



Wildcat CTF pwn.college

Players Guide



Why learn offensive security

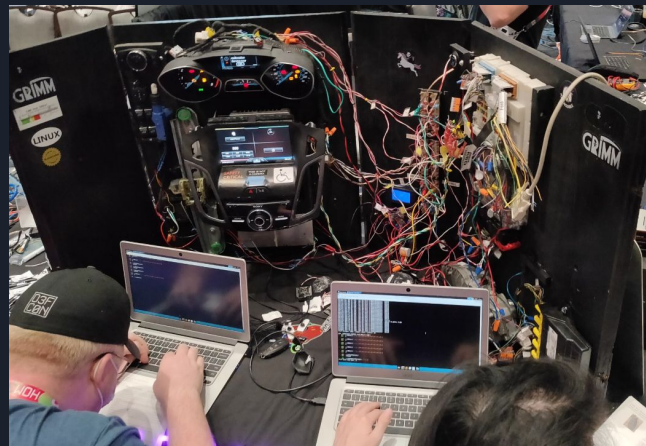
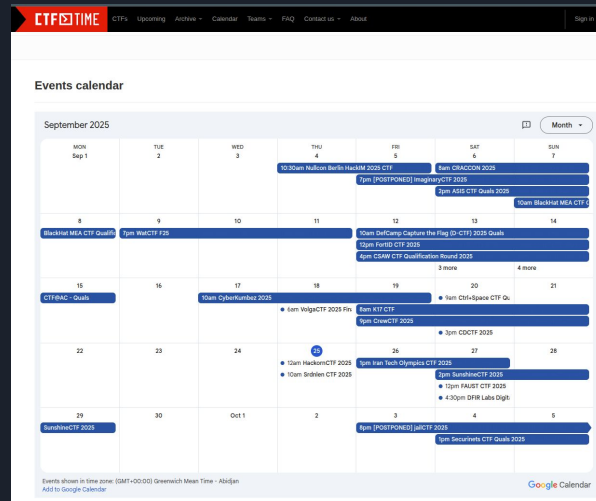
- Learning programming and scripting
- Learning how operating systems and access controls work
- Learn new software introspection techniques (debugging, tracing, emulation)
- Learn how code gets converted to executable code
 - How are symbols found?
 - How do function calls work?
 - Really understand C++ and vtables!
- Learning how vulnerabilities work gives you a foundation to avoid flaws in development
 - Why does a stack buffer overflow break / make a vulnerability
 - How can file access permissions be abused by attackers
 - How are cryptography failures exploited

Learn software cyber security by implementing common attacks

Cyber CTF

- Capture the Flag
- ctftime.org lists many upcoming challenges
 - Usually several each weekend
 - Some USA based, many international
 - Usually online, sometimes in-person
 - Sunshine CTF - Orlando, FL
 - DEFCON CTF - Las Vegas, NV
- Attackers try to capture flag (secrets)
 - Via bug / flaw in organizers challenge
 - Forensic research
 - From other teams when playing attack and defend

Digital (Software) version of an Escape Room





- Platform by former CTF players and ASU students (now professors)
- Heavily modified version of CTFd
- Part of ASU CS required curriculum

The Courses — Earning Credit

We leverage the above material to run a number of courses on this platform. For the most part, these courses import the above material, though some might introduce new concepts and challenges.

CSE 365 - Fall
2025

1 Module
149 Challenges

CSE 466 - Fall
2025

11 Modules
267 Challenges

CSE 539 - Spring
2025

7 Modules
44 Challenges

CSE 598 AVR - Fall
2024

7 Modules
62 Challenges

pwn.college | 🏠 Dojos 🖥️ Workspace ? Help 💬 Chat 🔍 Search



Getting Started — Learn the Basics!

These first few dojos are designed to help you Get Started with the platform. Start here before venturing onwards!

Start Here



2 Modules
11 Challenges

Linux Luminarium



16 Modules
126 Challenges

Computing 101



7 Modules
69 Challenges

Playing With Programs



4 Modules
116 Challenges

After completing the dojos above, dive into the Core Material below!

Core Material — Earn Your Belts!

