

Secure Programming Introduction

Jeffxx / Atdog / ddaa

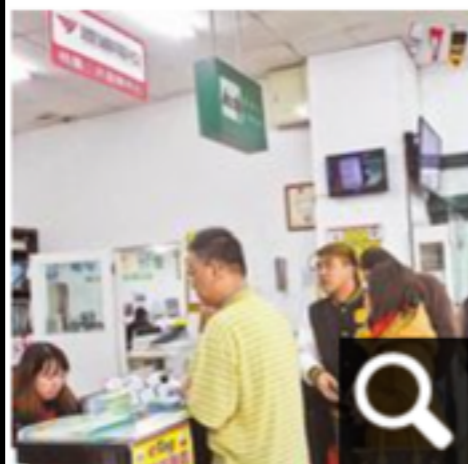
“Think Twice Before Choose this Course”

“Do Not break the law”

3駭客入侵遠通 不起訴

稱幫抓漏洞 一試就成功

2014年08月27日  讚 74  8+1 6



今年元旦eTag系統當機，害民眾在遠通桃園服務中心排隊枯等，檢警認為，起因是程式設計問題。資料照片

【吳珮如／台北報導】今年元旦遠通電收eTag系統發生大當機，遠通聲稱因App遭駭客攻擊八十二億次，七天後遠通官網主機也遭入侵，遠通隨即報案，但檢警追查發現並無駭客攻擊，而是系統故障，不過有三名男網友，為了「測試」遠通系統有無漏洞，入侵官網被逮，因三人已道歉，獲遠通和解撤告，士林地檢署昨給予三人不起訴處分。

今年國道計程收費一月二日正式實施，但前一天卻發生系統當機，民眾無法儲值和申裝eTag，遠通一開始宣稱，因App遭駭客攻擊，三個半小時有近八十二億次攻擊，連帶拖累整個系統。不過全案在報警處理後，遠通就在一月十六日致歉，發現「疑似不是網路異常攻擊」。

目前位置: [首頁](#) / [新聞](#) / [台大選課遭駭，校長開「東方神祕力量」課程？](#)

台大選課遭駭，校長開「東方神祕力量」課程？

[資安](#) [駭客](#) [台大](#)

撰文者：劉翰謙整理 發表日期：2011/08/04

[f 分享](#) [g+1](#) [推文](#) [in Share](#) [f 讚](#) [0](#)



最近世界各地，不少機構單位紛紛受到駭客「造訪」，儘管日前大駭四方的LulzSec主嫌才剛獲保釋，這股風波似乎還未落幕，現在甚至延燒到台灣的台大身上。

昨天凌晨，有台大學生發現選課系統中出現一門名為「東方神祕力量」的課程，開課教授竟是當今校長李嗣涔，而學分數高達100，消息傳開在ptt上引起熱烈討論，校方得知後，已緊急撤下該課程相關網頁。

台大主任秘書張培仁表示，目前學校還未正式開始選課，只是先公布課程給學生參考，所以該事件並未造成任何實際上的困擾，校長也表示不在意這樣的問題，不過，校方也會檢討目前的網路安全情形，彌補類似的漏洞。

天才駭客破解悠遊卡 盜刷39元

稱挑戰「不可能」 業者將升級防護

2011年09月28日



25

g+1

21



吳東霖歷經四個月埋首研究、重寫程式，破解可用自製讀卡機為悠遊卡竄改充值。翻攝畫面

【綜合報導】號稱不可能破解的台北悠遊卡，遭大學肄業生破解！上市敦陽科技公司一名資安顧問，歷時四個月撰寫程式，破解悠遊卡防護系統，成功盜刷六次、共消費六百零八元，扣除自己儲值金額，不法所得僅三十九元，他向檢方認罪，強調是為挑戰悠遊卡。面對駭客挑戰，悠遊卡公司將開發新一代晶片悠遊卡，提高防護功能。

警方調查，嫌犯吳東霖（二十四歲）是敦陽科技公司資訊安全顧問，獨自在北市內湖路二段租屋，他破解悠遊卡充值系統並盜刷消費，新聞昨披露後，他未到公司，也沒回租屋處。

駭悠遊卡 判2年緩刑5年

f 推薦 2

自由時報 自由時報 – 2013年3月2日 上午4:30

〔自由時報記者黃立翔、張慧雯／台北報導〕號稱「不可能被破解」的台北捷運悠遊卡，前年遭敦陽科技資安顧問吳東霖破解，士林地院昨以他意在破解技術而非牟利，依變造電子票證罪判刑2年，緩刑5年，賠償悠遊卡公司100萬元，並向檢方指定的機構，提供240小時的電腦資訊教育訓練。

