The Australian National University Computer Science Students' Association

Bush Week Tech Fest

Event Brief

10AM July 31st - 10PM August 2nd 2026

The ANU CSSA acknowledges the Australian Aboriginal and Torres Strait Islander peoples of this nation. We acknowledge the traditional custodians of the lands on which our organisation is located and where we conduct our business. We pay our respects to ancestors and Elders, past and present. The ANU CSSA is committed to honouring Australian Aboriginal and Torres Strait Islander peoples' unique cultural and spiritual relationships to the land, waters and seas and their rich contribution to society.

About The Bush Week Tech Fest by CSSA

The Australian National University Computer Science Students' Association (ANU CSSA) is the largest computing-related student society at the Australian National University and one of the most active student associations at the ANU, with a history of over 30 years. Bush Week runs after Orientation Week and is filled with events for new and existing students. **This year, CSSA will be running its first ever Techfest during Bush Week, championing a 48hr CTF titled BushBash CTF, Tech Talks with industry speakers, BBQs, a Movie Night, and a Networking and Drinks Night to cap it all off.** There will be no better way to spend the weekend of Semester 2, Week 1 than to learn, meet people, and have fun at Techfest.

The Capture the Flag competition will run between July 31st and August 2nd.

Event Schedule (as at 26th June 2026):

Friday 31st July	Saturday 1st August	Sunday 2nd August
Tech Talks (10am-4pm) *Includes Refreshments*	**Free BBQ Lunch (12pm)**	**Free BBQ Lunch (12pm)**
BushBash CTF Launch (5pm-10pm) *Includes Refreshments*	**BushBash CTF (10am-8pm)** *Includes Refreshments*	**BushBash CTF Finale and Prizes (10am-5:30pm)** *Includes Pizza Dinner*
	Movie Night (~6-10pm)	**Networking Drinks (~6-10pm)**

The goal of this Tech Fest is to invite new and existing students to have fun, learn a little, and in the case of the CTF challenge themselves to think critically. We welcome students who want to participate in the ANU Computing and Cyber community.

We really look forward to working with you all, and for a fantastic event ahead.

Peter Woodhead <----------> CSSA Cybersecurity Officer
Adrian Carpio <----> CSSA Competitive Programming Officer
Harold Gao <----------> CSSA International Officer

What is a Capture The Flag (CTF)?

A **Capture the Flag** is a type of competitive puzzle solving, vulnerability analysis and software exploitation challenge in which teams of players work through a collection of challenges across a few different categories, searching for a “flag” value, which is a predefined string of text (commonly CTF{flag_here}, or EVENTNAME{flag_here}. Ours is disorientation{CTF}) which can be input into a challenge submission website which handles point scoring and leaderboards among teams.

The point of the challenge is to exploit a vulnerability in either a set of files (static challenges) or in a live application (hosted service challenges) to retrieve the flag value hidden inside.

We’ll be writing challenges across the main CTF categories: Open-Source Intelligence (OSINT), Reverse Engineering (Rev), Binary Exploitation (Pwn), Web Exploitation (Web), Cryptography (Crypto), and Miscellaneous (Misc).

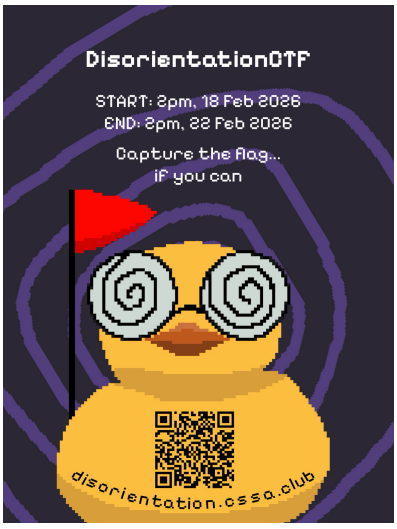
CTF Challenges are designed to be engaging, educational, and fun, with clear direction, minimal guesswork, and an appropriate level of difficulty. There are many ways to write a fun challenge, but really the focus is on breaking the Confidentiality, Integrity, or Availability of information in a digital environment. **The goal is to share core cybersecurity knowledge with everyone that plays, so that ultimately we can learn to write software that is not as vulnerable as these challenges will most certainly be**.

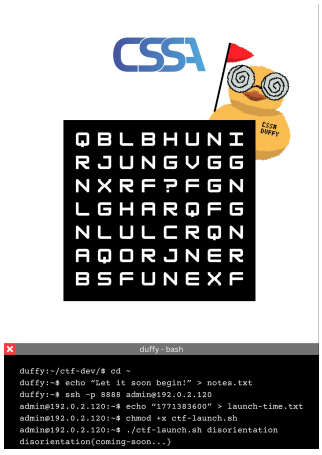
These challenges are highly popular in the security community as they are a great way to motivate problem solving and critical thinking. Competitions are often followed by community-driven posts containing write-ups of the process followed to find the flag, and this is a major source of learning for players as these skills can not only assist in the next challenge but also clearly dictate how to patch the vulnerability in new software.

