Open Innovation Lab
CUHK

CTF Training Camp for Hackers Information Session

CUHK Open Innovation Lab

Zeddy
Coordinator of CUHK Open Innovation Lab

CUHKOIL Discord Server

We use this server for

- Announcements
- Resources for Workshops and CTFs
- Discussion
- Chat! :)

Note: This link is only valid for 100 invites.
(For CUHK Students Only)

whoami

- Zeddy
- Coordinator of Open Innovation Lab
- First Year MPhil Student in Information Engineering, CUHK
- Founder of Water Paddler. Co-Founder of Blue Water. Both are international CTF teams.
- Interested in Web and Network Protocol Security

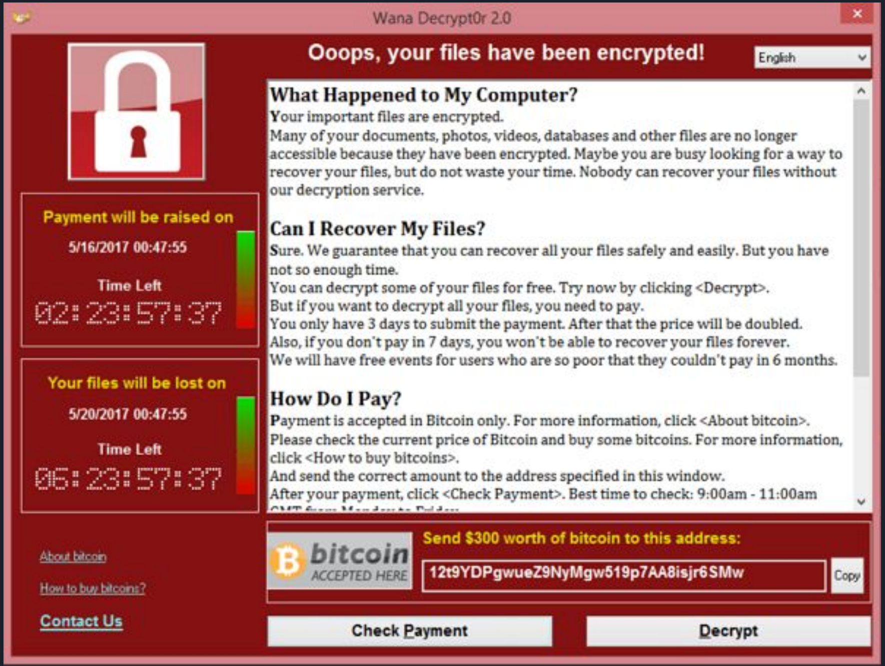
Who We Are: CUHK Open Innovation Lab

- Hub for advancing the movement of open source, open data, open culture and technology entrepreneurship among engineering students.
- participate in events like Hackathon, Bootcamps and Capture-The-Flag (CTF) competitions

What a hacker looks like?

Hacker(Physical)

Maybe?



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

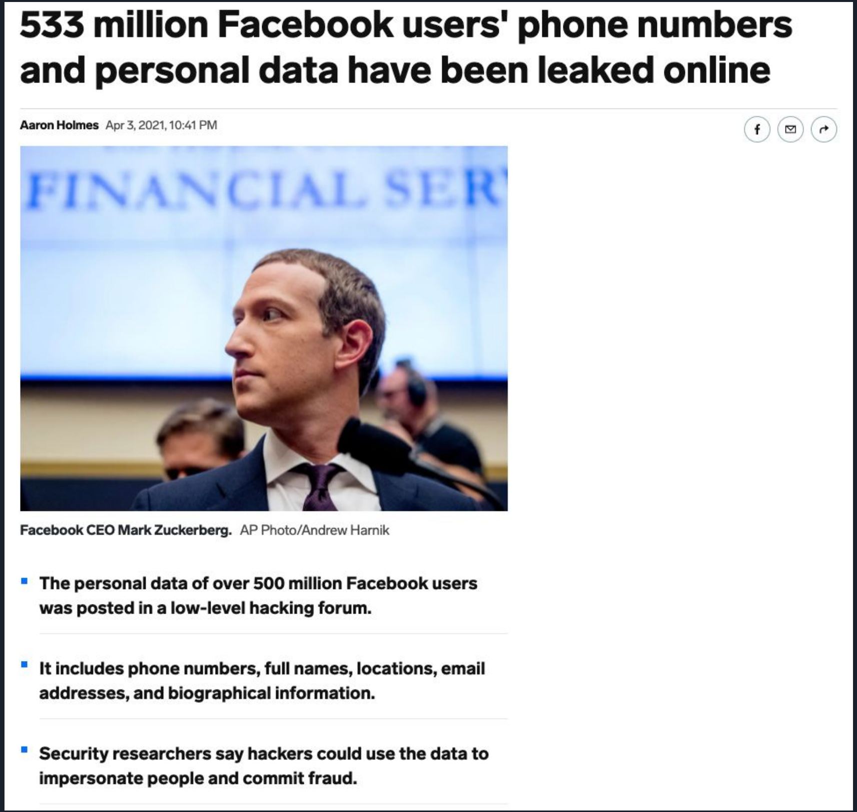
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 10:41 PM

Facebook CEO Mark Zuckerberg. AP Photo/Andrew Harnik

- The personal data of over 500 million Facebook users was posted in a low-level hacking forum.
- It includes phone numbers, full names, locations, email addresses, and biographical information.
- Security researchers say hackers could use the data to impersonate people and commit fraud.

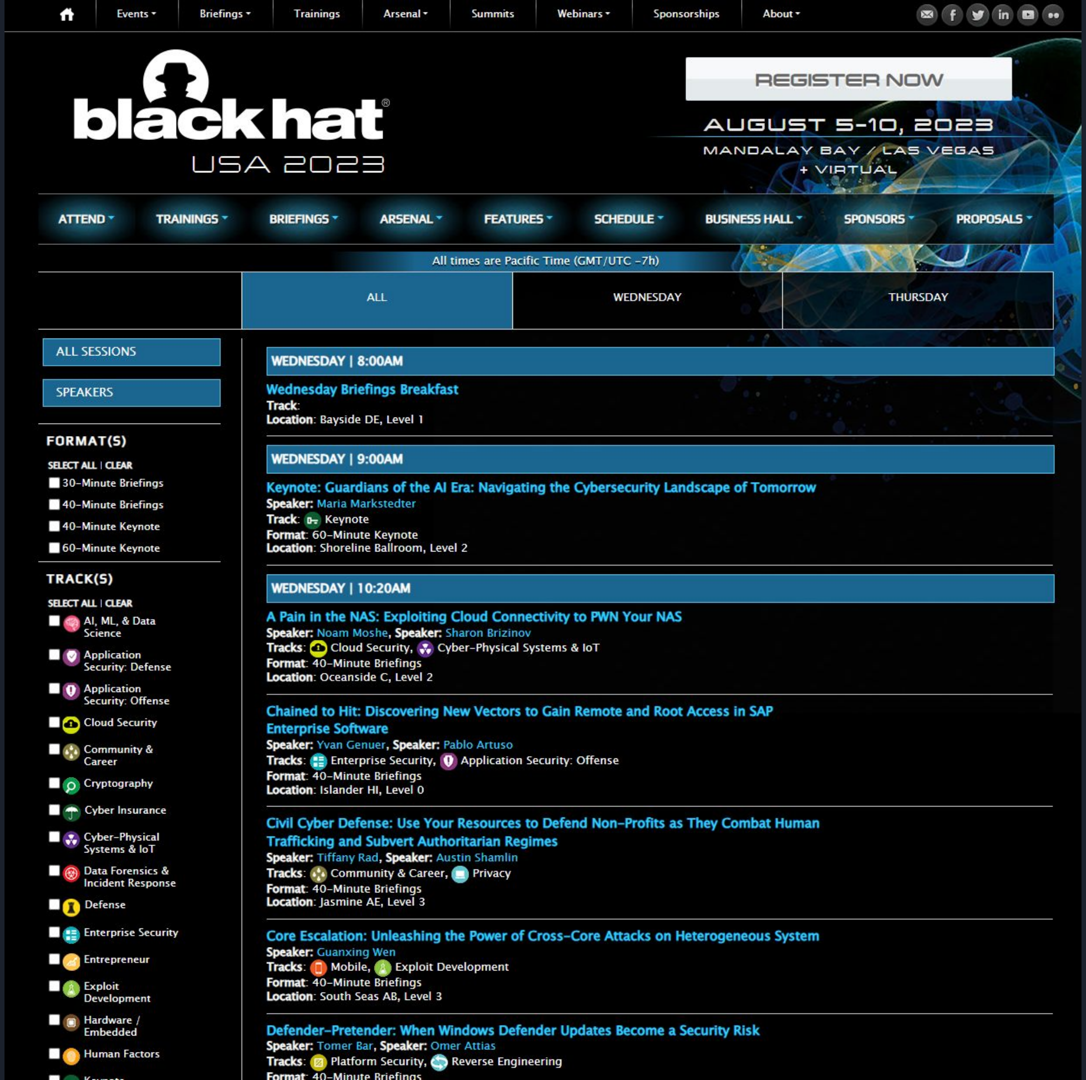
Credit: Business Insider
https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Hackers

- A black hat (black hat hacker or blackhat) is a computer hacker who violates laws or typical ethical standards for nefarious purposes, such as cybercrime, cyberwarfare or malice.

- A white hat (or a white-hat hacker, a whitehat) is an ethical security hacker. (Ethical hacking). The white hat is contrasted with the black hat, a malicious hacker

- There is a third kind of hacker known as a grey hat who hacks with good intentions but at times without permission.



All times are Pacific Time (GMT/UTC -7h)

FORMAT(S)

- □ 30-Minute Briefings
- □ 40-Minute Briefings
- □ 40-Minute Keynote
- □ 60-Minute Keynote

TRACK(S)

- □ AI, ML, & Data Science
- □ Application Security: Defense
- □ Application Security: Offense
- □ Cloud Security
- □ Community & Career
- □ Cryptography
- □ Cyber Insurance
- □ Cyber-Physical Systems & IoT
- □ Data Forensics & Incident Response
- □ Defense
- □ Enterprise Security
- □ Entrepreneur
- □ Exploit Development
- □ Hardware / Embedded
- □ Human Factors

WEDNESDAY | 8:00AM

Wednesday Briefings Breakfast
Track:
Location: Bayside DE, Level 1

WEDNESDAY | 9:00AM

Keynote: Guardians of the AI Era: Navigating the Cybersecurity Landscape of Tomorrow
Speaker: Maria Markstedter
Track: Keynote
Format: 60-Minute Keynote
Location: Shoreline Ballroom, Level 2

WEDNESDAY | 10:20AM

A Pain in the NAS: Exploiting Cloud Connectivity to PWN Your NAS
Speaker: Noam Moshe, **Speaker:** Sharon Brizinov
Tracks: Cloud Security, Cyber-Physical Systems & IoT
Format: 40-Minute Briefings
Location: Oceanside C, Level 2

Chained to Hit: Discovering New Vectors to Gain Remote and Root Access in SAP Enterprise Software
Speaker: Yvan Genuer, **Speaker:** Pablo Artuso
Tracks: Enterprise Security, Application Security: Offense
Format: 40-Minute Briefings
Location: Islander HI, Level 0

Civil Cyber Defense: Use Your Resources to Defend Non-Profits as They Combat Human Trafficking and Subvert Authoritarian Regimes
Speaker: Tiffany Rad, **Speaker:** Austin Shamlin
Tracks: Community & Career, Privacy
Format: 40-Minute Briefings
Location: Jasmine AE, Level 3

Core Escalation: Unleashing the Power of Cross-Core Attacks on Heterogeneous System
Speaker: Guanxing Wen
Tracks: Mobile, Exploit Development
Format: 40-Minute Briefings
Location: South Seas AB, Level 3