These dojos form the official pwn.college curriculum, taking you on a curated journey through the art of hacking. As you progress and build your skills, like in a martial art, you will earn **belts** for completing dojo after dojo. We won't stop you from jumping around if you want (and have the requisite skills), but you must earn belts sequentially.

Intro to Cybersecurity



7 Modules
183 Challenges

Program Security



7 Modules
188 Challenges

System Security



6 Modules
93 Challenges

Software Exploitation



6 Modules
103 Challenges

After completing the dojos above, not only will you be added to the **belts** page, but *we will send you actual pwn.college-embroidered belts*!

To get your belt, **send us an email** from the email address associated with your pwn.college account. We'll then get your belt over to you (eventually)! Note that, due to logistical challenges, we're currently only *shipping* belts to hackers after they earn their blue belt. Until then, we will belt you in person, at ASU or some security conference.

How to enroll

- [Register at pwn.college](https://pwn.college)
 - Username / Hacker Handle
 - Email Address
 - Integrity Pledge
- Earn your white belt!



Start Here



2 Modules
11 Challenges

Linux Luminarium



16 Modules
126 Challenges

Welcome to the Dojo

- Many Dojos available to teach new skills
- Each dojo has submodules on different subjects
- Module contents
 - Youtube lecture
 - Google slides
 - Challenges
- Completing Dojos earns you rewards
- Completing Core Dojos earns you an actual pwn.college belt!

Getting Started — Learn the Basics!

These first few dojos are designed to help you Get Started with the platform. Start here before venturing onwards!

Start Here	Linux Luminarium	Computing 101	Playing With Programs
2 Modules 11 Challenges	16 Modules 127 Challenges	7 Modules 69 Challenges	4 Modules 116 Challenges

After completing the dojos above, dive into the Core Material below!

Core Material — Earn Your Belts!

These dojos form the official pwn.college curriculum, taking you on a curated journey through the art of hacking. As you progress and build your skills, like in a martial art, you will earn **belts** for completing dojo after dojo. We won't stop you from jumping around if you want (and have the requisite skills), but you must earn belts sequentially.

Intro to Cybersecurity	Program Security	System Security	Software Exploitation
7 Modules 163 Challenges	5 Modules 163 Challenges	6 Modules 93 Challenges	5 Modules 90 Challenges

After completing the dojos above, not only will you be added to the **belts** page, but we will send you actual pwn.college-embroidered belts!

To get your belt, **send us an email** from the email address associated with your pwn.college account. We'll then get your belt over to you (eventually!) Note that, due to logistical challenges, we're currently only shipping belts to hackers after they earn their blue belt. Until then, we will belt you in person, at ASU or some security conference.

Community Material — Earn Badges!

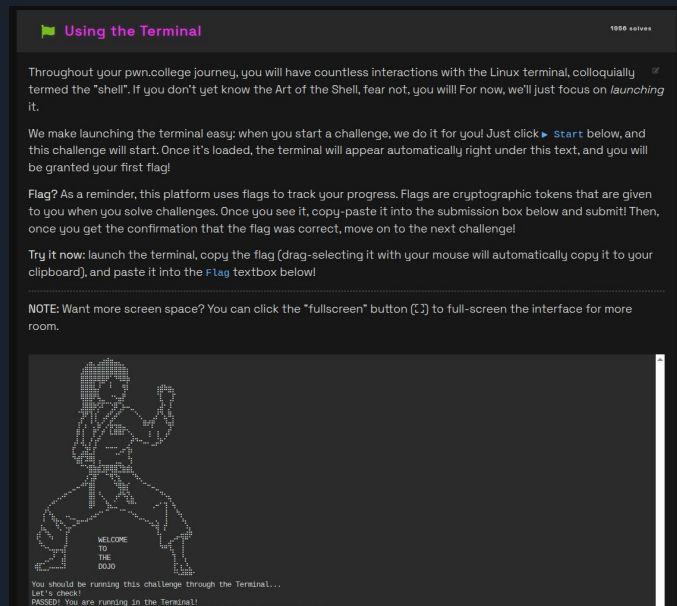
No matter how much material we create, there is always more to learn! This section contains additional dojos created by the pwn.college community. Some are designed to be tackled after you complete the dojos above, whereas others are open to anyone interested in more specialized topics.

