關於 HITCON CTF 的那些事

之Web 狗如何在險惡的 CTF 世界中存活？

Orange@chroot.org

About Me

- 蔡政達 a.k.a Orange
- CHROOT 成員 / HITCON 成員
- 國內外研討會 HITCON, AVTokyo, PHPConf 等講師
- 國內外駭客競賽 CTF 冠軍
- 揭露過 Microsoft IE, Django, Yahoo ... 等 0-DAY 漏洞
- 專精於駭客手法、Web Security 與網路滲透

#90後 #賽棍 #電競選手 #狗 #Web狗


HITCON
DEF CON 22 Capture the Flag
Legitimate Business Syndicate

About HITCON CTF Team

- 台灣駭客年會 (Hacks in Taiwan Conference)
  - 前身為 CHROOT 讀書會
- 目前比賽成員約 14 位，成員來自台灣各隊伍
- 過半數為學生

參與過賽事(決賽)

- 中國 BCTF
- 韓國 SECUINSIDE
- 美國 DEF CON
- 馬來西亞 HITB
- 日本 SECCON
- 韓國 CODEGATE
- 中國 0CTF
- …

HITCON

由三隻獨立隊伍所合併而成


HITCON
2019


@X

- DEFCON CTF 21 Quals
- 217 首度接觸 CTF！

FREEBUF

在Defcon CTF資格賽倒計時10小時25分，來自台灣的CHROOT戰隊，解出了長達6個多小時未被解出OMGACM 4分題，並開出OMGACM 5分彩蛋，這幾乎改變了整個比賽的局勢，在IRC中引起了各國隊伍的膜拜。（順便說一下，CHROOT戰隊也是HITCON的主辦單位，要想膜拜 就去HITCON走走吧）

2013-05

2014-05

- 中國百度 BCTF 決賽
- 首次參加的 Attack & Defense 比賽！

黑客競賽住宿飯店提供黑客蚊香片

2013-05

2014-05

2014-05

- DEFCON CTF 22 Quals
- 聚集各方戰力重新挑戰一次
- HITCON
- 台灣大學 217
- 交通大學成員

SICK

http://www.jeffxx.com/blog/2014/05/19/defcon-ctf-22-qual-sick-writeup/

2013-05

2014-05

2014-05

2014-07

- 韓國 SECUINSIDE CTF 決賽
- 發現跟國外隊伍差距多大


SECUINSIDE 2014
tomcr00se
koscom
CNSECURITY

DEF CON 22 CTF FINAL

2013-05

2014-05

2014-08

2014-05

2014-07

- 首次聚集台灣最強戰力挑戰 DEFCON 決賽
- 抵達美國過程一波三折

- 時差問題
- 食物只有漢堡王
- 設備？VLAN TAG 999

2014 DEF CON Capture the Flag by Legitimate Business Syndicate

Final Scores

Team	Score
Plaid Parliament of Pwning	11263
HITCON	7833
Dragon Sector	4421
Reckless Abandon	4020
blue-lotus	3233
(Mostly) Men in Black Hats	2594
raon_ASRT	2281
S[illegible]	1529
[illegible]	1519
[illegible]	1334
[illegible]ken	

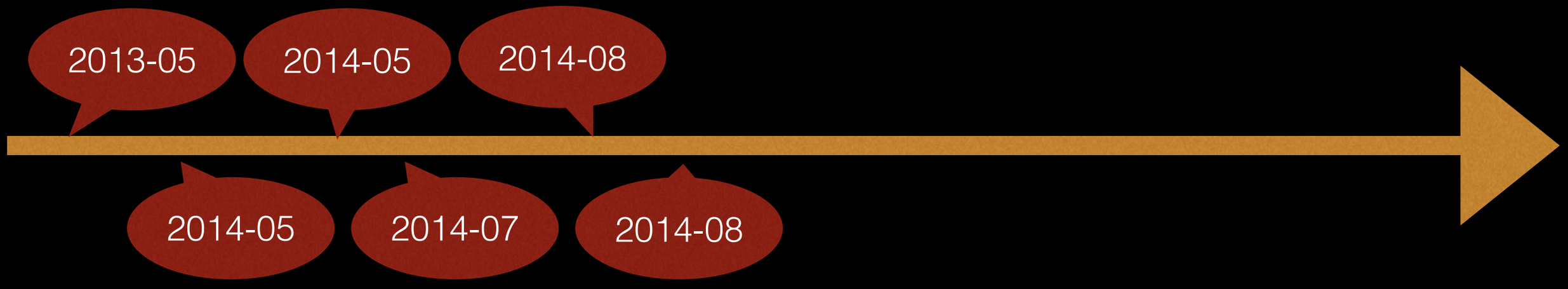
Thanks

2014 was our second year running DEF CON Capture the Flag, and we're still in shock at how well things went for our players and spectators. Here are our final thoughts about this year's game.

