Open-Source CTF Platform Manual

Version 1.0 - October 5, 2022

1 For Administrators

1.1 Videos

The following videos show a quick walkthrough of setting up the SEED Labs CTF and a quick tour of its usage:

- CTFd and `.zip` import
- SEED Labs CTF tour

1.2 CTFd

This project utilizes the open source CTFd capture the flag platform to host the infrastructure needed to operate a successful capture the flag challenge.

1.2.1 CTFd-as-a-service (hosted)

CTFd offers a hosted version of the platform, in which they will set up the infrastructure needed to run CTFd and give you access to the management interface. The CTFd hosted option is available for a cost, and more information can be found here.

1.2.2 Self-hosted

Please follow the CTFd Docker installation instructions to install the platform on your own hardware. By default CTFd does not have TLS enabled. There are tutorials online for enabling TLS on your CTFd Docker instance. For your convenience, this is a third-party GitHub repo with easy deployment instructions for CTFd with TLS enabled. Once CTFd is installed and running you're able to import the provided CTF challenges into the platform.

1.2.3 Admin Account Setup

1. Visit the CTFd site you launched above and click login.

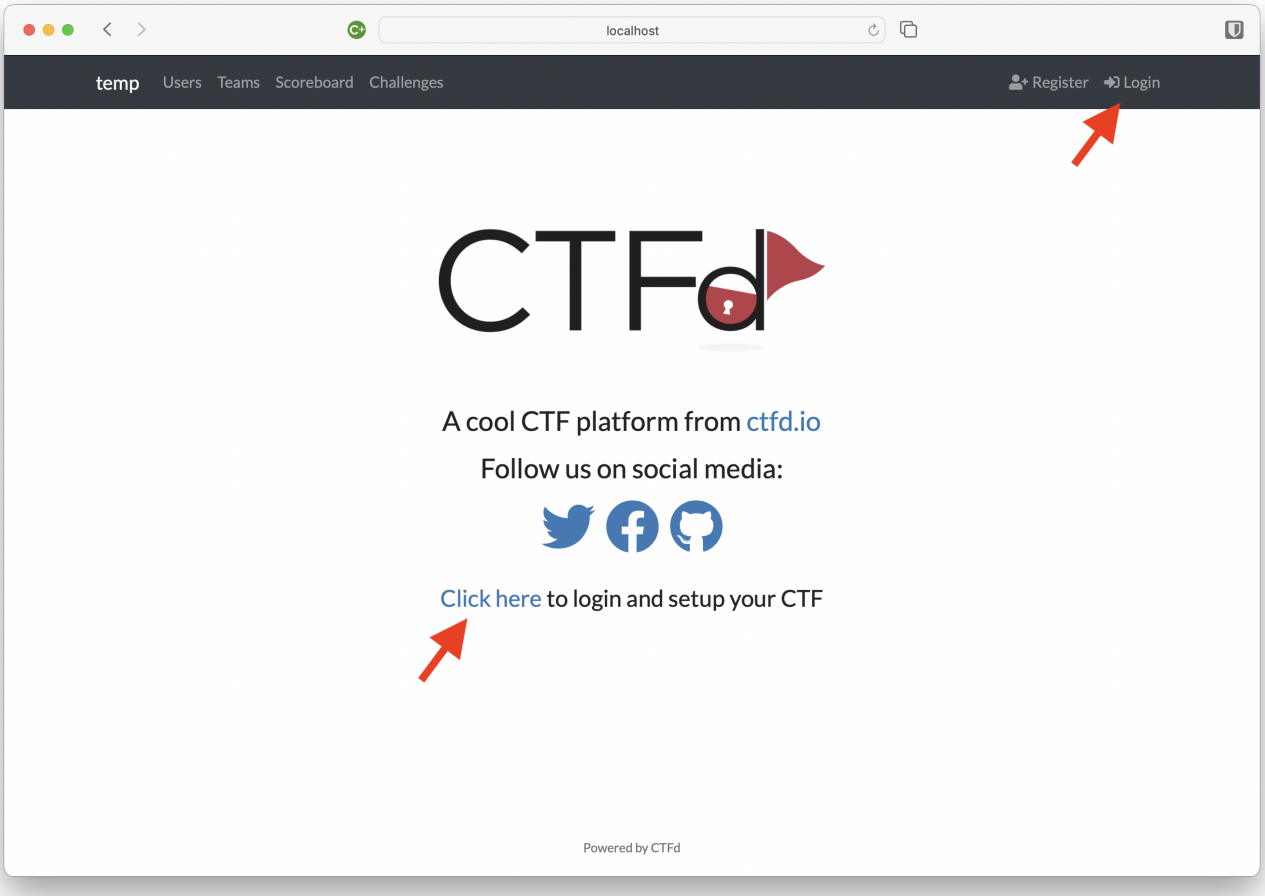

Figure 1: Click login on the CTFd landing page.

2. Login with default admin credentials (obtained by contacting the project maintainers; see bottom of page).

3. Change the default admin credentials to your desired credentials (see below for procedure).

1.2.4 Changing Admin Account Credentials

1. Login with the default admin credentials (obtained by contacting the project maintainers; see bottom of page), then navigate to the admin panel.