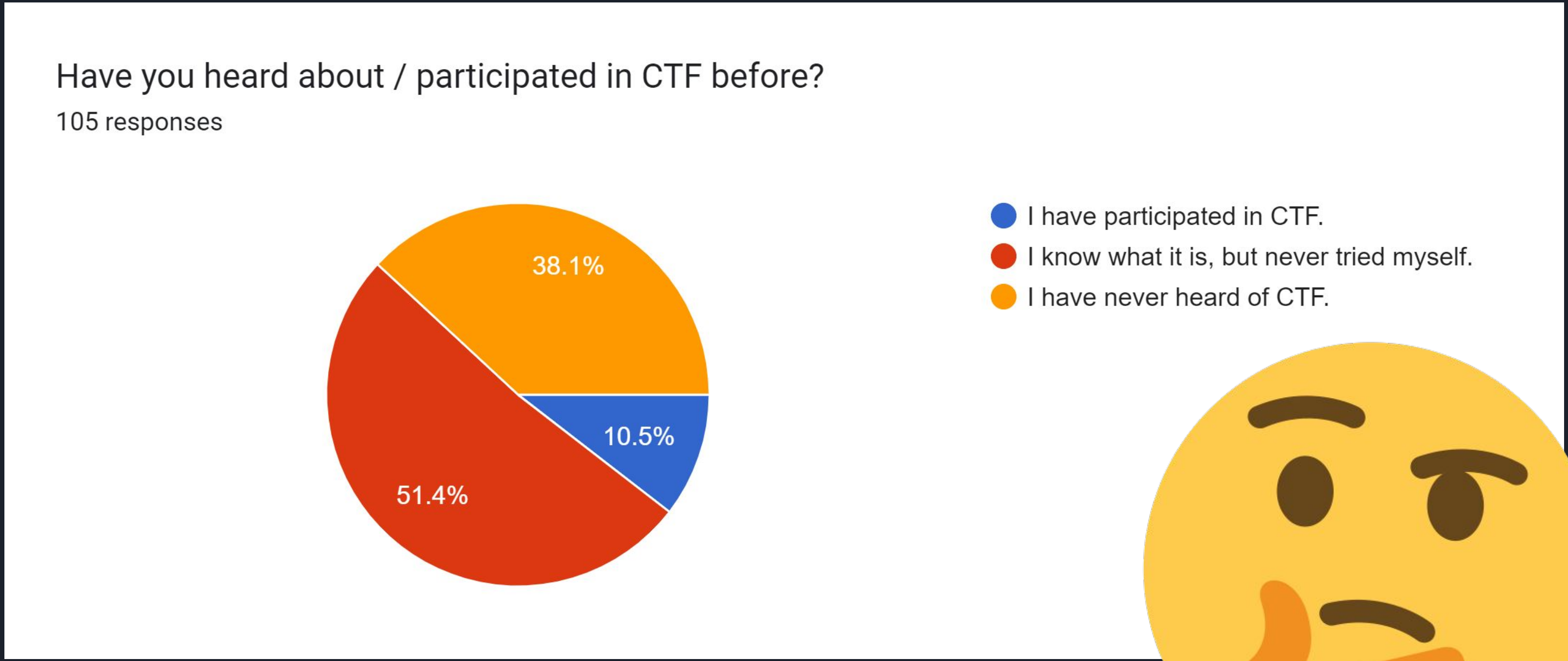
Defender-Pretender: When Windows Defender Updates Become a Security Risk
Speaker: Tomer Bar, **Speaker:** Omer Attias
Tracks: Platform Security, Reverse Engineering
Format: 40-Minute Briefings

With great power
comes great responsibility.

Ethics

- Ethical hacking: AUTHORIZED and APPROVED practice of hacking into computer system to identify potential vulnerabilities in the computer systems
- The purpose is to investigate vulnerabilities so that system administrators can fix it!
- Within the scope of assessment and plan
    - In CTF: DO NOT attack the CTF platform itself nor the players (in jeopardy CTFs)!
- Keep the learned vulnerabilities CONFIDENTIAL. NEVER utilize the vulnerabilities in a way detrimental to the owner of the system

- **DISCLAIMER: WE ASSUME NO RESPONSIBILITY FOR ANY ACTIONS PERFORMED OUTSIDE THE TRAININGS**



Have you heard about / participated in CTF before?

105 responses

~~Ha[illegible]on?~~

What is CTF?

- Capture The Flag
- Gamification of Hacking
- Two types of CTF
    - Jeopardy
        - Find a “Flag”: a piece of string
        - Most CTF are Jeopardy-style
    - Attack/Defense
        - Participants attack each others’ vulnerable server
        - Defend their own server by various mean
- Online or Onsite CTF

Google
CTF

DEFCON
CTF

HITCON

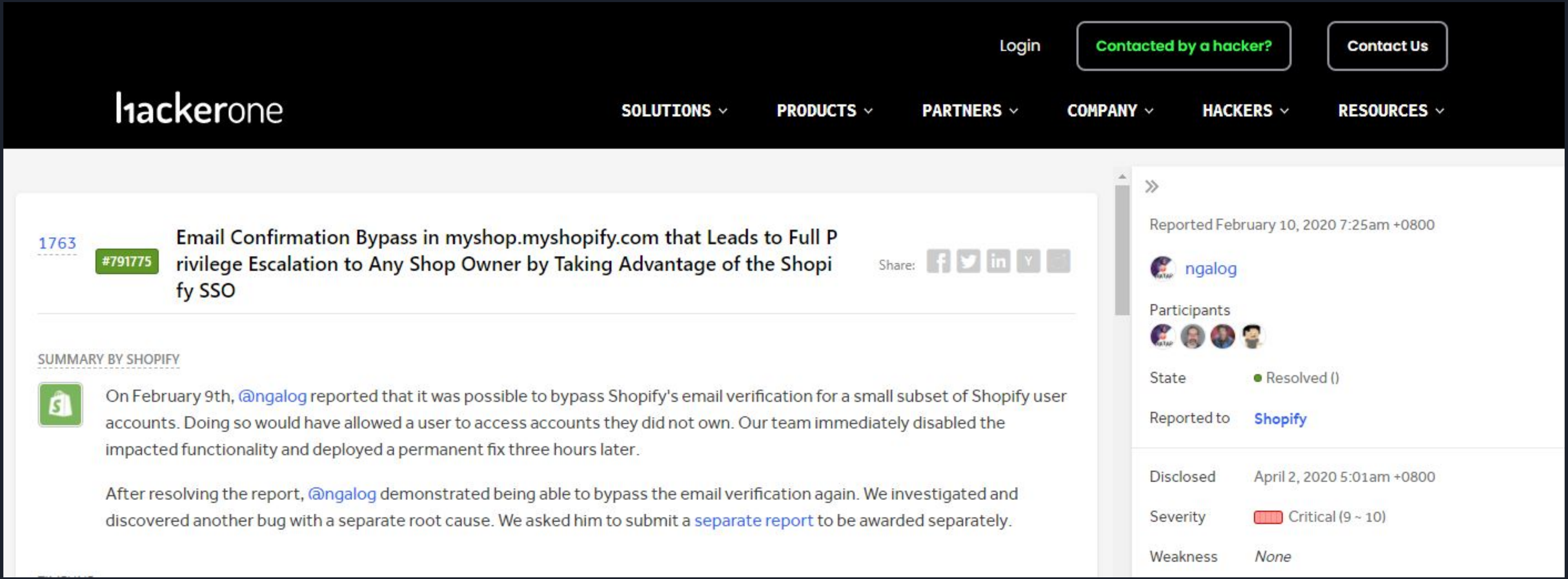
PPP

Why Play CTF?

- For the prizes
- To learn cybersecurity
  - Learn offense and defense
  - Security concepts always useful for devs
- Job in security field (?)
- It’s Fun! <- the most important part

Careers

- Penetration Tester (pentester)
- Security Audit
- Red team, Blue team
- Bug Bounty
- ...



1763 #791775 Email Confirmation Bypass in myshop.myshopify.com that Leads to Full Privilege Escalation to Any Shop Owner by Taking Advantage of the Shopify SSO

SUMMARY BY SHOPIFY

On February 9th, @ngalog reported that it was possible to bypass Shopify's email verification for a small subset of Shopify user accounts. Doing so would have allowed a user to access accounts they did not own. Our team immediately disabled the impacted functionality and deployed a permanent fix three hours later.

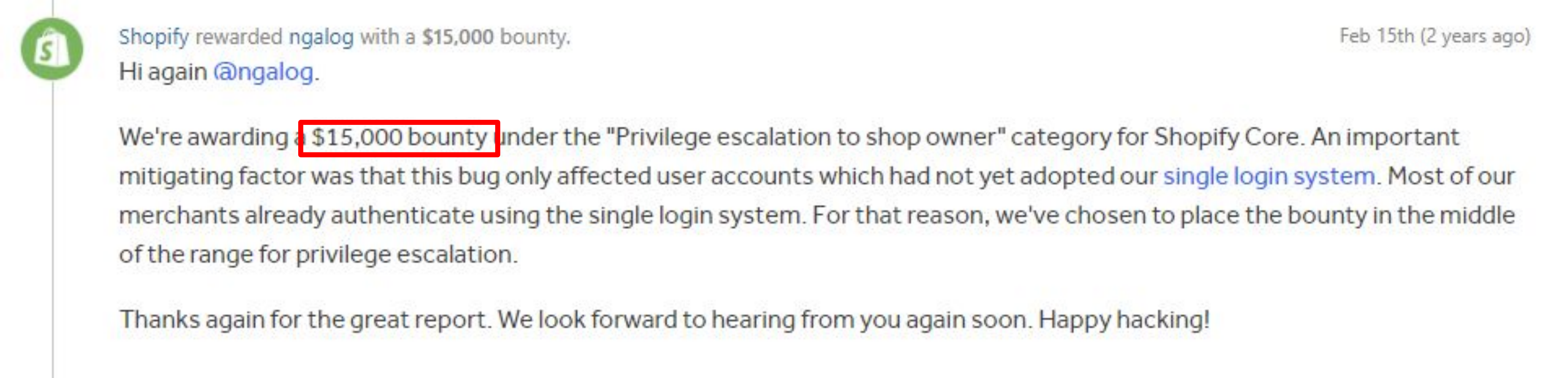
After resolving the report, @ngalog demonstrated being able to bypass the email verification again. We investigated and discovered another bug with a separate root cause. We asked him to submit a separate report to be awarded separately.

Reported February 10, 2020 7:25am +0800

ngalog

Participants

State	● Resolved ()
Reported to	Shopify
Disclosed	April 2, 2020 5:01am +0800
Severity	🟥 Critical (9 ~ 10)
Weakness	*None*



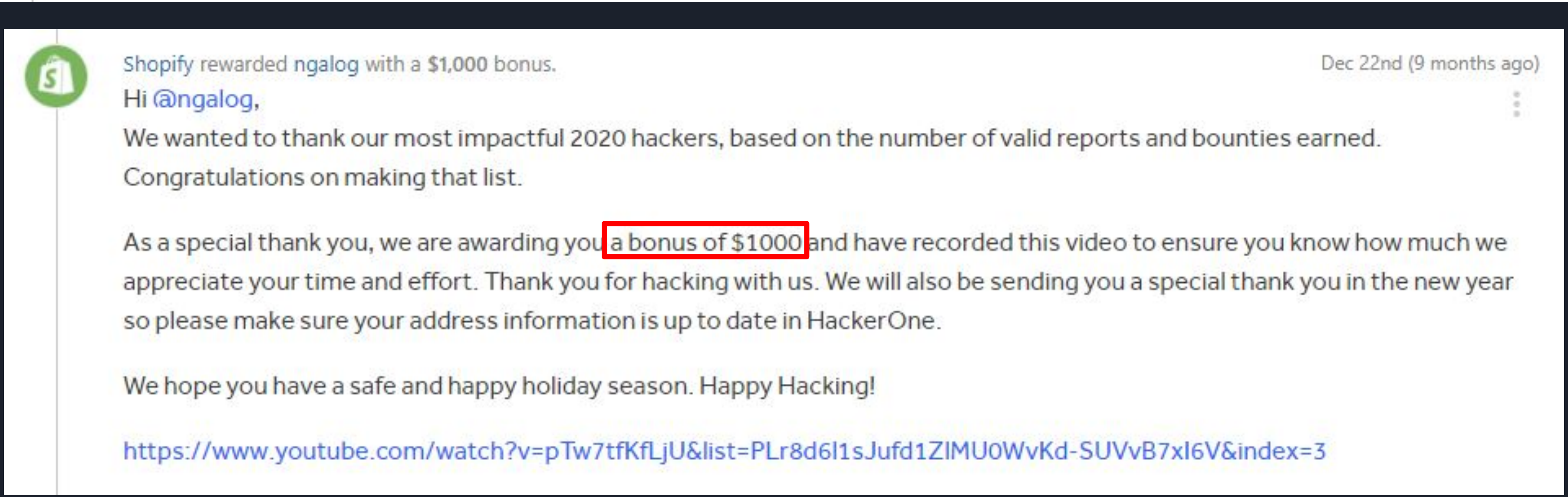
Shopify rewarded ngalog with a **$15,000** bounty.

Feb 15th (2 years ago)

Hi again @ngalog.

We're awarding a $15,000 bounty under the "Privilege escalation to shop owner" category for Shopify Core. An important mitigating factor was that this bug only affected user accounts which had not yet adopted our single login system. Most of our merchants already authenticate using the single login system. For that reason, we've chosen to place the bounty in the middle of the range for privilege escalation.

Thanks again for the great report. We look forward to hearing from you again soon. Happy hacking!



Shopify rewarded ngalog with a **$1,000** bonus.

