge 2015	11 九月 2015, 19:00 UTC — 12 九月 2015, 23:00 UTC	Jeopardy	On-line	**44** teams will participate
CSAW CTF Qualification Round 2015	18 九月 2015, 22:00 UTC — 20 九月 2015, 22:00 UTC	Jeopardy	On-line	**60** teams will participate
Trend Micro CTF Asia Pacific & Japan 2015 Online Qualifier	26 九月 2015, 04:00 UTC — 27 九月 2015, 04:00 UTC	Jeopardy	On-line	**62** teams will participate
ASIS CTF Finals 2015	10 十月 2015, 06:30 UTC — 12 十月 2015, 06:30 UTC	Jeopardy	On-line	**13** teams will participate
TUM CTF Teaser	24 十月 2015, 12:00 UTC — 25 十月 2015, 12:00 UTC	Jeopardy	On-line	**2** teams will participate
FAUST CTF 2015	13 十一月 2015, 14:00 UTC — 13 十一月 2015, 22:00 UTC	Jeopardy	On-line	**3** teams will participate

Problems in JeoPardy

- Web
- Crypto
- Forensic
- Reverse
- Pwn (Software Exploitation)

Attack & Defense

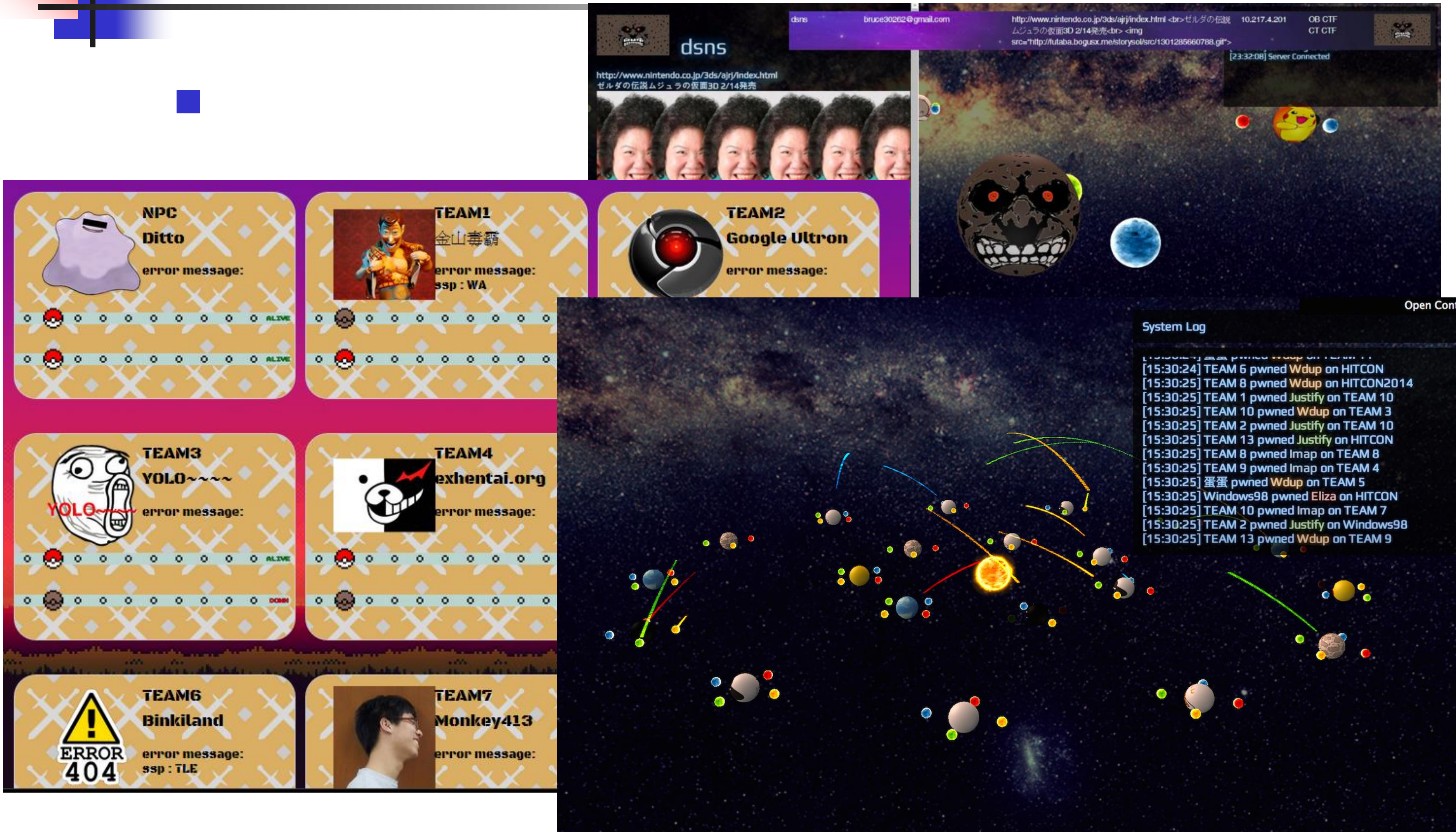
- The competitors are put into the closed environment and try to attack each other's.
  - The server with vulnerable programs running
- Competitor needed to patch(fix) the vulnerability and exploit(attack) the other teams