悠遊卡公司公關室科長陳志豪說，希望此案能起警惕之效，並重申悠遊卡系統非常可靠，竄改悠遊卡程式，馬上就會被系統察覺，勿以身試法。

判決書指，敦陽科技資安顧問吳東霖（23歲）前年5月間，找到破解悠遊卡加密的程式，自製感應線圈，將3張悠遊卡儲值金額各改為9000元（儲值上限）。

吳某曾以1卡查詢餘額被系統鎖卡，他不死心，以其中1卡到超商消費，並將另1張卡交給超商店員江俊達，同年9月23日吳被查獲。法院審理時江坦承知情，而他協助查詢悠遊卡餘額成功時，還向吳比出「讚」的手勢。

吳出庭稱是「道德駭客」，意在破解悠遊卡資安漏洞而非牟利。

“Still many thing you can hack”

The Heartbleed Bug


The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.



Backdoor found in D-Link router firmware code

The backdoor could be used to modify a router's settings, a dangerous vulnerability

By [Jeremy Kirk](#), IDG News Service | [Data Protection](#)  5



112



21

October 14, 2013, 12:49 AM — A backdoor found in firmware used in several D-Link routers could allow an attacker to change a device's settings, a serious security problem that could be used for surveillance.

[Craig Heffner](#), a vulnerability researcher with Tactical Network Solutions who specializes in wireless and embedded systems, found the vulnerability. Heffner wrote on his [blog](#) that the web interface for some D-Link routers could be accessed if a browser's user agent string is set to "xmlset_roodkcableoj28840ybtide."

Curiously, if the second half of the user agent string is reversed and the number is removed, it reads "edit by joel backdoor," suggesting it was intentionally placed there.

Smart LED light bulbs leak wi-fi passwords

By Jane Wakefield
Technology reporter

Security experts have demonstrated how easy it is to hack network-enabled LED light bulbs.

Context Security released details about how it was able to hack into the wi-fi network of one brand of network-enabled bulb, and control the lights remotely.

The LIFX light bulb, which is available to buy in the UK, has network connectivity to let people turn it on and off with their smartphones.

The firm behind the bulbs has since fixed the vulnerability.

Michael Jordon, research director at Context, explained how he was able to obtain the wi-fi username and password of the household the lights were connected to.

"We bought some light bulbs and examined how they talked to each other and saw that one of the messages was about the username and password," he told the BBC.



The hackers posed as a new light bulb joining the network

Related Stories

[Google's Nest unveils kit tie-ups](#)

KEEN TEAM OF CHINA TAKES DOWN SAFARI AND FLASH AT PWN2OWN

Related CVE Number | CVE-2014-3740

by **Michael Mimoso**

[Follow @mike_mimoso](#)

March 13, 2014 , 8:42 pm

VANCOUVER – One is the bug hunter, the other the exploit specialist.

Fang Jiahong and Liang Chen represented the Keen Team at Pwn2Own on Thursday, starting off the second day of the annual exploit festival with a quick takedown of Apple's Safari browser. They then wrapped up the contest with a successful zero-day exploit of Adobe Flash, the second time the Adobe product was toppled.

For 2½ years, this emerging team of eight vulnerability researchers and exploit developers from China has nudged its way into the fray that is bug hunting and exploitation. Today's Pwn2Own Safari win netted the Keen Team a \$40,000 prize; the Flash bug \$75,000. They said they will donate a portion of their winnings to charities representing the families of the missing Malaysian Airlines flight

Related Posts

Four Vulnerabilities Patched in IntegriXor SCADA Server

September 12, 2014 , 1:22 pm

Apache Warns of Tomcat Remote Code Execution Vulnerability

September 10, 2014 , 3:31 pm

“What You will Learn.”

Static analysis

- Decompiler / Disassembler
 - Objdump
 - IDA pro
 - DJ - Java Decompiler
- Source code analysis

Dynamic Analysis

- Debugger
 - GDB
 - Olly-dbg
- Fuzz
 - Peach
- Symbolic Execution
 - S2E
 - AEG
 - CRAX

Exploit (PWN)

- Stack Overflow - Smash the stack
- Heap Overflow - Heap fengshui
- Format String
- Uninitialized Variable
- Integer overflow
- Memory Leak

Exploit (Mitigation)

- Mitigation
 - Stack Guard
 - Data Execution Prevention (DEP)
 - Address space layout randomization (ASLR)
- Bypass
 - Rewrite GOT entry
 - Return to libc
 - Return Oriented Programming

Web

- OWASP TOP 10
- PHP
- Django
- Rails
- ...