Scoring

This year's scoring mostly worked as documented: each team's instance of a service started with 417 flags, flags remained with the service even as they moved through teams, and teams could in theory come back from their flags on a service zeroing out.

On Friday, we found a bug that caused round-end flag distribution to be run once for each enabled service in a given round, instead of once in a given round. We fixed this Fri[illegible]ternoon, and re-ran the scoring algorithm over the entire ga[illegible]rday. Additionally, we were able to re-run scoring when teams [illegible] checks due t[illegible]dware failures



- HITCON 舉辦首場開放世界報名的比賽 – HITCON CTF

- 列強環繞 – Bamboo Fox 成立

2015 HITCON CTF

You are the impossibility in the impossible universe.

Qualification:
Online Jeopardy ,Oct 17-18,2015

Final:
Attack & Defense , Dec 5-6, 2015
4 players / team

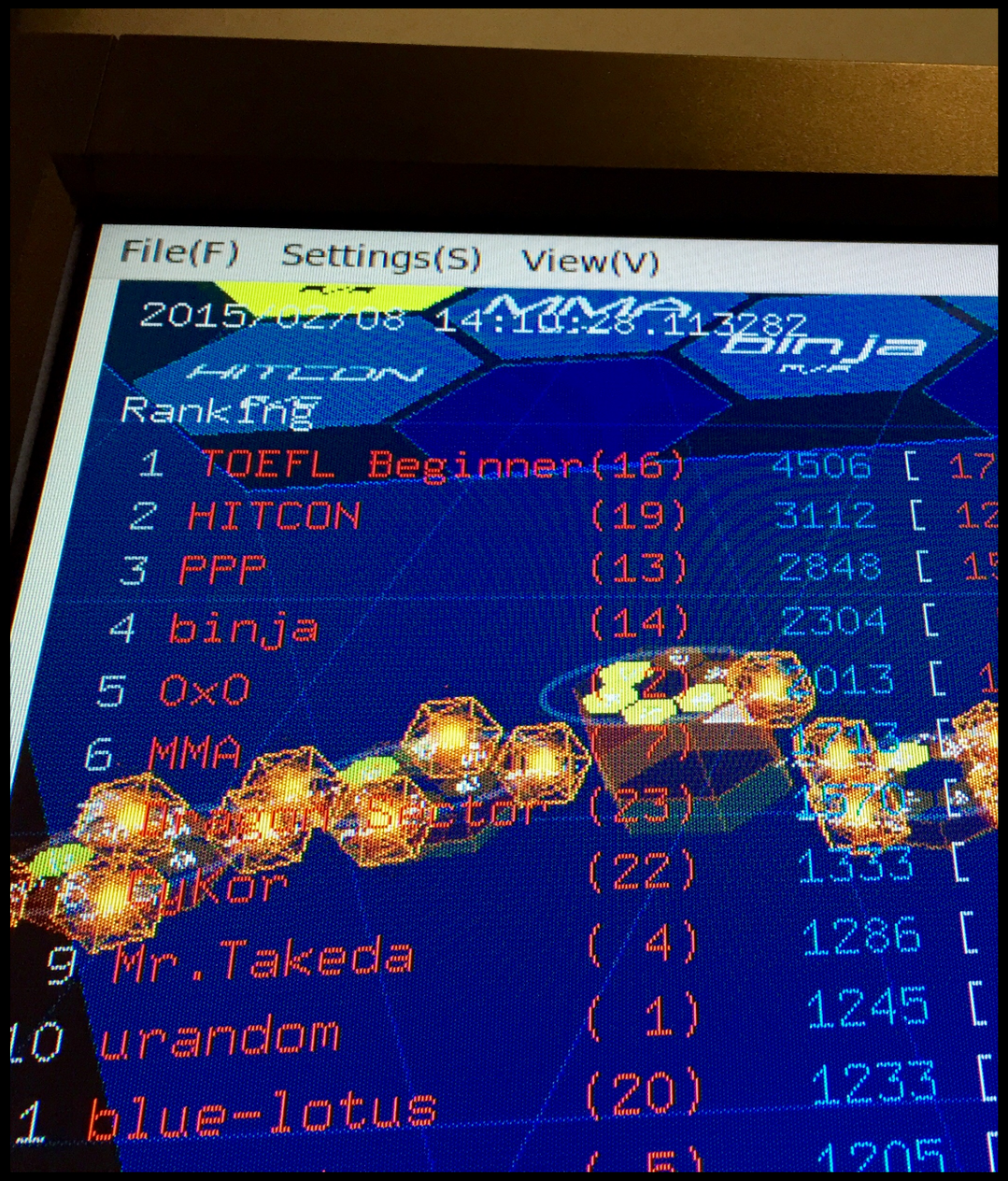
Currently 2015 HITCON CTF Qualifying Contests:
The champions of the following contests will qualify directly for the final in December and do not need to participate in the preliminary in 17th October.

