

Практическое задание для регионального этапа всероссийской олимпиады школьников по технологии 2023 – 2024 учебный год
Профиль «Информационная безопасность»
Практический тур
РУКОВОДСТВО ОРГАНИЗАТОРА – ЗОНА ВОСТОК

ВАЖНО:

- документ конфиденциален! не выдавайте участникам пароль от аккаунта администратора и архива с виртуальной машиной!
- руководство участника размещено на рабочем столе ВМ участника, а также в архиве с ВМ участника (на рабочем столе участника есть текстовый файл со списком дополнительно установленных утилит и расположению сопроводительных материалов)
- все тексты заданий участников дублируются в платформе для проведения практического тура

1. Доступ к виртуальным машинам

Практический тур проводится по правилам CTF – на Платформе CTFd. Для выполнения заданий необходимо скачать и развернуть виртуальную машину администратора (с установленной Платформой CTFd) и участников (с установленными утилитами для решения практических задач), согласно инструкциям ниже.

Виртуальные машины для выполнения заданий практического трека Олимпиады доступны для скачивания в сети Интернет за 2 (двое) суток до проведения Олимпиады по ссылкам ниже:

- Ссылки на скачивание виртуальных машин региона “ВОСТОК” доступны по ссылке https://miem.hse.ru/rosh/2024/download/vmlink_v_2024
Резервная ссылка: https://drive.google.com/drive/folders/1ySwwcXgG9o0tUnV9E1IM-gkNRr46_D5-?usp=sharing
- Зоны отправки заданий приведены в файле “Зоны отправки заданий.doc” убедитесь, что Вы скачали нужный архив с виртуальной машиной администратора
- В случае вопросов создана группа для оперативной связи в телеграмм: <https://t.me/+t84BinbRmoI1MTNi>
- Дополнительные инструкции по работе с Платформой CTF-d приведены на сайте <https://vsosh.miem.hse.ru>

Логины и пароли от административного интерфейса виртуальных машин предоставляются региональным операторам ВСОШ за 2 суток до проведения и приведены ниже в документе.

2. Логины и пароли для доступа к виртуальным машинам

НЕ ПЕРЕДАВАТЬ УЧАСТНИКАМ!

CTFd admin password: 96575ae2-1a83-46cd-847e-07c60c6d4353

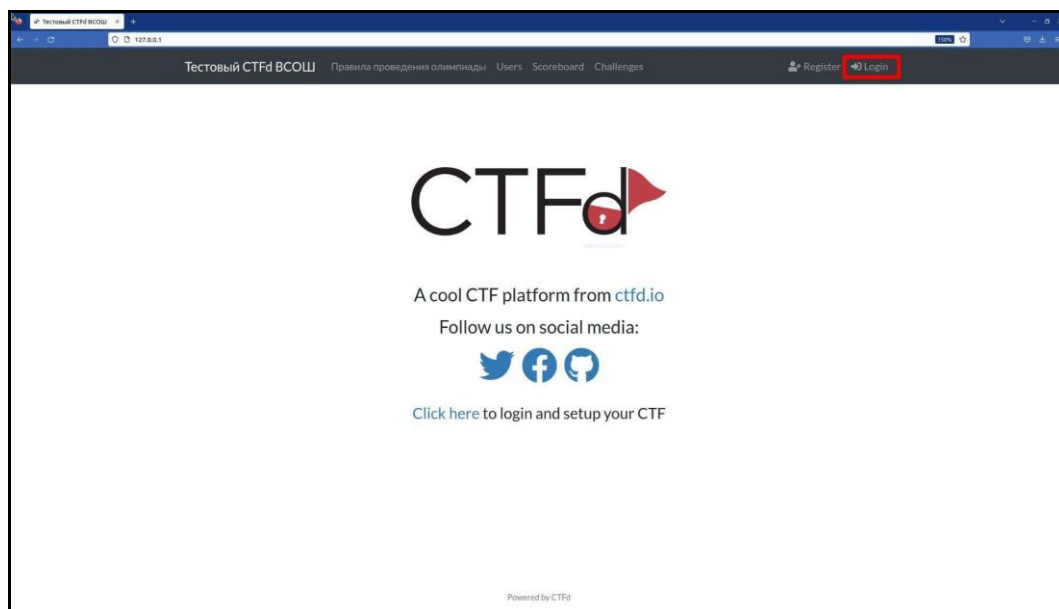
Ubuntu password: Pz@)qwgL&7V+*Q?

zip archive password: 2852253f-ea26-456a-b6ff-2585b87b2128

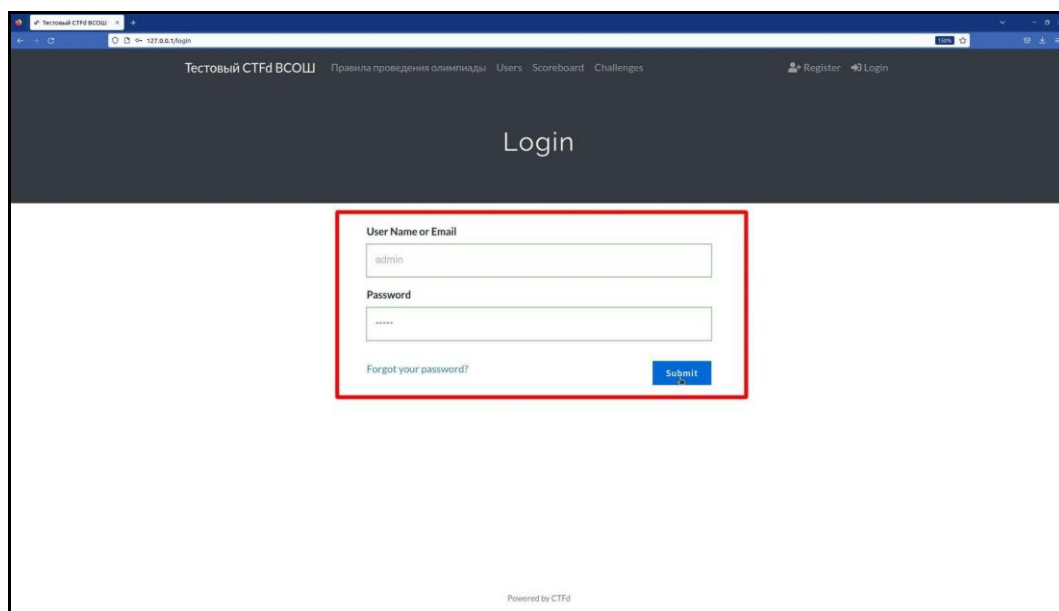
3. Инструкция по настройке виртуальной машины Администратора