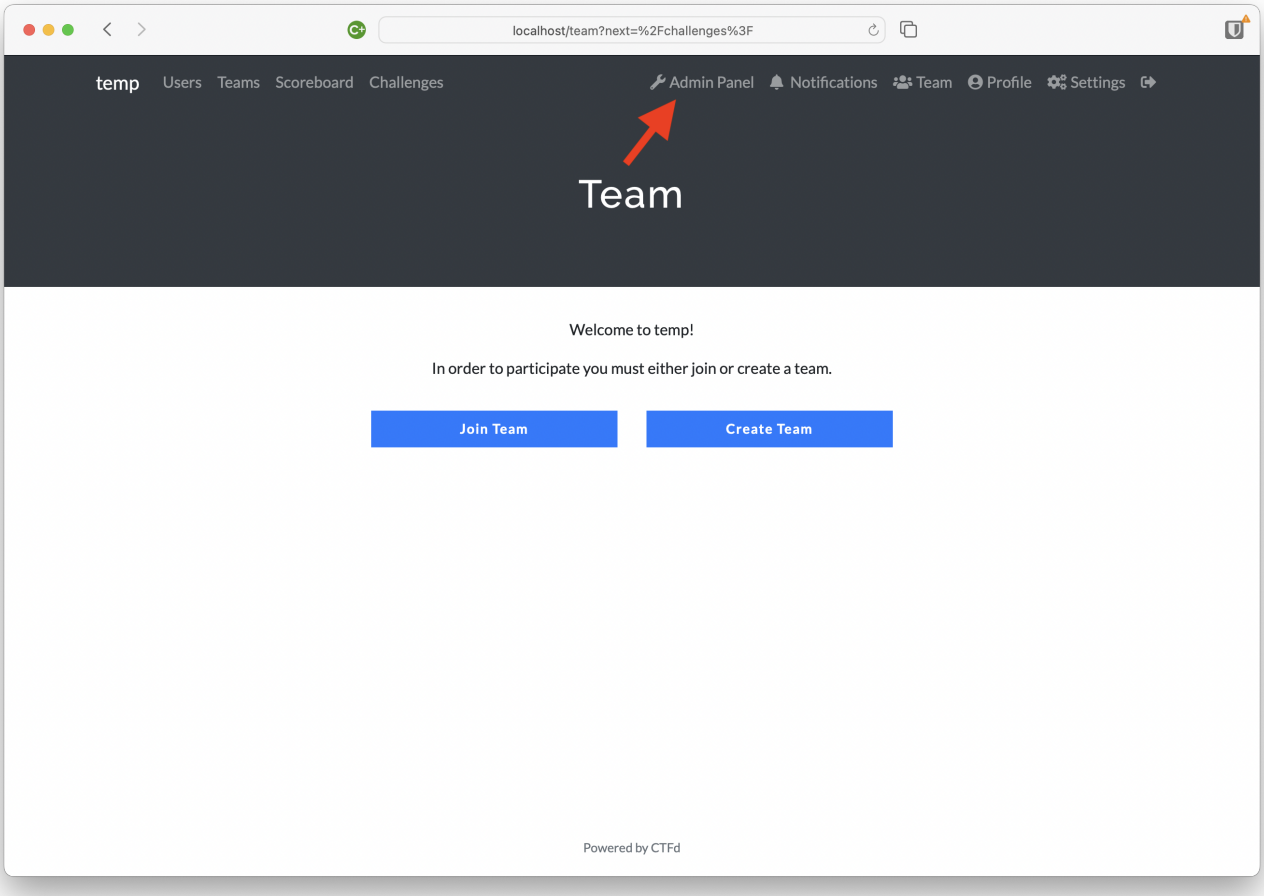

Figure 2: Select the Admin Panel.

2. Navigate to