Attack & Defense

- Need good support of networking environment
- Less CTFs are in Attack & Defense style
- Can do many interesting things
- Skills needed
  - Vulnerability discovery and patching
  - Network flow analysis
  - System administrator
  - Backdoor

CTCTF & NSCTF

-



dsns

http://www.nintendo.co.jp/3ds/ajrj/index.html
ゼルダの伝説ムジュラの仮面3D 2/14発売

```
dsns    bruce30262@gmail.com    http://www.nintendo.co.jp/3ds/ajrj/index.html <br>ゼルダの伝説    10.217.4.201    OB CTF
                                ムジュラの仮面3D 2/14発売<br> <img                                                  CT CTF
                                src="http://futaba.bogusx.me/storysol/src/1301285660788.gif">
[23:32:08] Server Connected
```

NPC
Ditto
error message:

TEAM1
金山毒霸
error message:
ssp : WA

TEAM2
Google Ultron
error message:

TEAM3
YOLO~~~~
error message:

TEAM4
exhentai.org
error message:

TEAM6
Binkiland
error message:
ssp : TLE

TEAM7
Monkey413
error message:

System Log

```
[15:30:24] TEAM 6 pwned Wdup on HITCON
[15:30:25] TEAM 8 pwned Wdup on HITCON2014
[15:30:25] TEAM 1 pwned Justify on TEAM 10
[15:30:25] TEAM 10 pwned Wdup on TEAM 3
[15:30:25] TEAM 2 pwned Justify on TEAM 10
[15:30:25] TEAM 13 pwned Justify on HITCON
[15:30:25] TEAM 8 pwned Imap on TEAM 8
[15:30:25] TEAM 9 pwned Imap on TEAM 4
[15:30:25] 蛋蛋 pwned Wdup on TEAM 5
[15:30:25] Windows98 pwned Eliza on HITCON
[15:30:25] TEAM 10 pwned Imap on TEAM 7
[15:30:25] TEAM 2 pwned Justify on Windows98
[15:30:25] TEAM 13 pwned Wdup on TEAM 9
```