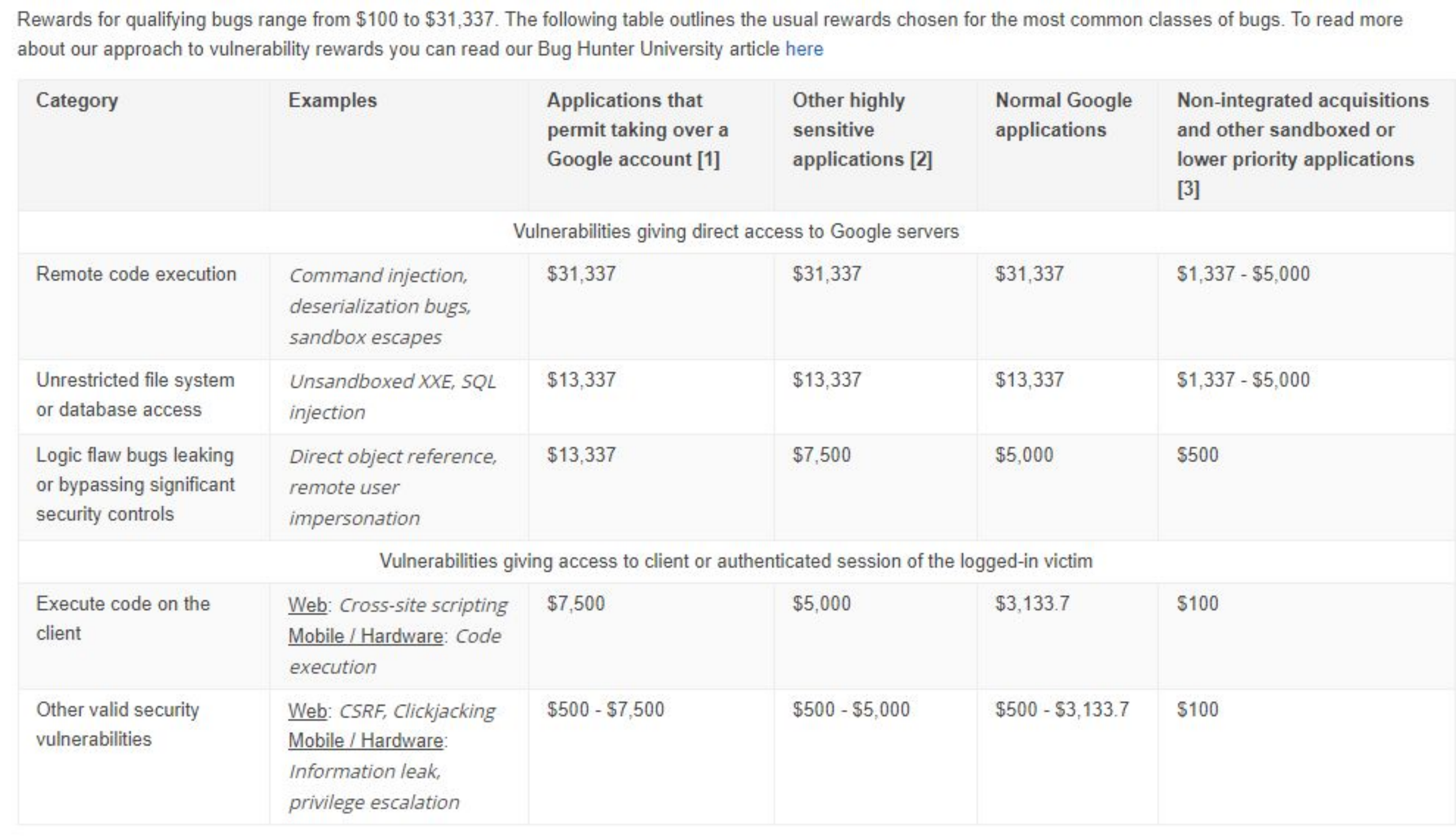
Dec 22nd (9 months ago)

Hi @ngalog,
We wanted to thank our most impactful 2020 hackers, based on the number of valid reports and bounties earned. Congratulations on making that list.

As a special thank you, we are awarding you a bonus of $1000 and have recorded this video to ensure you know how much we appreciate your time and effort. Thank you for hacking with us. We will also be sending you a special thank you in the new year so please make sure your address information is up to date in HackerOne.

We hope you have a safe and happy holiday season. Happy Hacking!

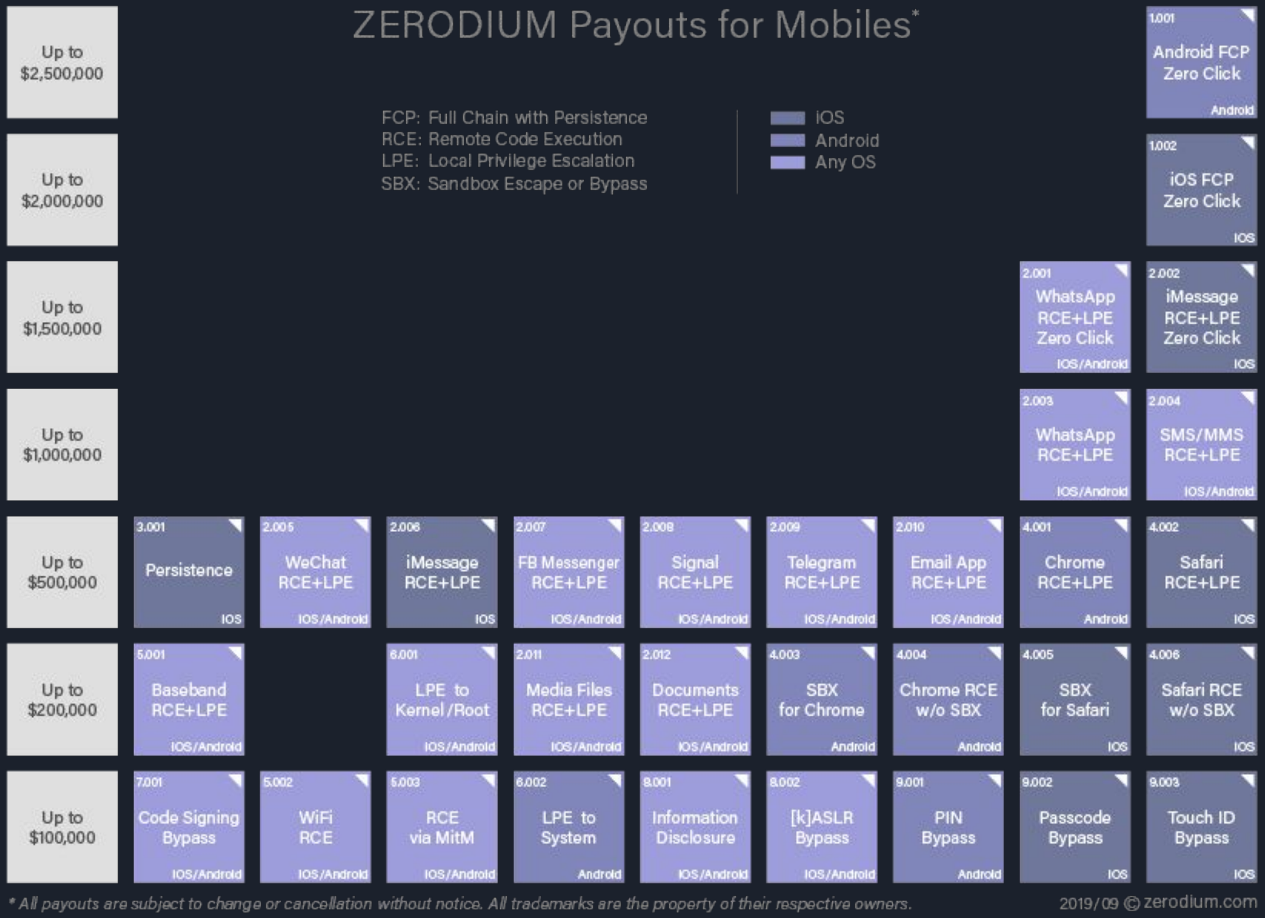
https://www.youtube.com/watch?v=pTw7tfKfLjU&list=PLr8d6l1sJufd1ZIMU0WvKd-SUVvB7xI6V&index=3



Rewards for qualifying bugs range from $100 to $31,337. The following table outlines the usual rewards chosen for the most common classes of bugs. To read more about our approach to vulnerability rewards you can read our Bug Hunter University article here

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$13,337	$13,337	$13,337	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$13,337	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile / Hardware: *Code execution*	$7,500	$5,000	$3,133.7	$100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile / Hardware: *Information leak, privilege escalation*	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

Bug bounty program for Google



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

▨ iOS
▨ Android
▨ Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Market for zero-days

Kylebot’s CTF Journey

- CUHK Alumni
- PhD @ Arizona State University
- A member of Shellphish(A CTF team based on ASU)

Categories of CTF

- Web
- Cryptography
- Reverse Engineering
- Binary Exploitation (Pwn)
- Forensics
- PPC
- Blockchain Security
- Cloud Security
- Misc (Riddle-type questions, the catch-all)
- Any combination of the above

Wouldn’t it be difficult to learn them all?

Yes.

That is why we play in teams.

Play in a Team

- We excel in different areas
- Collaborate to get the best of both worlds
- Learn from your teammates/friends!
- ~~Freeride your teammtes, while you only do sanity check~~

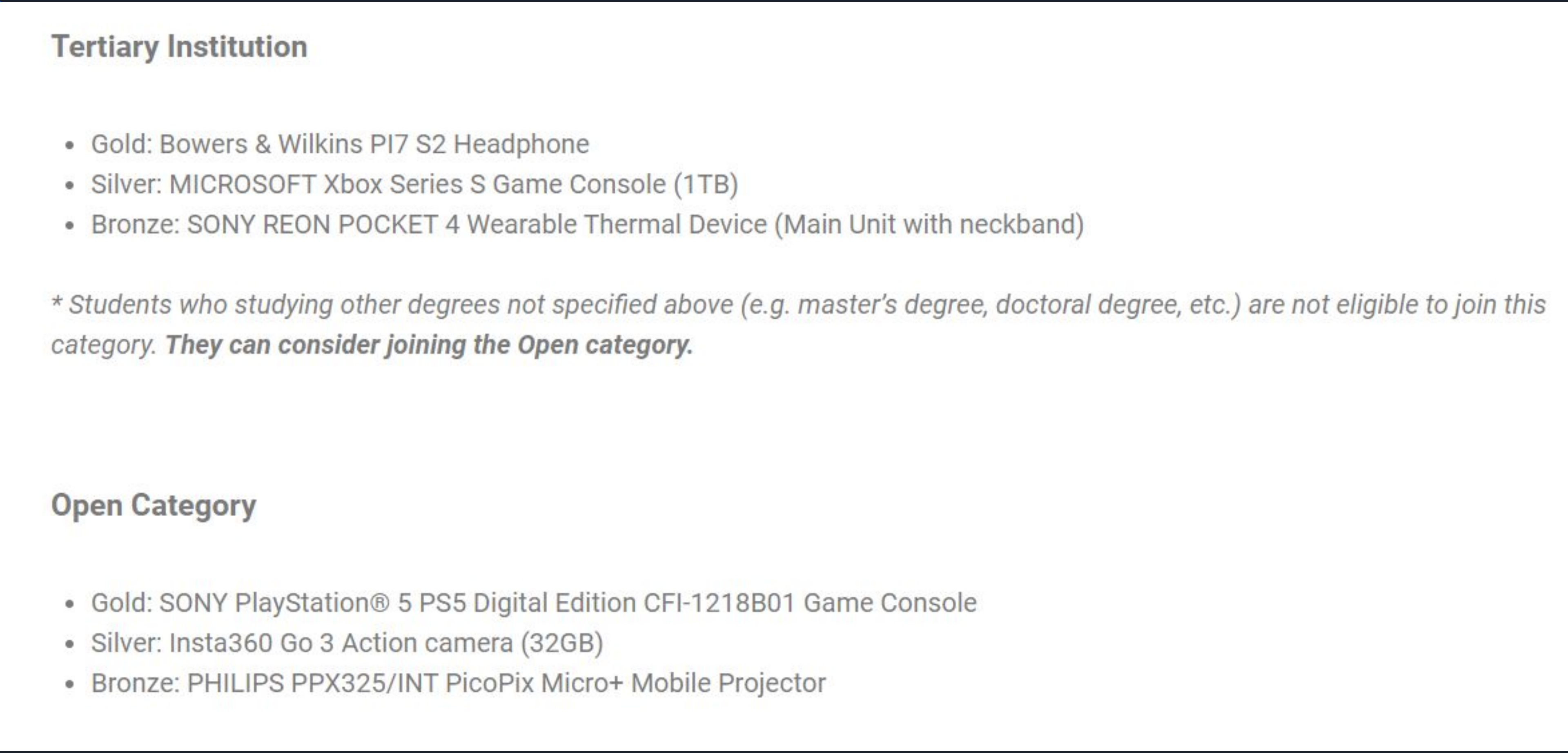
CTF Competitions Down the Line

- HKCERT CTF 2023
- PwC Hackaday
- picoctf

HKCERT CTF 2023

- Organized by Hong Kong Computer Emergency Response Team (香港電腦保安事故協調中心 HKCERT) and Hong Kong Productivity Council (香港生產力促進局 HKPC)
- Jeopardy-style Online CTF
- Nov 10 (Fri) 6 pm - Nov 12 (Sun) 6pm
- Team of 1 - 4
- Tertiary Category for Diploma, Higher Diploma, Assicoate Degree and Bachelor Degree students
  - Can team up with students in different schools
  - Unlimited number of teams per school
- Open Category for everyone

- Impression: Quite a number of 通靈 (Guessy) challenges
- Registration Already Open (Deadline: 31 Oct)
- https://ctf.hkcert.org/
- Workshops available next month



Tertiary Institution

- Gold: Bowers & Wilkins PI7 S2 Headphone
- Silver: MICROSOFT Xbox Series S Game Console (1TB)
- Bronze: SONY REON POCKET 4 Wearable Thermal Device (Main Unit with neckband)