the “Users” page.

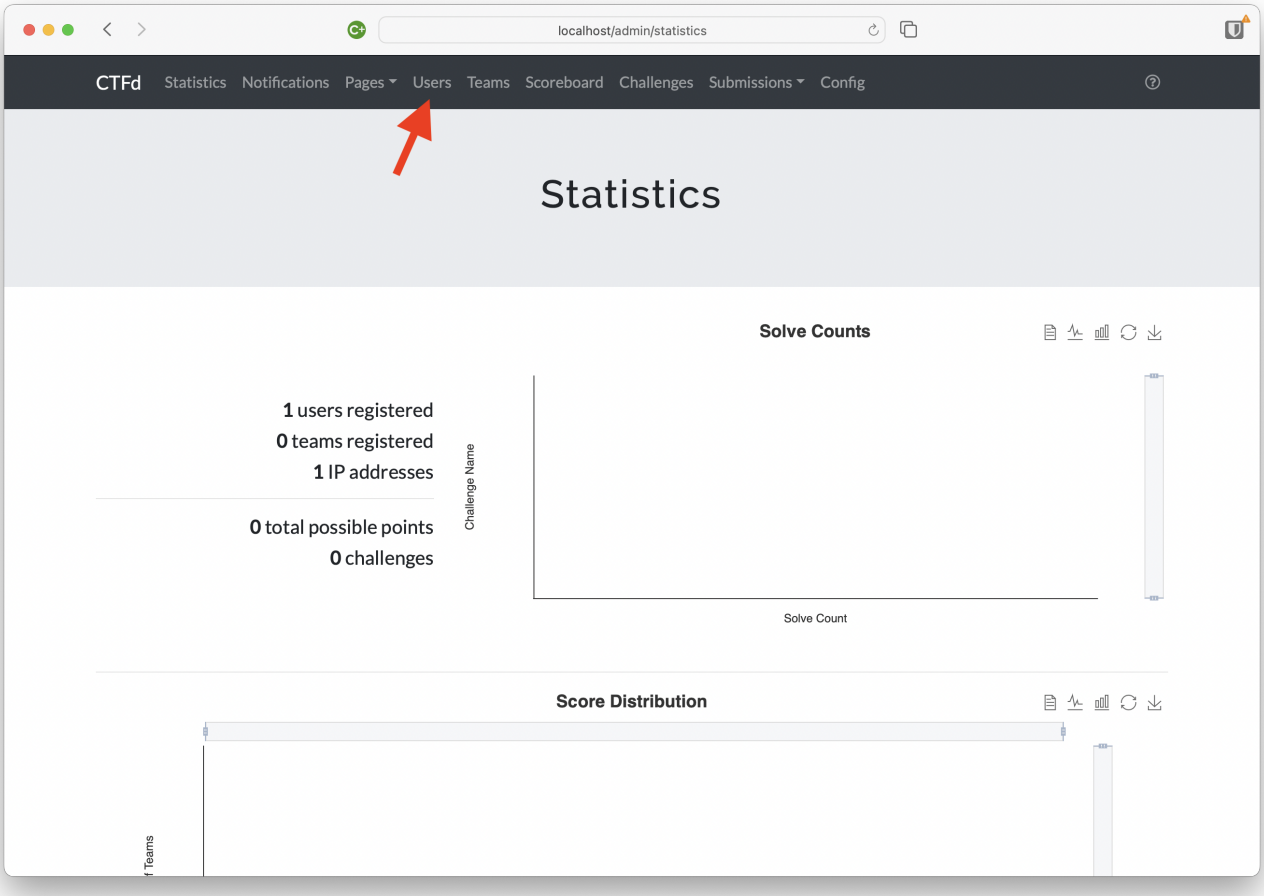

Figure 3: Select the Users page.

