ПОДМОСКОВНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ИНФОРМАТИКЕ
ПРОФИЛЬ “ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ”. 2025-2026 уч. г.
ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

ИНСТРУКЦИЯ ДЛЯ УЧАСТНИКА.

7 июня – Практический тур на профиле “Информационная безопасность”

Тематика заданий

В практическом туре необходимо решить как можно больше заданий за 4 часа олимпиады. Наборы заданий ориентированы на комплексную оценку навыков и охватывают:

- Навыки анализа WEB-Приложений (Web Security)
- Исследование артефактов инцидентов информационной безопасности (Digital Forensic)
- Знание и умение работать с криптографией (Crypto)
- Исследование скомпилированных программ (Reverse Engineering)
- Понимание механизмов работы компьютерных сетей (Networking)

Доказательством решения задания является ‘флаг’ – строка определённого формата, которую необходимо получить из задачи и сдать на платформе для получения баллов. Формат для этой олимпиады posh{…}, где на месте … может быть любая комбинация из букв, цифр и спецсимволов.

Инструменты для решения задач

Образ виртуальной машины взят с Всероссийской Олимпиады Школьников и в нём содержатся файлы, которые были необходимы для проведения заключительного этапа. Для решения задач нашей олимпиады они не требуются, всё что необходимо для решения олимпиады перечислено в инструкции участника далее и находится на платформе для решения задач.

На ПК участника олимпиады должен отсутствовать доступ в сеть “Интернет”, исключение - доступ к VPN платформы, в случае удаленного участия.

На ПК участника должен быть установлен гипервизор VirtualBox. Виртуальная машина участника должна быть развёрнута к моменту рассадки участников по аудиториям.

Участнику предоставляется образ виртуальной машины с необходимым программным обеспечением для решения заданий. Виртуальную машину (ВМ) участника требуется запустить до начала практического тура и проверить доступность аккаунта на платформе до начала аудитории. Обязательно отсутствие у участника Административных прав в хост- системе.

ВМ участника включает:

- Необходимый набор утилит для решения задач практической части.
- Cheatsheet (инструкции) с информацией по вариантам использования некоторого инструментария.

Дополнительно установленные утилиты:

- SREF Ghidra
- IDA Freeware 9.2
- gdb
- edb
- strace
- ltrace
- dirsearch
- curl

- Libreoffice
- binwalk

Дополнительно установленные модули Python 3:
- pwntools, pybase64, sympy

Дополнительно установленные расширения BurpSuite:
- JWT Editor

Volatility folder: /home/kali/volatility3
При использовании volatility3 надо активировать виртуальное окружение - source /home/kali/volatility3/venv/bin/activate

Путь до rockyou.txt :
/usr/share/wordlists/rockyou.txt

В рамках ограничений по времени и отсутствия подключения к Сети,
мы традиционно предоставляем документацию - hacktricks, OWASP CheatSheetSeries и PayloadAllTheThings.
Склонированные репозитории расположены на рабочем столе:
/home/kali/Desktop/hacktricks
/home/kali/Desktop/CheatSheetSeries
/home/kali/Desktop/PayloadAllTheThings

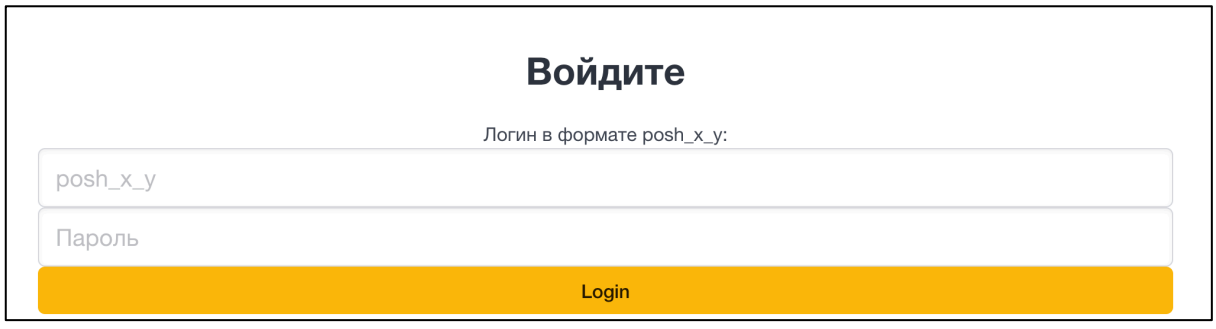
Дополнительно участникам предоставлен удобный инструмент для обработки данных Cyberchef. Он расположен по адресу https://cyberchef.informatics.ru.