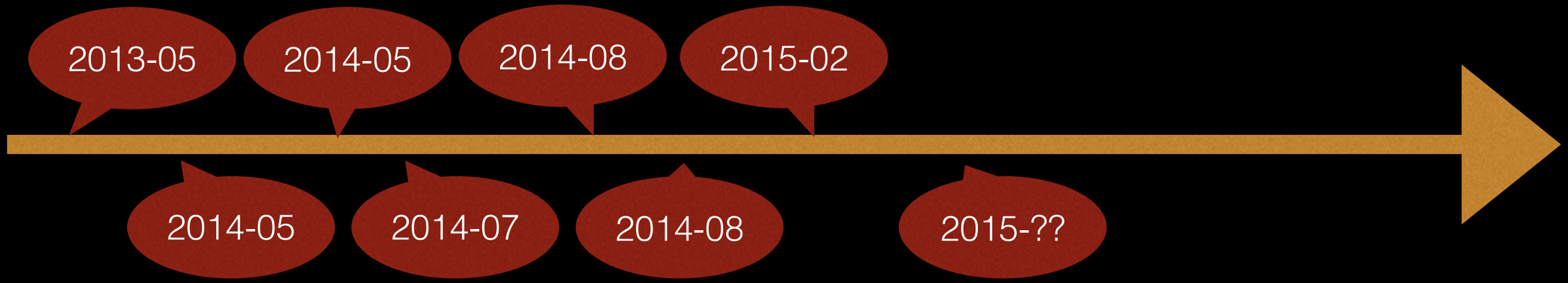
http://ctf.hitcon.org/

2013-05 2014-05 2014-08 2015-02

2014-05 2014-07 2014-08

- 日本 SECCON 決賽
- Kill of the Hill 賽制
- 看不懂規則以及網頁
  - 花了兩個小時 Fuzzing Protocol 找到 Overflow 後... 原來有提供 Binary





TO BE CONTINUED

「Web 狗如何在險惡的 CTF 世界中存活？」

「Web 狗如何在險惡的 CTF 世界中存活？」

DEFCON 22 CTF Quals Web x 1 of 21
DEFCON 23 CTF Quals Web x 1 of 24
Boston Key Party CTF 2015 Web x 0 of 31
PLAID CTF 2015 Web x 1 of 24

2015/5/18 上午7:59:02 <global>
SIXTY SECONDS #DEFCONCTF QUALS IT'S THE FINAL COUNTDOWN
2015/5/18 上午6:55:30 >private<
Your teammate L4ys solved shitcpu [Reverse Engineering] for 3 points.
2015/5/18 上午5:19:10 >private<
Your teammate ddaa solved int3rupted [Pwnable] for 5 points.
2015/5/18 上午4:40:26 <global>

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

PPP
DEF
944
Gal
HIT
blu
Spa
COI
Oop
Oda
Dra
She
LC4
Mo
Hac
San
KAI
Alt
Eat
Rou
bin
Wh
Blu
tas
int3
0x8

