



Hong Kong Cyber Security New Generation

Capture the Flag (CTF) Challenge 2022

Webinar 1

Ringo Lam
Cousin Wu

8 Oct, 2022



Speaker Bio



Ringo Lam

- Consultant / Penetration Tester
- CTF Player - Web



Cousin Wu

- MPhil Student in IE department of CUHK
- Coordinator of CUHK Open Innovation Lab: Promote CTF
- CTF Player - Crypto



b6a.black

@blackb6a

@blackb6a

/team/83678



Agenda

- Capture-the-Flag (CTF)
 - Why CTF?
 - What is CTF?
 - How to play CTF?
 - What can you get from playing CTF?
 - Some tips on the CTF!
- CTF challenges category: Web
 - How websites works
 - MitM yourself with Burp Suite
 - SQL injection
 - Tips and resources on web challenges
- CTF challenges category: Cryptography
 - Cryptography and your digital life
 - Classical cryptography: substitution cipher
 - Modern cryptography: RSA
 - Tips and resources on cryptography challenges

CTF 2022

香港 網絡 保安 新生代
Hong Kong Cyber Security New Generation

奪旗挑戰賽
Capture the Flag Challenge

Register now!

<https://ctf.hkcet.org/>

Sample Challenges:

<https://training.hkcet22.pwnable.hk/>

Discord channel:

<https://discord.gg/V6QGvWCmDm>



What is Capture-the-Flag (CTF)?



Hacking

but legal :)

中一學生駭入學校系統發警告 要求撤回這政策否則「hack所有嘢」

撰文：林卓恒

出版：2022-09-27 15:53 更新：2022-09-27 15:53



中一學生駭入學校系統發警告 要求撤回這政策否則「hack所有嘢」 | 昨日
(9月26日)在網上流傳幾張圖片，相信是一名代號為「ShadowLST」的
黑客駭入 [REDACTED] 書院學校電腦系統後經系統發出的電子郵件截圖。

駭客自稱是中一學生有7人團隊 指揮官IQ136



Cap. 200 Crimes Ordinance

161. Access to computer with criminal or dishonest intent

(1) Any person who obtains access to a computer—

- (a) with intent to commit an offence;
- (b) with a dishonest intent to deceive;
- (c) with a view to dishonest gain for himself or another; or
- (d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

(2) For the purposes of subsection (1) gain (獲益) and loss (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and—

- (a) gain (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and

- (b) loss (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.



上次我入侵學校早會宣布系統時，我給學校發了一封郵件。
我告訴你bug和backdoor。

服務器有兩個錯誤

25/tcp 過濾的 smtp
80/tcp 打開 http
111/tcp open rpcbind<--後門端口
443/tcp 打開 https
2049/tcp 打開 nfs<--錯誤



nmap

服務器：nginx

- + 反點擊劫持 X-Frame-Options 標頭不存在。
- + X-XSS-Protection 標頭未定義。此標頭可以提示用戶代理以防止某些形式的 XSS
- + X-Content-Type-Options 標頭未設置。這可能允許用戶代理以與 MIME 類型不同的方式呈現站點的內容
- + 未找到 CGI 目錄（使用 '-C all' 強制檢查所有可能的目錄）



nikto

1. 請給我們自由下載或者卸載mdm

否則我會hack學校的所有嘢。

這是最後的警告，沒有另外

該系統能夠被我一名中一學生破解。

但是，該系統每年要70港幣。

這完全沒有任何意義。

學校可以先問家長是否需要他們的學生安裝 mdm,然後決

定一琳瑯就好多啦。



Hack
MDM?

All

Videos

Images

Books

News

More

Tools

About 201,000 results (0.52 seconds)

Videos :



Hacking 101: single domain webapp recon with nmap, nikto ...

YouTube · The XSS rat
18 Apr 2020



10 key moments in this video



From 00:07
Bug Bounty
Hunting



From 00:37
Map Is a
Network
Mapper



From 03:37
Nmap Scan



From 06:17
Udp Ports



From 06:43
Ports >

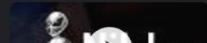


Scan for Vulnerabilities on Any Website Using Nikto [Tutorial]

YouTube · Null Byte
14 Mar 2019



10 key moments in this video



How to use Nikto in Kali Linux | Website Ethical Hacking ...

<https://www.xuehua.us> › lang=zh-hk ▾ このページを訳す

黑客工具 | 2021年十大黑客工具列表- 雪花新闻

Nmap 是跨平臺的，適用於Mac、Linux 和Windows。由於其易用性和強大的搜索和掃描能力，...

Nikto 是另一個受歡迎的工具，作為Kali Linux 發行版的一部分而廣為人知。

<https://qiita.com> › Security ▾

【セキュリティ】脆弱性診断・検査ツール on Kali Linux - Qiita

2018/12/09 — Metasploit、**Nikto**、**Nmap**、Sqlmap、WPScanなど60種類以上のペネトレーションテストツールに対応して ... <docs.kali.org/pdf/kali-book-zh-hans.pdf> ...

<https://www.oschina.net> › 关键词 ▾ このページを訳す

nmap如何快速扫描全端口- OSCHINA - 中文开源技术交流社区

python-nmap 是一个用来帮助用户使用**nmap** 端口扫描器的Python 库，可让用户轻松 ... 通过管道交给**nikto**进行扫描 #!bash **Nmap Nikto Scan nmap** -p80 10.0.1.0/24 -oG ...

<https://forum.90sec.com> › topic ▾ このページを訳す

渗透测试全流程归纳总结(by Mr.M) - 账号审核 - 90Sec

2021/03/15 — 检查是否存在常见漏洞**nmap** -n -p445 --script=broadcast ... -oG - | **nikto** -host - # 利用**nmap**扫描开放80端口的IP段并且oG (**nmap**结果输出并整理) 通过 ...

<https://tech.akat.info> › ... ▾

Hack The Box – Curling – Walkthrough – 忘れるために記す

2020/08/28 — 10243/tcp filtered unknown. **Nmap** done: 1 IP address (1 host up) scanned in 185.92 seconds. # perl **nikto.pl** -h <http://curling.htb/>.



Why CTF?

- Hacker tools are readily available on the Internet
- With a little bit of time for research, you can conduct an 'attack' just like the F1 student! (not endorsing)
 - Enjoy the consequence too!
 - 凡走過必留下痕跡

Hacking without prior consent is illegal

未經事先同意的黑客行為是非法的



Why CTF?

Can we enjoy the fun of hacking legally?

Yes, CTF!

CTF provides a safe, fun, and profitable way for anyone to legally hack their system, as long as you obey some rules and do no harm.

* not a legal advice / P.S.: we do not use automated tools (nmap/nikto) in CTF



What is CTF

Capture-the-flag (CTF) is a computer security contest that allows you to 'hack' into system legally. The target is a "flag" (secret file) inside the vulnerable system.