1. Необходимо установить VirtualBox¹
 - a. на машины участников;
 - b. на машину Администратора.
2. В виртуальной машине Администратора установлен контейнер с Платформой для проведения практического тура по правилам CTF – платформой CTFd. В виртуальную машину включено всё необходимое для проведения практического тура:
 - a. Платформа CTFd (установлена);
 - b. Задания в виде docker-контейнеров (установлены).
3. Внутри машины организатора находится архив (папка с заданиями). Необходимо перейти в неё:
`cd /home/CTFd`
4. Запуск платформы осуществить следующей командой:
`sudo docker-compose -f single.yml up -d --force-recreate`
5. После завершения запуска платформы перейти в окне браузера по адресу:
<http://127.0.0.1:80>
6. Вам откроется интерфейс платформы:

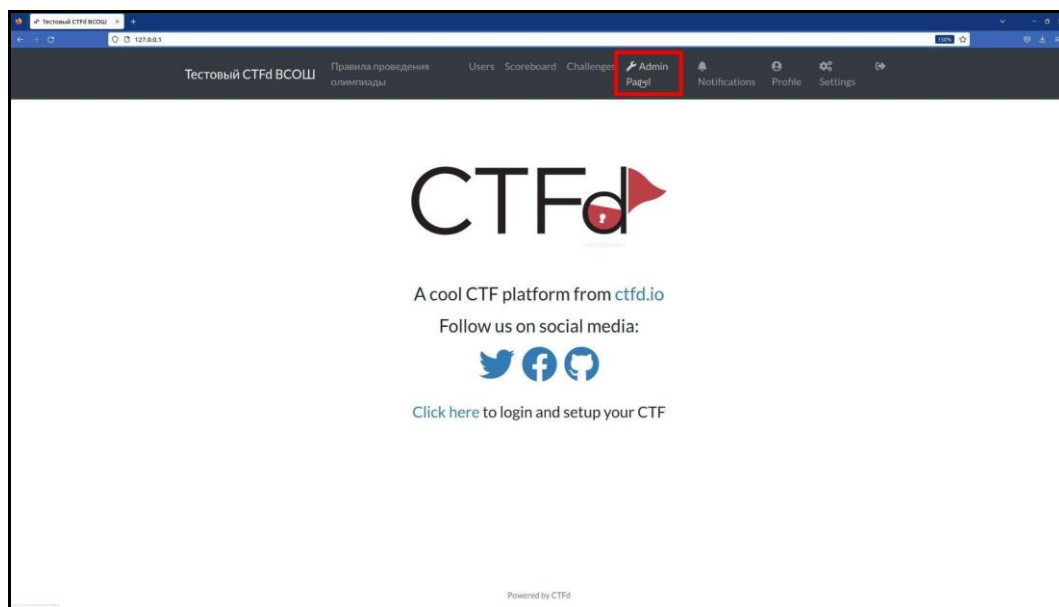
¹ <https://www.virtualbox.org/wiki/Downloads>



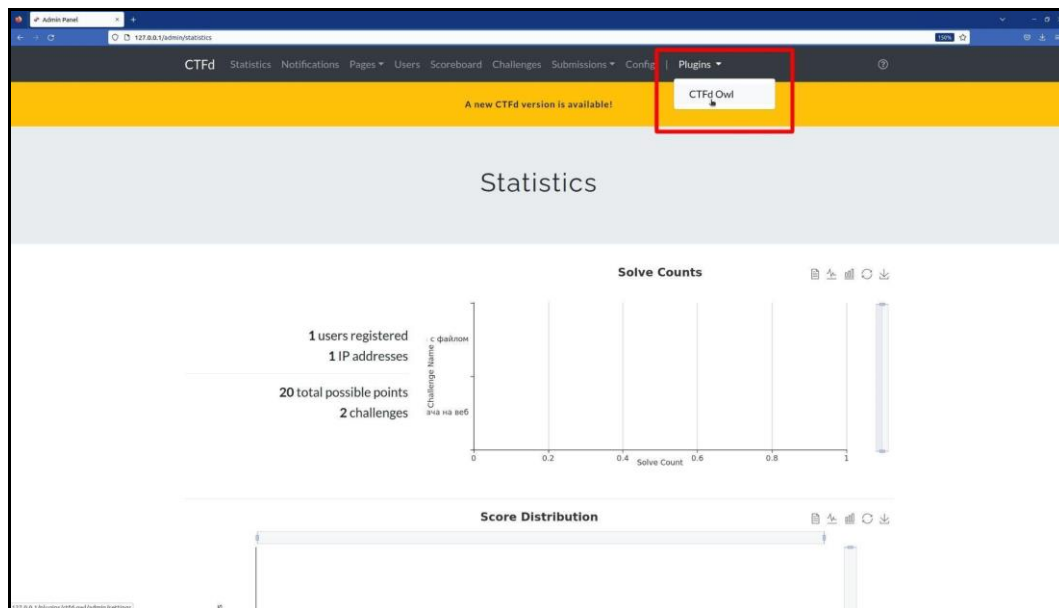
7. Войдите под учетной записью admin (пароль также admin):