看到都快哭出來了

Web 為何弱勢？

- 代碼數量
  - 你不會為了出一道題目去寫幾十萬行代碼
- 技術 v.s. 思路 v.s. ...滲透？
  - 漏洞利用的藝術
  - 想想假使 WordPress / Discuz 出了一個任意變量覆蓋要如何 優雅 的利用？
  - 跳個 alert 也是利用，遠端代碼執行也是利用

CodeGate CTF 2015 Final Web Pseudo Code

```
#  login page
r = query("SELECT pwd FROM users WHERE user = '%s'" % username)

if r.pwd == password:

    session['username'] = username
```

```
# index page
username = session['username']

r = query("SELECT point FROM users WHERE user = '%s'" % username)

print r.point
```

CodeGate CTF 2015 Final Web Pseudo Code

- 4 / 10 隊伍解出
- 技術很簡單，成功登入後可以看到 session 對應的分數
  - 不過在沒有原始碼狀況下難度增加
  - 對於黑箱測試來說只有登入成功以及失敗的結果可知

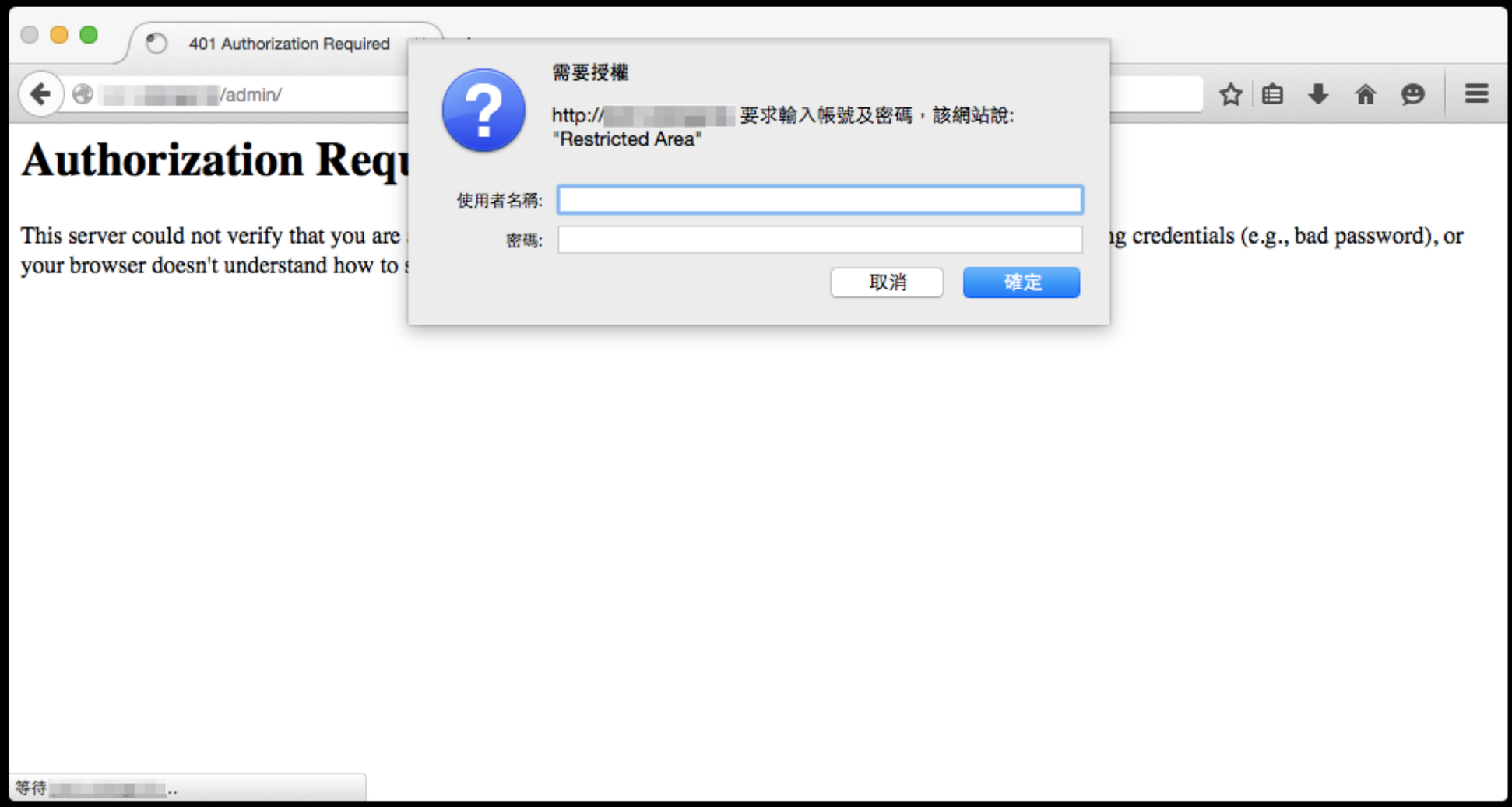
Q: 在沒有錯誤、無法讀寫、無法多語句的前提下，如何用最快的方式取得資料？

核心概念 – 單次輸入但構造出不同的結果

*' UNION SELECT (SELECT CASE WHEN random()*2>1 THEN 'password'*
ELSE (SELECT sql FROM sqlite_master limit 1) END)--+

核心概念 – 單次輸入但構造出不同的結果

' UNION SELECT (SELECT CASE WHEN datetime('now')>'2015-06-22 00:00:00' THEN 'password' ELSE (SELECT sql FROM sqlite_master limit 1) END)--+



HITCON CTF 2014 Web LEENODE

HITCON CTF 2014 Web
LEENODE

- 2 / 1020 隊伍解出
- Web 分層架構漏洞
  - ColdFusion with Apache Connector
  - 舊版本 ColdFusion Double Encoding 造成資訊洩漏漏洞