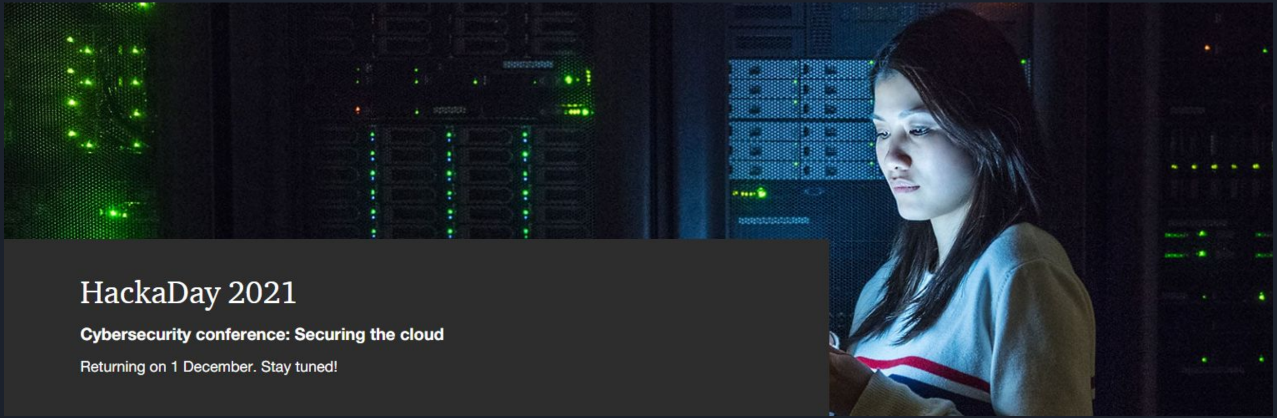
** Students who studying other degrees not specified above (e.g. master's degree, doctoral degree, etc.) are not eligible to join this category.* ***They can consider joining the Open category.***

Open Category

- Gold: SONY PlayStation® 5 PS5 Digital Edition CFI-1218B01 Game Console
- Silver: Insta360 Go 3 Action camera (32GB)
- Bronze: PHILIPS PPX325/INT PicoPix Micro+ Mobile Projector

PwC Hackaday

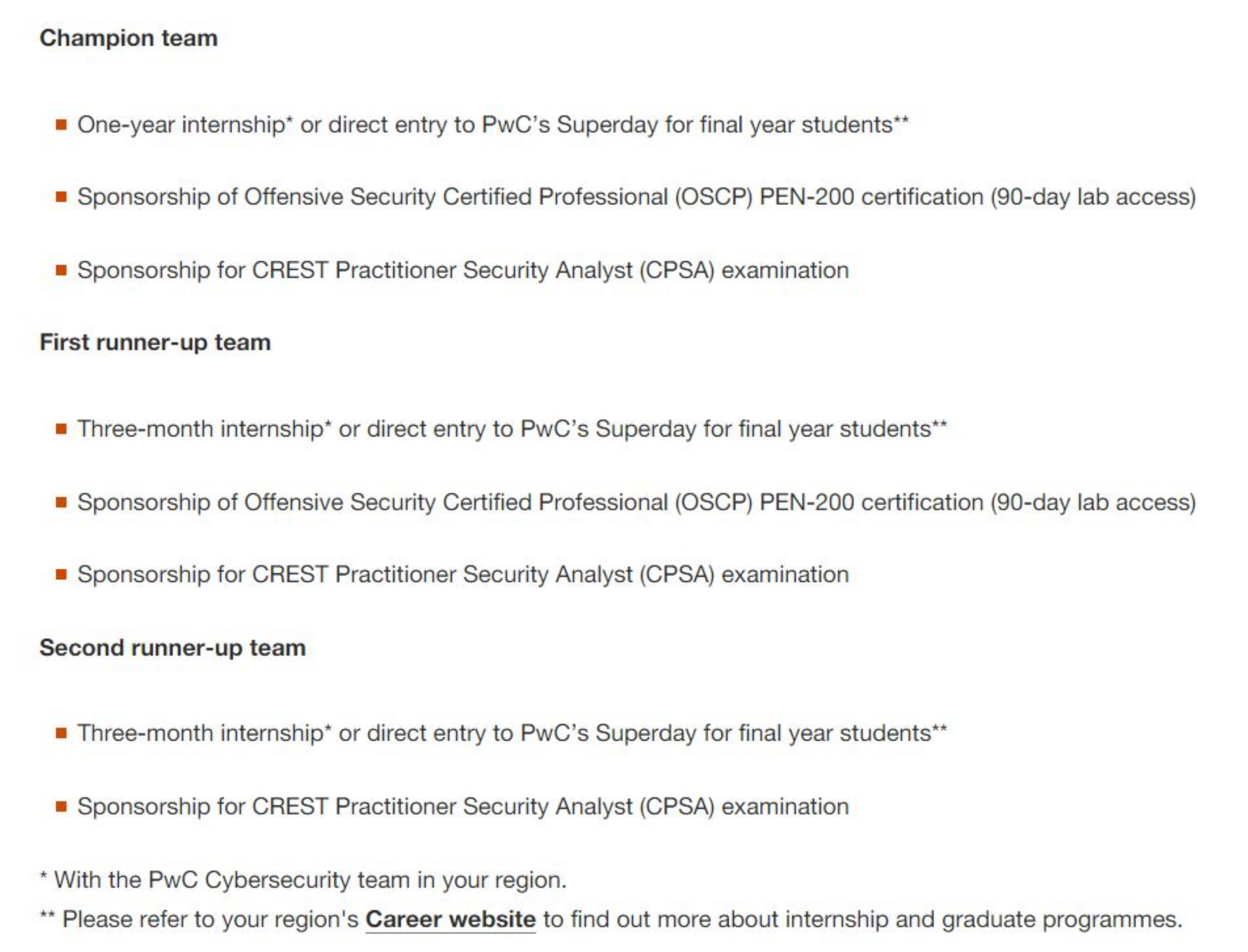
- Held by Darklab of PricewaterhouseCoopers (One of the “Big 4 accounting firms”)
- Jeopardy-style
- Tuesday, 7 November 2023
- For Hong Kong (and Macau) University undergraduates only
- CANNOT mix with students from other schools
- Max 4 students per team, maximum 3 teams per school



HackaDay 2021

Cybersecurity conference: Securing the cloud

Returning on 1 December. Stay tuned!



Champion team

- One-year internship* or direct entry to PwC's Superday for final year students**
- Sponsorship of Offensive Security Certified Professional (OSCP) PEN-200 certification (90-day lab access)
- Sponsorship for CREST Practitioner Security Analyst (CPSA) examination

First runner-up team

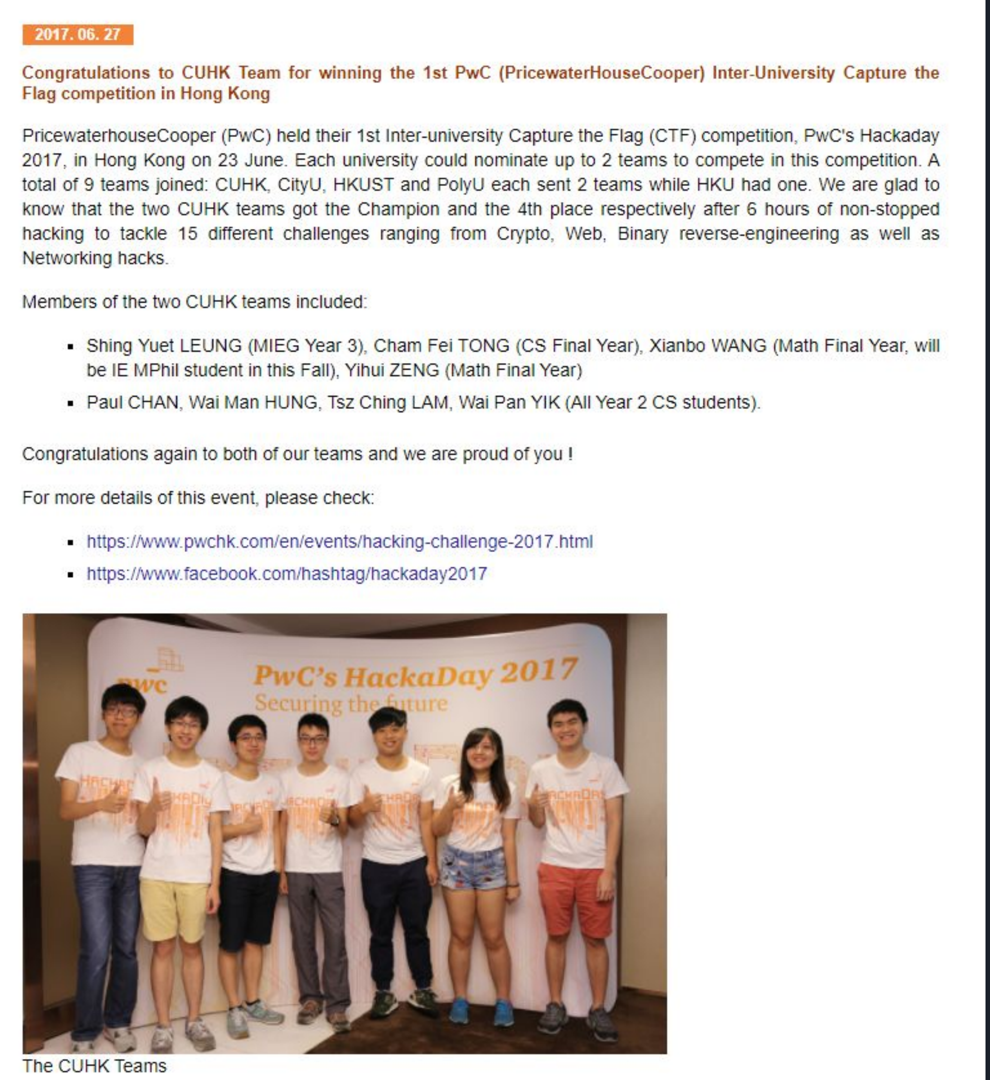
- Three-month internship* or direct entry to PwC's Superday for final year students**
- Sponsorship of Offensive Security Certified Professional (OSCP) PEN-200 certification (90-day lab access)
- Sponsorship for CREST Practitioner Security Analyst (CPSA) examination

Second runner-up team

- Three-month internship* or direct entry to PwC's Superday for final year students**
- Sponsorship for CREST Practitioner Security Analyst (CPSA) examination

* With the PwC Cybersecurity team in your region.

** Please refer to your region's **Career website** to find out more about internship and graduate programmes.



2017. 06. 27

Congratulations to CUHK Team for winning the 1st PwC (PricewaterHouseCooper) Inter-University Capture the Flag competition in Hong Kong

PricewaterhouseCooper (PwC) held their 1st Inter-university Capture the Flag (CTF) competition, PwC's Hackaday 2017, in Hong Kong on 23 June. Each university could nominate up to 2 teams to compete in this competition. A total of 9 teams joined: CUHK, CityU, HKUST and PolyU each sent 2 teams while HKU had one. We are glad to know that the two CUHK teams got the Champion and the 4th place respectively after 6 hours of non-stopped hacking to tackle 15 different challenges ranging from Crypto, Web, Binary reverse-engineering as well as Networking hacks.

Members of the two CUHK teams included:

- Shing Yuet LEUNG (MIEG Year 3), Cham Fei TONG (CS Final Year), Xianbo WANG (Math Final Year, will be IE MPhil student in this Fall), Yihui ZENG (Math Final Year)
- Paul CHAN, Wai Man HUNG, Tsz Ching LAM, Wai Pan YIK (All Year 2 CS students).

Congratulations again to both of our teams and we are proud of you !

For more details of this event, please check:

- https://www.pwchk.com/en/events/hacking-challenge-2017.html
- https://www.facebook.com/hashtag/hackaday2017

The CUHK Teams

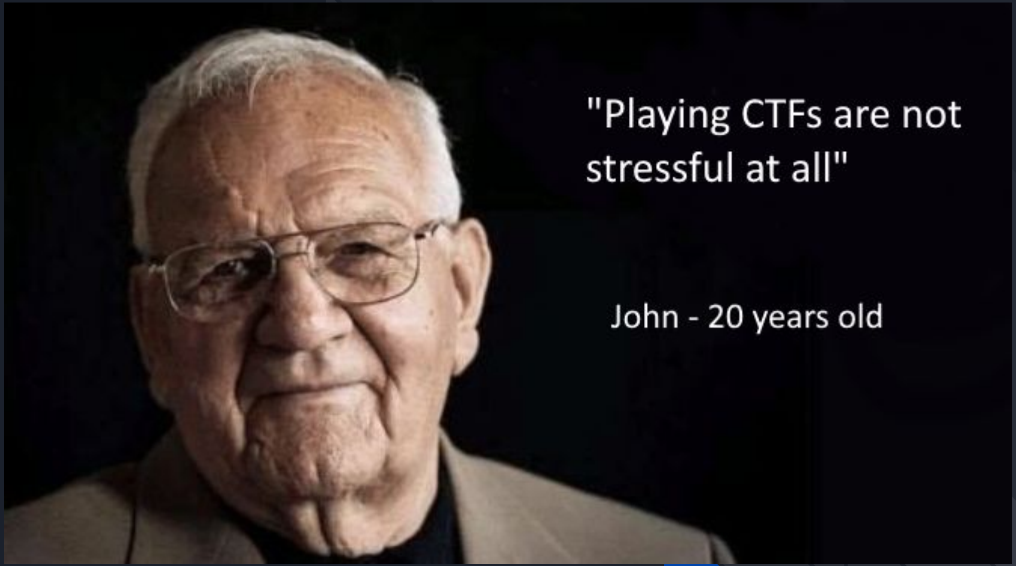
picoCTF

- held by CMU (Carnegie Mellon University)
- Online Introduction-level CTF
- Practice questions open all year round
- Competition on March next year (tentative)
- No prizes (since prizes are for US Middle/highschoolers only)
- https://play.picoctf.org/

Real World CTF

https://youtu.be/2S_TXaGYD8E?si=HT9t20yzDPhtHTPq

Break (?), Q&A



How to play CTF?