- Served as a security training, or exchange of ideas
- Competitors need to exploit the systems to find the flags
- CTF is not an examination but a learning process.
- You are not expected to
 - know everything prior the game starts
 - solve all of the challenges when the game ends
- Permission granted, under the CTF rule, to hack the CTF challenges

https://en.wikipedia.org/wiki/Hacker_culture



CTF events around the world







Long running CTF events (Wargame)



picoCTF

Get Started

Learn ▾

Practice

Compete ▾

About ▾

Log In

Carnegie
Mellon
University

CFG to C

Wouldn't it be cool to be able to have one of these patrol drones to do your bidding?! Figure out the correct sequence of C functions uses the following control flow graphs and you should be well on your way.
Submit the correct order of functions.

input

picoCTF

The free, fun way to learn and practice cybersecurity.

Leaderboard

Hint

Run

Get Started

Sign Up

Sign up is open year-round for anyone 13 and older to learn, practice, and compete.

Jeopardy-style CTF

- CTF challenges are set up by authors. Players need to tackle the challenges to get flags
 - Team's gain points for every task solved, with more complicated tasks earning more points.
 - At the end of the game, the team with the most points wins!



Jeopardy-style CTF Categories

- Web
- Cryptography
- Pwn (Binary Exploitation)
- Reverse Engineering
- Misc. (Forensic, etc.)



CTF - Web

- Hack a website!
- Involve common web vulnerability (e.g. XSS / injection / ...)
- Steal password (from admin)!
- Read arbitrary file in the system!
- Run arbitrary command in the system!
- (Relate to bug bounty / pentest more as most software today are website)



CTF - Web

HTTP

HTML

JavaScript

PHP

OWASP Top 10

SQL Injection

IDOR

XSS

▼ General

Request URL: https://example.com/

Request Method: GET

Status Code: 200

Remote Address: 127.0.0.1:8080

Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers

age: 330101

cache-control: max-age=604800

content-length: 1256

content-type: text/html; charset=UTF-8

date: Thu, 06 Oct 2022 00:43:51 GMT

etag: "3147526947+gzip"

expires: Thu, 13 Oct 2022 00:43:51 GMT

HTML

CSS

JS





CTF - Cryptography

- Attack cryptosystem
- Maybe encryption, decryption, signature, hashes
- Common crypto used in real life
- Cryptanalysis: Is the system flawed?
- Implementation issue? Side channel?
- Randomness: Is it predictable?

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```



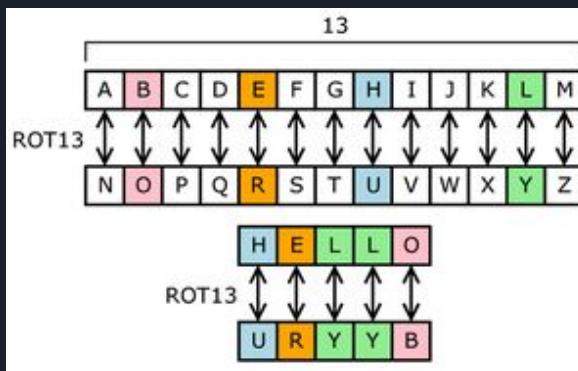
CTF - Cryptography

Classical cipher

RSA

AES

Maths!



<https://play.google.com/apps/details> · Translate this page :

VPN—Secure&Fast VPN Proxy - Google Play 上的应用

Android平台上最安全的私聊VPN应用！凭借高水平的安全性和军用级加密，您可以通过安缦私下进行游戏、工作、观看视频，为您带来安全、快速、私密的网络。

★★★★★ Rating: 4.2 · 2,070 votes · Free · Android · Utilities/Tools

[https://www.vpn\[REDACTED\].com/zh-hans](https://www.vpn[REDACTED].com/zh-hans) · Translate this page :

最佳加密VPN [2022年更新] - VPNRanks

此基于英属维尔京群岛的VPN服务提供出色的隐私功能和VPN协议，如OpenVPN UDP、OpenVPN TCP、L2TP/IPSec、SSTP和PPTP协议。此外，[REDACTED] VPN提供256位军用级加...

"Military-grade" refers to AES-256 encryption. This standard was established in order to be in compliance with the Federal Information Processing Standards (FIPS) that govern the handling of sensitive data. It offers 128-bit block encryption via the use of cryptographic keys.



CTF - Reverse Engineering

- Given an binary / executable / software (without source code), understand what the software actually do
- Is the program hiding something?
- Can I patch the program to change logic?
- Is there bugs / error in the program that I can use? (Game hack etc)
- Reverse the logic: What input do I need to “get flag”?

CTF - Pwn (Binary Exploitation)

- Attack an service with an binary / executable / software!
- Most of the time you have the binary
- Find vulnerability
- Craft and fire exploit to get access to remote service!



CTF - Reverse / Pwn

Cheat engine





CTF - Misc

- Forensics
 - Find target data (flag, important document, ...) in (disk, usb, phone image, drones...)
 - Photo / Audio / Video analysis: any information hid inside? (Steganography)
- Programming Language: how interesting feature in programming language can be used in hacking
- Professional Programming & Coding (PPC): Coding challenges
- And more...



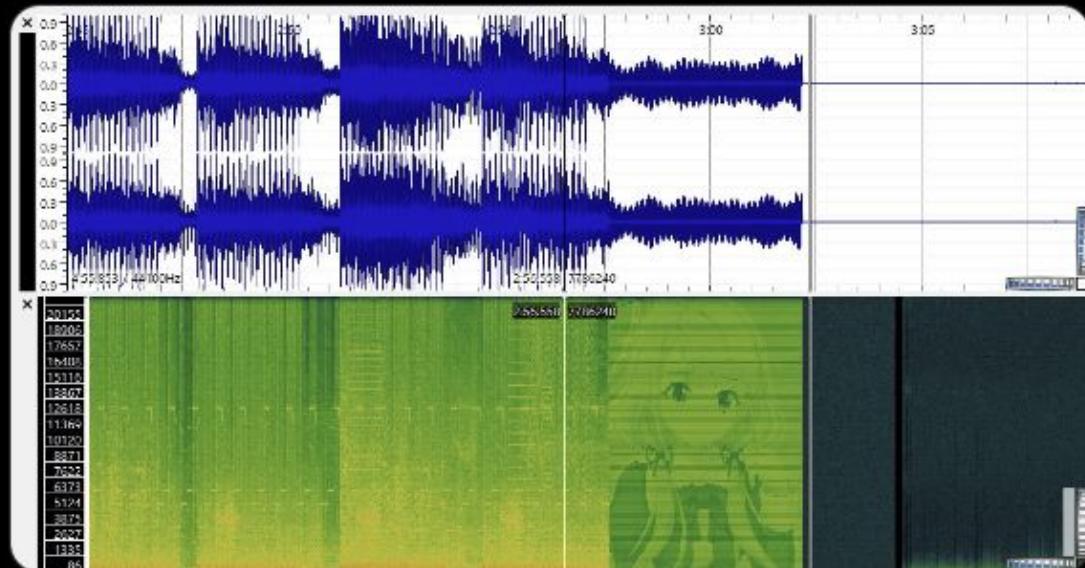
諦メロン
 @_Akira_Melon_

CTF - Misc

Steganography:

hiding image in soundtrack

14平米にスーザニア 広川恵一Remixで一番ヤバいのは、スペクトログラムを表示すると凧の絵が出現すること



午後10:52 · 2022年6月18日 · Twitter Web App

9,075 件のリツイート 335 件の引用ツイート 1.3万 件のいいね

CTF - Misc

```
server.py
1 import os
2 暗號 = '山竹牛肉'
3 print('暗號?', '_' * len(暗號))
4 if(input() == 暗號):
5     print(os.getenv('FLAG', '唔喎'))
6 else:
7     print('錯呀')
```

