Discord

10

**Miscellaneous**

Join our [Discord server](https://discord.gg/KRqsec6) to stay up-to-date on everything!

## Survey

### 10

Please give us some feedback, it'll help with HSCTF next year!

<https://forms.gle/63Ka4dVCEeeGeYhu6>

## Verbose

### 118

Written by: dwang

My friend sent me this file, but I don't understand what I can do with these 6 different characters...

#verbose.txt

Locked Up

132

**Miscellaneous** **cppio**

Written by: cppio

My friend gave me a zip file with the flag in it, but the zip file is encrypted. Can you help me open the zip file?

Hint

Try opening it. What happens?

#locked.zip

## Admin Pass

### 144

Written by: Weastie

Hey guys, found a super cool website at [http://misc.hsctf.com:8001](http://misc.hsctf.com:8001/)!

Edit: If the site is blocked by school filters, try

[http://misc.hsctf.com](http://misc.hsctf.com/) or [http://misc.hsctf.com:8080](http://misc.hsctf.com:8080/); both will work!

A Simple Conversation

159

**Miscellaneous** **cppio**

Written by: cppio

Someone on the internet wants to talk to you. Can you find out what they want?

nc misc.hsctf.com 9001

##### **Hint**

×

Are you sure it's run the way you expect?

#talk.py

The Real Reversal

276

**Miscellaneous** **cppio**

Written by: cppio

My friend gave me some fancy text, but it was reversed, and so I tried to reverse it but I think I messed it up further. Can you find out what the text says?

##### **Hint**

×

What happens if the file is reversed?

#reversed.txt

## Broken GPS

### 282

Written by: Disha and Shray

Ella is following a broken GPS. The GPS tells her to move in the opposite direction than the one she should be travelling in to get to her destination, and she follows her GPS exactly. For instance, every time she is supposed to move west, the GPS tells her to move east and she does so. Eventually she ends up in a totally different place than her intended location. What is the shortest distance between these two points? Assume that she moves one unit every time a direction is specified. For instance, if the GPS tells her to move "north," she moves one unit north. If the GPS tells her to move "northwest," then she moves one unit north and one unit west.

# **Input Format:**

You will receive a text file with N directions provided to her by the GPS (the ones that she will be following) (1<=N<=1000). The first line in the file will be N, and each consequent line will contain a single direction: “north,” “south,” “east,” “west,” “northwest,” “northeast,” “southwest,” or “southeast.”

# **Output Format:**

Round your answer to the nearest whole number and then divide by 26. Discard the quotient (mod 26). Each possible remainder corresponds to a letter in the alphabet. (0=a, 1=b… 25=z).

Find the letter for each test case and string them together. The result is the flag. (For instance, a, b, c becomes “abc”). Remember to use the flag format and keep all letters lowercase!

#input.zip

## Hidden Flag

### 290

Written by: Tux

This image seems wrong.....did Keith lose the key **again**?

#chall.png

## Keith Bot

### 410

Written by: dwang

Keith made a Discord bot so he could run commands on the go, but there were some bugs

DM Keith Bot#3149 (found in the Discord server)

Note: The flag is in flag.txt

#bot.py #eval.py

Broken REPL

411

**Miscellaneous**

Written by: cppio

My friend says that there is a bug in my REPL. Can you help me find it?

nc misc.hsctf.com 8550

##### **Hint**

×

What happens to the given input?

#repl.py

## 64+word

### 423

Written by: Tux

Help Keith with his word search!!!! Where is the flag?

#64word.py

JSON Info

428

**Miscellaneous** **cppio**

Written by: cppio

I made a simple program to analyze my JSON files.

nc misc.hsctf.com 9999

Note: You must send an EOF (normally Ctrl-D) to get a response. If netcat quits before showing any response, you may have to use socat.

socat - tcp:misc.hsctf.com:9999

Alternatively, try netcat's -q flag.

nc -q 1 misc.hsctf.com 9999

##### **Hint**

×

Try to make it fail.

English Sucks

487

**Miscellaneous** **cppio**

Written by: cppio

English is such a confusing language. Can you help me understand it?

nc misc.hsctf.com 9988

##### **Hint**

×

Watch out for the order of the output.

#mt.cpp

Tasty Snack

494

**Miscellaneous** **cppio**

Written by: cppio

I have just discovered the tastiest snack in the entire universe.

nc misc.hsctf.com 9977

##### **Hint**

×

Read the pickle documentation and source code.