- Play with teams
  - Online CTF: Usually unlimited amount of players per team
  - Onsite CTF: Usually only 3-4 players per team
- Choose some suitable CTFs to play
  - ctftime.org
  - View Upcoming CTFs
  - Scores decided by the community
  - Global or Local Ranking
    - Like Chinese Ranking in https://www.xctf.org.cn/
  - Write-ups can be found

How to play CTF? (cont’d)

- Write and Read Write-ups
  - Describe how you solve a challenge, all the hoops you have gone through
  - Learn while doing a challenges, but also while writing and reading write-ups
- Sometimes Questions can troll, be guessy (通靈)
- Check the question title and description! Those could be hints.
- Google is your friend (or any search engine of choice)
- **Try Harder…**

しゃろ @Charo_IT · May 13

CTFは健康に悪い

Translated from Japanese by Microsoft

CTF is bad for your health.

Sneak peak at Different Categories

Web Security 🕸

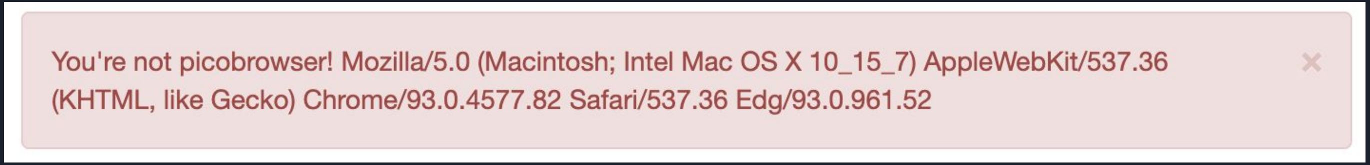
Web security

- Everything about the world wide web
- PHP, Node.js, SQL
- wasm (?)
- OWASP Top 10

Level 1: Do You Know How (not) to Use a Browser?

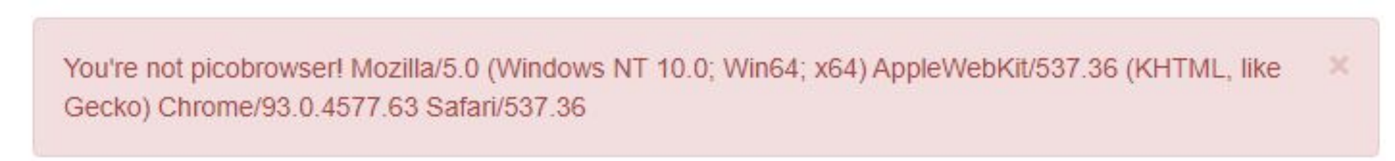
- picoctf practice: Insp3ct0r
  - https://jupiter.challenges.picoctf.org/problem/44924/
- picobrowser
  - https://jupiter.challenges.picoctf.org/problem/50522/
  - “This website can be rendered only by picobrowser, go and catch the flag!”

Microsoft Edge on M1 Mac



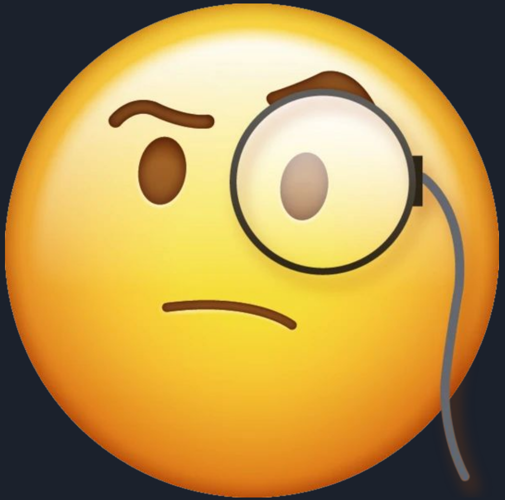
You're not picobrowser! Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36 Edg/93.0.961.52

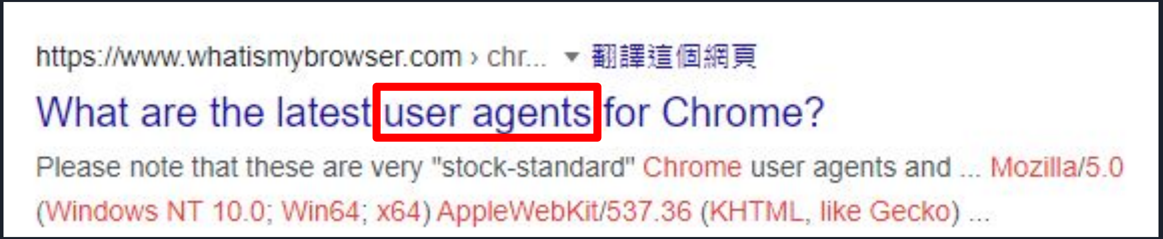
Chrome on Windows



You're not picobrowser! Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36

How?

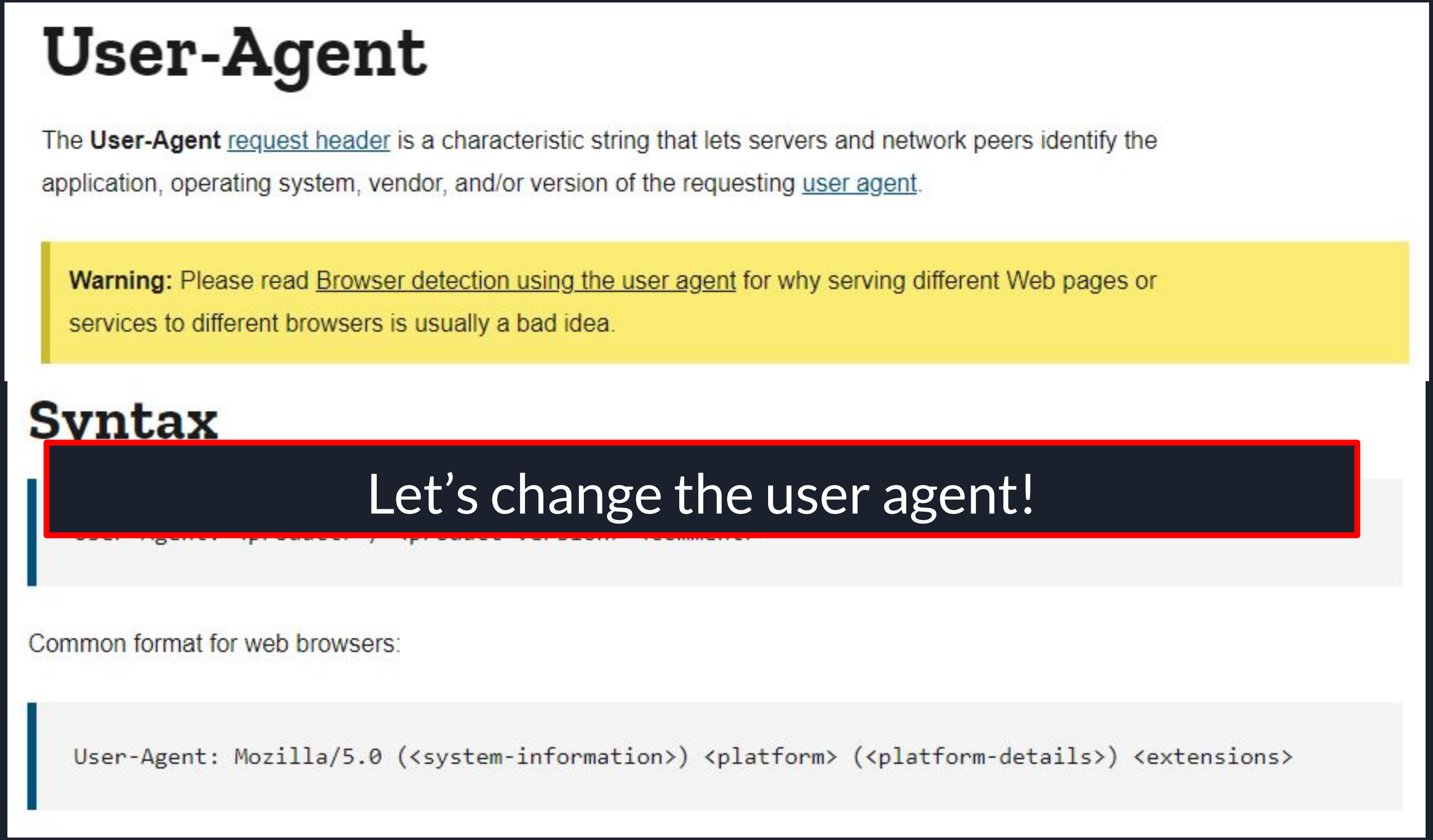




https://www.whatismybrowser.com › chr... ▾ 翻譯這個網頁

What are the latest user agents for Chrome?

Please note that these are very "stock-standard" Chrome user agents and ... Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) ...



User-Agent

The **User-Agent** request header is a characteristic string that lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent.

Warning: Please read Browser detection using the user agent for why serving different Web pages or services to different browsers is usually a bad idea.

Syntax

Common format for web browsers:

```
User-Agent: Mozilla/5.0 (<system-information>) <platform> (<platform-details>) <extensions>
```

Let’s change the user agent!

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

Time to use… the terminal

Why Terminal?

- Many tools are command-line only.
- Sometimes (when you ssh into a remote server somewhere in a data center overseas) all you have is a shell!
- Command-line interfaces are much faster and more efficient IF you know what you are doing.

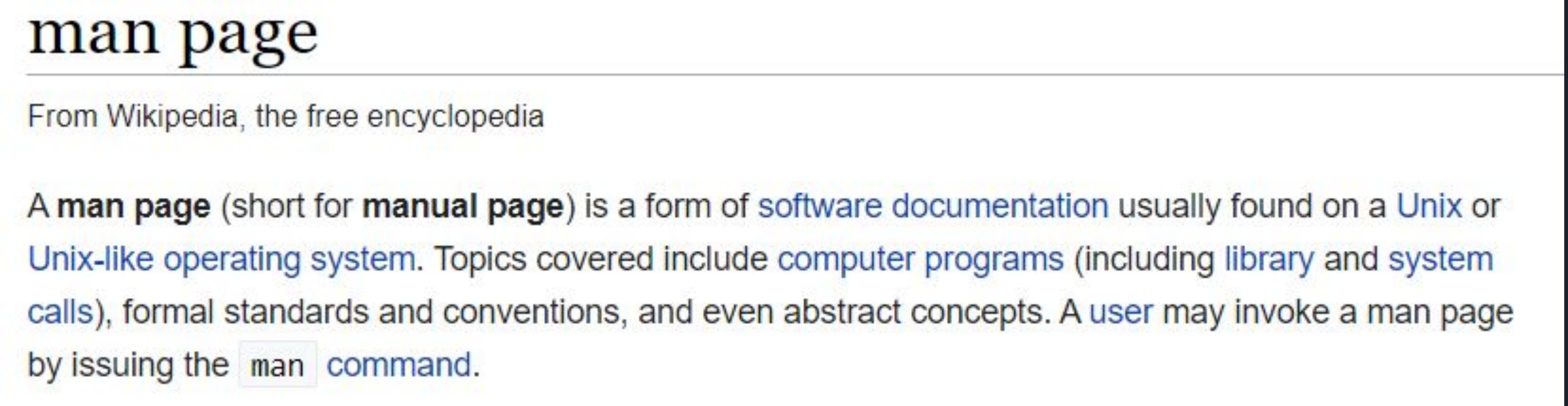
```
00252d0 32 d1 af 60 81 65 0d 58 3f a0 c0 c0 74 08 03 1a
00252e0 3c 68 e8 05 88 87 84 06 05 2f af d8 2b 2a cc 61
00252f0 de 07 01 ad 78 89 62 4a d7 1e 37 18 bf 6a 5a 20
0025300 5f 77 19 df 69 a7 c5 06 29 c4 2c 5e ea 8a 28 26
0025310 ab a3 90 89 2f 73 12 f7 a9 4b 72 d2 41 8b e5 b1
0025320 53 d3 f2 1c b0 be ec ac 51 2c 3b c0 aa 74 24 39
0025330 54 dd 92 3c d0 06 35 a1 26 32 8e 92 b1 11 21 5f
0025340 43 01 bb 8b cb 77 f2 85 5e dc 71 9d 15 ae bf 28
0025350 e7 8a db ca f7 15 fb 08 99 df dd df 7d c2 57 77
0025360 96 8f 75 55 66 5f 52 7c 64 70 64 f3 06 02 73 ab
0025370 9d 0b c7 5a 81 01 33 65 8c 6c e2 e0 2a a7 38 06
0025380 e0 41 c9 29 72 b0 c7 84 0b ef 64 e2 4d 59 39 96
0025390 72 4b 1d 56 2c ba 37 ad 1e d9 6f 7f 82 5b 97 bb
00253a0 7d dc e6 3d 97 d5 2b c4 08 1f 87 1f d2 aa 1e c9
00253b0 7d 89 29 8b ec b6 fd 08 96 54 26 b5 49 87 d8 24
00253c0 dd 0d ad 42 0e 5c 21 b7 6e 5c 95 20 3e 60 ac 40
00253d0 e0 b7 1e 40 84 7d e4 bf eb 81 09 ae f5 3f 7b e4
00253e0 46 3e 7e be 3c bb bb bf bb f6 23 9a 8e 7a 1c 8f
00253f0 b2 62 1c 06 bf 4d 71 75 50 89 23 3f f5 ad 34 d3
0025400 a4 4a 04 57 89 54 3b a1 06 64 62 04 c9 47 0a 3e
0025410 3c a3 97 b5 2b 34 f0 d3 bb a1 fb ac 7a af dd df
0025420 71 37 2f 7b bb bc be 25 54 57 da 42 7b ca 42 29
0025430 73 bf 04 56 df 82 27 8a a0 23 aa 62 70 6a 0c b1
```

We use the command line tool `curl` for this.