Challenge: 點點心 / Steamed Meatball

Homoglyph attack

<https://www.xn--80ak6aa92e.com/>

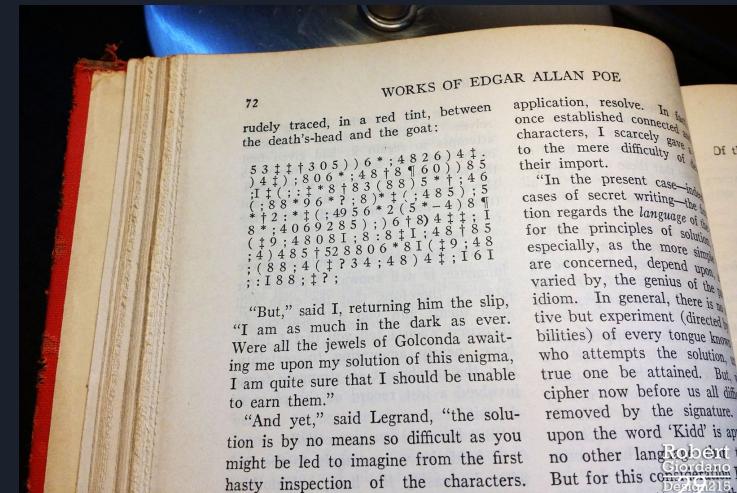
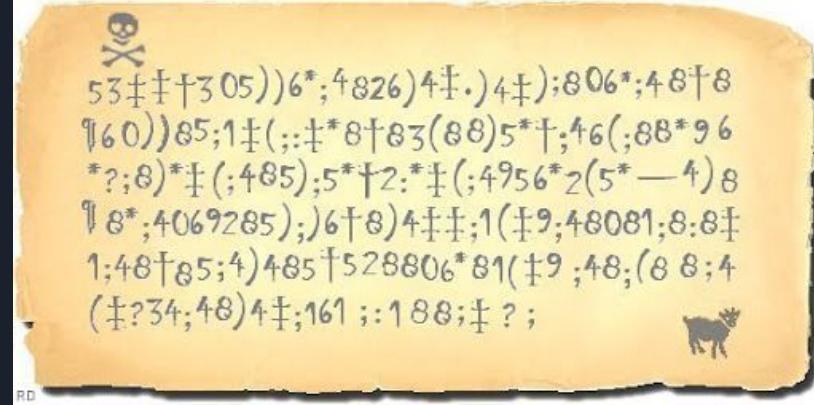
Confusable Characters

	
2F2D	5C71
KANGXI RADICAL MOUNTAIN	CJK UNIFIED IDEOGRAPH-5C71
	
2F75	7AF9
KANGXI RADICAL BAMBOO	CJK UNIFIED IDEOGRAPH-7AF9
	
2F5C	725B
KANGXI RADICAL COW	CJK UNIFIED IDEOGRAPH-725B
	
2F81	8089
KANGXI RADICAL MEAT	CJK UNIFIED IDEOGRAPH-8089

Total raw values: 16

Hacker beyond security

- Brain teaser
 - <https://oddpawn.com/>
- Just like solving riddles or puzzles, but on computers
 - <https://oddpawn.com/>
- Puzzle Hunt
 - Gold-bug Defcon
- Recover audio from muted video
 - <https://www.youtube.com/watch?v=FKXOucXB4a8>





What you can get from playing CTF?

- **Be attentive:** The devil is hidden in the details
- **Be creative:** What you learn from school may not help... think out of the box
- **Be absorbing:** Read write-ups from players and challenge authors
- **Be a team player:** Team up! No one is an island nor all-rounded
- **Don't worry to fail:** We compete to learn in CTFs



Career Prospect



CTF and Security community

CTF is a platform for security researcher / practitioner to communicate their thoughts.

- Lots of practitioners joined the ctf in 2021 and provided positive feedback (thanks!)

CTF events are often supported and sponsored by govt and commercial

Security

- Increasing reliance on computer technologies
- Increasing importance
 - Hong Kong cybersecurity law
 - HKMA iCAST

Black and White hats hacker

Same methodologies, different purpose

- White Hat Hackers
 - work with the permission of system administrators
 - improve cyber defenses
- Black Hat Hackers (Crackers)
 - steal data, criminal purposes
 - without authorization
 - illegal





Career Prospect

- Bug Hunter
- Penetration tester (pentester)
- R & D Engineer

- Red Team
- Blue Team

- IT Auditor
- Chief Information Security Officer
- Security Researcher (Industrial / Academic)

Bug Bounty Platform: hackerone

[hackerone](#)

SOLUTIONS ▾ PRODUCTS ▾ PARTNERS ▾ COMPANY ▾ HACKERS ▾ RESOURCES ▾

7	 insecure gitlab repositories at [REDACTED] [HtUS]	By thpless to U.S. Dept Of Defense	Resolved	High	disclosed 3 days ago	
26	 Open Redirect on www.redditinc.com via `failed` query param	By lu3ky-13 to Reddit	Resolved	Medium	disclosed 8 days ago	
21	 Add products to any livestream.	By datph4m to TikTok	Resolved	Medium	disclosed 9 days ago	
42	 Abuse cookie-modification, toast HTML and expired domain in CSP-form-action replacing login-page at www.dropbox.com/login to submit creds externally	By fransrosen to Dropbox	Resolved	High	\$6,909.00	disclosed 16 days ago
46	 HTML Injection in email via Name field	By mega7 to HackerOne	Resolved	Low	\$500.00	disclosed 13 days ago
3	 DNS rebinding in --inspect (insufficient fix of CVE-2022-32212 affecting macOS devices)	By zeyu2001 to Node.js	Resolved	High	disclosed 3 days ago	
9	 com.basecamp.bc3 Webview Javascript Injection and JS bridge takeover	By fr4via to Basecamp	Resolved	High	disclosed 8 days ago	
100	 One-click account hijack for anyone using Apple sign-in with Reddit, due to response-type switch + leaking href to XSS on www.redditmedia.com	By fransrosen to Reddit	Resolved	Critical	\$10,000.00	disclosed 2 months ago