## Reverse Search Algorithm

### 131

Written by: Tux

# **Reverse Search Algorithm**

WWPHSN students, gotta get these points to boost your grade.

n = 561985565696052620466091856149686893774419565625295691069663316673425409620917583731032457879432617979438142137

e = 65537

c = 328055279212128616898203809983039708787490384650725890748576927208883055381430000756624369636820903704775835777

## Super Secure System

### 191

Written by: Tux

Keith made a SUPER SECURE SYSTEM!!! He claims it is so secure as long as he doesn't reuse his key...

nc crypto.hsctf.com 8111

## A Lost Cause

### 198

Written by: Disha Name Credits: Shray

Pirate Keith loves cryptography and has protected his treasure with a very annoying caesar shift. He has witten “CGULKVIPFRGDOOCSJTRRVMORCQDZG” on his treasure chest and has left a piece of paper with the following message: “every subsequent letter is shifted one less than the previous.” Knowing this, can you unlock Pirate Keith’s treasure chest?

Massive RSA

257

**Cryptography** **cppio**

Written by: cppio

I was scared that my RSA would be broken, so I made sure that the numbers were massive.

##### **Hint**

×

The numbers are really big...

#massive.txt

Really Secure Algorithm

316

**Cryptography** **cppio**

Written by: cppio

I heard about RSA, so I took a go at implementing it.

##### **Hint**

×

The numbers are decently large...

#secure.txt

## Welcome to Crypto Land

### 340

Written by: Tux

Crypto land is fun! Decrypt:

KZ6UaztNnau6z39oMHUu8UTvdmq1bhob3CcEFdWXRfxJqdUAiNep4pkvkAZUSn9CvEvPNT5r2zt6JPg9bVBPYuTW4xr8v2PuPxVuCT6MLJWDJp84

Tux's Kitchen

405

Written by: Tux

I need to bake it!

nc crypto.hsctf.com 8112

#problem.py

## Bomb

### 452

Written by: Tux

Keith found a weird message on his desk along with a drawing:

JGYJZ NOXZX QZRUQ KNTDN UJWIA ISVIN PFKIR VWKWC UXEBH RFHDI NMOGQ BPRHW CXGAC ARBUN IHOWH QDDGL BBZYH HEJMV RBLJH CLHYP FSAAA KNRPX IKSNX QASGI XBMNP FLAFA KFEGV YWYUN JGBHH QDLZP UJWMO CCEUL YFIHR GTCOZ GEQML VFUAV URXUU BBGCI YZJQQ ROQFU SJDVR JILAJ XYCBC IGATK LQMAP UDPCG ONWFV MHBEC CLBLP JHZJN HMDNY YATIL FQSND AOCAM MGVRZ FEVKL CEDMG AIWXG QPCBI VTVZU HQGFD ZJICI EIWLP IFKAB LNVZI XRZTR SLGCA SZPFF HGBUK JAXNN JHUSV UFPIM ZZLAW SYOHB TOLRF KWANX FNEFD XXLNR LLGYS VTGXP NJQMC WAKRP JKWDP WVTNP WRYEJ RSODI QDYOQ DJDBI SLAVB UPDDR ATHYG ANJQR XPGFM FAMJR ZSJHC SYWQQ VBIHX XCQFW XZBUH ZRXWV TPESM EGVVY PBJSS

Reflector: B

Rotors: 3,2,4

Crib: the secret to life is

Keith is very confused. Help Keith find out what the message means.

nc crypto.hsctf.com 8100

#bomb.png

## Spooky ECC

### 457

Written by ValarDragon

Bigger curves means better right?

#Intercept.txt

#problem.sage

## Marginally More Spooky ECC

### 473

Written by ValarDragon

Now marginally more spooky!

#intercept.txt

#problem.sage

## Multiplication Service

### 490

Written by ValarDragon

Multiplication is safe, right?

nc crypto.hsctf.com 8113

* Intended solution runs well under < 30 seconds on my laptop

#problem.sage

## Intro to Netcat

### 51

Written by: Ptomerty

Hey there! This challenge is a quick introduction to netcat and how to use it. Netcat is a program that will help you "talk" with many of our challenges, especially pwn and misc. To begin, Windows users should download this file:

[Mirror 1 (may have DLL errors)](https://drive.google.com/open?id=1wwT0vjzEj00F_NFGG0QVlNdn9BL8W9SD)

[Alternative download that might work](https://joncraton.org/blog/46/netcat-for-windows/)

[Nmap download; will get flagged by school filters](https://nmap.org/download.html)

Extract the file, then open a command prompt and navigate to the directory using cd <download-directory>. From there, you can run nc misc.hsctf.com 1111 to get your first flag.

Have fun!