“What Ability You Will Have”

Bug Bounty

- <https://hackerone.com>
- <https://bugcrowd.com/list-of-bug-bounty-programs>

GitHub launches Bug Bounty program, offers between \$100 and \$5,000 for security vulnerabilities



	accounts.google.com	Other highly sensitive services [1]	Normal Google applications	Non-integrated acquisitions and other lower priority sites [2]
Remote code execution	\$20,000	\$20,000	\$20,000	\$5,000
SQL injection or equivalent	\$10,000	\$10,000	\$10,000	\$5,000
Significant authentication bypass or information leak	\$10,000	\$5,000	\$1,337	\$500
Typical XSS	\$3,133.7	\$1,337	\$500	\$100
XSRF, XSSi, and other common web flaws	\$500 - \$3,133.7 (depending on impact)	\$500 - \$1,337 (depending on impact)	\$500	\$100

CVE

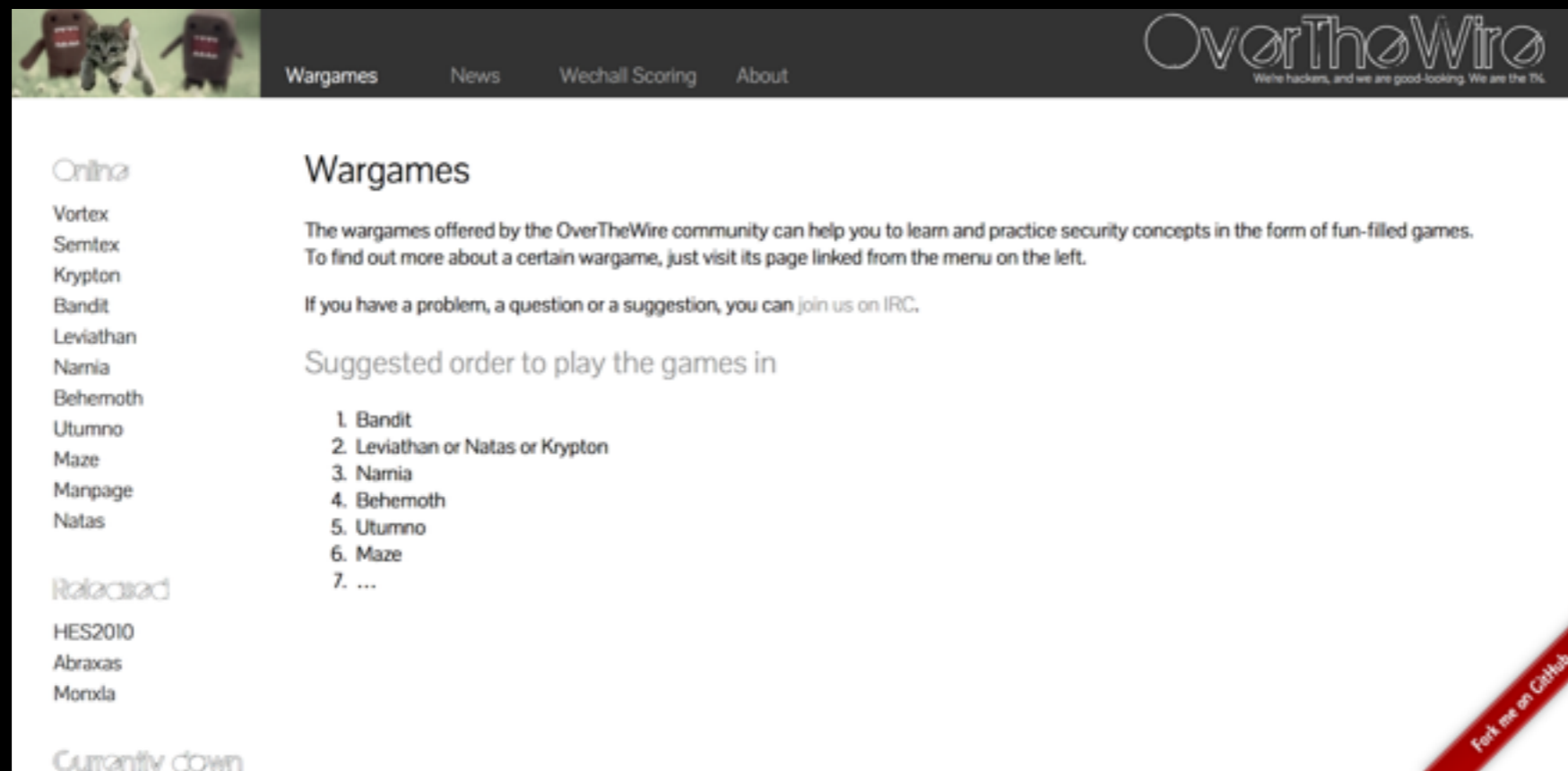


Everyday is Zero Day
Today is Flash Player

By Lucas Leong

Wargame

- <http://wargame.cs.nctu.edu.tw>
- <http://overthewire.org>



The screenshot shows the 'OverTheWire' website's 'Wargames' page. The header includes the site logo 'OverTheWire' with the tagline 'We're hackers, and we are good-looking. We are the TK.' and navigation links for 'Wargames', 'News', 'Wechall Scoring', and 'About'. The main content area is titled 'Wargames' and contains the following text: 'The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games. To find out more about a certain wargame, just visit its page linked from the menu on the left.' Below this, it says 'If you have a problem, a question or a suggestion, you can join us on IRC.' A section titled 'Suggested order to play the games in' lists: 1. Bandit, 2. Leviathan or Natas or Krypton, 3. Narnia, 4. Behemoth, 5. Utumno, 6. Maze, 7. ... On the left side, there are two vertical menus: 'Online' with links to Vortex, Semtex, Krypton, Bandit, Leviathan, Narnia, Behemoth, Utumno, Maze, Manpage, and Natas; and 'Related' with links to HES2010, Abraxas, and Monxia. At the bottom left, it says 'Currently down'. A red diagonal banner in the bottom right corner says 'Find me on GitHub'.

Capture The Flag

- CTFTIME
 - <https://ctftime.org>