What is curl?

Let’s use the command tool `man` to see what curl does

What is man?

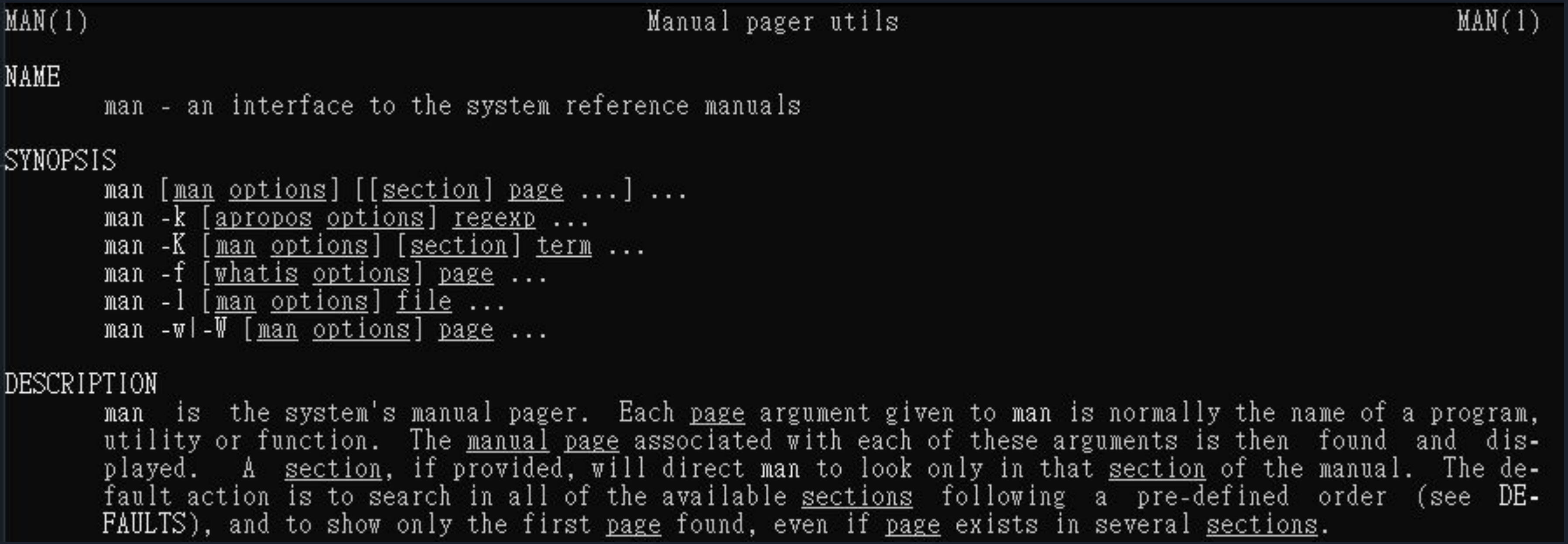


man page

From Wikipedia, the free encyclopedia

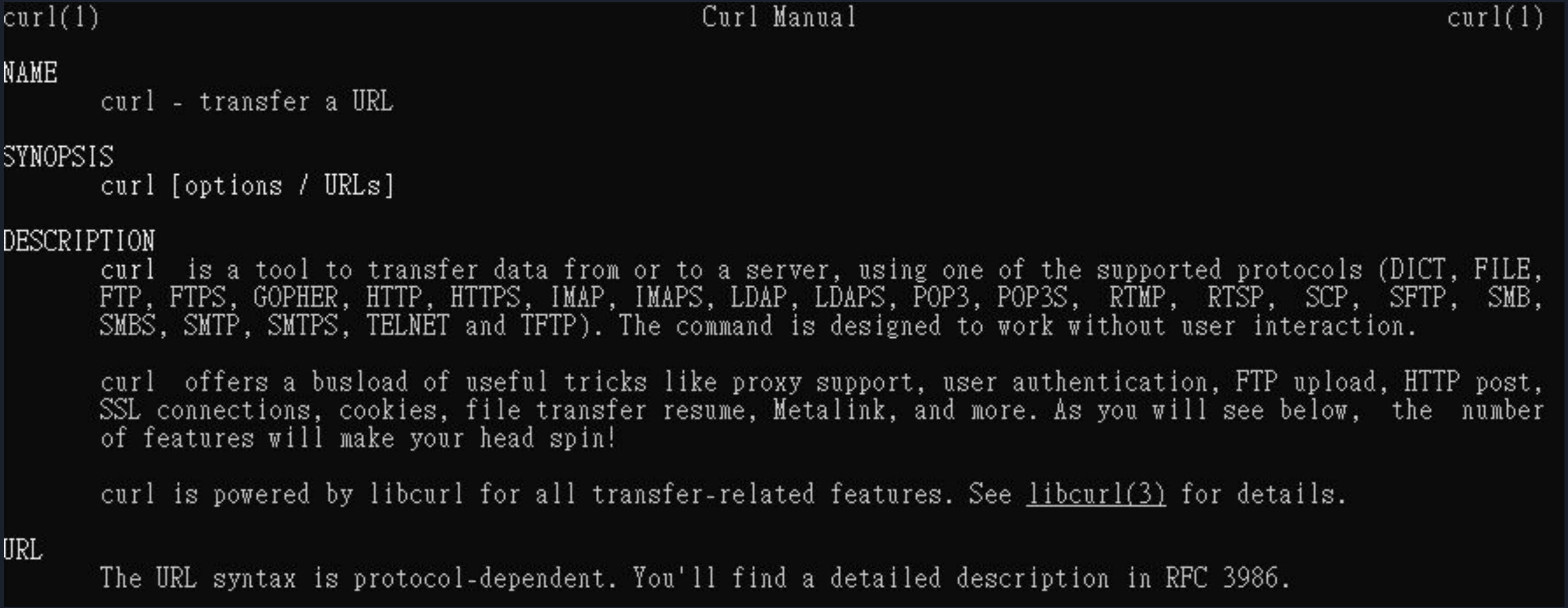
A **man page** (short for **manual page**) is a form of software documentation usually found on a Unix or Unix-like operating system. Topics covered include computer programs (including library and system calls), formal standards and conventions, and even abstract concepts. A user may invoke a man page by issuing the `man` command.

man man



```
MAN(1)                          Manual pager utils                          MAN(1)

NAME
       man - an interface to the system reference manuals

SYNOPSIS
       man [man options] [[section] page ...] ...
       man -k [apropos options] regexp ...
       man -K [man options] [section] term ...
       man -f [whatis options] page ...
       man -l [man options] file ...
       man -w|-W [man options] page ...

DESCRIPTION
       man  is  the system's manual pager.  Each page argument given to man is normally the name of a program,
       utility or function.  The manual page associated with each of these arguments is then  found  and  dis-
       played.   A  section, if provided, will direct man to look only in that section of the manual.  The de-
       fault action is to search in all of the available sections  following  a  pre-defined  order  (see  DE-
       FAULTS), and to show only the first page found, even if page exists in several sections.
```

man curl



```
curl(1)                                  Curl Manual                                  curl(1)

NAME
       curl - transfer a URL

SYNOPSIS
       curl [options / URLs]

DESCRIPTION
       curl  is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE,
       FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S,  RTMP,  RTSP,  SCP,  SFTP,  SMB,
       SMBS, SMTP, SMTPS, TELNET and TFTP). The command is designed to work without user interaction.

       curl  offers a busload of useful tricks like proxy support, user authentication, FTP upload, HTTP post,
       SSL connections, cookies, file transfer resume, Metalink, and more. As you will see below,  the  number
       of features will make your head spin!

       curl is powered by libcurl for all transfer-related features. See libcurl(3) for details.

URL
       The URL syntax is protocol-dependent. You'll find a detailed description in RFC 3986.
```

Let’s use curl to send the request!

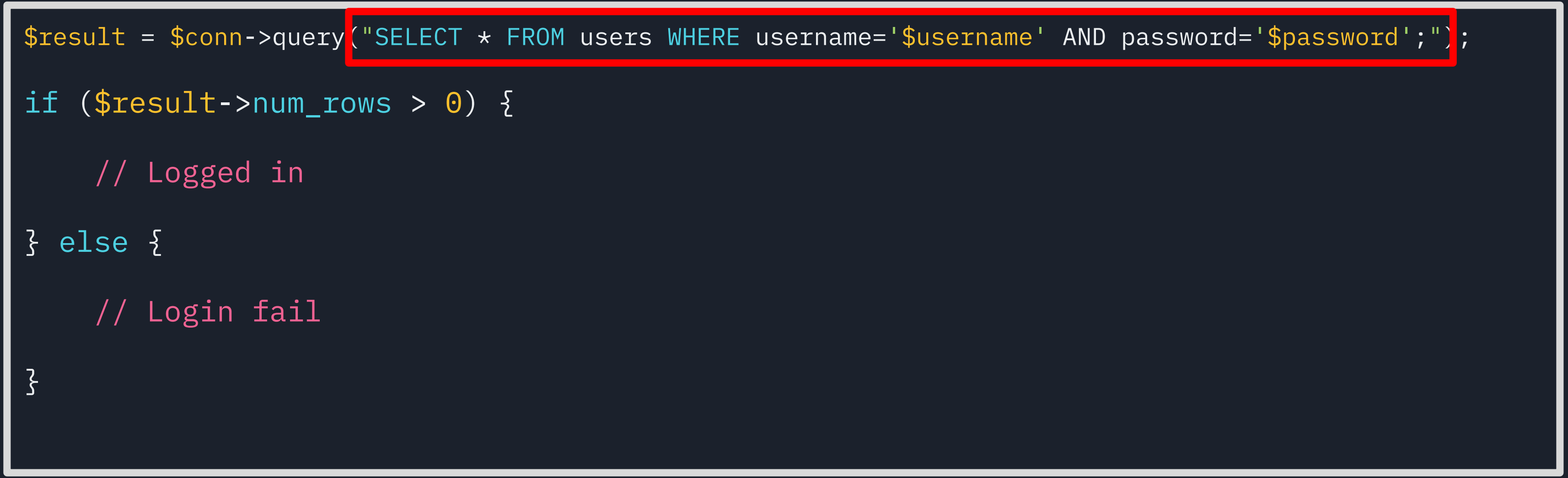
```
curl 'https://jupiter.challenges.picoctf.org/problem/50522/flag'
```

```
curl 'https://jupiter.challenges.picoctf.org/problem/50522/flag' -H
'User-Agent: picobrowser'
```

Level 2: Wait, you can do THAT?