3. Select the ⊕ symbol to add a new user.

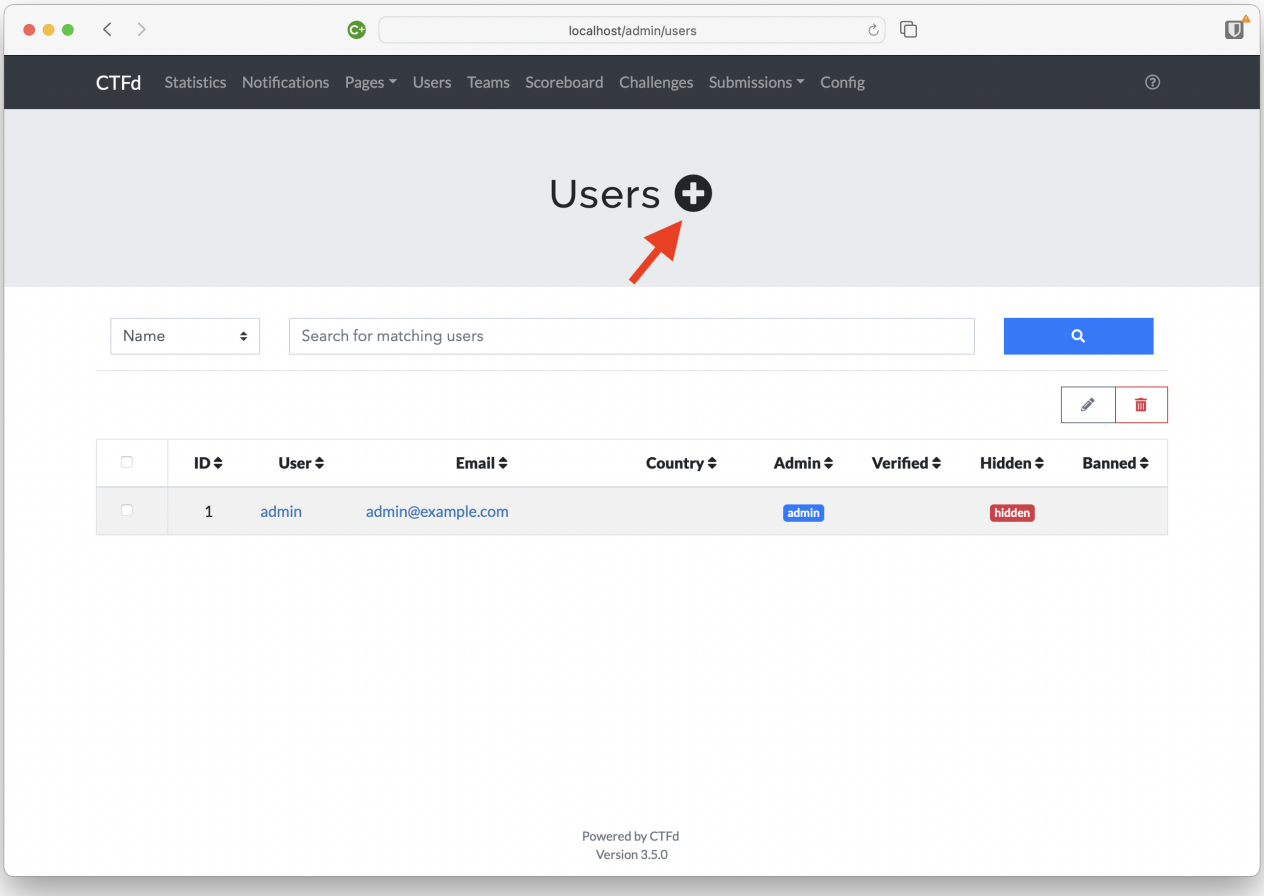

Figure 4: Select the "plus" symbol to add a new user.

