Intro to *nix and Shells

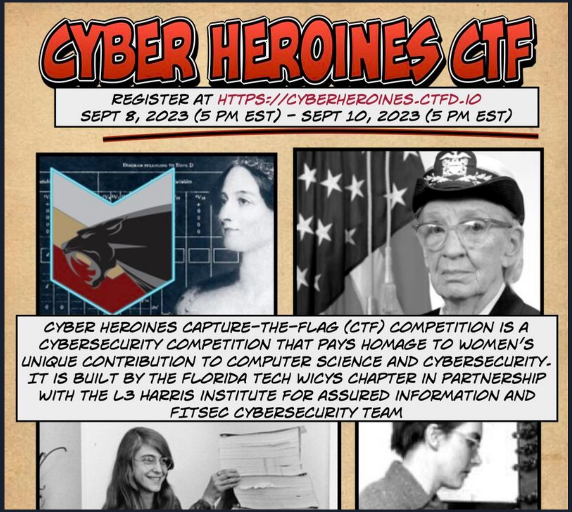
Level 0x01: The Shell

Quick Overview

- Upcoming Events
- Shell Commands
- Linux

Cyber Heroines CTF

- Online CTF
  - CSAW ‘24 Quals
  - CSAW ctfd page
  - Starts: Friday Sept 6, 2024 NOON EST
  - Ends: Sunday Sept 8, 2024 NOON EST
  - Designed as an entry-level, jeopardy-style CTF, this competition is for students who are trying to break into the field of security, as well as for advanced students and industry professionals who want to practice their skills.
- Sponsored by Vector35



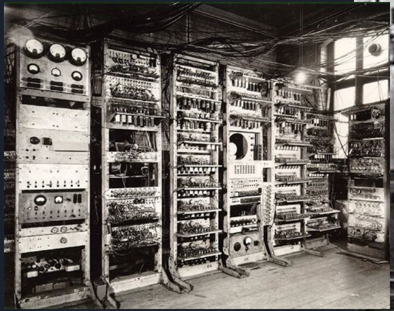
CYBER HEROINES CTF

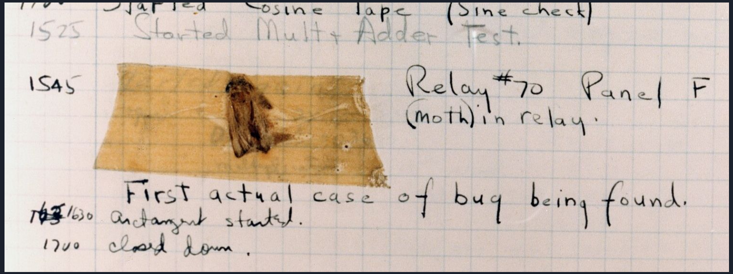
REGISTER AT HTTPS://CYBERHEROINES.CTFD.IO
SEPT 8, 2023 (5 PM EST) - SEPT 10, 2023 (5 PM EST)

CYBER HEROINES CAPTURE-THE-FLAG (CTF) COMPETITION IS A CYBERSECURITY COMPETITION THAT PAYS HOMAGE TO WOMEN'S UNIQUE CONTRIBUTION TO COMPUTER SCIENCE AND CYBERSECURITY. IT IS BUILT BY THE FLORIDA TECH WICYS CHAPTER IN PARTNERSHIP WITH THE L3 HARRIS INSTITUTE FOR ASSURED INFORMATION AND FITSEC CYBERSECURITY TEAM

Hacker History - Grace Hopper

- Joined US Navy at age 34 in WWII
- Mark I computer programmers
- Invented A-0 programming language
  - One of the first compiled languages
  - One of the first to have English terms
- Worked on team that created COBOL
- Retired from Navy in 1986 at age 79
- USS Hopper is Guided Missile Destroyer
- Received Medal of Freedom in 2016 (posthumously)





Started Cosine Tape (Sine check)

1525 Started Mult + Adder Test.

1545 Relay #70 Panel F (moth) in relay.

First actual case of bug being found.