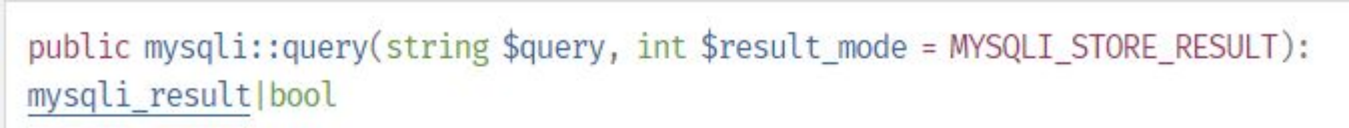
- picoctf practice: cass (Cowsay As a Service)
    - https://caas.mars.picoctf.net/
- Irish-Name-Repo 1
    - https://jupiter.challenges.picoctf.org/problem/50009/

Guessing the Source Code

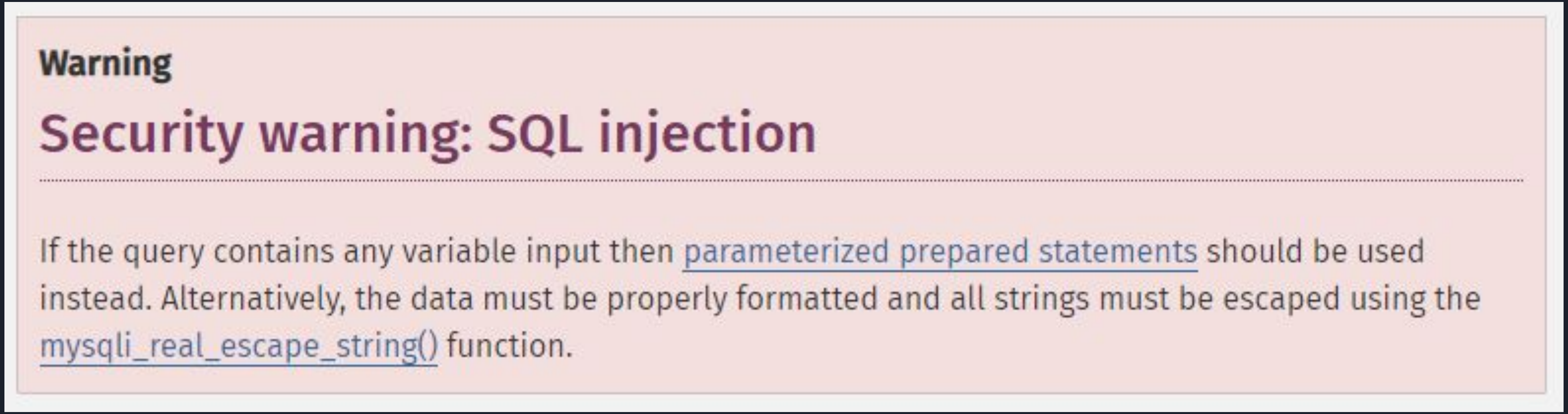


```
$result = $conn->query("SELECT * FROM users WHERE username='$username' AND password='$password';");

if ($result->num_rows > 0) {

    // Logged in

} else {

    // Login fail

}
```

php documentation



```
public mysqli::query(string $query, int $result_mode = MYSQLI_STORE_RESULT):
mysqli_result|bool
```



Warning

Security warning: SQL injection

If the query contains any variable input then parameterized prepared statements should be used instead. Alternatively, the data must be properly formatted and all strings must be escaped using the mysqli_real_escape_string() function.

SQL

```
SELECT * FROM users WHERE username='$username' AND password='$password';
```

I don’t know the username, let alone the password...

```
SELECT * FROM users WHERE username='OIL' AND password='haha';
```

- password: haha

What if… we type a single-quote into password?

!!!

```
SELECT * FROM users WHERE username='OIL' AND password=''';
```

- password: '

Now we can type SQL code!

```
SELECT * FROM users WHERE username='OIL' AND password='' OR 1=1';
```

- password: `' OR 1=1`

1=1 is always true, so the whole condition is always true!

Fixing the Junk after...

```
SELECT * FROM users WHERE username='OIL' AND password='' OR 1=1;--';
```

- password: `' OR 1=1;--`
- The part after `--` is regarded as comment

Cryptography 😭

Cryptography

- All about secure communication in the presence of adversarial behavior (from wiki)
- In CTF: You are the adversary
- Breaking weak cryptosystems
- Break bad implementations of (otherwise strong) cryptosystems
- Play with cutting edge stuff (e.g. lattice, quantum crypto)
- Quite heavy in mathematics (which may be a good thing to some of you)

Classical Cryptography

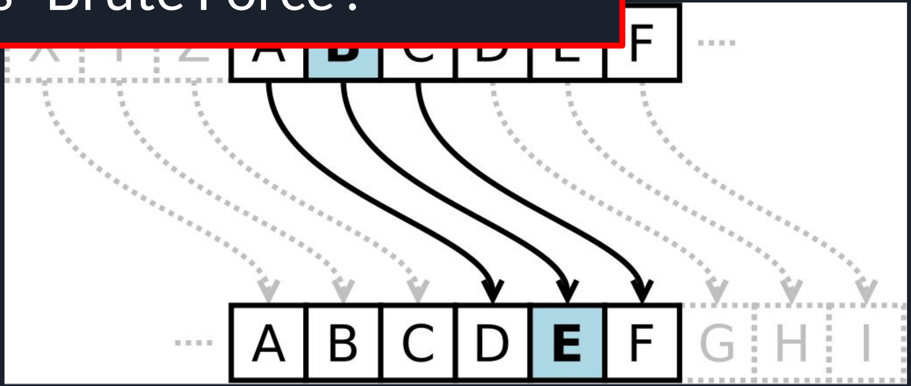
- (probably) can be done using pen and paper
- 13
    - Cryptography can be easy, do you know what ROT13 is?
    - `cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}`

Caesar Salad

Caesar Cipher

- Shifts characters around
- Caesar: move by 3
- ROT13: move by 13
    - What happens if you apply ROT13 twice?

Just try every possibilities from 0 to 25…
This is known as “Brute Force”.



Modern Cryptography

- You need a computer to do it
- Based on difficult math or complex mechanisms
- You may need to search paper
- Crypto:
  - Symmetric Cryptography, represented by DES, AES, and RC4.
  - Asymmetric Cryptography, represented by RSA, ElGamal, elliptic curve encryption.
  - Hash function, represented by MD5, SHA-1, SHA-512, etc.
  - Digital Signature, represented by RSA signature, ElGamal signature, and DSA signature.

Reverse Engineering

Reverse Engineering

- Deconstruct an object to reveal how it works
- Then exploit it!
- Given an executable file (e.g. .exe for windows)
- Understand how certain languages work in certain platforms
- Open up the executable in a disassembler or decompiler (if available)
- Code reading (static analysis)
- Run the program with different inputs to see what happens (dynamic analysis)
- Malware analysis, anti-virus softwares, game cheats, key-gen, ...

- picoctf practice: asm1
    - Assembly code
    - What does asm1(0x8be) return? Submit the flag as a hexadecimal value (starting with'0x’).
    - https://jupiter.challenges.picoctf.org/static/66c927e32f3d7be7a62d13a7c2250943/test.S

test.S

```
asm1:
  <+0>:   push   ebp
  <+1>:   mov    ebp,esp
  <+3>:   cmp    DWORD PTR [ebp+0x8],0x71c
  <+10>:  jg  0x512 <asm1+37>
  <+12>:  cmp  DWORD PTR [ebp+0x8],0x6cf
  <+19>:  jne  0x50a <asm1+29>
  <+24>:  add  eax,0x3
  <+27>:  jmp  0x529 <asm1+60>
  <+29>:  mov  eax,DWORD PTR [ebp+0x8]
  <+37>:  cmp  DWORD PTR [ebp+0x8],0x8be
  <+44>:  jne  0x523 <asm1+54>
  <+46>:  mov  eax,DWORD PTR [ebp+0x8]
  <+49>:  sub  eax,0x3
  <+52>:  jmp  0x529 <asm1+60>
  <+54>:  mov  eax,DWORD PTR [ebp+0x8]
  <+57>:  add  eax,0x3
  <+60>:  pop  ebp
  <+61>:  ret
```

What even is this language?

This is x86 assembly language.

Translated to C:

```
// <+0>:  push  ebp
// <+1>:  mov   ebp,esp
   int x = 0x8be;
// <+3>:  cmp   DWORD PTR [ebp+0x8],0x71c
// <+10>: jg    0x512 <asm1+37>
   if(x > 0x71c) goto label_a;
// <+12>: cmp   DWORD PTR [ebp+0x8],0x6cf
// <+19>: jne   0x50a <asm1+29>
   if(x != 0x6cf) goto label_b;
// <+21>: mov   eax,DWORD PTR [ebp+0x8]
// <+24>: add   eax,0x3
// <+27>: jmp   0x529 <asm1+60>
   x += 0x3;
   goto end;
label_b:
// <+29>: mov   eax,DWORD PTR [ebp+0x8]
// <+32>: sub   eax,0x3
// <+35>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
```

```
label_a:
// <+37>: cmp   DWORD PTR [ebp+0x8],0x8be
// <+44>: jne   0x523 <asm1+54>
   if(x != 0x8be) goto label_c;
// <+46>: mov   eax,DWORD PTR [ebp+0x8]
// <+49>: sub   eax,0x3
// <+52>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
label_c:
// <+54>: mov   eax,DWORD PTR [ebp+0x8]
// <+57>: add   eax,0x3
   x += 0xa;
end:
// <+60>: pop   ebp
// <+61>: ret
   return;
```

x = 0x8be

Translated to C:

```
//  <+0>:   push   ebp
//  <+1>:   mov    ebp,esp
    int x = 0x8be;
//  <+3>:   cmp    DWORD PTR [ebp+0x8],0x71c
//  <+10>:  jg     0x512 <asm1+37>
    if(x > 0x71c) goto label_a;
//  <+12>:  cmp    DWORD PTR [ebp+0x8],0x6cf
//  <+19>:  jne    0x50a <asm1+29>
    if(x != 0x6cf) goto label_b;
//  <+21>:  mov    eax,DWORD PTR [ebp+0x8]
//  <+24>:  add    eax,0x3
//  <+27>:  jmp    0x529 <asm1+60>
    x += 0x3;
    goto end;
label_b:
// <+29>:  mov    eax,DWORD PTR [ebp+0x8]
// <+32>:  sub    eax,0x3
// <+35>:  jmp    0x529 <asm1+60>
    x -= 0x3;
    goto end;
```

```
label_a:
//  <+37>:  cmp    DWORD PTR [ebp+0x8],0x8be
//  <+44>:  jne    0x523 <asm1+54>
    if(x != 0x8be) goto label_c;
//  <+46>:  mov    eax,DWORD PTR [ebp+0x8]
//  <+49>:  sub    eax,0x3
//  <+52>:  jmp    0x529 <asm1+60>
    x -= 0x3;
    goto end;
label_c:
//  <+54>:  mov    eax,DWORD PTR [ebp+0x8]
//  <+57>:  add    eax,0x3
    x += 0xa;
end:
//  <+60>:  pop    ebp
//  <+61>:  ret
    return;
```

x = 0x8be

Translated to C:

```
// <+0>:   push   ebp
// <+1>:   mov    ebp,esp
    int x = 0x8be;
// <+3>:   cmp    DWORD PTR [ebp+0x8],0x71c
// <+10>:  jg     0x512 <asm1+37>
    if(x > 0x71c) goto label_a;
// <+12>:  cmp    DWORD PTR [ebp+0x8],0x6cf
// <+19>:  jne    0x50a <asm1+29>
    if(x != 0x6cf) goto label_b;
// <+21>:  mov    eax,DWORD PTR [ebp+0x8]
// <+24>:  add    eax,0x3
// <+27>:  jmp    0x529 <asm1+60>
    x += 0x3;
    goto end;
label_b:
// <+29>:  mov    eax,DWORD PTR [ebp+0x8]
// <+32>:  sub    eax,0x3
// <+35>:  jmp    0x529 <asm1+60>
    x -= 0x3;
    goto end;
```

```
label_a:
// <+37>:  cmp    DWORD PTR [ebp+0x8],0x8be
// <+44>:  jne    0x523 <asm1+54>
    if(x != 0x8be) goto label_c;
// <+46>:  mov    eax,DWORD PTR [ebp+0x8]
// <+49>:  sub    eax,0x3
// <+52>:  jmp    0x529 <asm1+60>
    x -= 0x3;
    goto end;
label_c:
// <+54>:  mov    eax,DWORD PTR [ebp+0x8]
// <+57>:  add    eax,0x3
    x += 0xa;
end:
// <+60>:  pop    ebp
// <+61>:  ret
    return;
```

x = 0x8be

Translated to C:

```
// <+0>:   push   ebp
// <+1>:   mov    ebp,esp
   int x = 0x8be;
// <+3>:   cmp    DWORD PTR [ebp+0x8],0x71c
// <+10>:  jg     0x512 <asm1+37>
   if(x > 0x71c) goto label_a;
// <+12>:  cmp    DWORD PTR [ebp+0x8],0x6cf
// <+19>:  jne    0x50a <asm1+29>
   if(x != 0x6cf) goto label_b;
// <+21>:  mov    eax,DWORD PTR [ebp+0x8]
// <+24>:  add    eax,0x3
// <+27>:  jmp    0x529 <asm1+60>
   x += 0x3;
   goto end;
label_b:
// <+29>:  mov    eax,DWORD PTR [ebp+0x8]
// <+32>:  sub    eax,0x3
// <+35>:  jmp    0x529 <asm1+60>
   x -= 0x3;
   goto end;
```

```
label_a:
// <+37>:  cmp    DWORD PTR [ebp+0x8],0x8be
// <+44>:  jne    0x523 <asm1+54>
   if(x != 0x8be) goto label_c;
// <+46>:  mov    eax,DWORD PTR [ebp+0x8]
// <+49>:  sub    eax,0x3
// <+52>:  jmp    0x529 <asm1+60>
   x -= 0x3;
   goto end;
label_c:
// <+54>:  mov    eax,DWORD PTR [ebp+0x8]
// <+57>:  add    eax,0x3
   x += 0xa;
end:
// <+60>:  pop    ebp
// <+61>:  ret
   return;
```