Подробная инструкция по выполнению заданий на платформе YATB.

Логин на платформу

На вашем рабочем месте помимо ноутбука и бланка регистрации должен быть маленький лист, который содержит пару логин:пароль в формате posh_x_y : abcdef_abcdef
Вам необходимо войти с этими учётными данными на платформу чтобы начать решение задач.

Прямая ссылка на форму входа – posh.informatics.ru/login .



ПОДМОСКОВНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ИНФОРМАТИКЕ
ПРОФИЛЬ “ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ”. 2025-2026 уч. г.
ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

Обзор панели с тасками (задачами)

Задачи появятся на платформе в момент начала олимпиады. Пример того, как они будут выглядеть, вы можете посмотреть ниже.

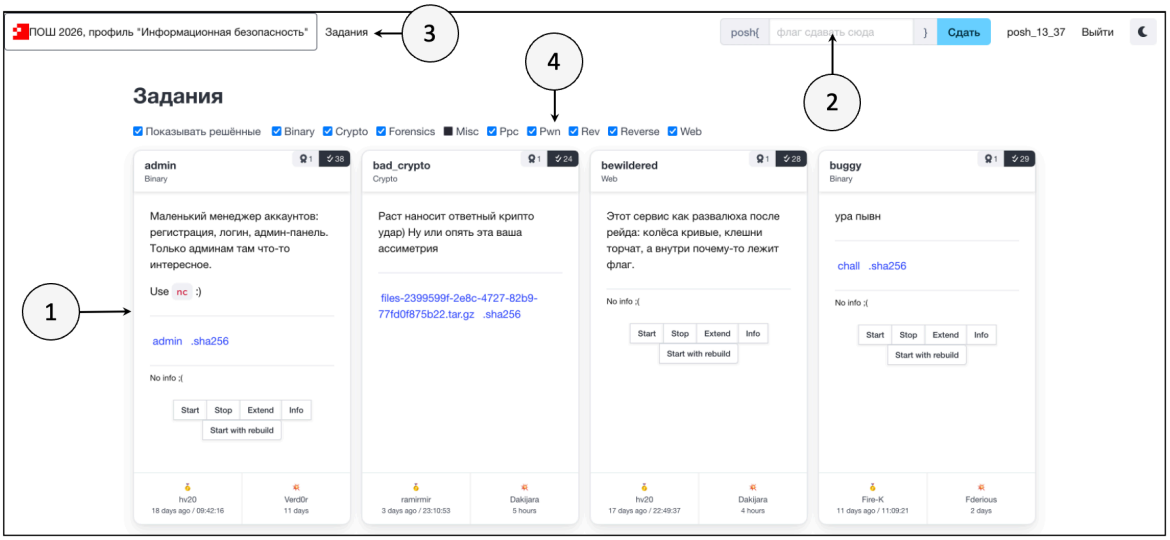
Интерфейс платформы выглядит следующим образом:

1) Панель с задачами. Вы можете нажать на название задачи чтобы войти в полноэкранный режим отображения задачи. Каждая задача содержит “флаг”, который необходимо найти в задаче путём её решения и сдать в систему чтобы получить баллы за решение задачи.

2) Форма для сдачи ответов – флагов в формате posh{…}, где на месте … может быть любая комбинация букв, цифр и спецсимволов. Вы можете сдать флаг без обёртки posh{}.