8. Перейдите в Admin Panel:

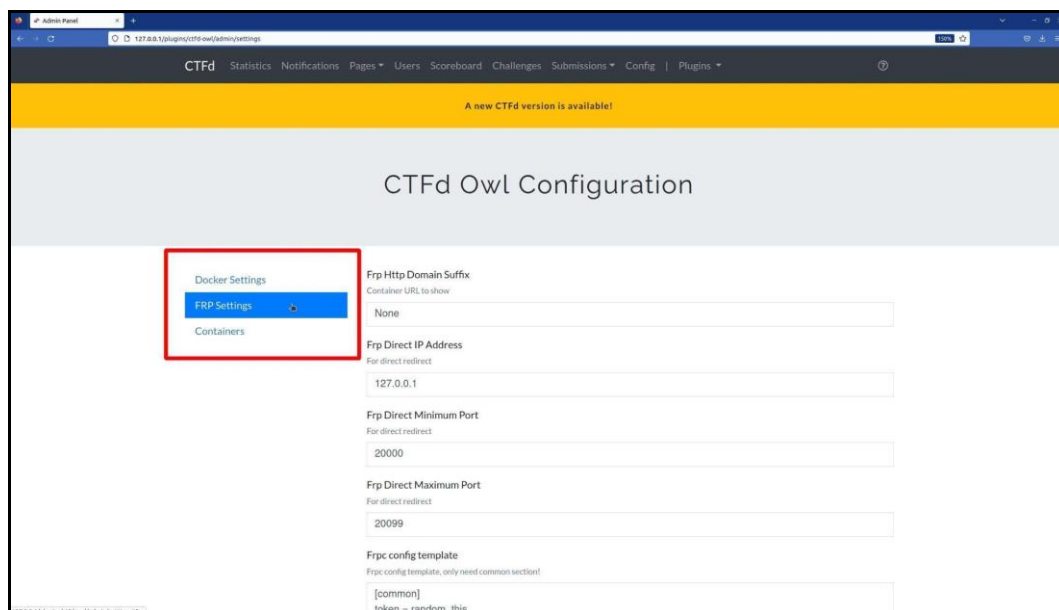


9. Перейдите в Plugins, затем в CTF owl.



10. В разделе FRP Settings замените ip-адрес 127.0.0.1 на ip-адрес Вашей реальной машины в локальной сети, доступной компьютерам участников.

a. Перейдите в раздел FRP Settings:



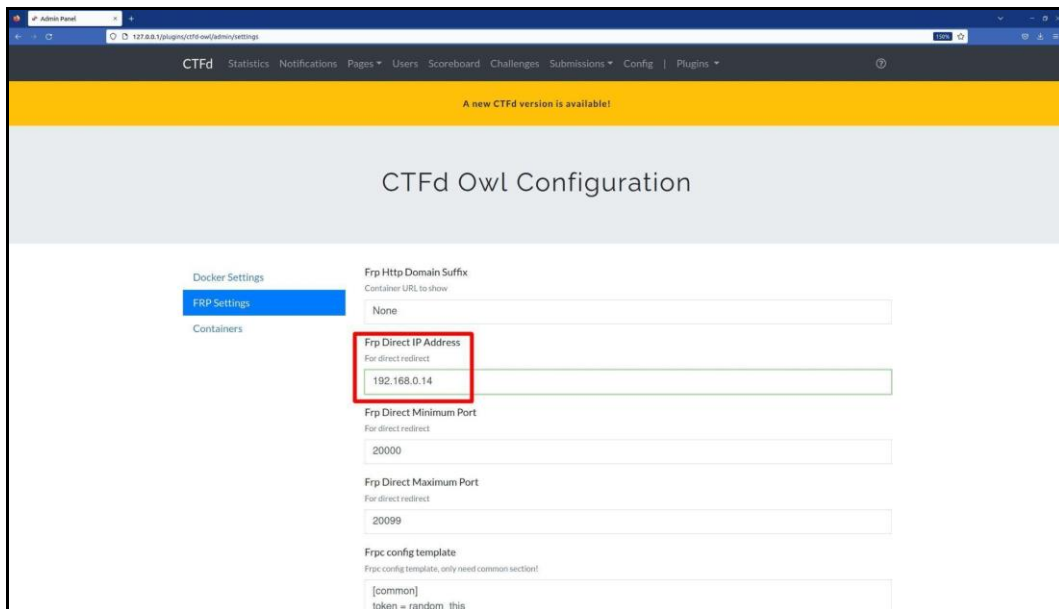
b. Узнать требуемый ip-адрес можно командой:

ip a

Пример:

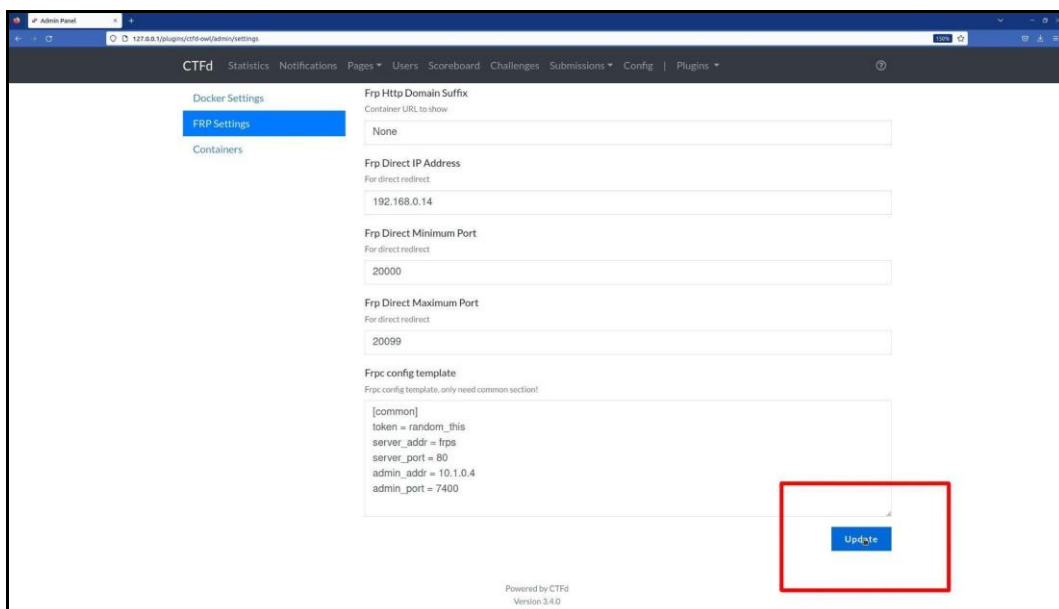
```
: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
   link/ether f8:89:d2:7c:80:8f brd ff:ff:ff:ff:ff:ff
   inet 192.168.0.14/24 brd 192.168.0.255 scope global dynamic noprefixroute wlp2s0
       valid_lft 77545sec preferred_lft 77545sec
```

- с. Замените ip-адрес 127.0.0.1 на ip-адрес Вашей реальной машины в локальной сети, доступной компьютерам участников.



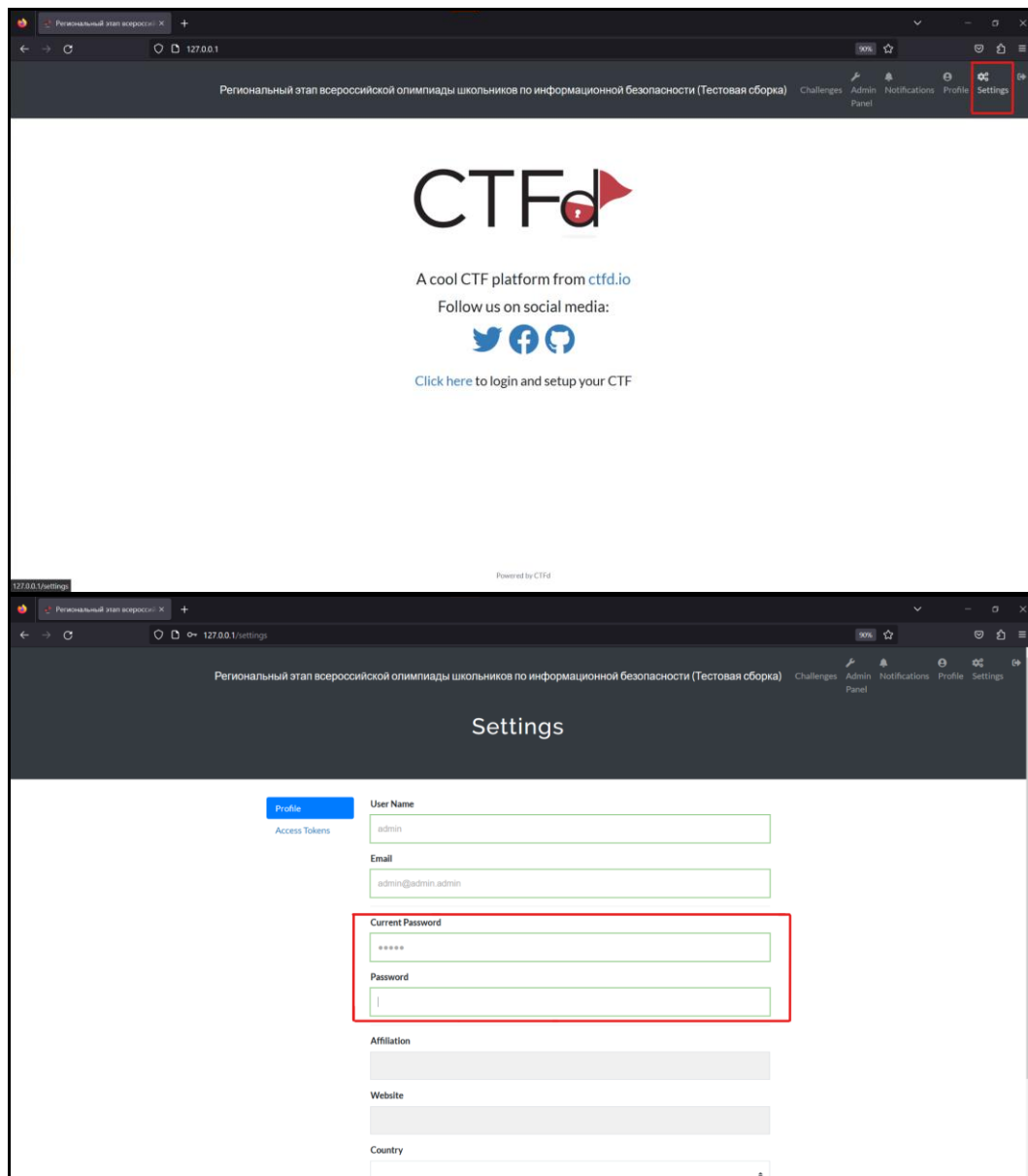
The screenshot shows the CTFd Owl Configuration page. The 'FRP Settings' tab is selected. The 'Frp Direct IP Address' field is highlighted with a red box and contains the value '192.168.0.14'. Other fields include 'Frp Http Domain Suffix' (None), 'Frp Direct Minimum Port' (20000), 'Frp Direct Maximum Port' (20099), and 'Frp config template' ([common]).