- HITCon CTF
- Defcon Final
 - Defcon final, RuCTFe, Ghost in the shellcode, Olympic CTF,
 - Boston Key party, Codegate Final, PHDays, Secuinside

The screenshot shows the CTFTIME website interface. The top navigation bar includes links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, About, and Contact us. The main content is divided into two sections: 'Team rating' and 'Last events'.

Team rating

Place	Team	Country	Rating
1	Dragon Sector	RU	1261.302
2	Paid Parliament of Pening	RU	1260.307
3	More Smoked Leet Chicken	RU	955.390
4	StratumAkhur	RU	742.888
5	Isomorph	RU	650.838
6	penthackon	RU	571.800
7	Bemuni	RU	531.917
8	Int2pids	RU	511.809
9	Eindlauren	RU	473.587
10	HITCON	RU	414.225

Last events

VolgaCTF Finals 2014
Sept. 11, 2014, 7 p.m. | Semera, Russia

Place	Team	Country	Points
1	BalalakaCr3w	RU	20.000
2	LightsOut	RU	14.806
3	Singularity	RU	13.021

17 teams total | [Tasks and writeups](#)

HITCON CTF 2014
Aug. 18, 2014, 4 a.m. | Online

Place	Team	Country	Points
1	fuzz0	RU	60.000
2	Dragon Sector	RU	44.440
3	9447	RU	38.285

“What You Must Do.”

Scoring

- Homework 30%
 - 6 CTF (5% for each)
 - 2-3 wargame
- Final Exam 30%
 - On-site bug analysis and exploit development.
 - Competition with NTU
- Project 40%
 - Choose a target, conduct penetration test and summarise vulnerability.
- Bonus 20%
 - Attend worldwide CTF
 - Write-up

Homework 0

- Wargame 0-1 Magic
 - secprog.cs.nctu.edu.tw:6666
- Wargame 0-2 Overflow
 - secprog.cs.nctu.edu.tw:8888
- Wargame 0-3 ROP
 - secprog.cs.nctu.edu.tw:7777
 - http://docs.cs.up.ac.za/programming/asm/derick_tut/syscalls.html
- Only 140.113.0.0/24 can access.

Project

Bonus

- Attend Worldwide CTF
 - Group in 2-5
 - Submit Your ranking and write-up
- Next Week
 - ALI CTF - <http://www.alictf.com>
 - CSAW CTF - <https://ctf.isis.poly.edu>



ALICTF
2014
GHOST ON THE CLOUD

CTF TIME: 09.09 ~ 10.15

微信号: freebuf

Course Information

- Course WebSite
 - <http://secprog.cs.nctu.edu.tw>
- IRC
 - Freenode: #nctusp
- E-mail
 - nctusp@googlegroups.com
- Facebook
 - [Secure Programming@NCTU](#)