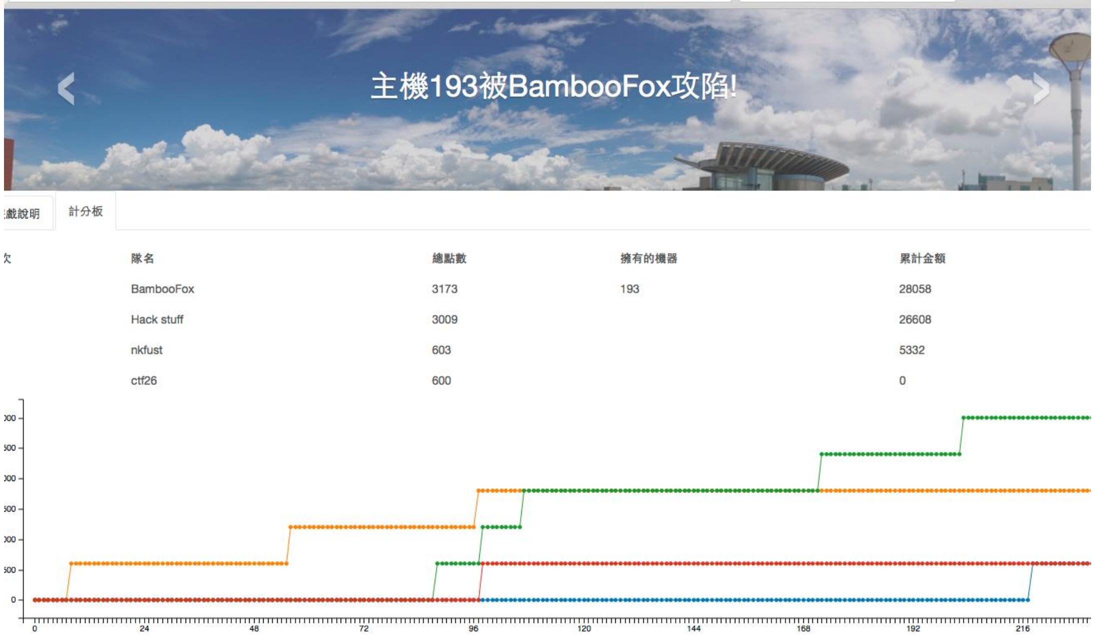
Attack & Defense

- iCTF
- RuCTF
- CTCTF
- Final project of network security last year
- Defcon Final
- HITCON Final
- SECCON Final

King of Hill

- There are several servers provided
- Competitors should compromise and keep control to the server
    - The more time you own the machine, the more score can be got
- Just like real-world cyber war
    - Attack not only need to attack, but also need to prevent other exploit server you owned

King of Hill



主機193被BambooFox攻陷!

戲說明 計分板

次	隊名	總點數	擁有的機器	累計金額
	BambooFox	3173	193	28058
	Hack stuff	3009		26608
	nkfust	603		5332
	ctf26	600		0

Which CTF to play?