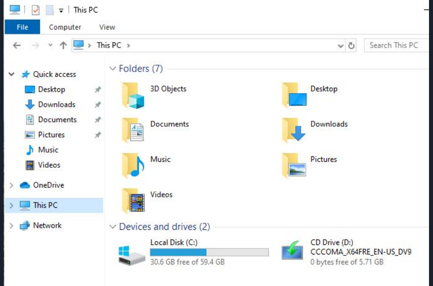
~~143~~ 1630 Arctangent started.

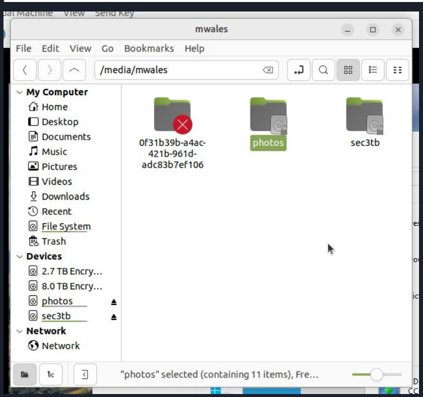
1700 closed down.

What is a nano-second?

Filesystem

- Filesystem is usually a directory of files on your SSD / hard disk
  - Windows: C: D: (drive letters)
  - *nix: / /mnt /media/cdrom
- Each directory can have thousands of files and other directories





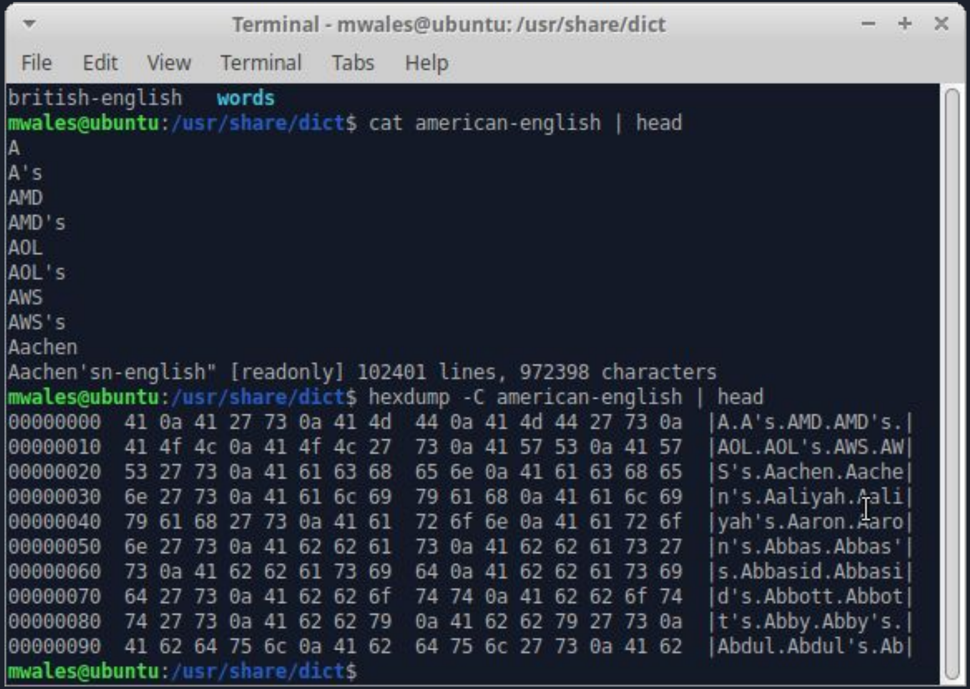
Linux Command	Windows/DOS Command	Explanation
`pwd`	`cwd`	**P**resent **w**orking **d**irectory (or **c**urrent **w**orking **d**irectory)
`ls`	`dir`	**Lis**t contents of a directory

Directory Commands

Linux	Windows / DOS	Explanation
`mkdir DIRECTORY`	`mkdir`	**M**a**k**es a new **dir**ectory
`cd DIRECTORY`	`cd`	**C**hanges **d**irectory
`cd ..`	`cd ..`	Changes to the parent directory
`rmdir DIRECTORY`	`rmdir`	**R**e**m**oves a **dir**ectory (must be empty)
`ls`	`dir`	Lists directory contents
`tree`	`dirtree`	Lists all files / subdirectories