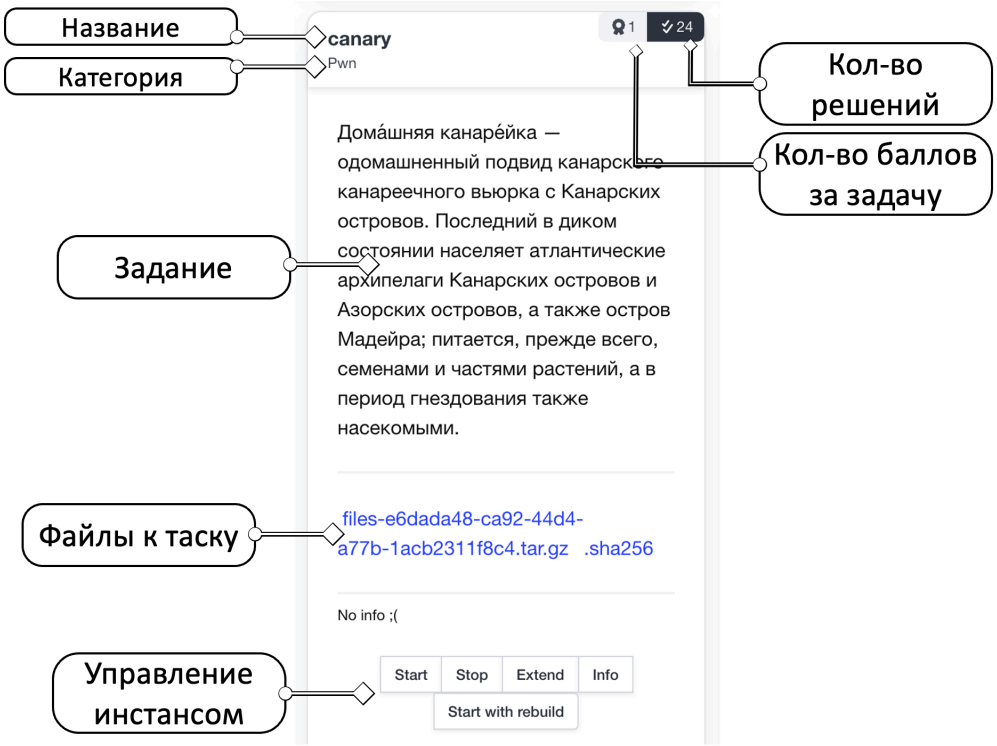
3) Если вы захотите вернутся на панель задач, то нажмите кнопку “Задания” в верхней левой части экрана.

4) Вы можете отфильтровать таски по категориям. На панели задач будут отображаться только те задачи, у которых проставлена галочка в фильтрации.



Из чего состоит задача (таск)

Каждая задача состоит из нескольких информативных частей.



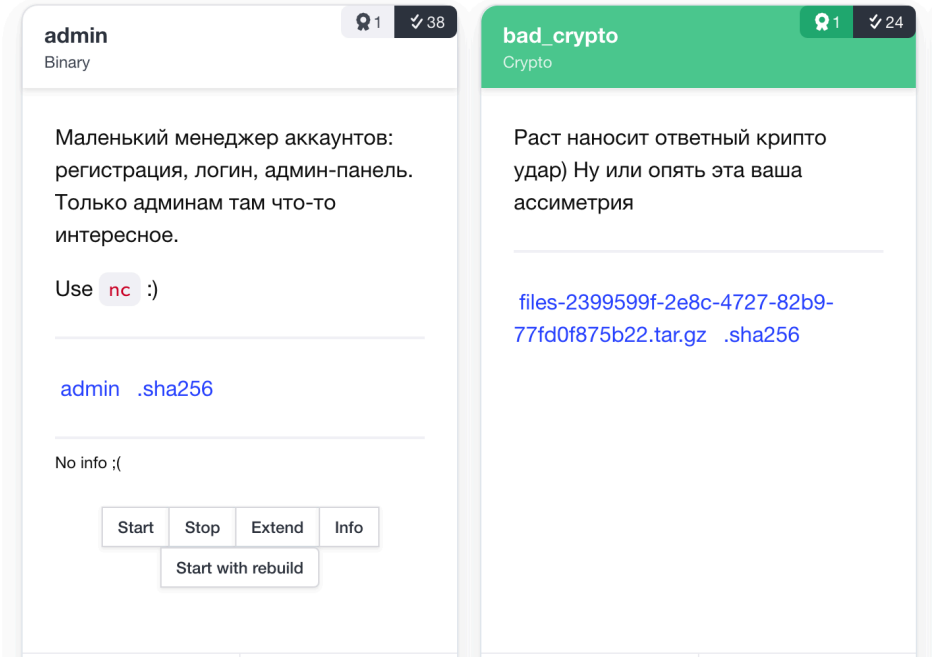
Обратите внимание, что если у задачи есть хотя бы один файл, то будет автоматически сгенерирован и предоставлен ещё один файл .sha256 для проверки целостности скачанных файлов.