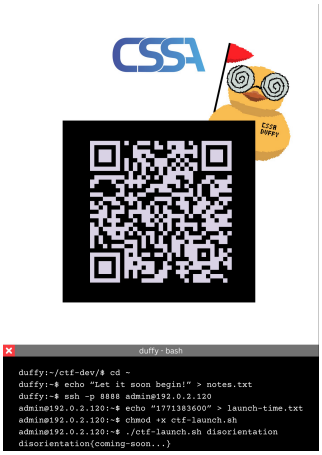
Reviewing Disorientation CTF – Feb 18-22

In February the CSSA ran our first Orientation Week CTF. On learning of the ASD's retreat from Campus CTF Events we wanted to take matters into our own hands to continue community cyber engagement and friendly competition. It was massively successful – over 130 participants from four universities (ANU, UTS, UNSW, Deakin), and over fifty high quality challenges for players to attempt. Better yet, we had a range of industry sponsors including Tanto Security, InfoSect, and BSides Hackercon, who enabled a fantastic prize pool worth thousands.

The following were some of our teaser and advertising posters:







With great feedback for the event, and a motivation to make our next one even better, we're aiming for 250 participants for BushBash CTF. Changes will include reducing the total challenge timeframe from 96 hours to 48 hours, improving engagement with a greater focus on in-person activities, and facilitating non-technical engagement activities such as GeoGuessr and Wikipedia racing for people to play when looking for a brain break. Many great things to come!

CTF Challenge Writing Brief - Passed to Writing Team

Part 1: Creating a Challenge

1. **Idea proposal**

   Challenge idea, difficulty, and category is proposed. A tracking issue in Github is created (use template).

2. **Challenge Writing and Development**

   The challenge writer (aka author) creates a new branch with the name "**challenge/<challenge-name>**". You can then write your Challenge code, assets, docs, and solution... reminder that flags look like this: **disorientation{<flag-text-here>}.** Another thing to note - you can have multiple solutions if you really think this will add to your challenge, just clearly document the possible options. Our infra also allows for regex-matched flags. Feel free to ask for help at this step! This stage is where you'll get most of your work done.

   You'll find a folder titled "_template" in the challenges dir in the repo. Duplicate and rename to match your branch name. You'll find a build dir, for hosted services (dockerise this!), a ctf dir for static challenge files (all contents of this folder will be available to the challenge participant), and a solution dir which is the best place to put challenge solution software. The _template/challenge.md file is the source of truth for key information about the challenge, so make sure you fill out the challenge details here, including the user-facing noCTF challenge description (which is in markdown) and the flag value.

3. **Initial readiness**

   Commits continue until the challenge runs end-to-end, documentation is complete, and a full solution is written (including clear flag format). At this stage, the challenge should be 'Done'.

Definition of Done

All flags are subject to approval by the committee and the university's Information Security Office. We can't guarantee any particular idea will go ahead. To give you the best chance of writing a good challenge, you should have the following ready before preparing to merge into main: **Player-facing description written in Markdown, Intended difficulty level, Intended Point Score (100 to 500 points), Category, Flag format Description for players, Correct Flag Solutions for Infra, Full solution write-up, and Description of Intended Solve Path.**

Part 2: Challenge Review and Submission

4. **Pull Request**

   PR will be opened from the challenge branch to prepare for a merge into the main branch. The tracking issue should be linked to the PR, and two playtesters will be assigned to challenge review.

5. **First playtest & review**

   The first Playtester attempts the challenge as any player would. Code, docs, and solve path reviewed, and feedback is left for the author directly on the PR. Review should also consider any necessary changes to difficulty rating or to point score associated with the challenge.

6. **Author revisions**

   The author applies requested improvements, and updates are pushed to the PR branch.

7. **Second playtest & final review**

   Revised challenge is playtested again, and final notes are recorded in PR tracking issue.

8. **Merge**

   With two successful playtests and two approvals, the PR is merged into main.

Part 3: Migrating Challenge to noCTF and kCTF Infra

9. **Infrastructure validation**

   Challenge descriptions and correct flags are added to noCTF, as well as any files, code, binaries, or images which need to be made available to players to download. These are uploaded to the noCTF instance directly. Large files (>15MB) should be hosted in a google drive or similar and a link made available in the description of the challenge. This is also the stage where flags are entered into our challenge software.

   Challenges that have services which need to be running and hosted will need to be running in a docker container and deployed via kCTF on GCloud. Peter and Alyssa from the CSSA team will be assisting in this part of the process. kCTF works by allowing every new TCP connection to the IP address to have a new instance of the challenge, so players will not break the challenge service for any other players. An example of this would be a web page which needs to be hosted, or a command line service which would be connected to via ssh or netcat. Compatibility, stability, and scaling are checked at this stage.

10. **Completion**

    Challenge marked as complete and ready for O-Week!