- д. Обновите настройки.



The screenshot shows the CTFd Owl Configuration page. The 'FRP Settings' tab is selected. The 'Frp Direct IP Address' field is highlighted with a red box and contains the value '192.168.0.14'. Other fields include 'Frp Http Domain Suffix' (None), 'Frp Direct Minimum Port' (20000), 'Frp Direct Maximum Port' (20099), and 'Frp config template' ([common]). The 'Update' button is highlighted with a red box.

11. Из соображений безопасности измените пароль Администратора в разделе настроек (обратите внимание, что пароль должен быть сложным - **не менее 10 символов, включая заглавные буквы, цифры, а также спецсимволы**):



Regional Stage of the All-Russian Olympiad for Schoolchildren in Information Security (Test Set)

Profile

Access Tokens

Username

admin

Email

admin@admin.admin

Current Password

Password

Affiliation

Website

Country

Submit

Success! Your profile has been updated

Submit

12. Перед началом олимпиады требуется включить виртуальную машину на каждом компьютере участников и перейти в окне браузера ВМ участников по адресу:

[http://\[ip-адрес на IP Вашей виртуальной машины в локальной сети, доступной компьютерам участников\]:80](http://[ip-адрес на IP Вашей виртуальной машины в локальной сети, доступной компьютерам участников]:80)

Пример:

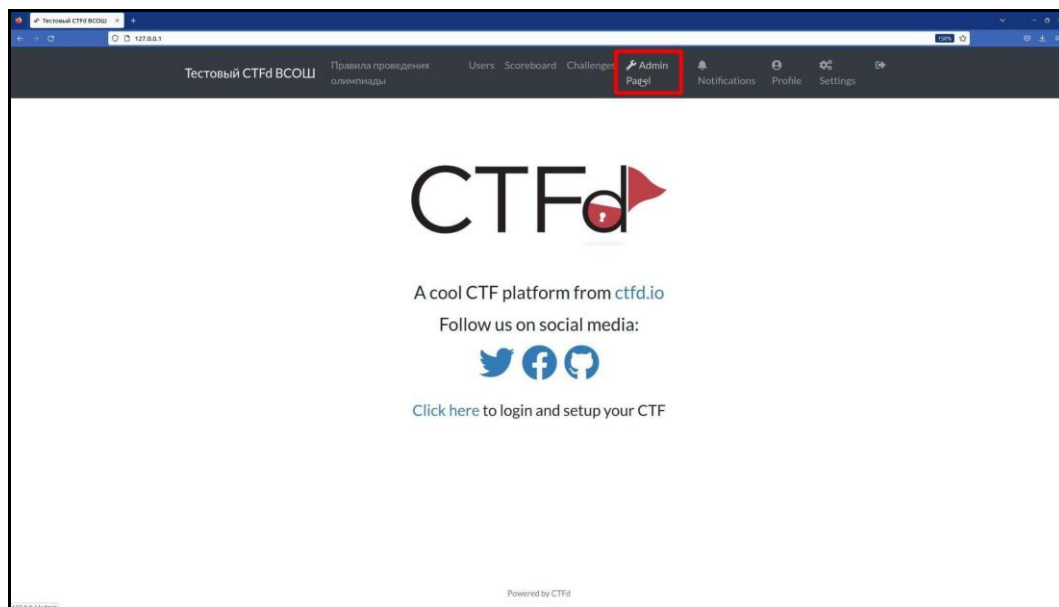
<http://192.168.0.14:80>

13. Проверьте доступность и работоспособность заданий. Для этого зарегистрируйте тестового пользователя и приступите к выполнению одного из заданий.

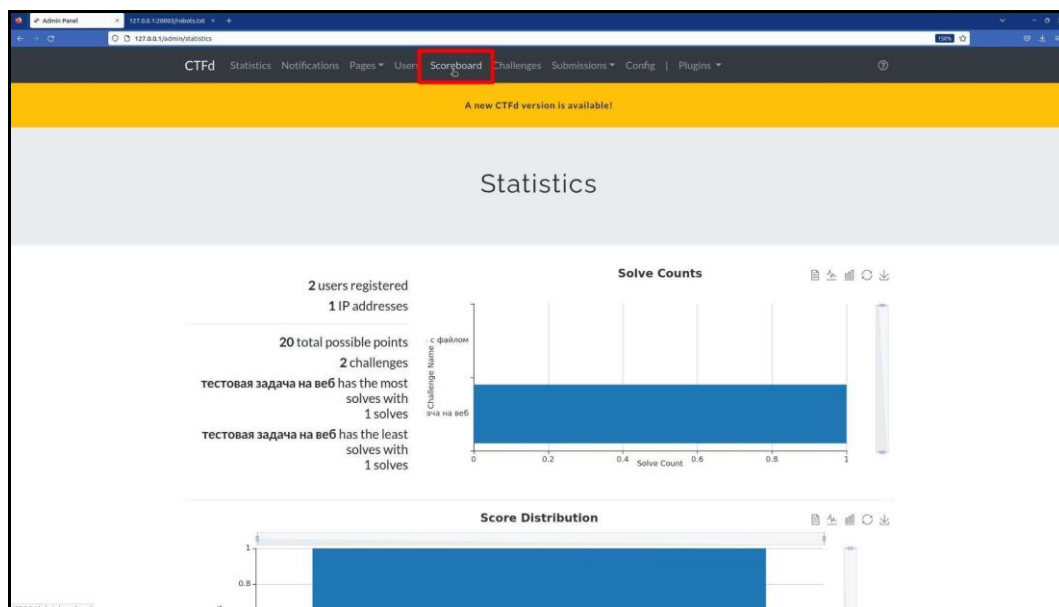
14. **Перед началом практического тура объявите о том, что участники должны зарегистрироваться через Web-интерфейс платформы, используя свой код (id) участника олимпиады в формате v00.000.000 (или используя ФИО в формате фамилия-инициалы - пример для Иванова Ивана Ивановича : ivanov-ii). Попросите участников**