Универсальный совет – решайте в первую очередь те задачи, у которых больше всего решений.

Решение задачи подразумевает анализ предоставленной информации (включая название задания и его текст), предоставленных файлов и/или ссылок с целью найти “флаг”, который является доказательством решения задачи и который необходимо сдать на платформе в соответствующую форму. Различные категории задачи подразумевают различных подход к решению задач, но не ограничиваются им.

- Задачи категории **WEB** подразумевают в первую очередь анализ WEB-приложений и поиск типовых уязвимостей с целью их эксплуатации.
- Задачи категории **Binary** подразумевают в первую очередь анализ, при помощи специальных программ, скомпилированные программы с целью повторения реализованного алгоритма либо поиска низкоуровневых уязвимостей
- Задачи категории **Crypto** подразумевают в первую очередь анализ и поиск проблем в предоставленной математической модели шифра, экземпляра шифротекста либо программы, в которой реализован какой-нибудь криптографический алгоритм.
- Задачи категории **Forensic** подразумевает в первую очередь анализ артефактов некого инцидента информационной безопасности. Обычно это сетевой трафик, дамп оперативной памяти или образ диска.
- Задачи категории **Misc** включают в себя различные другие темы, которые не получается подвести под какую-то одну большую категорию. Например, в этом контесте вы найдёте задачи категории “Networking”, которые проверяют навыки работы с компьютерными сетями.

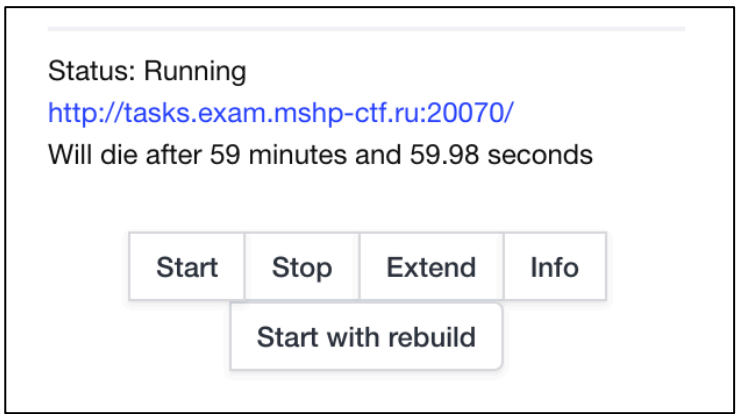
При успешной сдаче флага от какой-либо задачи карточка этой задачи изменит свой дизайн:



Ваша задача – сделать так чтобы все карточки задач имели зелёный заголовок :)

Работа с инстансами задач

Платформа олимпиады поддерживает “инстансы” – выделенные экземпляры задачи для каждого из участников. Не у всех задач есть механизм выделенных экземпляров задач, но у некоторых вы найдёте меню управления инстансом задачи. После запуска инстанса задачи подождите 1-2 минуты пока контейнер развернётся. После вы можете решать таск по предоставленным ссылкам или файлам.



Кнопка “Запустить” (“Start”) позволяет запросить экземпляр задачи у платформы, кнопка “Остановить” (“Stop”) позволяет выключить и удалить экзепмляр задачи.
Инстансы по умолчанию активны один астрономический час. Если вы решаете таск дольше этого времени - не забудьте нажать кнопку “Продлить” (“Extend”). В ином случае прогресс решения задачи будет удалён когда таймер достигнет нуля. Нажмите кнопку “Info” чтобы посмотреть актуальный таймер инстанса.
Если вам кажется, что вы что-то сломали в вашем экземпляре задачи, то нажмите кнопку “Перезапустить с пересборкой” (“Start with rebuild”).

ЧЕРНОВИК