  - 同樣漏洞，出現兩種思路兩種解法

/admin%252f%252ehtpasswd%2500.cfm

<FilesMatch "^\.ht"> 會被 *Apache* 處理

使用 *Double Encoding* 繞過 *Apache* 處理

.cfm 會被 *JRun* 處理

使用 *Null Byte* 截斷 *.cfm*

JRun 讀取 *.htpasswd* 原始碼並送回

/.%5Cadmin%5C.htpasswd%253b.jsp

<FilesMatch "^\.ht"> 會被 *Apache* 處理

使用反斜線繞過 *Apache* 處理

.jsp 會被 *JRun* 處理

使用 *;* 截斷 *.jsp*

JRun 讀取 *.htpasswd* 原始碼並送回

所以說

「Web 狗如何在險惡的 CTF 世界中存活？」

「Web 狗如何在險惡的 CTF 世界中存活？」

– 怎麼可能存活，想多了

「Web 狗如何在險惡的 CTF 世界中存活？」

– 為了存活下來，不得不強迫自己學其他技能

「Web 狗如何在險惡的 CTF 世界中存活？」

- 但是密碼學、堆棧溢出是高富帥的領域怎麼辦？

DAWN 隊伍專訪節錄

微博 大家正在搜：井柏 … 首页 发现 游戏 Ora…

DAWN队员：基友你有啥想法，**基友**：顺其自然！

DAWN队员：额，我们战队的发展，我们教练的想法就是多从新人里（大一）挖掘一些好的苗子，然后由我们这些老队员来带，还有从我们学校里SM~~（小编：是我想多了吗）~~队里找一些人来培养。

因为我们看到217那五个大神里面有三个都是搞SM出身的，他们做这个特别厉害。然后，我本身也是搞SM得，我们老师也觉得搞SM的人，可能上手更快一点，感觉会好培养一些。

從用得上的實例學起

- Web Hacking
- Reversing + Pwnable
  - /cgi-bin/ 下的 ELF
  - 嵌入式設備總會遇到
  - 滲透後主機提權要自己改 Exploit Code
- Cryptography
  - Padding Oracle / Bit Flipping Attack / Length Extension Attack ...

「Web 狗如何在險惡的 CTF 世界中存活？」

– 人在江湖，身不由己

Web 狗額外優勢

- 網頁端的資訊洩漏 (Flag ?)
  - /server-status/
  - /.git/ .DS_Store
- 針對出題者的資訊蒐集？
  - 蒐集題目作者習慣 Code Snippet / Coding Style
- 還有哪些只有 Web 狗能做的事情？

結論

Q & A