pwn.college Archives	ACSAC 2024 CTF	ARM Architecture	CTF Archive
7 Modules 201 Challenges	1 Module 11 Challenges	2 Modules 28 Challenges	89 Modules 690 Challenges

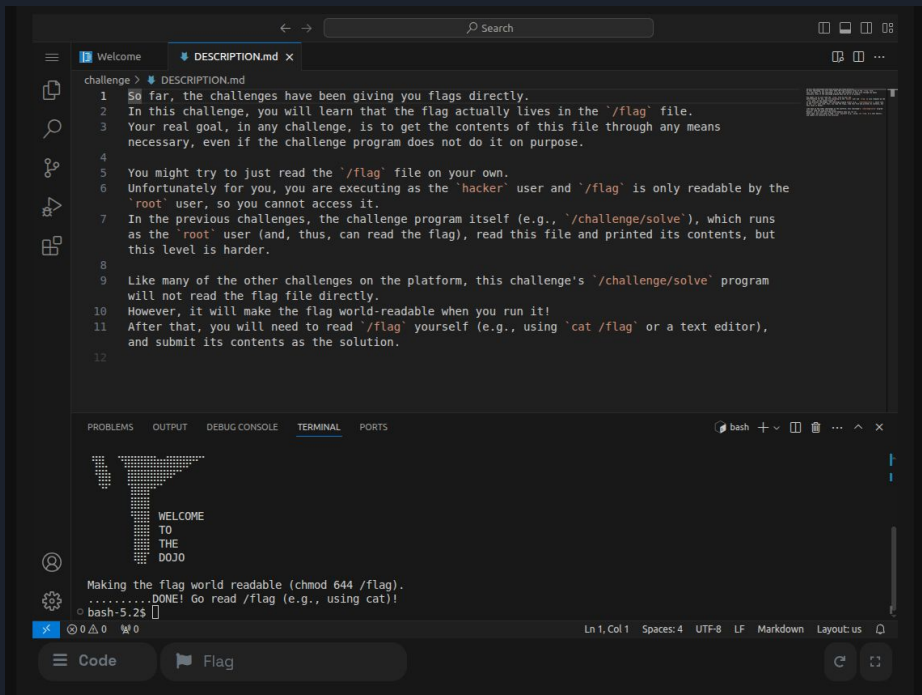
Demo dojo	Intro to Programming Languages	The Quarterly Quiz	Windows Warzone
1 Module 0 Challenges	23 Modules 219 Challenges	2 Modules 13 Challenges	2 Modules 17 Challenges

Completing Challenges

- Pwn.college hosts a VM in the cloud (ASU)
 - You don't need a powerful computer
 - Just need a web browser
 - Security and development tools already installed!
- Core challenges are designed
 - Teach security concepts
 - Demonstrate new skills
 - Small incremental steps
- Start the challenge
 - Web-terminal
 - VS Code
 - Desktop
 - SSH mode