More than 100 CTF’s each year, you can find the proper CTF

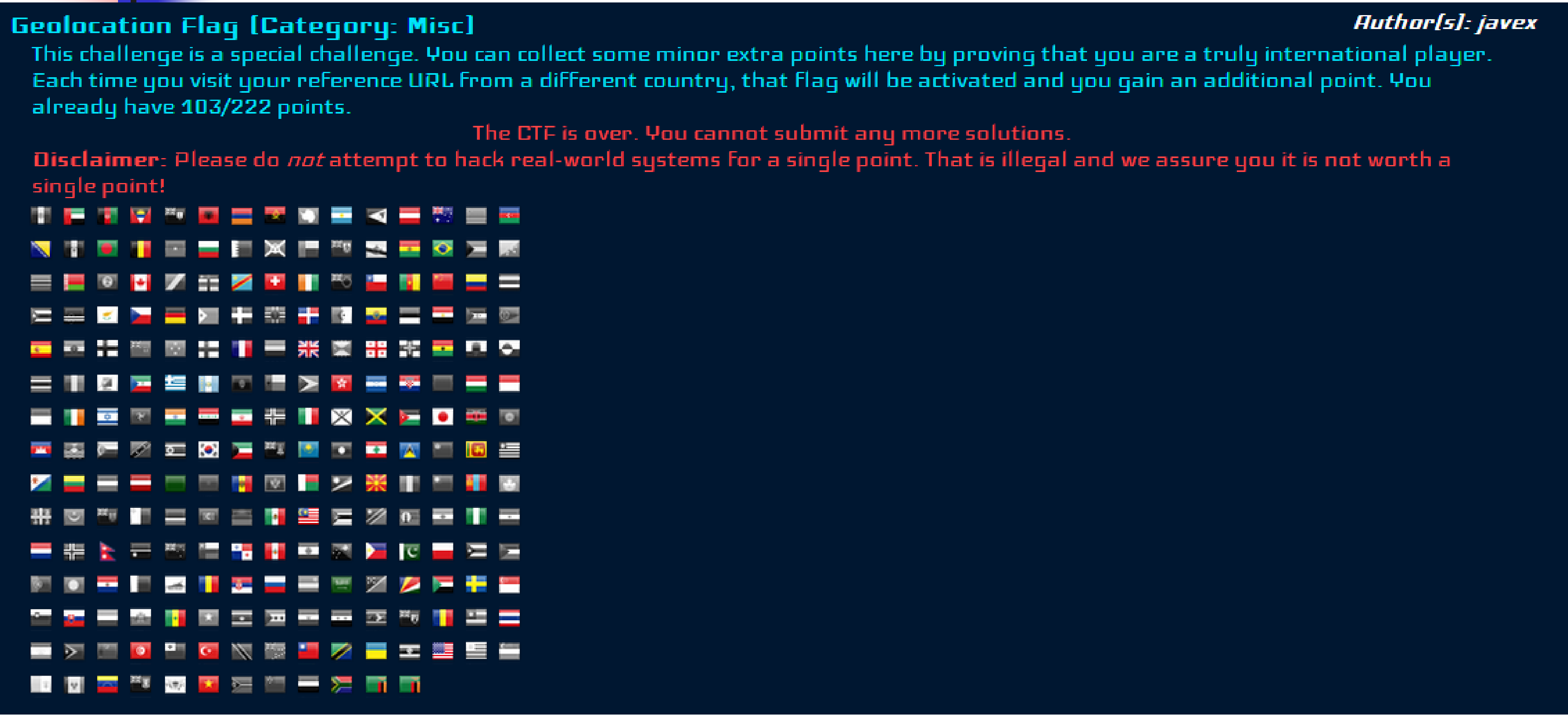
Beginner CTFs

- Backdoor
- CSAW Qualification
- ASIS

Advanced CTFs

- DEFCON
- PlaidCTF
  - 最強PPP組織的比賽
- CodeGate
  - 韓國
- SECCON
  - 日本
- PHD Qals

Travel Around the World



Geolocation Flag [Category: Misc]