#nc.zip

## Return to Sender

### 170

Written by: Ptomerty

Who knew the USPS could lose a letter so many times?

nc pwn.hsctf.com 1234

Note: If you're trying to use python or a similar program to run your exploit, make sure to keep stdin alive with cat, like this: (python; cat -) | nc pwn.hsctf.com <port>

6/3/19 7:34 AM: Updated binary, SHA-1:104fb76c3318fb44130c4a8ee50ac1a2f52d4082 return-to-sender

##### **Hint**

×

This might come in handy: <https://en.wikipedia.org/wiki/Stack_buffer_overflow>

#return-to-sender.c

#return-to-sender

## Combo Chain Lite

### 245

Written by: Ptomerty

Training wheels!

nc pwn.hsctf.com 3131

Note: If you're trying to use python or a similar program to run your exploit, make sure to keep stdin alive with cat, like this: (python; cat -) | nc pwn.hsctf.com <port>

##### **Hint**

×

What's a ROP?

#combo-chain-lite.c

#combo-chain-lite

## Storytime

### 334

Written by: Tux

I want a story!!!

nc pwn.hsctf.com 3333

#storytime

## Combo Chain

### 368

Written by: Ptomerty

I've been really into Super Smash Brothers Melee lately...

nc pwn.hsctf.com 2345

Note: If you're trying to use python or a similar program to run your exploit, make sure to keep stdin alive with cat, like this: (python; cat -) | nc pwn.hsctf.com <port>

libc SHA-1: 238e834fc5baa8094f5db0cde465385917be4c6a libc.so.6 libc6\_2.23-0ubuntu11\_amd64

6/3/19 7:35 AM: Binary updated, SHA-1:0bf0640256566d2505113f485949ec96f1cd0bb9 combo-chain

##### **Hint**

×

What's a ROP?

#combo-chain

#combo-chain.c

## Bit

### 401

Written by: Arinerron

Just get the flippin' flag.

nc pwn.hsctf.com 4444

#bit

## Caesar's Revenge

### 431

Written by: Ptomerty

Julius Caesar's back, and he's not happy...

nc pwn.hsctf.com 4567

Note: If you're trying to use python or a similar program to run your exploit, make sure to keep stdin alive with cat, like this: (python; cat -) | nc pwn.hsctf.com <port>

6/3/19 7:36 AM: Binary updated, SHA-1:42280638b188cea498e7b6c55462dbf0351056f4 caesars-revenge

#caesars-revenge.c

#caesars-revenge

## Byte

### 431

Written by: Arinerron

Free arbitrary null write primitive, get the flag

nc pwn.hsctf.com 6666

Binary updated without breaking changes: 5223e3fe7827c664a5adc5e0fa6f2c0ced8abaaf byte

#byte

## Aria Writer

### 452

Written by: NotDeGhost

Rob wants to write a song, but he doesn't know what to say. Help him write his way to a shell.

nc pwn.hsctf.com 2222

#aria-writer

#libc-2.27.zip

## Aria Writer v3

### 468

Written by NotDeGhost

After all that writing, Rob's gone blind. He still needs to finish this song though :(

nc pwn.hsctf.com 2468

#aria-writer-v3

#libc-2.27.zip

## Hard Heap

### 480

Written by: poortho

Remember halcyon heap? Well, it was too easy so I made it hard ;)

nc pwn.hsctf.com 5555

#hard-heap

#libc.so.6.zip

## A Byte

### 180

Written by: ItzSomebody

Just one byte makes all the difference.

#a-byte

License

252

Written by: ItzSomebody

Description: Keith made a cool license-checking program but he forgot the flag he used to create the key! To make matters worse, he lost the source code and stripped the binary for his license-generator program. Can you help Keith recover his flag? All he knows is:

* The license key is 4-EZF2M-7O5F4-V9P7O-EVFDP-E4VDO-O
* He put his name (in the form of 'k3ith') as the first part of the flag
* There are 3 underscores
* The flag is in the format hsctf{}
* The flag doesn't have random character sequences (you should be able to read the entire flag easily).
* The flag only contains lowercase English letters and numbers.
* The generator might produce the same keys for different inputs because Keith was too lazy to write the algorithm properly.

#license

## DaHeck

### 295

Written by: ItzSomebody

Unicode? ...da heck?

#DaHeck.java

## VirtualJava

### 357

Written by: ItzSomebody

There's nothing like executing my own code in Java in my own special way.

#VirtualJava.java

## Bitecode

### 377

Written by: ItzSomebody

Keith went crazy and told me to work on the compiled form of Java instead of the source code. Unfortunately, all decompilers I've tried crash on attempting to decompile. Can you help out?

#BiteCode.class

## I Thought Trig Was Really Easy

### 377

Written by: v1sanjay

After finishing a hard lesson in geometry class, Keith decided that he wanted to put your understanding of trig and python to the test. Can you solve his challenge?

