

How to make CTF

skateboarding dog

Questions

1. What makes a CTF challenge?
2. What makes a challenge guessy?
3. What makes a challenge fun?
4. How to design against AI solvability?
5. What are some tips for coming up with novel challenge ideas, without them being too niche?

What makes a CTF challenge

Think about what it's like to solve a CTF challenge. At the very highest level, you are presented with a problem and the goal is to get the flag.

The problem you are given should **guide you to getting the flag** by demanding of you three things: **knowledge, skills, and creativity / problem-solving**.

What makes a CTF challenge

Knowledge: what you already know coming into the challenge. E.g. bug classes, algorithms, techniques, protocols, theorems, etc.

Skills: Your ability to perform tasks required to solve the challenge, e.g. reading/writing code, using a debugger, reading disassembly, reading technical documents to improve knowledge in real time

Creativity: Using lateral thinking to come up with ideas that can be used to solve the given problem

These three are not fully disconnected - creativity is fuelled by knowledge (knowing things helps to make connections and generate ideas)

Question yourself which aspects should be applied to your challenge

What makes a challenge guessy?

The challenge should guide you to getting the flag: it should be fairly clear what the challenge is asking of you.

Good: Web application with source code given, with a /flag route accessible only by admin users => How do I make myself admin or bypass the access controls?

Bad: Website with no hand out, with the description of the challenge talking about robots => Is the author obsessed with robots?


What makes a challenge guessy?

If two participants work on a challenge during the CTF and only one participant completes the challenge, the difference between their solving methods should not involve “luck”.



A participant who does not solve a challenge should feel like they have learnt something after reading the intended solution.

<https://bit.ly/ctf-design>

Inspiration matrix

Tasks that need  +  are	little work	some work	a lot of work	too much work
little inspiration	Very easy	Relaxing Disappointing	Uninteresting	Boring
some inspiration	Easy Satisfying	Fun	Exhausting	Frustrating
a lot of inspiration	Surprising Insightful	Challenging	Very hard	Very frustrating
too much inspiration	Guessy	Frustrating	Very frustrating	Unreasonable

Inspiration matrix

Things players  +  are	they actually know	they actually don't know
think they know	Obvious, Easy	Surprising, Hard
think they don't know	Insightful, Hard	Educational, Interesting

What makes a CTF challenge fun?

While solving the challenge:

- Working on the challenge should make them feel like they are doing something smart/cool/interesting
- The player should be presented with a setting in which they feel somewhat comfortable in, and then ask a question that challenges their knowledge
- Having an idea of what to do next - the challenge should provide leads in the direction of the solution so that the player does not become stuck
- All of these things contribute to being in a solving “flow state”

What makes a CTF challenge fun?

After solving the challenge or while reading the solution:

- Having an appreciation for how interesting/creative the challenge construction itself is, e.g. “impossible challenges”
- Feeling like they have learnt something from the challenge

Challenge difficulty

Difficulty comes from adjusting the amount of knowledge/skills/creativity required to solve the challenge.

Challenges intended for less experienced CTF audiences should be light on the knowledge and skills aspects.

We often joke of the “hard easy” CTF challenge, where the amount of creativity required is much greater than prior knowledge.

Challenge difficulty

Ideally, the challenge should present things in a way that makes it easy for the solver to digest what's happening and have an idea of what the solution should look like.

But you do not necessarily need to remove creative aspects (a sharp CTF beginner can have very strong problem solving skills) - just give them the puzzle pieces and let them solve it as a puzzle.

More difficulty DOES NOT equal better challenge.

How to design against AI solvability?

- Don't focus on it to begin with
- Generally, challenges with more puzzle/lateral thinking elements are more difficult for AI to solve
- Consider alternative approaches to fixing the AI problem in CTFs: small in-person CTF => enforce no AI in the rules
- Consider “waterfall” puzzle design

Waterfall puzzle design

- Two or more unrelated bugs in one challenge, in which the product of one bug becomes the input used to exploit the other, hence “waterfall”
- The earlier bugs can pose constraints on the inputs on the later bugs
- Tests knowledge of existing bug classes to identify the different bugs
- Tests solvers’ creativity to “create an input that works”

Waterfall puzzle design examples

- E.g. Web challenge by hashkitten:
<https://github.com/AustlCCQuals/Challenges2025/tree/main/web/login>
- E.g. “easy” crypto challenge by josep
<https://github.com/AustlCCQuals/Challenges2024-Public/tree/main/crypto/echo-command-breaker>
- Purely a puzzle (since I know most of you have solved it):
<https://github.com/skateboardingdog/bsides-cbr-2025-challenges/tree/main/misc/raining-dogs-and-dogs>

How to come up with challenges

- Start with what you already know and like
 - This can be a bug you recently learnt about
 - Could be a competitive programming “trick”
- Figure out your objective
 - Where do you estimate your challenge will fall on the inspiration matrices? What are the pitfalls that could occur for a challenge like yours? E.g. Too much work, too much inspiration
- Start implementation ASAP
 - Luckily CTF challenges aren’t large pieces of software that need to be maintained, they can be written and torn down with relative ease
 - As you are building your challenge you will often tweak it/come up with new ideas

How to come up with challenges

- It is a creative process - difficult/counterproductive to be “forced”
- Inspiration from other CTF challenges (but do not copy too closely) - playing a lot of challenges gives ideas
- Keep track of your potential ideas somewhere - write it down whenever you have a thought
- Sometimes you can start from the solution, i.e. if you have an interesting bug or exploitation technique, you just need to package that into a challenge in a nice way

Discussion time