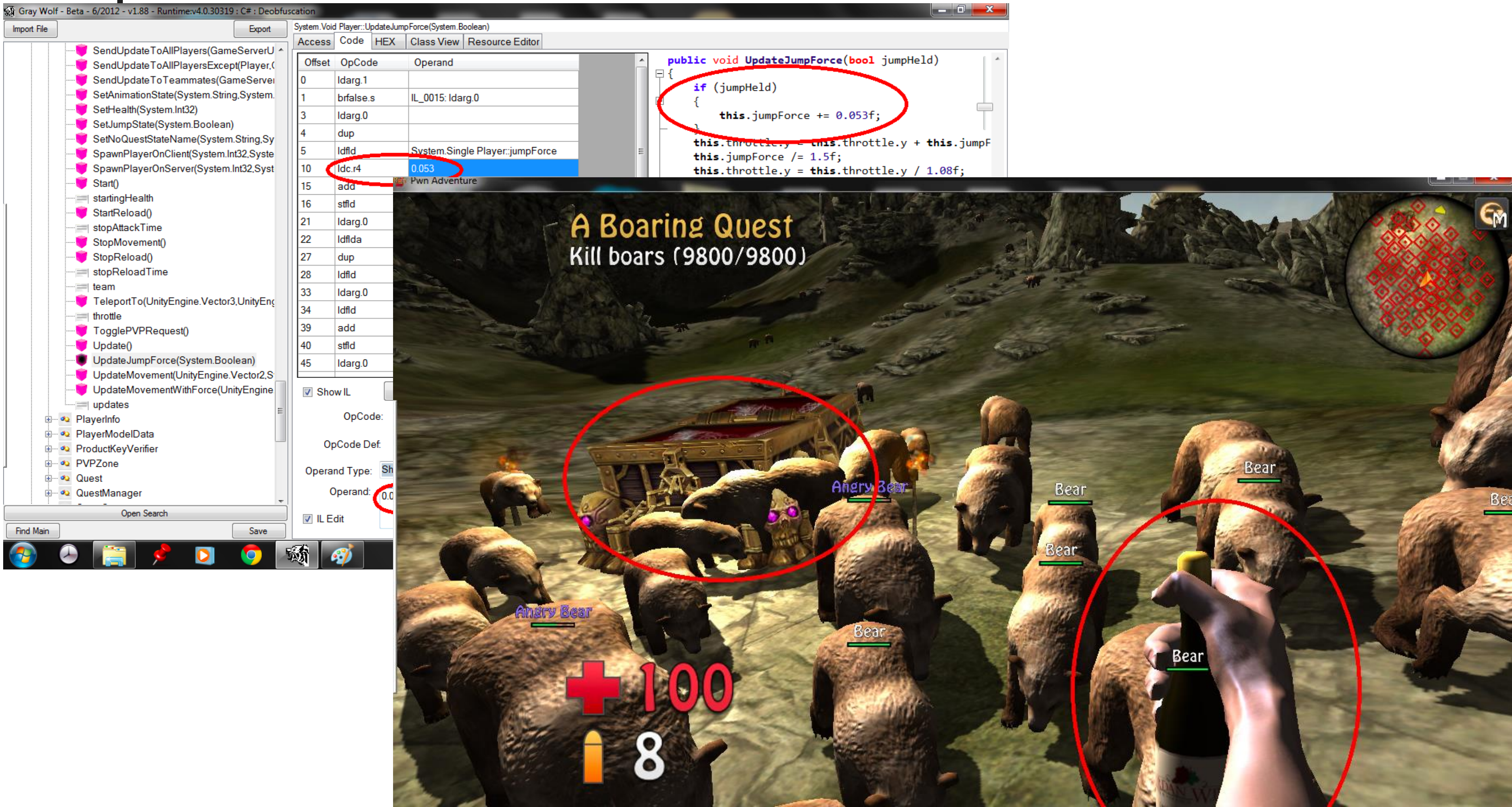
Author[s]: javex

This challenge is a special challenge. You can collect some minor extra points here by proving that you are a truly international player. Each time you visit your reference URL from a different country, that flag will be activated and you gain an additional point. You already have 103/222 points.

The CTF is over. You cannot submit any more solutions.

Disclaimer: Please do *not* attempt to hack real-world systems for a single point. That is illegal and we assure you it is not worth a single point!

Game Hacking



Gray Wolf - Beta - 6/2012 - v1.88 - Runtime:v4.0.30319 : C# : Deobfuscation

SendUpdateToAllPlayers(GameServerU
SendUpdateToAllPlayersExcept(Player,(
SendUpdateToTeammates(GameServe
SetAnimationState(System.String,System.
SetHealth(System.Int32)
SetJumpState(System.Boolean)
SetNoQuestStateName(System.String,Sy
SpawnPlayerOnClient(System.Int32,Syste
SpawnPlayerOnServer(System.Int32,Syst
Start()
startingHealth
StartReload()
stopAttackTime
StopMovement()
StopReload()
stopReloadTime
team
TeleportTo(UnityEngine.Vector3,UnityEng
throttle
TogglePVPRequest()
Update()
UpdateJumpForce(System.Boolean)
UpdateMovement(UnityEngine.Vector2,S
UpdateMovementWithForce(UnityEngine
updates
PlayerInfo
PlayerModelData
ProductKeyVerifier
PVPZone
Quest
QuestManager

System.Void Player::UpdateJumpForce(System.Boolean)