##### **Hint**

×

Align each letter of input with its corresponding group of characters for output.

#trig\_is\_really\_hard.py

## Tux Talk Show 2019

### 411

Written by: Tux

Tux Talk Show 2019. Yes, this is trash.

nc rev.hsctf.com 6767

#trash

## Paint

### 411

Written by: dwang

Windows? :thonk:

##### **Hint**

×

dll injection? (for the fun and easy route)

#paint.dll

## Forgot Your Password?

### 467

Written by: Ptomerty

Help! I got this new lock for Christmas, but I've forgotten the first two values. I know the last value is hsctfissocoolwow. I also managed to grab a copy of their secret key generator. Can you help me out?

Note: submit the first two combo values separated by a space in hex format.

#generator.py

## Chicken Crossing

### 53

Written by: Jeremy Hui

Keith is watching chickens cross a road in his grandfather’s farm. He once heard from his grandfather that there was something significant about this behavior, but he can’t figure out why. Help Keith discover what the chickens are doing from this seemingly simple behavior.

#hsctf-chicken\_crossing.jpg

## Cool Image

### 101

**Forensics** **cppio**

Written by: cppio

My friend told me he found a really cool image, but I couldn't open it. Can you help me access the image?

#hsctf-chicken\_crossing.jpg

##### **Hint**

×

Is the file really a PDF?

#cool.pdf

## Cool Image 2

### 106

**Forensics** **cppio**

Written by: cppio

My friend sent me this image, but I can't open it. Can you help me open the image?

##### **Hint**

×

Try looking at the raw contents of the file.

#cool.png

## Slap

### 109

Written by: Shray Vats, Jasper

Don't get slapped too hard.

#slap.jpg

## Logo Sucks Bad

### 168

Written by: Tux

This logo sucks bad.

#logo.png

## Fish

### 237

Written by: Tux

I got a weird image from some fish. What is this?

#fish.jpg

## Double Trouble

### 399

Written by: Shray Vats

What is a koala anyway?

#koala.png

#koala2.png

## Skywriting v2

### 461

Written by: NotDeGhost

Fortnite Battle Royale contains a variety of weapons and this page lists every weapon in Fortnite along with their weapon stats like damage, DPS, fire rate, magazine size, and reload speed.

Note: This was a throwback to the original skywriting which included many big leaps of intuition.

This problem has now been modified to make it more doable.

Hint 1: I like xoring together the names of "Rifle"s together. Hint 2: Try googling the first sentence of this problem.

Flag: LjUlMiA9LxI1GTUTNiodECAtUSx5YxY4

##### **Hint**

×

From each name derives a key, equal to chr \* len(name)where chr is some char and name is the name. XOR all the keys w/ the cipher to get the flag.

## Inspect Me

### 51

Written by: dwang

Keith's little brother messed up some things...

[https://inspect-me.web.chal.hsctf.com](https://inspect-me.web.chal.hsctf.com/)

Note: There are 3 parts to the flag!

##### **Hint**

×

Right click does not work intentionally

## Agent Keith

### 101

Written by: dwang

Keith was looking at some old browsers and made a site to hold his flag.

[https://agent-keith.web.chal.hsctf.com](https://agent-keith.web.chal.hsctf.com/)

##### **Hint**

×

Check the source?

## S-Q-L

### 101

Written by: dwang

Keith keeps trying to keep his flag safe. This time, he used a database and some PHP.

<https://s-q-l.web.chal.hsctf.com/>

## The Quest

### 102

**Web** **cppio**

Written by: cppio

You think you are worthy of obtaining the flag? Try your hand at [The Quest to Obtain the Flag](https://forms.gle/7pyAWuG3GvYL443NA).

##### **Hint**

×

Maybe you don't have to complete the challenges...

## Keith Logger

### 216

Written by: dwang

Keith is up to some evil stuff! Can you figure out what he's doing and find the flag?

Note: nothing is actually saved

#extension.crx

## md5--

### 233

Written by: dwang

md5-- == md4

https://md5--.web.chal.hsctf.com

Note: If the link above doesn't work, try [https://md4.web.chal.hsctf.com](https://md4.web.chal.hsctf.com/)

## Accessible Rich Internet Applications

### 241

Written by: NotDeGhost

A very considerate fellow, Rob believes that accessibility is very important!

NOTE: The flag for this challenge starts with flag{ instead of hsctf{

#index.html

## Networked Password

### 317

**Web** **cppio**

Written by: cppio

Storing passwords on my own server seemed unsafe, so I stored it on a seperate one instead. However, the connection between them is very slow and I have no idea why.

<https://networked-password.web.chal.hsctf.com/>

##### **Hint**

×

You know the flag format.