4. Fill out the new user account details. Ensure that you set the account type to "Admin".

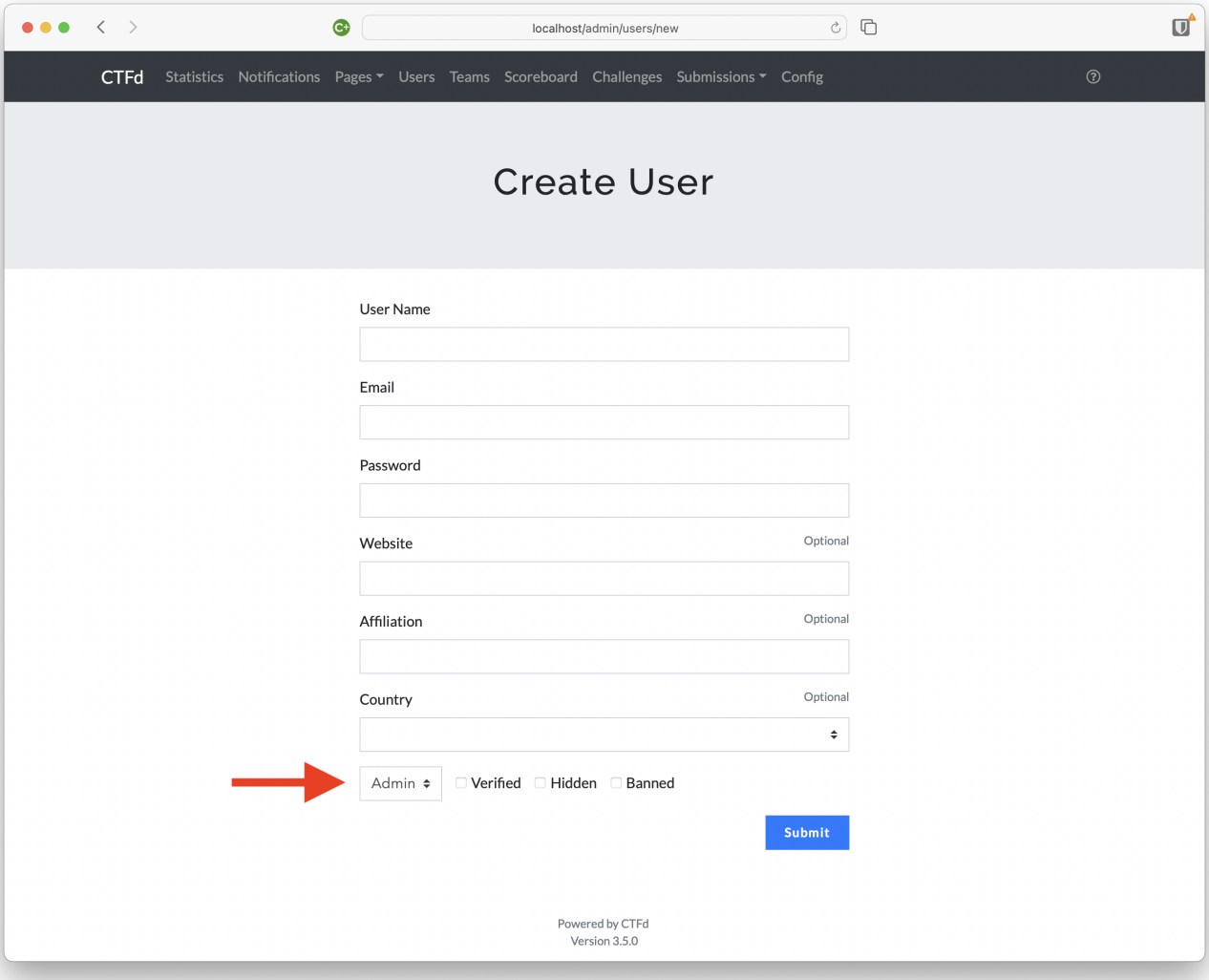

Figure 5: Set the new user account type to "Admin".