x = 0x8be

Translated to C:

```
// <+0>:  push  ebp
// <+1>:  mov   ebp,esp
   int x = 0x8be;
// <+3>:  cmp   DWORD PTR [ebp+0x8],0x71c
// <+10>: jg    0x512 <asm1+37>
   if(x > 0x71c) goto label_a;
// <+12>: cmp   DWORD PTR [ebp+0x8],0x6cf
// <+19>: jne   0x50a <asm1+29>
   if(x != 0x6cf) goto label_b;
// <+21>: mov   eax,DWORD PTR [ebp+0x8]
// <+24>: add   eax,0x3
// <+27>: jmp   0x529 <asm1+60>
   x += 0x3;
   goto end;
label_b:
// <+29>: mov   eax,DWORD PTR [ebp+0x8]
// <+32>: sub   eax,0x3
// <+35>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
```

```
label_a:
// <+37>: cmp   DWORD PTR [ebp+0x8],0x8be
// <+44>: jne   0x523 <asm1+54>
   if(x != 0x8be) goto label_c;
// <+46>: mov   eax,DWORD PTR [ebp+0x8]
// <+49>: sub   eax,0x3
// <+52>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
label_c:
// <+54>: mov   eax,DWORD PTR [ebp+0x8]
// <+57>: add   eax,0x3
   x += 0xa;
end:
// <+60>: pop   ebp
// <+61>: ret
   return;
```

x = 0x8be

Translated to C:

```
// <+0>:   push   ebp
// <+1>:   mov    ebp,esp
   int x = 0x8be;
// <+3>:   cmp    DWORD PTR [ebp+0x8],0x71c
// <+10>:  jg     0x512 <asm1+37>
   if(x > 0x71c) goto label_a;
// <+12>:  cmp    DWORD PTR [ebp+0x8],0x6cf
// <+19>:  jne    0x50a <asm1+29>
   if(x != 0x6cf) goto label_b;
// <+21>:  mov    eax,DWORD PTR [ebp+0x8]
// <+24>:  add    eax,0x3
// <+27>:  jmp    0x529 <asm1+60>
   x += 0x3;
   goto end;
label_b:
// <+29>:  mov    eax,DWORD PTR [ebp+0x8]
// <+32>:  sub    eax,0x3
// <+35>:  jmp    0x529 <asm1+60>
   x -= 0x3;
   goto end;
```

```
label_a:
// <+37>:  cmp    DWORD PTR [ebp+0x8],0x8be
// <+44>:  jne    0x523 <asm1+54>
   if(x != 0x8be) goto label_c;
// <+46>:  mov    eax,DWORD PTR [ebp+0x8]
// <+49>:  sub    eax,0x3
// <+52>:  jmp    0x529 <asm1+60>
   x -= 0x3;
   goto end;
label_c:
// <+54>:  mov    eax,DWORD PTR [ebp+0x8]
// <+57>:  add    eax,0x3
   x += 0xa;
end:
// <+60>:  pop    ebp
// <+61>:  ret
   return;
```

x = 0x8be

Translated to C:

```
// <+0>:  push  ebp
// <+1>:  mov   ebp,esp
   int x = 0x8be;
// <+3>:  cmp   DWORD PTR [ebp+0x8],0x71c
// <+10>: jg    0x512 <asm1+37>
   if(x > 0x71c) goto label_a;
// <+12>: cmp   DWORD PTR [ebp+0x8],0x6cf
// <+19>: jne   0x50a <asm1+29>
   if(x != 0x6cf) goto label_b;
// <+21>: mov   eax,DWORD PTR [ebp+0x8]
// <+24>: add   eax,0x3
// <+27>: jmp   0x529 <asm1+60>
   x += 0x3;
   goto end;
label_b:
// <+29>: mov   eax,DWORD PTR [ebp+0x8]
// <+32>: sub   eax,0x3
// <+35>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
```

```
label_a:
// <+37>: cmp   DWORD PTR [ebp+0x8],0x8be
// <+44>: jne   0x523 <asm1+54>
   if(x != 0x8be) goto label_c;
// <+46>: mov   eax,DWORD PTR [ebp+0x8]
// <+49>: sub   eax,0x3
// <+52>: jmp   0x529 <asm1+60>
   x -= 0x3;
   goto end;
label_c:
// <+54>: mov   eax,DWORD PTR [ebp+0x8]
// <+57>: add   eax,0x3
   x += 0xa;
end:
// <+60>: pop   ebp
// <+61>: ret
   return;
```

x = 0x8bb

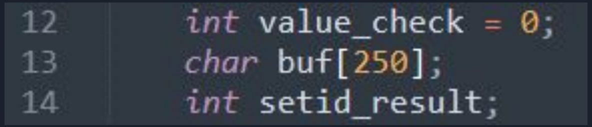
Binary Exploitation/Pwn01

Binary Exploitation

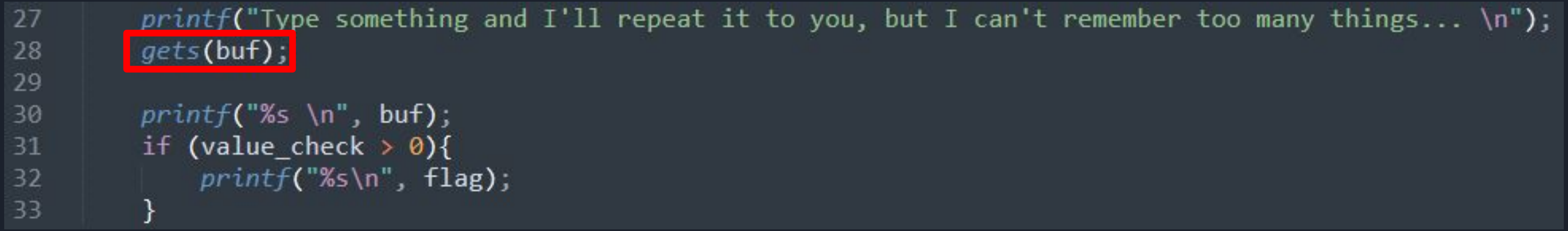
- Exploiting vulerabilities in executables (binaries)
- Make it do what it is not supposed to do
  - e.g. access files that requires special privilege, execute any code you want (RCE)
- Many of which involve messing with the memory (e.g. stack, heap)
- Understand how a program is compiled and run

Let’s recall our memory

- Parrot
  - Sometimes programs don't work the way they are supposed to. Sometimes people don't do what they are told
  - `nc chal.firebird.sh 33001`
  - https://files.firebird.sh/intro-2021/overflow.c

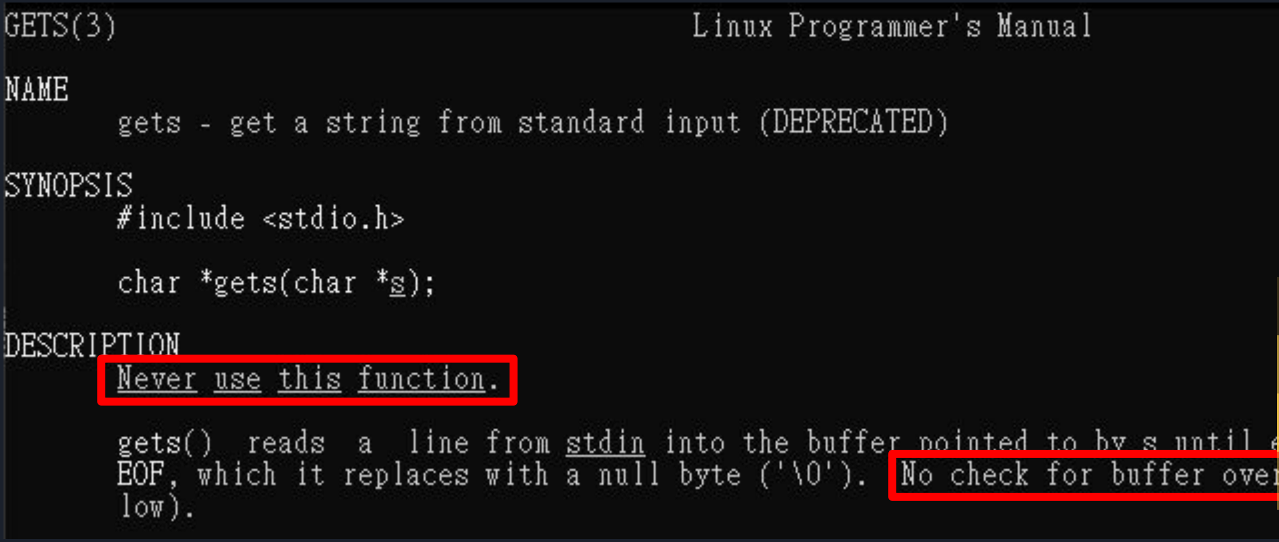


```c
    int value_check = 0;
    char buf[250];
    int setid_result;
```

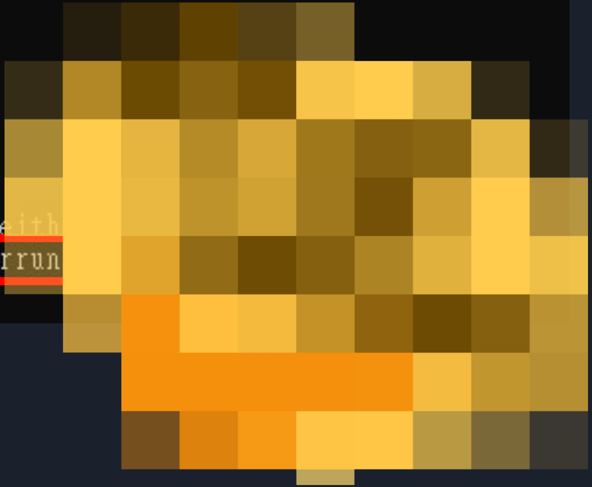


```c
    printf("Type something and I'll repeat it to you, but I can't remember too many things... \n");
    gets(buf);

    printf("%s \n", buf);
    if (value_check > 0){
        printf("%s\n", flag);
    }
```

man gets



```
GETS(3)                    Linux Programmer's Manual                    GETS(3)

NAME
       gets - get a string from standard input (DEPRECATED)

SYNOPSIS
       #include <stdio.h>

       char *gets(char *s);

DESCRIPTION
       Never use this function.

       gets()  reads  a  line from stdin into the buffer pointed to by s until eith
       EOF, which it replaces with a null byte ('\0').  No check for buffer overrun
       low).
```



Stack Structure

Higher
Address

Memory Location	Memory Content
1254	
1250	
1246	
1242	
...	...
1004	
1000	

Lower
Address

Stack Structure

Higher Address

Memory Location	Memory Content
1254	...
1250	0xdeadbeef (-272716322)
1246	0x62366100 “b6a\0”
1242	0x6a6f696e “join”
...	...
1004	0x6f696c20 “oil “
1000	0x6375686b “cuhk“

Lower Address

`int value_check`

`char buf[250]`

Stack Structure

```
gets(buf);
```

	Memory Location	Memory Content	
Higher Address	1254	...	
	1250	0x00000000	int value_check

What if… we enter more than 250 characters?😱

	Memory Location	Memory Content	
	1242	0x00000000	

Let's enter 254 A's (0x41) !

	Memory Location	Memory Content	
			buf[250]
	1004	0x00000000	
Lower Address	1000	0x00000000	

(Over-simplified) Buffer Overflow

	Memory Location	Memory Content	
Higher Address	1254	...	
	1250		int value_check
	1246	0x41414141 “AAAA”	char buf[250]
	1242	0x41414141 “AAAA”	
	...	...	
	1004	0x41414141 “AAAA”	
Lower Address	1000	0x41414141 “AAAA”	

(Over-simplified) Buffer Overflow

!!!

Higher Address

Memory Location	Memory Content
1254	...
1250	**0x41414141 (1094795585)**
1246	0x41414141 “AAAA”
1242	0x41414141 “AAAA”
...	...
1004	0x41414141 “AAAA”
1000	0x41414141 “AAAA”

Lower Address

int value_check

char buf[250]

Forensics

- Information hidden in files…
  - metadata
  - Hide data in plain sight: steganography
  - Hide file in files?
- Analysing memory, disk image, network traffic…
  - Analyse pcap files
  - memory dump
  - disk image for deleted (partially corrupt) files
- Used in real life for crime investigations

CTF Training for Hackers

1. Basic
2. Web Security
3. Cryptography
4. Binary Exploitation/ Reverse Engineering
5. Potential Invited Talks

- Date: TBA, Weekly Training/Biweekly Training
- Time: 6:30 pm or 7:30 pm
- Join our discord to get new updates.
- Bring your laptop! (If you don’t have a laptop, it may be hard to play CTF.)

- No need to attend all trainings! You can just attend trainings that you are interested in.
- Think back about the team thing: find teammates that accel at different categories.

- After local competitions, we will hold write-up sharing events to let everyone learn from each other. Stay tuned.

Some Learning Materials

- https://ctf101.org/
- https://github.com/apsdehal/awesome-ctf
- OverTheWire
- cryptopals (for cryptography)
- https://pwnable.kr/ for beginner pwn challenges
- https://pwnable.tw/ for the real deal pwn challenges

Credit

- Cousin(co-coordinator)
- Kylebot @ ASU/Shellphish

End!

- Feel free to join our discord server for further discussion! We will have other events and invited talks so stay tuned for more CUHKOIL activities.
- We are recruiting CTF players! Join by sharing your write-ups with us. Join the discord server for more details. (CUHK students only)
- Like our facebook page https://www.facebook.com/cuhkoil also for events!

Facebook

Discord
Note: This link is only valid for 100 invites.