<https://hackerone.com/hacktivity>



看我如何再一次駭進 Facebook，一個在 MobileIron MDM 上的遠端程式碼執行漏洞！

Advisory, CVE, RCE, Facebook, BugBounty

By  Orange Tsai on 2020-09-12

English Version

中文版本



Bug Bounty programme



Info



Thanks



Hacker Plus programme



Integrity Safeguards



Education



Payout guidelines



Data Abuse Bounty programme



Report vulnerability form



FBDL

Meta Bug Bounty programme info

(Last updated 31 August 2022)

Meta recognises the value external security researchers can bring to the security of Meta systems, and we welcome and seek to reward eligible contributions from security researchers, as outlined below. If you believe you have found a security vulnerability on Meta technologies and programs, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to quickly fix the problem. Before reporting, though, please review this page, including our Responsible Disclosure Policy, Reward Guidelines and scope of the programme.

If you are looking to report another type of issue, please use the links below for assistance.

- If your account or a friend's account is sending out suspicious links: <https://www.facebook.com/help/hacked>
- To report abuse: <https://www.facebook.com/help/reportlinks>
- For any other questions or concerns, please visit our Help Centre: <https://www.facebook.com/help>
- For programme updates and news from our Bug Bounty team, please like our Facebook page: <https://www.facebook.com/bugbounty>

Responsible Research and Disclosure Policy

For you to participate in the programme, we require that:

- You do not interact with an individual account (which includes modifying or accessing data from the account) without the account owner's explicit consent in writing, which you must produce upon request.
- You make a good faith effort to avoid privacy violations and disruptions to others, including (but not limited to) unauthorised access to or destruction of data, and interruption or degradation of our services. You must not intentionally violate any applicable laws or regulations, including (but not limited to) laws and regulations prohibiting the unauthorised access to data.
- If you inadvertently access another person's data or Meta company data without authorisation while investigating an issue, you must promptly cease any activity that might result in further access of user or Meta company data and notify Meta what information was accessed (including a full description of the contents of the information) and then immediately delete the information from your system. Continuing to access another person's data or company data may demonstrate a lack of good faith and disqualify you from any benefit of the Safe Harbour Provisions described below. You must also acknowledge the inadvertent access in any related bug bounty report that you may subsequently



How CTF

Computer knowledge

- Linux
 - How to navigate using the command line?
- Programming
 - For scripting, and reading source code in challenges

Research

- Google
 - Do you really know how to use the search engine to its fullest?
- Writeup

Practice

Persistence





Writeup

Writeups are solution of past challenges!

Learn from writeup!

Google

"hkcert21" 山竹牛肉

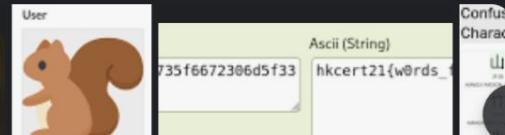


<https://ne-np.facebook.com> › photos · Translate this page · :

nc 連到chalp.hkcert21.

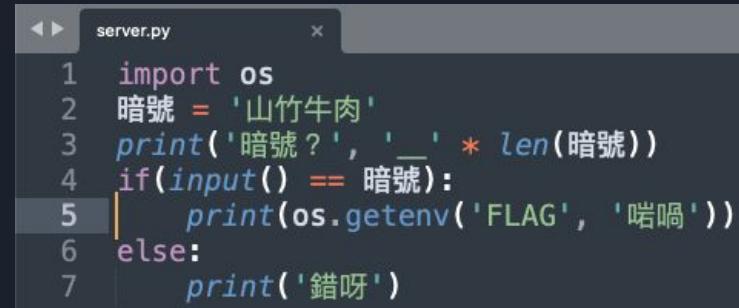
... 幅圖，但係好多玩家send 呀山竹牛肉四個字之後就彈咗「錯呀」呢兩隻字，拎唔到flag。大家可以喺我哋解題之前挑戰吓：nc 連到chalp.hkcert21.pwnable.hk:28338，試 ...

Images for "hkcert21" 山竹牛肉



How CTF (non-technical)

- Sleep well (before and during the CTF)
- Pick challenges that fits your skill level (B1 vs B2)
- Not to focus on a single challenge too hard
- Keep a log for everything you have tried in a challenge
- Be really careful!
 - Always scrutinize what you see



```
server.py
1 import os
2 暗號 = '山竹牛肉'
3 print('暗號?', '_' * len(暗號))
4 if(input() == 暗號):
5     print(os.getenv('FLAG', '啞喲'))
6 else:
7     print('錯呀')
```



CTF Categories for HKCERT 2022

- Web
- Cryptography
- Pwn (Binary Exploitation)
- Reverse Engineering
- Misc. (Forensic, etc.)



CTF Difficulty (HKCERT CTF)

Five difficulty level

- ★☆☆☆☆: Hands-on challenges
- ★★☆☆☆: Secondary
- ★★★☆☆:
 Tertiary
- ★★★★☆:
- ★★★★★: Challenge yourself!



Tools



Online Resource

- Wikis
 - <https://ctf101.org/>
 - <https://ctf-wiki.org/en/>
- Course
 - <https://pwn.college/>
- Wargame
 - <https://picoctf.org/>
- VTuber
 - <https://www.youtube.com/c/kurenaiif>



General Tools for CTF

- Virtual Machines
 - Hypervisor: VirtualBox, VMWare, ...
 - OS: Kali Linux, Ubuntu, ...
- Search Engine
 - Google, Bing, ...
 - Search for past write-up
- Basic Programming Skills
 - Python, C++, PHP, JavaScript, ...



General Tools for CTF

- General
 - netcat, pwntools
- Web
 - Web Browser, cURL, Burp Suite, ...
- Pwn / Reverse
 - IDA, Ghidra, Angr / z3, Radare2, ...
 - objdump, Vim, gdb, ...
- Cryptography
 - quipqiup, hashcat, pkcrack, yafu, ...
- Forensic / MISC
 - Wireshark, binwalk, stegsolve, ...

Training Platform

<https://training.hkcet22.pwnable.hk/>

Challenges

* New challenges are highlighted in green.

Leaked Secret

forensics, ★☆☆☆☆

Scratch Passcode

misc, ★☆☆☆☆

Base64 Encryption

crypto, ★☆☆☆☆

CrackMe Revenge

reverse, ★☆☆☆☆

Questionnaire on CTF Training

web, ★☆☆☆☆

Admin panel

web, ★☆☆☆☆

Shellcode Runner

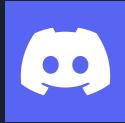
pwn, ★☆☆☆☆

Absolute Gambler

pwn, ★☆☆☆☆

Post-it

reverse, ★☆☆☆☆



Join our Discord channel

Discord will be used as an official communication channel

<https://discord.gg/V6QGvWCmDm>

Feel free to discuss, ask questions and learn together!