Offset	OpCode	Operand
0	ldarg.1	
1	brfalse.s	IL_0015: ldarg.0
3	ldarg.0	
4	dup	
5	ldfld	System.Single Player::jumpForce
10	ldc.r4	0.053
15	add	
16	stfld	
21	ldarg.0	
22	ldflda	
27	dup	
28	ldfld	
33	ldarg.0	
34	ldfld	
39	add	
40	stfld	
45	ldarg.0	

☑ Show IL

OpCode:

OpCode Def:

Operand Type: Sh

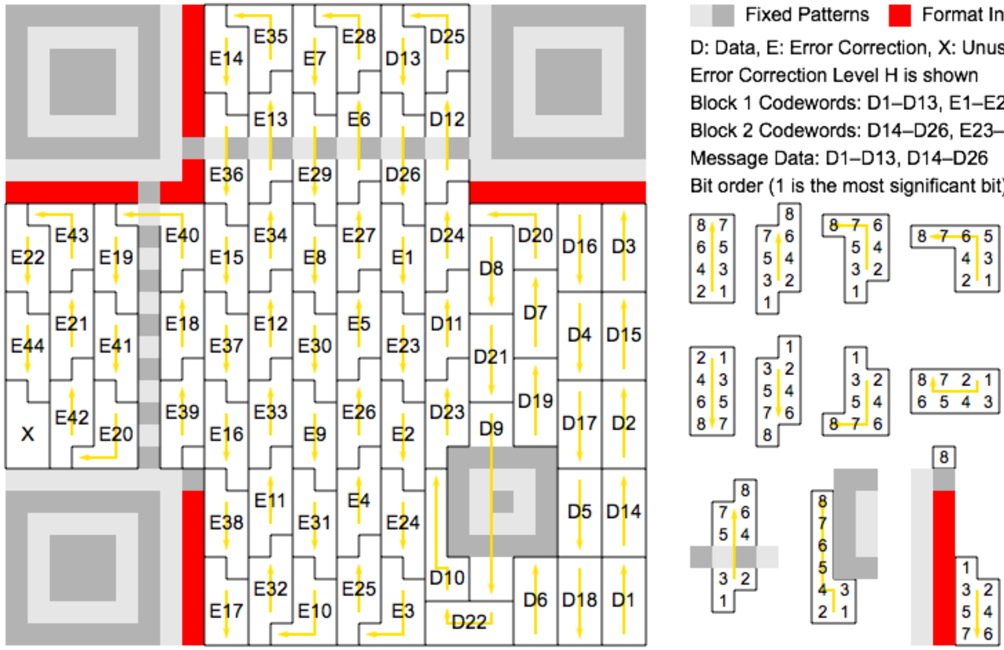
Operand: 0.0

☑ IL Edit

```
public void UpdateJumpForce(bool jumpHeld)
{
    if (jumpHeld)
    {
        this.jumpForce += 0.053f;
    }
    this.throttle.y = this.throttle.y + this.jumpF
    this.jumpForce /= 1.5f;
    this.throttle.y = this.throttle.y / 1.08f;
```