Files

- Common contents of a file
  - Text
  - Executable Programs
  - Databases (SQL)
  - Compressed Archive
  - Images
  - Word document
    - Compressed Archive
    - Text
    - Images



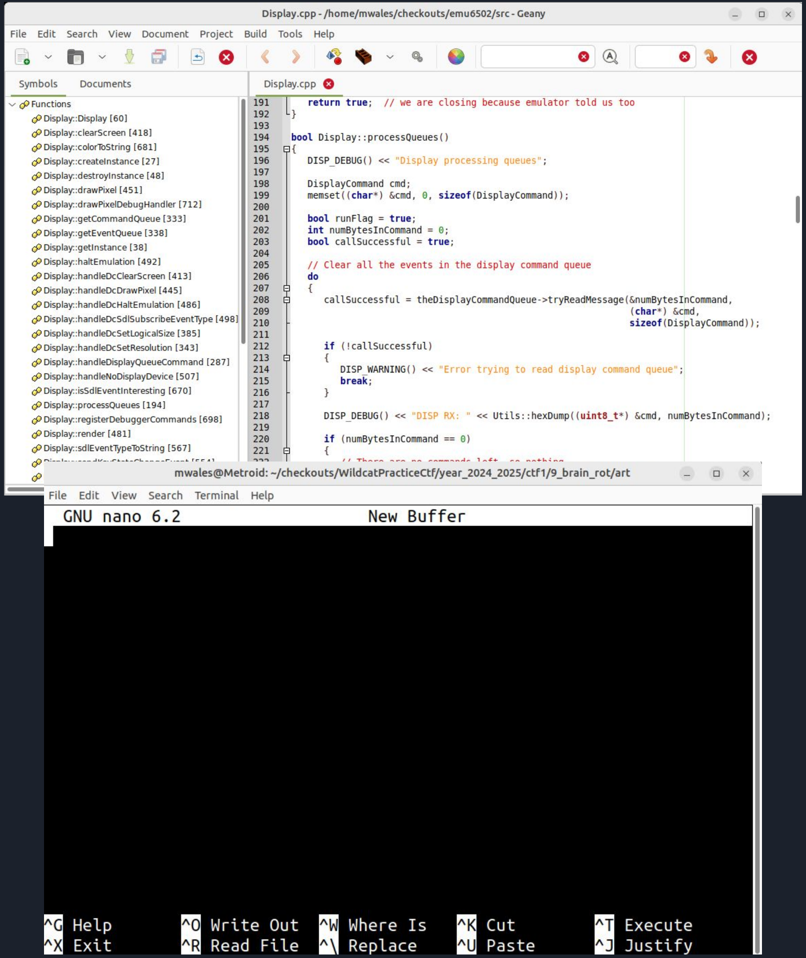
```
british-english   words
mwales@ubuntu:/usr/share/dict$ cat american-english | head
A
A's
AMD
AMD's
AOL
AOL's
AWS
AWS's
Aachen
Aachen'sn-english" [readonly] 102401 lines, 972398 characters
mwales@ubuntu:/usr/share/dict$ hexdump -C american-english | head
00000000  41 0a 41 27 73 0a 41 4d  44 0a 41 4d 44 27 73 0a  |A.A's.AMD.AMD's.|
00000010  41 4f 4c 0a 41 4f 4c 27  73 0a 41 57 53 0a 41 57  |AOL.AOL's.AWS.AW|
00000020  53 27 73 0a 41 61 63 68  65 6e 0a 41 61 63 68 65  |S's.Aachen.Aache|
00000030  6e 27 73 0a 41 61 6c 69  79 61 68 0a 41 61 6c 69  |n's.Aaliyah.Aali|
00000040  79 61 68 27 73 0a 41 61  72 6f 6e 0a 41 61 72 6f  |yah's.Aaron.Aaro|
00000050  6e 27 73 0a 41 62 62 61  73 0a 41 62 62 61 73 27  |n's.Abbas.Abbas'|
00000060  73 0a 41 62 62 61 73 69  64 0a 41 62 62 61 73 69  |s.Abbasid.Abbasi|
00000070  64 27 73 0a 41 62 62 6f  74 74 0a 41 62 62 6f 74  |d's.Abbott.Abbot|
00000080  74 27 73 0a 41 62 62 79  0a 41 62 62 79 27 73 0a  |t's.Abby.Abby's.|
00000090  41 62 64 75 6c 0a 41 62  64 75 6c 27 73 0a 41 62  |Abdul.Abdul's.Ab|
mwales@ubuntu:/usr/share/dict$
```