5. After you have created the new Admin account, make sure to delete the old one from the "Users" page.

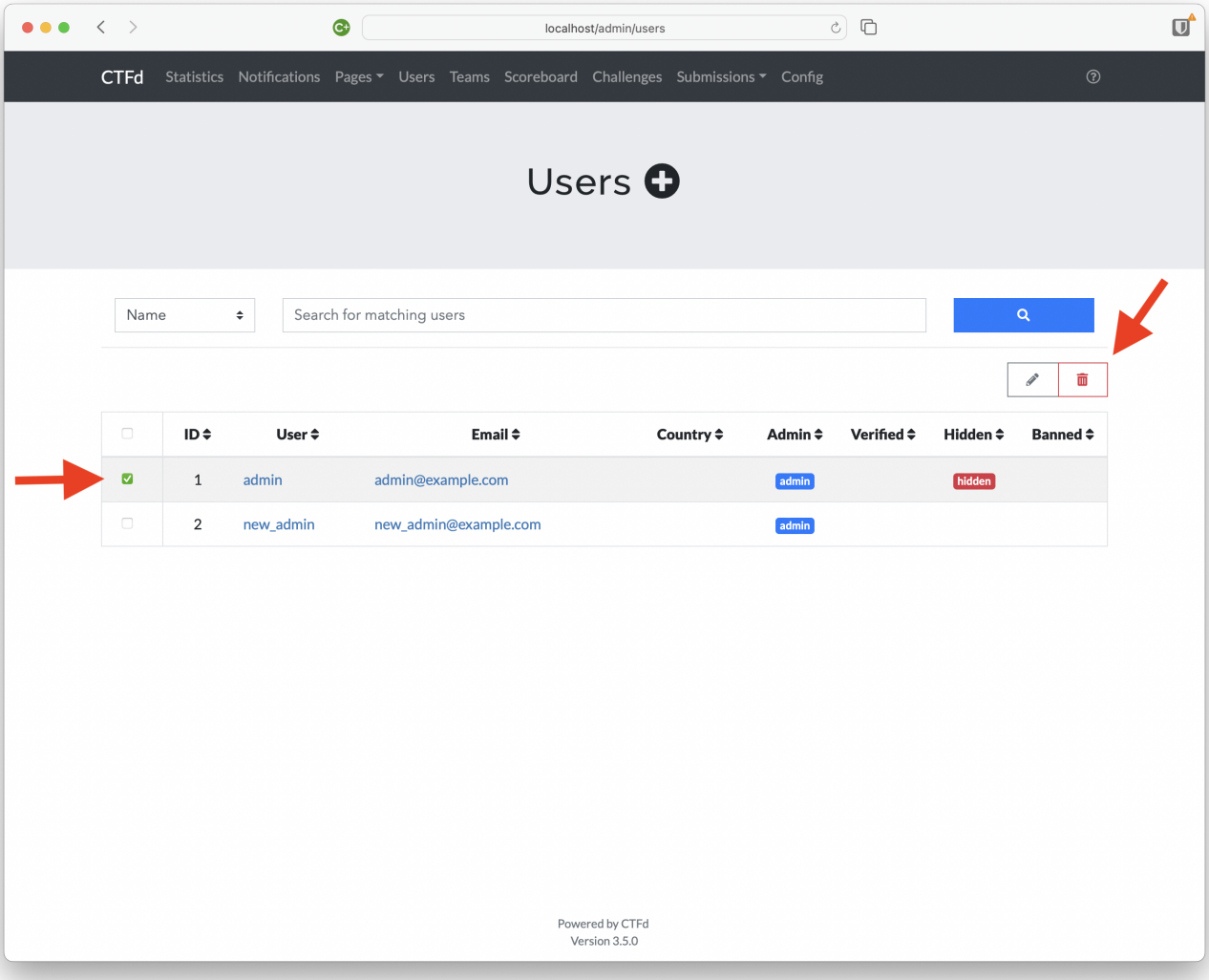

Figure 6: Delete the old Admin account.