Pwn Adventure

QR Code



▨ Fixed Patterns 🟥 Format Info

D: Data, E: Error Correction, X: Unused

Error Correction Level H is shown

Block 1 Codewords: D1–D13, E1–E22

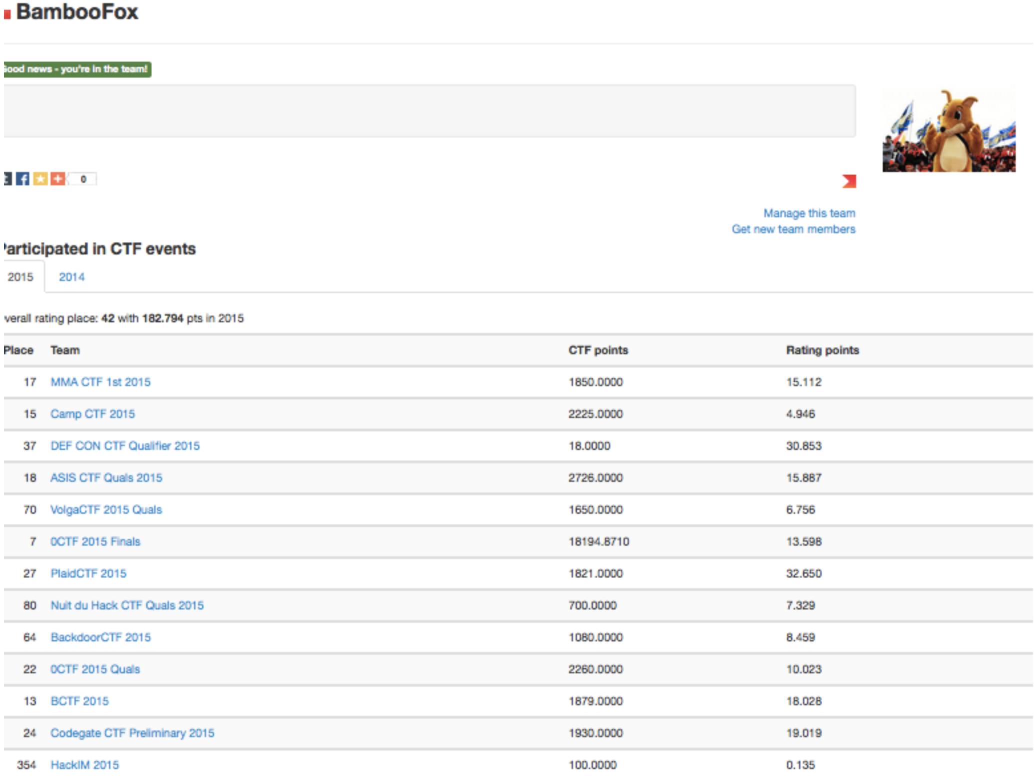
Block 2 Codewords: D14–D26, E23–E44

Message Data: D1–D13, D14–D26

Bit order (1 is the most significant bit):

BambooFox

- Our team, most students come from NCTU and NCU



BambooFox

ood news - you're in the team!

0

Manage this team
Get new team members

'articipated in CTF events

2015 2014

verall rating place: **42** with **182.794** pts in 2015

Place	Team	CTF points	Rating points
17	MMA CTF 1st 2015	1850.0000	15.112
15	Camp CTF 2015	2225.0000	4.946
37	DEF CON CTF Qualifier 2015	18.0000	30.853
18	ASIS CTF Quals 2015	2726.0000	15.887
70	VolgaCTF 2015 Quals	1650.0000	6.756
7	0CTF 2015 Finals	18194.8710	13.598
27	PlaidCTF 2015	1821.0000	32.650
80	Nuit du Hack CTF Quals 2015	700.0000	7.329
64	BackdoorCTF 2015	1080.0000	8.459
22	0CTF 2015 Quals	2260.0000	10.023
13	BCTF 2015	1879.0000	18.028
24	Codegate CTF Preliminary 2015	1930.0000	19.019
354	HackIM 2015	100.0000	0.135

EXPERIENCE SHARING

Focus !

- When you start to CTF, it is best to focus on one type of problem.
  - E.g. Pwn, Reverse, Web….
- When playing CTF, keep up with 1 problem in the same time

Following New Techniques

- Hackers like new techniques
- CTF organizer often proposes problem with these new techniques
- Follow up new technique
  - Freebuf
  - Reddit Hacking, NetSec and ReverseEngineering Channel

Customize Your CTF Toolset

- Prepare your own environment
  - With your favorite tools
  - Customize it. Make your operation more efficient.
  - Keep and refine the toolset and program after every CTF
    - Even better to come up with the writeup

Review the Problems

- Review the problem you are unable to solve during CTF
- Read the writeup

Practice, practice and practice

- Experience and proficiency play the important role in CTF
- Experience make you find the right way earlier
- Proficiency make you try more approaches than others
- Practice, practice ,practice , practice …..

Enjoy the Game

- Don't panic. Keep calm and carry on.

Q&A