File Commands

Linux	Windows / DOS	Explanation
`touch FILE`	`copy con FILE`	Creates a blank file
`cat FILE`	`type FILE [FILE2 …]`	Displays contents of a file, or con**cat**enates files
`head FILE`		Displays beginning (the **head**) of a file
`tail FILE`		Displays ending of a file (the **tail**)
`hexdump -C FILE`		Displays contents of a binary in **hex**adecimal
`file FILE`		Tells you what type of a file

Editors

- GUI
  - Simple: write text, save to a file
    - Gedit, Mousepad, Notepad
  - Coding: automatic coloring, auto-complete
    - Geany
    - Sublime ($)
    - Atom
  - IDE: integrated development environment
    - Qt Creator
    - Visual Studio
    - CLion
- Command Line
  - nano, pico
  - vi / vim, emacs


Display.cpp - /home/mwales/checkouts/emu6502/src - Geany
File
Edit
Search
View
Document
Project
Build
Tools
Help
Symbols
Documents
Display.cpp
mwales@Metroid: ~/checkouts/WildcatPracticeCtf/year_2024_2025/ctf1/9_brain_rot/art
File
Edit
View
Search
Terminal
Help

Functions
- Display::Display [60]
- Display::clearScreen [418]
- Display::colorToString [681]
- Display::createInstance [27]
- Display::destroyInstance [48]
- Display::drawPixel [451]
- Display::drawPixelDebugHandler [712]
- Display::getCommandQueue [333]
- Display::getEventQueue [338]
- Display::getInstance [38]
- Display::haltEmulation [492]
- Display::handleDcClearScreen [413]
- Display::handleDcDrawPixel [445]
- Display::handleDcHaltEmulation [486]
- Display::handleDcSdlSubscribeEventType [498]
- Display::handleDcSetLogicalSize [385]
- Display::handleDcSetResolution [343]
- Display::handleDisplayQueueCommand [287]
- Display::handleNoDisplayDevice [507]
- Display::isSdlEventInteresting [670]
- Display::processQueues [194]
- Display::registerDebuggerCommands [698]
- Display::render [481]
- Display::sdlEventTypeToString [567]

```
   return true;  // we are closing because emulator told us too
}

bool Display::processQueues()
{
   DISP_DEBUG() << "Display processing queues";

   DisplayCommand cmd;
   memset((char*) &cmd, 0, sizeof(DisplayCommand));

   bool runFlag = true;
   int numBytesInCommand = 0;
   bool callSuccessful = true;

   // Clear all the events in the display command queue
   do
   {
      callSuccessful = theDisplayCommandQueue->tryReadMessage(&numBytesInCommand,
                                                              (char*) &cmd,
                                                              sizeof(DisplayCommand));

      if (!callSuccessful)
      {
         DISP_WARNING() << "Error trying to read display command queue";
         break;
      }

      DISP_DEBUG() << "DISP RX: " << Utils::hexDump((uint8_t*) &cmd, numBytesInCommand);

      if (numBytesInCommand == 0)
      {
```

```
  GNU nano 6.2                     New Buffer













^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

File Commands

Command	Explanation
`strings FILE`	Prints out printable strings of a binary file
`sort [FILE]`	Prints lines in alphabetical order
`uniq [FILE]`	Removes redundant lines out output
`wc [FILE]`	**W**ord **c**ount. Counts number of words in a file
`dos2unix / unix2dos [FILE]`	Converts file line endings
`more / less [FILE]`	Shows output 1 page at a time
`grep needle [FILEs]`	Searches for a string

Standard Input / Output

- 3 file descriptors open by CLI application
  - 0 = stdin (standard input)
  - 1 = stdout (standard output)
  - 2 = stderr (standard error)
- Pipes (|) can be used to connect output from one application to input of another application

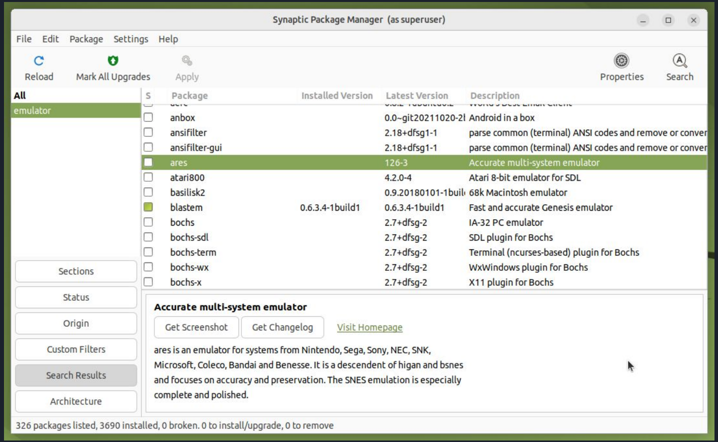
```
strings somefile | grep -i password