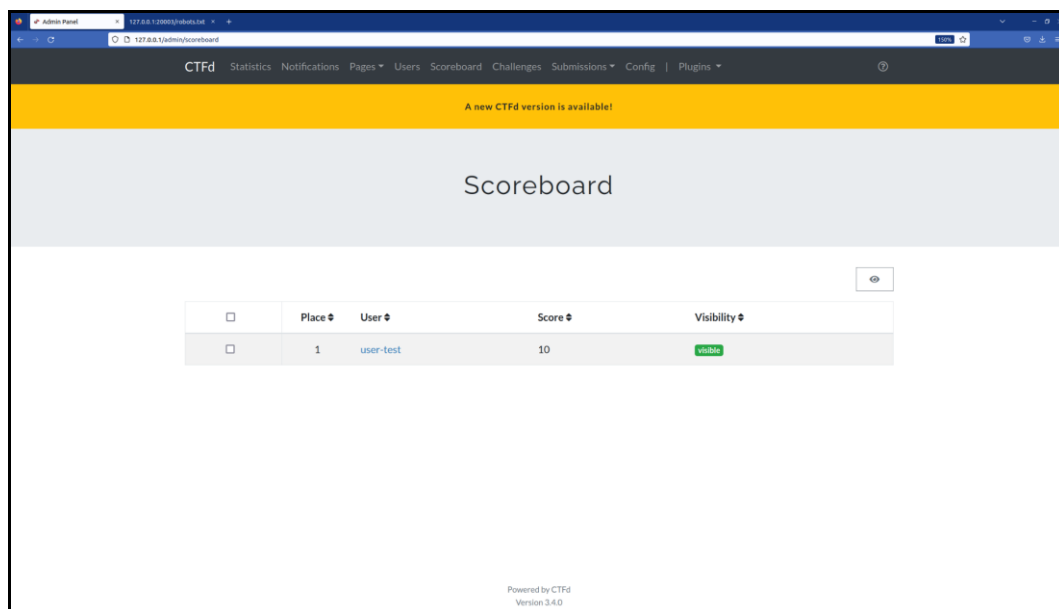
ввести свой код \ имя пользователя и остаться на странице регистрации - проверьте корректность заполнения. После этого объявите о начале практического тура.

15. По окончании тура перейдите в Admin Panel:



16. Откройте раздел Scoreboard (Страница с результатами) и перенесите баллы участников, а также их id на бланк-протокол. Также требуется создать pdf страницы с итоговыми результатами и приложить к итоговому протоколу:





4. Инструкция по настройке виртуальной машины участника и выполнению задания

1. Виртуальная машина участника (скачанная по ссылкам выше), устанавливаемая на компьютерах участников, включает:
 1. Необходимый набор утилит для решения задач практической части.
 2. README.txt с их перечнем.
 3. Cheatsheet с дополнительной информацией по заданиям.
2. Виртуальные машины участников должны быть установлены и запущены под управлением монитора виртуальных машин (VMM) Virtual Box (см. выше)
3. Перед началом олимпиады требуется включить виртуальную машину на каждом компьютере участников и перейти в окне браузера ВМ участников по адресу:

`http://[ip-адрес на IP Вашей виртуальной машины в локальной сети, доступной компьютерам участников]:80`

Пример:

`http://192.168.0.14:80`

4. Необходимо настроить и проверить доступ к Платформе CTF-d из браузеров с виртуальных машин участников.



5. Перед началом практического тура участники должны зарегистрироваться через Web-интерфейс платформы, используя свой код (id) участника олимпиады в формате v00.000.000 (или используя ФИО в формате фамилия-инициалы - пример для Иванова Ивана Ивановича : ivanov-ii)

Тестовый CTFd ВСОШ Правила проведения олимпиады Users Scoreboard Challenges Register Login

Register

User Name
user-1
Your username on the site

Email
example@example
Never shown to the public

Password
.....
Password used to log into your account

Submit

Powered by CTFd

6. Вам откроется страница с заданиями по темам:

Тестовый CTFd ВСОШ Правила проведения олимпиады Users Scoreboard Challenges Notifications Profile Settings