Join HKCERT CTF 2022!
<https://ctf.hkcet.org/>



Agenda

- Capture-the-Flag (CTF)
 - Why CTF?
 - What is CTF?
 - How to play CTF?
 - What can you get from playing CTF?
 - Some tips on the CTF!
- CTF challenges category: Web
 - How websites works
 - MitM yourself with Burp Suite
 - SQL injection
 - Tips and resources on web challenges
- CTF challenges category: Cryptography
 - Cryptography and your digital life
 - Classical cryptography: substitution cipher
 - Modern cryptography: RSA
 - Tips and resources on cryptography challenges

Q & A?

CTF 2022

香港 網絡 保安 新生代
Hong Kong Cyber Security New Generation

奪旗挑戰賽
Capture the Flag Challenge

Register now!

<https://ctf.hkcert.org/>

Sample Challenges:

<https://training.hkcert22.pwnable.hk/>

Discord channel:

<https://discord.gg/V6QGvWCmDm>



Break (5 min)

Web



Code of Ethics

- The exercises should be attempted ONLY INSIDE THE SECLUDED LAB ENVIRONMENT documented or provided. Please note that most of the attacks described in the slides would be ILLEGAL if attempted on machines that you do not have explicit permission to test and attack. The university, course lecturer, lab instructors, teaching assistants and the speaker assume no responsibility for any actions performed outside the secluded lab.
- The challenge server should be regarded as a hostile environment. You should not use your real information when attempting challenges.
- Do not intentionally disrupt other player who are working on the challenges or disclose private information you found on the challenge server (e.g. IP address of other players). Please let us know if you accidentally broke the challenge.

FAIL





Do you write / develop / deploy websites?

If no, nvm, but if you are here, you use webpages

- Mobile apps
- Web apps
 - Discord
 - Google Classroom
 - Google Doc
- Websites
 - Gov
 - Bank
 - School
 - Points card / Lucky draw



checkitin

@hackers room

HOME

RECORDS

OTHERS

ADMIN

>> Welcome to

Checkitin Member Area

Summary

Total: 178.5 hr(s)

Last Record: 1970-01-01 00:00:00

ID	Username	Year	Month	Hours
1	applelam	2011	12	3
2	applelam	2012	1	73
5	applelam	2012	2	103
8	applelam	2012	3	2.5

<- Previous Page

Page 1 of 1

Next Page ->

Welcome, Apple Lam!

Apple Lam

Site Administrator

Notification Messages

Settings Logout

ID: applelam

Total: 178.5 Hours

UID: 3

What to do?

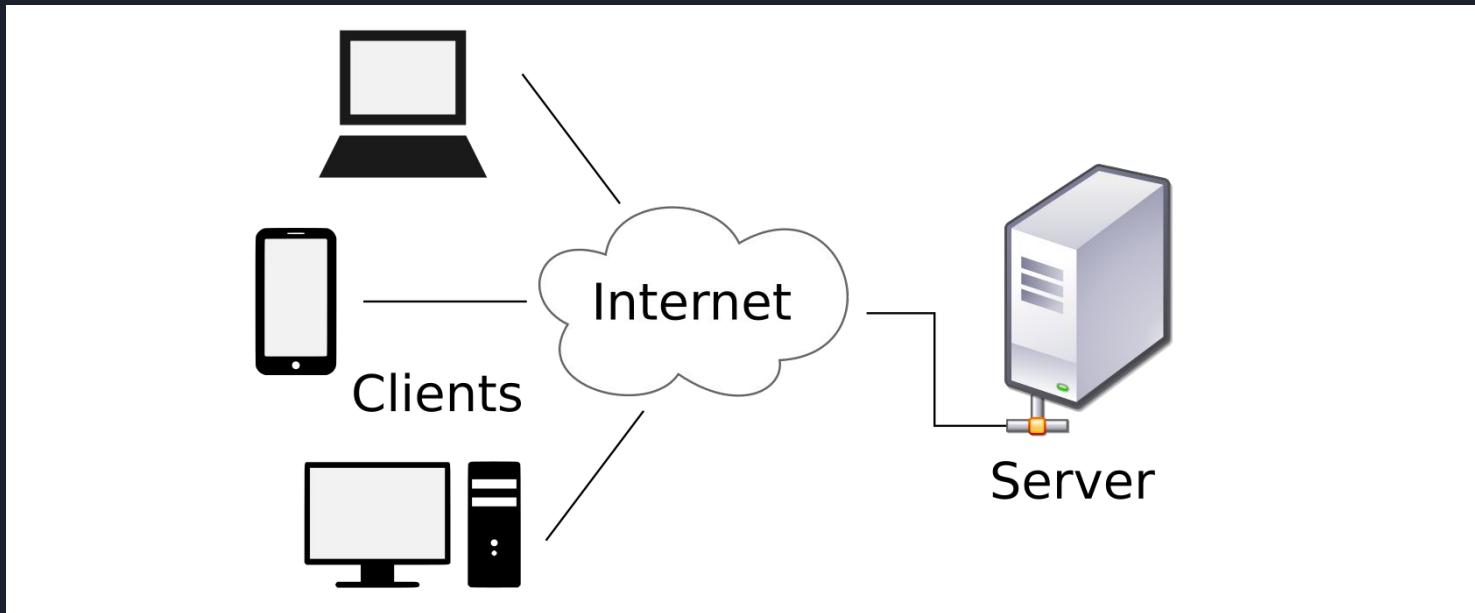
Suggest a idea

Join a project

Chat!