cat logfile | sort | uniq
```

I/O Redirection

- Using “`> file.txt`” after a command causes output from stdout to be redirected into a file
  - You won’t be able to see it on screen
  - stderr will still be displayed
- Using “`2> file.txt`” after a command causes stderr to be redirected into file
- `tee` will write standard output to a file and also write it to the screen
  - Ex: `./myprogram arg1 arg2 | tee logfile.txt`
- >> will append to existing file, > overwrites it

Packages

Easy to search for and add new software (like Steam store, but everything is free)



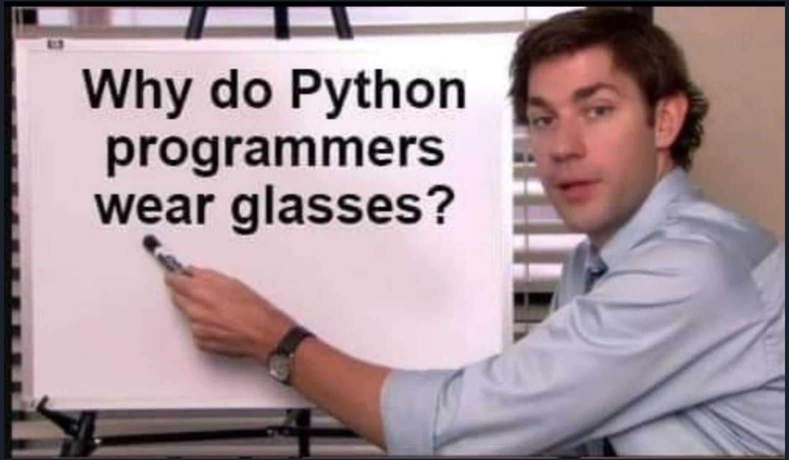
S	Package	Installed Version	Latest Version	Description
□	anbox		0.0~git20211020-2l	Android in a box
□	ansifilter		2.18+dfsg1-1	parse common (terminal) ANSI codes and remove or conver
□	ansifilter-gui		2.18+dfsg1-1	parse common (terminal) ANSI codes and remove or conver
□	ares		126-3	Accurate multi-system emulator
□	atari800		4.2.0-4	Atari 8-bit emulator for SDL
□	basilisk2		0.9.20180101-1buil	68k Macintosh emulator
🟩	blastem	0.6.3.4-1build1	0.6.3.4-1build1	Fast and accurate Genesis emulator
□	bochs		2.7+dfsg-2	IA-32 PC emulator
□	bochs-sdl		2.7+dfsg-2	SDL plugin for Bochs
□	bochs-term		2.7+dfsg-2	Terminal (ncurses-based) plugin for Bochs
□	bochs-wx		2.7+dfsg-2	WxWindows plugin for Bochs
□	bochs-x		2.7+dfsg-2	X11 plugin for Bochs

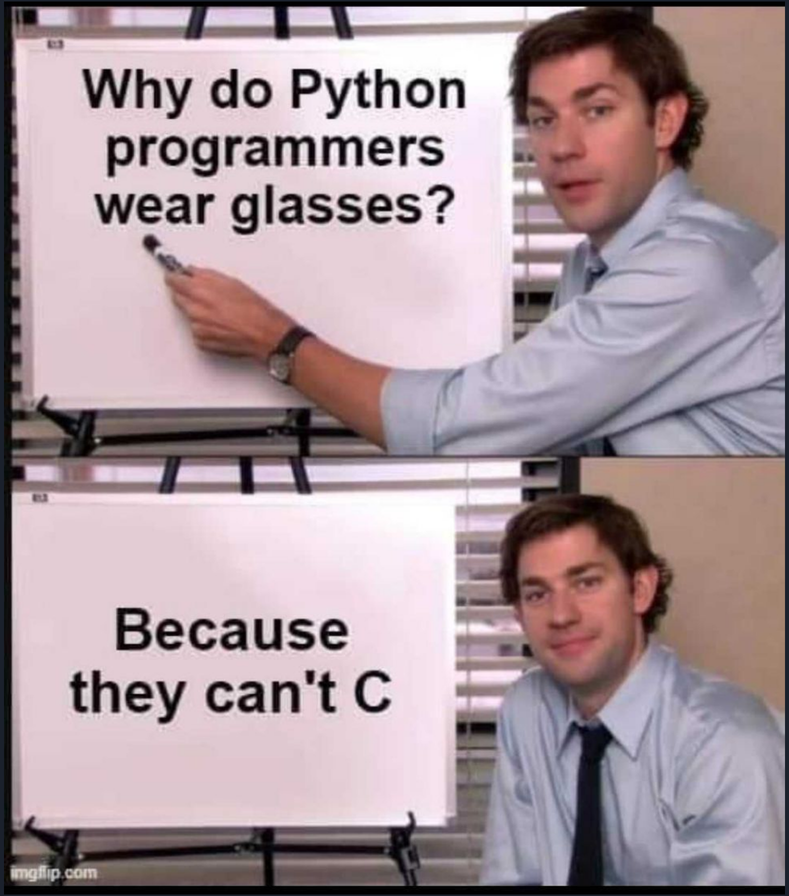
Accurate multi-system emulator

ares is an emulator for systems from Nintendo, Sega, Sony, NEC, SNK, Microsoft, Coleco, Bandai and Benesse. It is a descendent of higan and bsnes and focuses on accuracy and preservation. The SNES emulation is especially complete and polished.