Challenges

Форензика

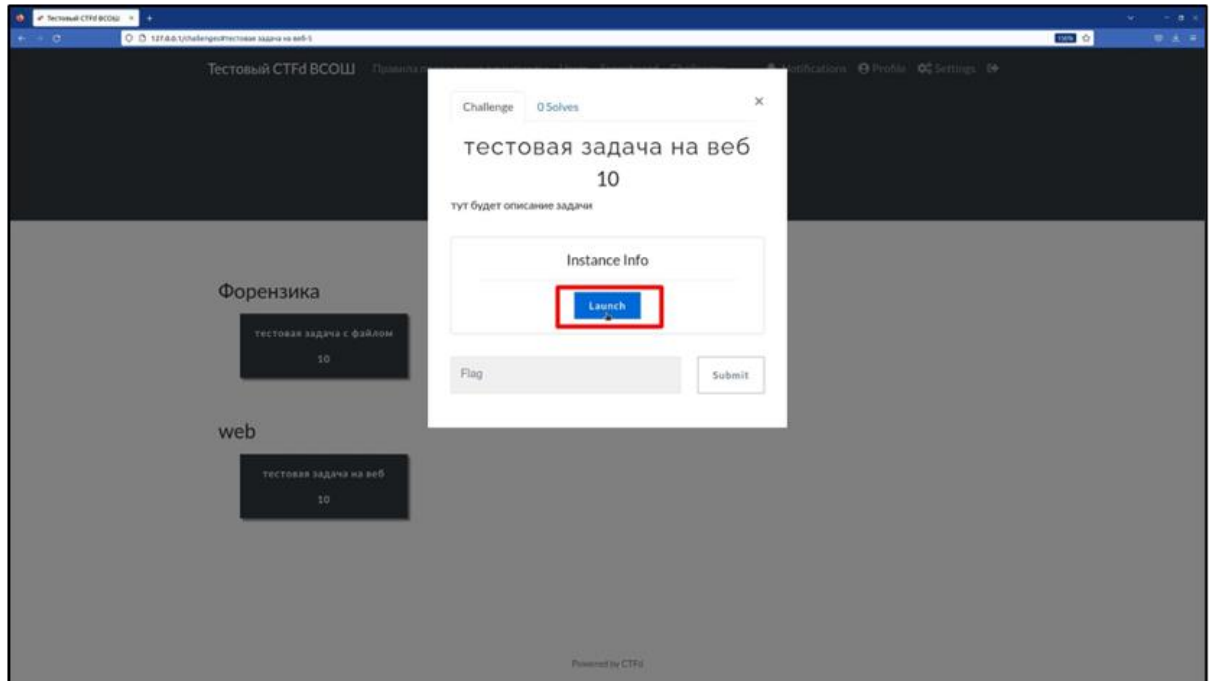
тестовая задача с файлом
10

web

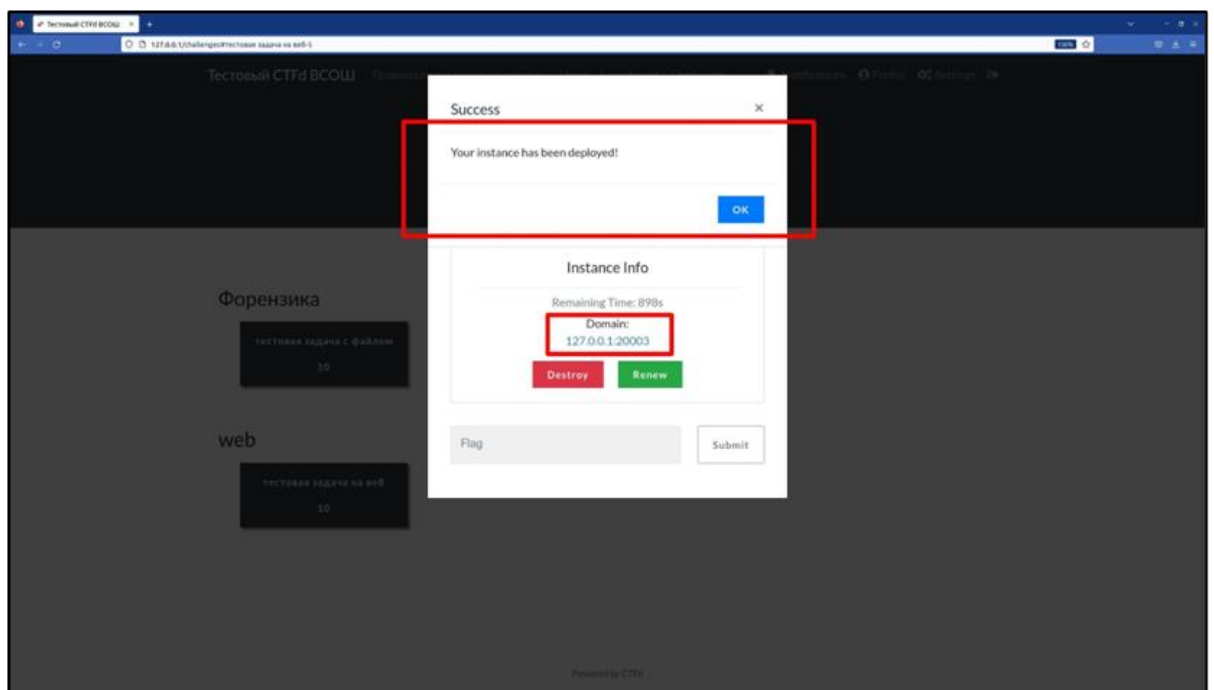
тестовая задача на веб
10

Powered by CTFd

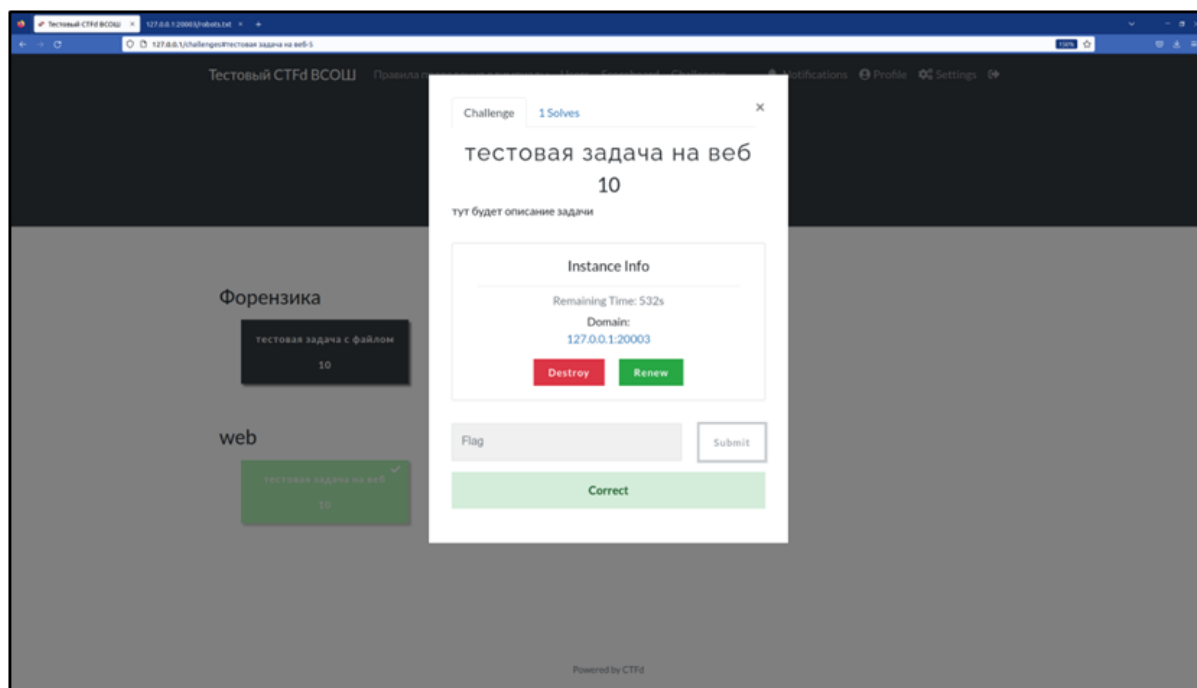
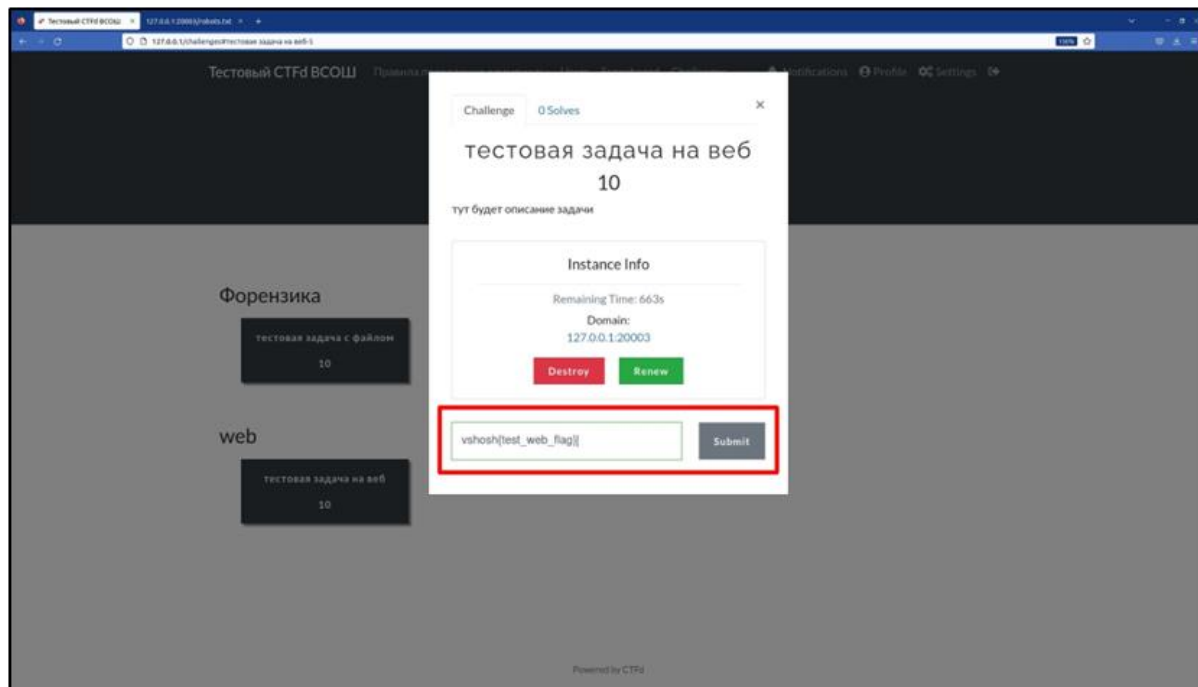
7. При открытии задания Вы увидите краткое описание задания и необходимую справочную информацию, если присутствует – нажмите кнопку Launch:



8. Дождитесь запуска задания и перейдите по указанному адресу (в случае задачи не на веб, более подробные инструкции по подключению к задаче будут указаны в описании задания):



9. Ваша цель – выполнить как можно больше заданий. Оценка заданий производится автоматически по факту размещения участником в поле для ввода корректного флага – строки определенного вида (`vsosh{последовательность цифр, букв и спецсимволов}`), например - `vsosh{s0m3s7r1n6}`), доступ к которому является индикатором успешного решения задания:



10. Максимально возможное число баллов за практический тур указано в задании.