View Notice

Client-Server arch





What you see is not the whole picture

How to use the browser

- View source
- Developer tools
 - View network
 - View cookie



Demo: Natas0

<http://natas0.natas.labs.overthewire.org/>

Username: natas0

Password: natas0



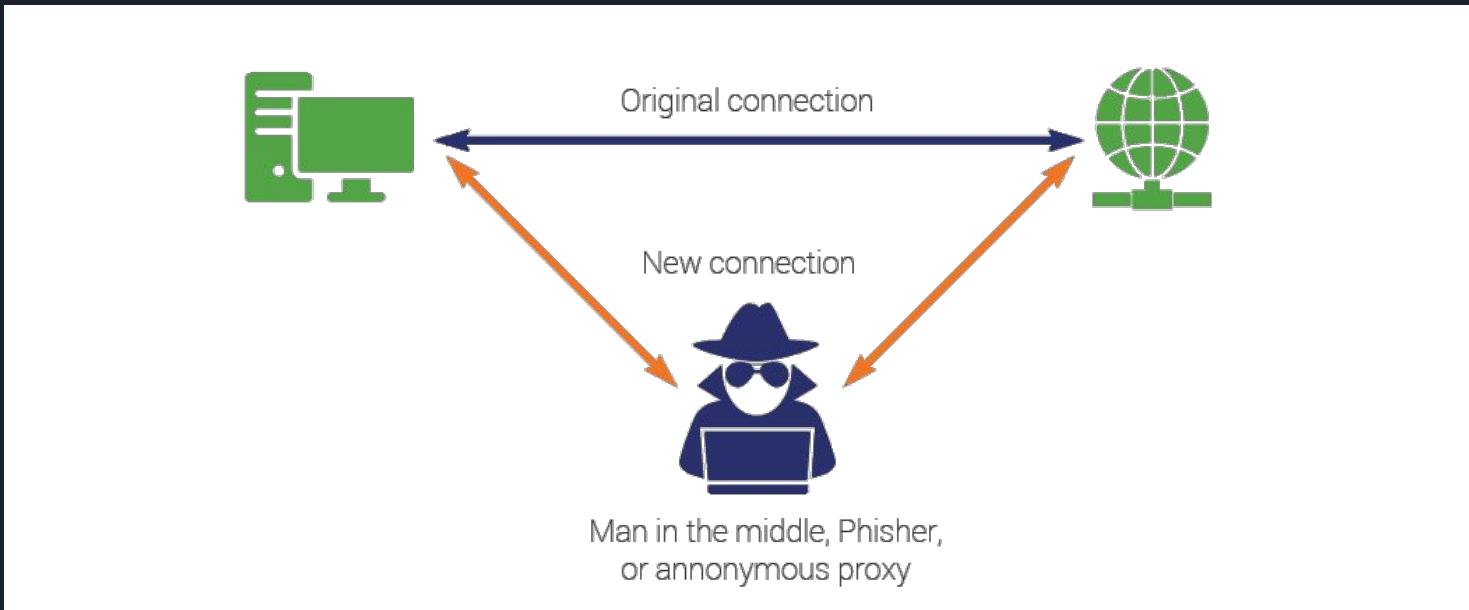
Demo: Natas1 (Web Proxy)

<http://natas1.natas.labs.overthewire.org/>

Username: natas1

Password: g9D9cREhs1qBKtcA2uocGHPfMZVzeFK6

Man-in-the-Middle (MitM): Web Proxy



Web Proxy to MitM yourself



We will be using Burp Suite today.



Demo: Training platform

<https://training.hkcet22.pwnable.hk/>

HTTP is stateless

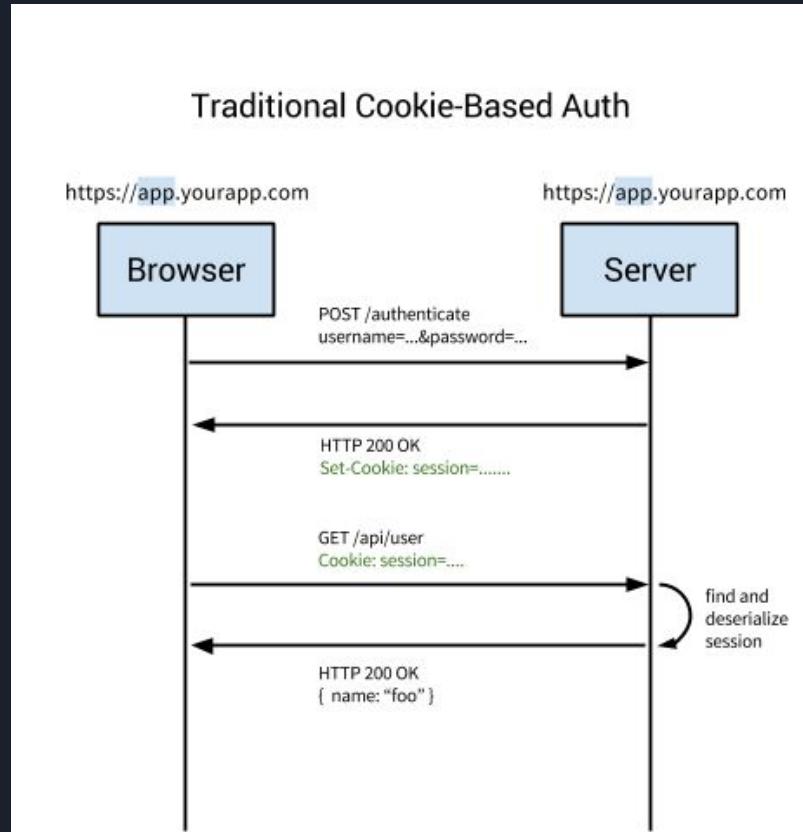
Request - Response

Cookie



AuthBypass: Normal Auth flow

1. Browser send username and password to server
2. Server check if the username and password token are correct, if so, return a token identifying the user
3. In subsequent requests, the browser (client) send the token to identify itself