Other options

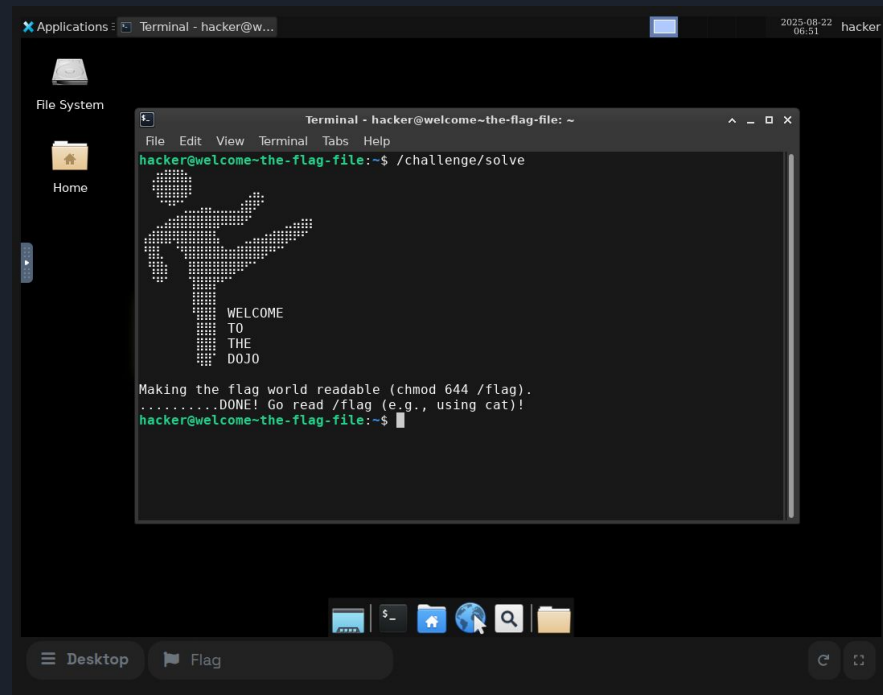


The screenshot shows a code editor with a file named `DESCRIPTION.md` open. The file contains a challenge description with 12 lines of text. Below the editor, there is a terminal window. The terminal shows a ASCII art of a person standing, followed by the text "WELCOME TO THE DOJO". Below this, it says "Making the flag world readable (chmod 644 /flag).DONE! Go read /flag (e.g., using cat)!". The terminal prompt is `bash-5.2$`.

```
challenge > DESCRIPTION.md
1 50 far, the challenges have been giving you flags directly.
2 In this challenge, you will learn that the flag actually lives in the '/flag' file.
3 Your real goal, in any challenge, is to get the contents of this file through any means
4 necessary, even if the challenge program does not do it on purpose.
5
6 You might try to just read the '/flag' file on your own.
7 Unfortunately for you, you are executing as the 'hacker' user and '/flag' is only readable by the
8 'root' user, so you cannot access it.
9 In the previous challenges, the challenge program itself (e.g., '/challenge/solve'), which runs
10 as the 'root' user (and, thus, can read the flag), read this file and printed its contents, but
11 this level is harder.
12
13 Like many of the other challenges on the platform, this challenge's '/challenge/solve' program
14 will not read the flag file directly.
15 However, it will make the flag world-readable when you run it!
16 After that, you will need to read '/flag' yourself (e.g., using 'cat /flag' or a text editor),
17 and submit its contents as the solution.
```

```
WELCOME
TO
THE
DOJO

Making the flag world readable (chmod 644 /flag).
.....DONE! Go read /flag (e.g., using cat)!
bash-5.2$
```



The screenshot shows a terminal window titled "Terminal - hacker@w...". The terminal prompt is `hacker@welcome-the-flag-file:~$`. The user has entered the command `/challenge/solve`. The output shows a ASCII art of a person standing, followed by the text "WELCOME TO THE DOJO". Below this, it says "Making the flag world readable (chmod 644 /flag).DONE! Go read /flag (e.g., using cat)!". The terminal prompt is `hacker@welcome-the-flag-file:~$`.

```
hacker@welcome-the-flag-file:~$ /challenge/solve

WELCOME
TO
THE
DOJO

Making the flag world readable (chmod 644 /flag).
.....DONE! Go read /flag (e.g., using cat)!
hacker@welcome-the-flag-file:~$
```


Westshore Dojo

1. Register and sign in to pwn.college first
2. <https://pwn.college/dojo/westshore-cs-club~0b45ad3f/join/>



Modules

Pseudo Random
Number
Generators
(PRNG)