326 packages listed, 3690 installed, 0 broken. 0 to install/upgrade, 0 to remove

sudo apt update	Update package lists / versions
sudo apt upgrade	Upgrade installed packages (takes a while)
apt-cache search searchTerm	Searches for packages that match search term
sudo apt install packageName	Installs a new package (and any packages required by that package)
Synaptic Package Manager	GUI for the package manager


Why do Python programmers wear glasses?


Why do Python programmers wear glasses?
Because they can't C
imgflip.com

10/10
x6
002844
44
HIGH SCORE
521
imgflip.com

Shell scripts

- A series of commands in a text file
  - Linux
    - Can start text file with #! (shebang) and make executable
    - Can call interpreter directly
  - Windows
    - .bat (batch) files
    - Windows Power Shell
- Can take arguments ($1, $2)
- Number of arguments ($#)
- Command Substitution (not just for scripts)
  - ``echo “There are `ls *.txt | wc -l` files in this directory”``
  - `echo “There are $(ls *.txt | wc -l) files in this directory”`

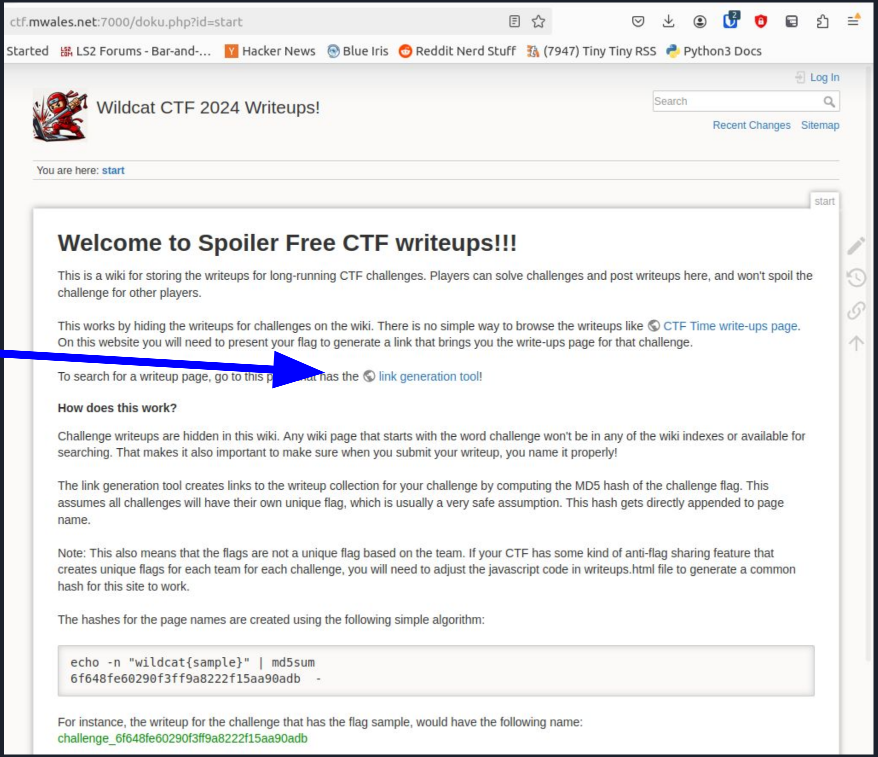
Executable Files

- Linux - permissions bits
  - Permission bits for user, then group, then others
  - r = read, w = write, x = executable
  - `$ ls -l`

    ```
    -rwxrwxr-x 1 mwales mwales 16784 Feb  1  2023 a.out
    -rw-rw-r-- 1 mwales mwales    26 Feb  1  2023 flag.txt
    -rwxrwxr-x 1 mwales mwales  3969 Feb  3  2023 judge.py
    -rw-rw-r-- 1 mwales mwales   330 Feb  2  2023 solution.c
    ```
  - `chmod` can change file permissions
- Windows - file extension
    - .bat (batch) and .cmd (command) script files
    - .exe and .com binary files
    - Many others

CTF Writeups

- URL of page
- Doku wiki
  - Anyone can change
- Get a flag