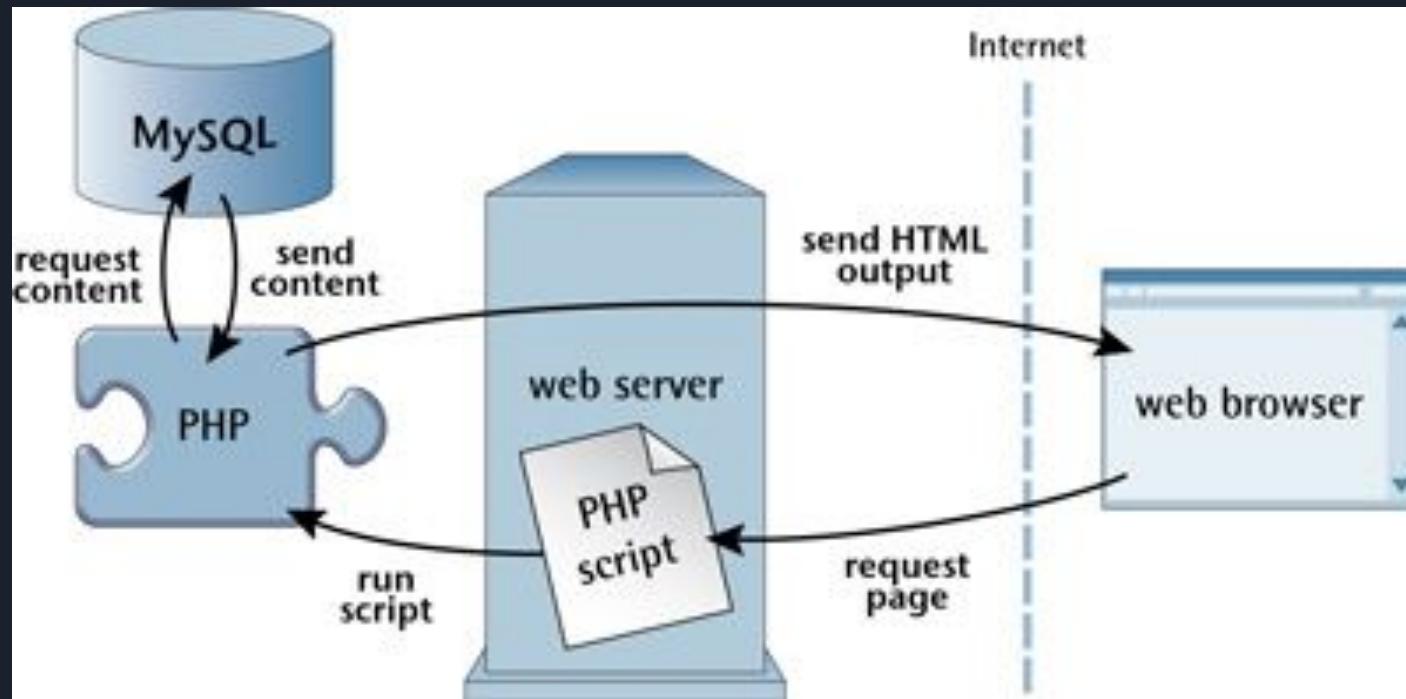
Demo: AuthBypass Natas5

<http://natas5.natas.labs.overthewire.org/>

Username: natas5

Password: Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD

Three-tier architecture



Demo: SQL injection (Natas14)

<http://natas14.natas.labs.overthewire.org/>

Username: natas14

Password: qPazSJBrmmU7UQJv17MHk1PGC4DxZMEP

	A	B	C	
1	username	password	名稱	
2	ringo	123456	Ringo Lam	
3	cousin	223456	Cousin Wu	
4	peter	323456	Peter Chan	
5				



SQL injection

When logging in, web application will query database for the username to check if the user exists and if the password is correct. For example (bad example):

```
SELECT * from users  
where username="ringo" and password="123456"
```

We can write anything into the blank.

Can we login to the system without knowing the password?

SQL injection

```
SELECT * from users
```

```
where username="" or True -- # and password="123456"
```

OR Truth Table		
A	B	Y
0	0	0
0	1	1
1	0	1
1	1	1

Other types of attacks

Server-side attacks

- SQL injection

Client-side attacks

- Cross-site scripting (XSS injection)

OWASP Top 10

- <https://owasp.org/www-project-top-ten/>

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey



Tips on Web challenges

Input - Process - Output

- Enumerate all inputs

Practices

- Natas - OverTheWire: Natas teaches the basics of serverside web-security
 - <https://overthewire.org/wargames/natas/>
- picoCTF - CMU Cybersecurity Competition
 - <https://picoctf.org/>

Writeups

- The write up of these challenges are readily available on the Internet, do search!! In doubt, feel free ask in discord!

Crypto



Crypto

- Not Cryptocurrency
- Cryptography: Secure communication under existence of adversary
 - Data is kept secret, with integrity (accurate and trustworthy)
- Cryptanalysis: Break cryptography



Why care?

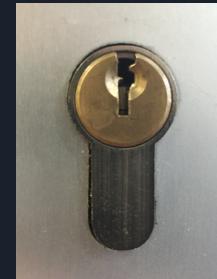
- If you have ever seen this lock  in your browser, then you have used cryptography (without even knowing it). The Transport Layer Security (SSL/TLS) protocol made use of crypto to make your connection secure **if done correctly**.
- Blockchain! The technology relies on cryptography.

- Basic building blocks:
 - Encoding/Decoding: Translating data between different forms
 - Encryption/Decryption: With a key(s), mangle (resp. unmangle) your message to become “ciphertext”
 - Digital Signature: Make sure a message is sent from a particular person, and ensures integrity (the message is not altered)
 - Hashing: “Summarizing” any data into a fixed-length string such that
 1. (Trapdoor) easy to compute but hard to reverse
 2. (Collision-resistant) hard to find two set of data that outputs the same hash
 3. (Avalanche) changing a little bit of data changes the hash by a lot
 - Pseudo-random number generator: Generate “random” numbers from deterministic seed such that it is unpredictable and uniformly random

Symmetric Crypto vs Public Key Crypto

Symmetric Key Cryptography (對稱加密)

- Use a key to lock and unlock a lock
- In crypto: just 1 key



Public Key Cryptography (公開金鑰密碼學)

- Padlock and key
- Use padlock to lock, key to unlock
- Can't use padlock to unlock, key to lock
- Everyone can obtain a padlock to lock, but only the person with the key can unlock
- In crypto: a public key that everyone has, private key that is kept... private

Classical Crypto

- 2000 years ago, until the age of computers
- Done with pen and paper
- Some make use of machines
 - Enigma machine used by the Nazis



Caesar Salad, yum.



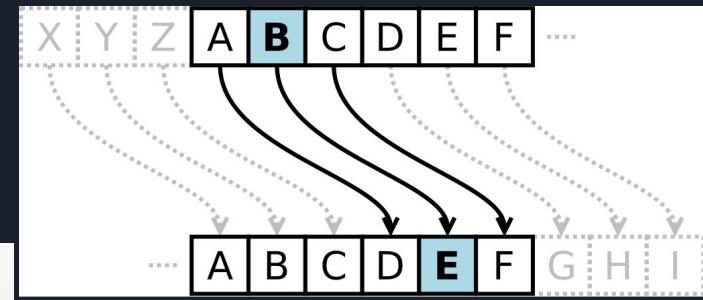
Enigma Variations

Classical Crypto

- 2000 years ago, until the age of computers
- Done with pen and paper
- Some make use of machines
 - Enigma machine used by the Nazis



Enigma Machine



Caesar Cipher, a cipher used by Caesar 2000 years ago.



Decrypt this.

Xu'tu kr sdtokguts dr crvu
Qrl akrx dzu tlcus okh sr hr p
O mlcc brnnpdnukd's xzod P'n dzpkapkg rm
Qrl xrlchk'd gud dzps mtrn okq rdzut glq
P elsd xokko ducc qrl zrx P'n muucpkg
Grddo noau qrl lkhutsdokh

Kuvut grkko gpvu qrl lj
Kuvut grkko cud qrl hrxk
Kuvut grkko tlk otrlhk okh husutd qrl
Kuvut grkko noau qrl btq
Kuvut grkko soq grrhwqu
Kuvut grkko ducc o cpu okh zltd qrl

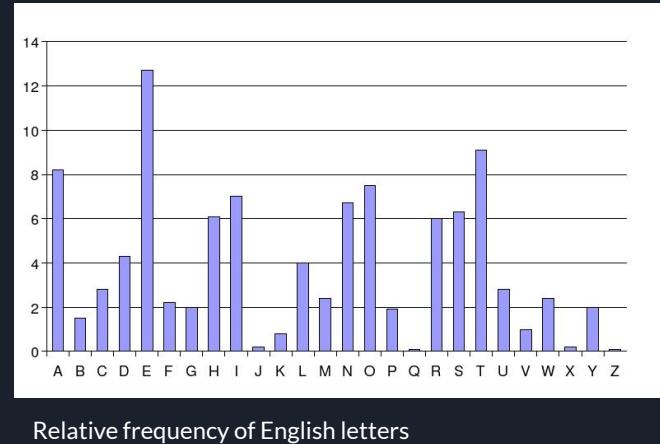
- Observation: This is probably a substitution cipher.
 - Symmetric key cryptography
 - A single “p” and “o” occurring, p occurring twice
 - Either translates to “I” or “A”?
 - a can’t really occur at the end of a sentence => “p” should be “I”!
 - => then “o” is “A”.
 - P’n => I’m, so “n” should be “M”.
- You can recover a lot just by reasoning on the English Language.