0 / 2

Hashing

0 / 2

Cryptography

0 / 6

Cracks and
Keygens

0 / 2

General Skills

1 / 2

Pwn

0 / 1

Coding

0 / 1

Reverse
Engineering

0 / 6

Forensics

0 / 1

Impossible

0 / 1

Arizona State University



- Computer Science (Cybersecurity), BS - 120 credit hours

Computer Science Lower Division
CSE 110 Principles of Programming (QTRS)
EEE 120 Digital Design Fundamentals
CSE 205 Object-Oriented Programming and Data Structures (QTRS)
CSE 230 Computer Organization and Assembly Language Programming
CSE 240 Introduction to Programming Languages
FSE 100 Introduction to Engineering
Computer Science Upper Division
CSE 301 Computing Ethics
CSE 310 Data Structures and Algorithms
CSE 330 Operating Systems
CSE 340 Principles of Programming Languages
CSE 355 Introduction to Theoretical Computer Science
CSE 360 Introduction to Software Engineering
CSE 365 Information Assurance
CSE 485 Computer Science Capstone Project I
CSE 486 Computer Science Capstone Project II
MAT 343 Applied Linear Algebra
IEE 380 Probability and Statistics for Engineering Problem Solving (QTRS)

pwn.college

Plus CSE598 - Special Topics

- Fall 24-Applied Vulnerability Research
- Spring 24 - Advanced SW Exploitation

Cybersecurity Focus Courses
^ Upper Division Cybersecurity Focus Courses
CSE 466 Computer Systems Security
CSE 467 Data and Information Security
CSE 468 Computer Network Security
CSE 469 Computer and Network Forensics
CSE 494 Topic: Artificial Intelligence for Cyber Security
CSE 412 Database Management
OR CSE 434 Computer Networks
OR CSE 445 Distributed Software Development
^ Upper Division Cybersecurity Electives
CSE 445 Distributed Software Development
CSE 460 Software Analysis and Design
CSE 463 Introduction to Human Computer Interaction
CSE 464 Software Quality Assurance and Testing
CSE 466 Computer Systems Security
CSE 467 Data and Information Security
CSE 468 Computer Network Security
CSE 469 Computer and Network Forensics
CSE 471 Introduction to Artificial Intelligence
CSE 494 Topic: Artificial Intelligence for Cyber Security




Coursework -> Belts



- CSE 240 Intro to Programming Languages
 - Intro to Programming Languages Model
 - Linux, C, C++, Scheme (functional programming)
- CSE 365 Information Assurance (most of the orange belt)
- CSE 466 Computer Systems Security 🥷 (yellow and green belts)
 - Binary and system exploitation
- CSE 598 Special Topics
 - Applied Vulnerability Research
 - Advanced SW Exploitation

The material offered on pwn.college is serious CS coursework / academic level.

IMO, a MUCH better use of your time than many certifications / tests in EIT field



Our obligation to ASU Students and Faculty



- Much of pwn.college is integrated into ASU coursework
 - Pwn.college solve percentage is most / all of their students grade
 - See ASU academic integrity policy
-
- No write-ups
 - No solutions on Github
 - No sharing of flags

Plagiarism and Cheating

Plagiarism or any form of cheating in assignments or projects is subject to serious academic penalty. To understand your responsibilities as a student read: [ASU Student Code of Conduct](#) and [ASU Student Academic Integrity Policy](#). There is a zero tolerance policy in this class: any violation of the academic integrity policy will result in a zero on the assignment and the violation will be reported to the Dean's office. Plagiarism is taken very seriously in this course.

Examples of academic integrity violations include (but are not limited to):

- Sharing code with a fellow student (even if it's only a few lines).
- Collaborating on code with a fellow student (unless explicitly allowed).
- Using another student's solution to solve a challenge and get a flag.
- Sharing a flag with another student (NEVER ALLOWED UNDER ANY CIRCUMSTANCES).

Posting your assignment solutions online is expressly forbidden, and will be considered a violation of the academic integrity policy. Note that this includes working out of a public Github repository. The [Github Student Developer Pack](#) provides unlimited private repositories while you are a student, making it easy to begin with a private GitHub repository.

pwn.college dojo order

1. [Start Here](#) - Teach how pwn.college works
2. [Linux Luminarium](#) - How to use Linux

Once you have powered up with the first 2 dojos, you can try these next dojos in any order / what interests you

- [Playing with Programs](#) - Data, HTTP, suid
- [Westshore Jr/Sr HS CS Club](#) - Beginner CTF
- [Intro to Programming Languages](#) - C / C++
- [Computing 101](#) - Assembly and GDB





Questions

My response time can be a little slow:

`mwales3 at gmail dot com`