1.2.5 Importing challenges

There are two main ways to import CTF challenges into the CTFd application. First, make sure the CTFd application is running, then login to the admin portal using admin credentials. Next, navigate to `Admin Panel > Config > Backup`. From here there are two options: importing a `.zip` or importing `.csv`. There are a few differences between the two import options:

1.2.6 Importing challenges in `.zip` files

- **This will overwrite any existing configurations you have in place**, including user accounts, challenges, files, etc. This essentially imports a snapshot of the CTFd application at the time the `.zip` file was generated.
- Multiple challenges can be imported in a single `.zip` file.
- Files needed to complete the challenges will be included when imported.

1.2.7 Importing challenges in `.csv` files

- This will not overwrite any existing configurations you have in place.
- Multiple challenges can be imported in a single `.csv` file.
- Files needed to complete the challenge **will not** be included when imported.

1.2.8 Challenge Docker Containers

Most of the CTF challenges will require spinning up a Docker container that will host the infrastructure that is unique to running that challenge. The pertinent information for setting up challenge specific Docker containers will be included in a `README.md` file along with the other CTF challenge files.

1.3 Management & Troubleshooting

Student passwords can be reset through the admin panel by clicking on the user in the "Users" tab. If the server goes down, the containers for both CTFd and the docker challenges may need to be restarted. Use the same docker command from the CTFd setup instructions to launch CTFd, and use the "start containers" bash script in the server challenges folder to restart all challenge containers. It is possible you may need to forcibly shut down and remove old container versions if the server restarts. Challenges can be enabled/disabled/modified on the fly using the admin panel of the platform online. Challenge solutions are available to instructors upon request (see bottom of page for contact info).

2 For Students

These instructions can be copied to students to introduce them to CTFs and inform them of how to participate in this CTF platform. Note that you (the administrator) need to plug in the web address of the CTF server in the instructions.

2.1 What is a CTF?

A CTF (Capture The Flag) is a kind of information security competition that can challenge contestants to solve a variety of challenges, ranging from a scavenger hunt on Wikipedia to basic programming exercises, to hacking your way into a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag, hence the name! In the context of this class, these challenges are in CTF format, where each submission consists of a string of text. The challenges are designed to test your mastery of the hands-on security material covered in class, as well as proficiency with the security tools used.

2.2 How to participate

Please navigate to the following link: [your server DNS here]. You may get a security notification that the site is not secure; if so, go to the "advanced" option continue anyway. If Chrome does not work as a browser, Firefox should. Please register a new account using your school email address and a username. Make sure you also remember your password for future logins. Once you log in, you should see a page with challenges for you to complete. Use the prompts and files provided to find the flags!

3 Credits

- Some challenges are based on existing challenges from CTF sources PicoCTF, DEFCON Biohacking, and CSICTF.
- This platform was originally developed by Zack Kaplan as part of a Master's project at Washington University in St. Louis (WUSTL).
- The work is being continued by Dylan Simmons as part of a Master's project at WUSTL.
- The project development is being advised by Steve Cole.

4 Feedback and Collaboration

We'd love to hear your feedback and work together on this project!

- If you're using this platform in your class, please send us an e-mail – we'd love to know how and where the platform is being used.
- If you'd like to fix a bug or generate a new challenge, you may fork this repo and initiate pull requests against it.
- If you'd like to discuss the project and how you might use it in our class, please feel free to contact us directly via e-mail and we'd be happy to talk more about that.

5 Publications

1. Zack Kaplan, Ning Zhang, and Stephen V. Cole. A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class. (ACM ITiCSE'22)

6 Contact Information

Please contact Dylan Simmons or Steve Cole with any:

- Requests for admin credentials for the CTF challenges
- Requests for CTF challenge solutions
- Questions
- Comments
- Suggestions