Xu'tu kr sdtokguts dr crvu
Qrl akrxuzu tlcus okh sr hr [p]
[O]mlcc brnnpdnukd's xzod [P'n]dzpkapkg rm
Qrl xrlchk'd gud dzps mtrn okq rdzut glq
[P]elsd xokko ducc qrl zrx p'n muucpkg
Grddo noau qrl lkhutsdokh

Kuvut grkko gpvu qrl lj
Kuvut grkko cud qrl hrxk
Kuvut grkko tlk otrlkoh husutd qrl
Kuvut grkko noau qrl btq
Kuvut grkko soq grrhwqu
Kuvut grkko ducc o cpu okh zltd qrl

Frequency Analysis

- Note that the distribution of English letters is not uniform.
- Thus, by comparing the distribution of letters in the problem text vs the normal English text, we can recover the original plaintext!
- <https://quipqiup.com/> 譏諷機楓



Uhhh...

Puzzle:

Kuvut grkko gpvu qrl lj
Kuvut grkko cud qrl hrxk
Kuvut grkko tlk otrkh okh husutd qrl
Kuvut grkko noau qrl btq
Kuvut grkko sqg grrhwqu
Kuvut grkko ducc o cpu okh zltd qrl

Clues: For example G=R QVV=THE

P=I O=A N=M

Solve

ⓘ automatically selected statistics mode; you can override by using the drop down menu next to the solve button.

0 -1.599 We're no strangers to love You know the rules and so do i A full commitment's what I'm thinking of You wouldn't get this from any other guy I just wanna tell you how I'm feeling Gotta make you understand Never gonna give you up Never gonna let you down Never gonna run around and desert you Never gonna make you cry Never gonna say goodbye Never gonna tell a lie and hurt you

1 -3.111 We've no utsanggesu to love For know the srleu and uo do i A prll commitment'u what I'm thinking op For worldn't get thiу psom anf othes grf I brut wanna tell for how I'm peeling Gotta make for rndesutand Neves gonna give for rj Neves gonna let for down Neves gonna srn asornd and deuest for Neves gonna make for csf Neves gonna uaf goodyfe Neves gonna tell a lie and hrst for

2 -3.130 We've no stcangeecs to lobe For know the crles and so do i A prll jommitempty's what I'm thinking op For worldn't get this pcom anf othec grf I urst wanna tell for how I'm peeling Gotta make for rndecstand Nebec gonna gibe for rv Nebec gonna let for down Nebec gonna crn acornd and desect for Nebec gonna make for jcf Nebec gonna saf goodyfe Nebec gonna tell a lie and hrct for

3 -3.134 We've no stcangeecs to lobe For know the crles and so do i A prll jommitempty's what I'm thinking op For worldn't get this pcom anf othec grf I vrst wanna tell for how I'm peeling Gotta make for rndecstand Nebec gonna gibe for rx Nebec gonna let for down Nebec gonna crn acornd and desect for Nebec gonna make for jcf Nebec gonna saf goodyfe Nebec gonna tell a lie and hrct for



Modern Cryptocurrency

- Smart Contracts
 - Solidity
 - Reentrancy
 - Scope
 - fallback functions



Modern Cryptography

- Uses computer to do
- Usually involve more maths
- Commonly used encryptions (AES, RSA, ...) are considered secure **if used correctly**



Known Attacks

- Known attacks exists for modern ciphers **in certain circumstances**.
- Do the formulation of the challenge match the **certain circumstances** for that attack?
- E.g.
 - Padding Oracle for AES only works for CBC mode.
 - Broadcast attack for RSA only works if you can get the unknown to be smaller than the product of moduli.
- Ad hoc attacks: figure it out yourself :)



RSA

Encryption using RSA is just first taking the plaintext m (a number) to the e -th power, then divide n and take the remainder as our ciphertext. (m is the plaintext)

$$m^e \div n = ??? \dots \text{ciphertext}$$

In math jargon we say

$$\text{ciphertext} = m^e \pmod{n}$$

For now you should know that n is a product of two large primes, and **the prime number itself must be kept secret, otherwise we can decrypt the ciphertexts easily.** n , on the other hand, is public knowledge. (n and e form the public key.)



Sum-O-Primes (picoCTF 2022)

We have so much faith in RSA we give you not just the product of the primes, but their sum as well!

<https://artifacts.picoctf.net/c/180/gen.py>

<https://artifacts.picoctf.net/c/180/output.txt>

They not only give you $n = p \cdot q$, but also give you $p+q$.

```
25  x = p + q
26  n = p * q
27
35  print(f'x = {x:x}')
36  print(f'n = {n:x}')
```

Maths... 😱

Since $(p+q)$ and (pq) is known, then we can construct the quadratic equation

$$x^2 - (p + q)x + pq = 0$$

And the solution of the equation is exactly p and q . (Why? Review your DSE Core Maths.)

Solution: left as exercise.



Tips

- Resources:
 - <https://cryptohack.org/> is a wargame containing basic crypto knowledge
 - <https://cryptopals.com/> is more for self-learning
- Learn your maths
 - Knowing existing attacks probably help, but instead of being a script kiddie,
 - Really understand how things work
- Write down everything
- Know what computer could do for you, and what you can only do by hand



Training Platform



Training Platform

<https://training.hkcet22.pwnable.hk/>

賽前遊樂場

語言 / Language: 中文 • English

挑戰

* 新挑戰以綠色熒光顯示

秘密流出

鑑證, ★☆☆☆☆

Scratch 密碼

其他, ★☆☆☆☆

龐然微站 II

密碼學, ★★★☆☆

CrackMe 復仇

逆向工程, ★★★☆☆

CTF 訓練問卷調查

互聯網, ★☆☆☆☆

管理員介面

互聯網, ★☆☆☆☆



Q&A

CTF 2022

香港 網絡 保安 新生代
Hong Kong Cyber Security New Generation

奪旗挑戰賽
Capture the Flag Challenge

Register now!

<https://ctf.hkcet.org/>

Sample Challenges:

<https://training.hkcet22.pwnable.hk/>

Discord channel:

<https://discord.gg/V6QGvWCmDm>