- Click link generation tool
- Enter flag
- Generate Link
- Click Link



ctf.mwales.net:7000/doku.php?id=start

Wildcat CTF 2024 Writeups!

You are here: start

Welcome to Spoiler Free CTF writeups!!!

This is a wiki for storing the writeups for long-running CTF challenges. Players can solve challenges and post writeups here, and won't spoil the challenge for other players.

This works by hiding the writeups for challenges on the wiki. There is no simple way to browse the writeups like CTF Time write-ups page. On this website you will need to present your flag to generate a link that brings you the write-ups page for that challenge.

To search for a writeup page, go to this page that has the link generation tool!

How does this work?

Challenge writeups are hidden in this wiki. Any wiki page that starts with the word challenge won't be in any of the wiki indexes or available for searching. That makes it also important to make sure when you submit your writeup, you name it properly!

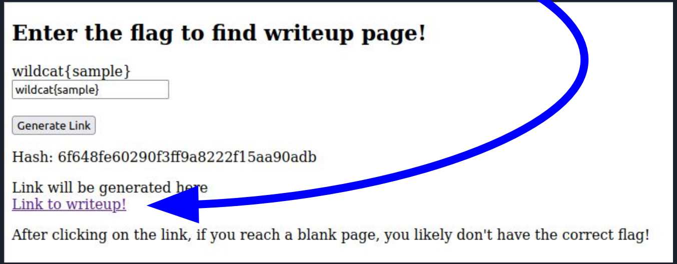
The link generation tool creates links to the writeup collection for your challenge by computing the MD5 hash of the challenge flag. This assumes all challenges will have their own unique flag, which is usually a very safe assumption. This hash gets directly appended to page name.

Note: This also means that the flags are not a unique flag based on the team. If your CTF has some kind of anti-flag sharing feature that creates unique flags for each team for each challenge, you will need to adjust the javascript code in writeups.html file to generate a common hash for this site to work.

The hashes for the page names are created using the following simple algorithm:

```
echo -n "wildcat{sample}" | md5sum
6f648fe60290f3ff9a8222f15aa90adb  -
```

For instance, the writeup for the challenge that has the flag sample, would have the following name: challenge_6f648fe60290f3ff9a8222f15aa90adb



Enter the flag to find writeup page!

wildcat{sample}

wildcat{sample}

Generate Link

Hash: 6f648fe60290f3ff9a8222f15aa90adb

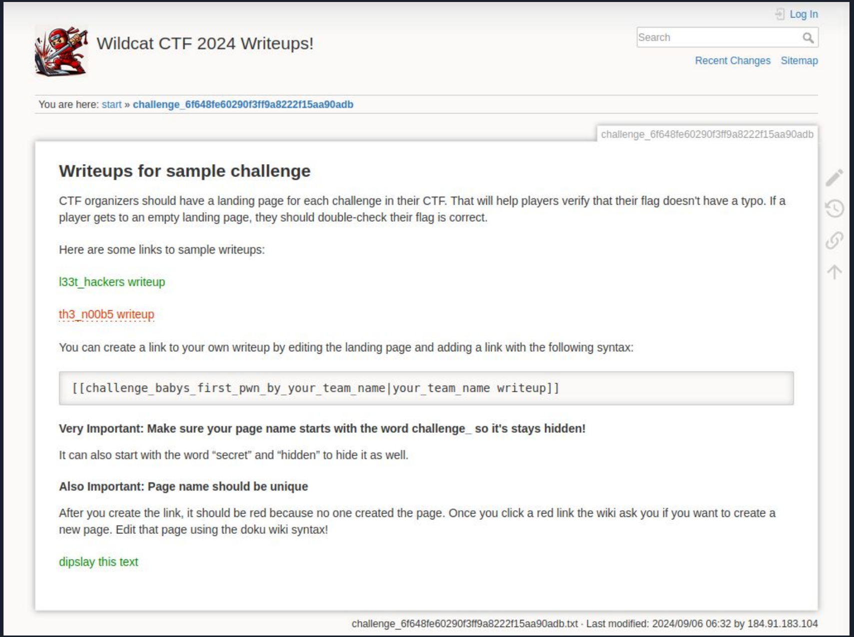
Link will be generated here
Link to writeup!

After clicking on the link, if you reach a blank page, you likely don't have the correct flag!

CTF Writeups

- Secret pages
    - challenge_
    - secret_
    - hidden_
- No limit on writeups for chals
- Link to your writeup from this page
- Make your page a secret page
- Give it a unique name

- wildcat{la-speed-check} demo



Wildcat CTF 2024 Writeups!

You are here: start » **challenge_6f648fe60290f3ff9a8222f15aa90adb**

challenge_6f648fe60290f3ff9a8222f15aa90adb

Writeups for sample challenge

CTF organizers should have a landing page for each challenge in their CTF. That will help players verify that their flag doesn't have a typo. If a player gets to an empty landing page, they should double-check their flag is correct.

Here are some links to sample writeups:

l33t_hackers writeup

th3_n00b5 writeup

You can create a link to your own writeup by editing the landing page and adding a link with the following syntax:

```
[[challenge_babys_first_pwn_by_your_team_name|your_team_name writeup]]
```

Very Important: Make sure your page name starts with the word challenge_ so it's stays hidden!

It can also start with the word “secret” and “hidden” to hide it as well.

Also Important: Page name should be unique

After you create the link, it should be red because no one created the page. Once you click a red link the wiki ask you if you want to create a new page. Edit that page using the doku wiki syntax!

dipslay this text

challenge_6f648fe60290f3ff9a8222f15aa90adb.txt · Last modified: 2024/09/06 06:32 by 184.91.183.104

Attributions

- Debian Family Tree: Andreas Lundqvist, Donjan Rodic from wikimedia.org