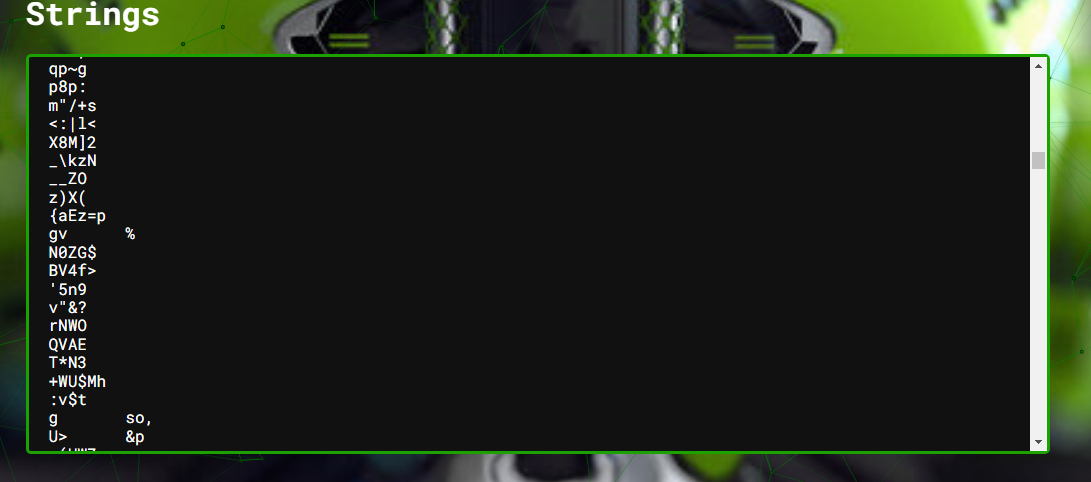
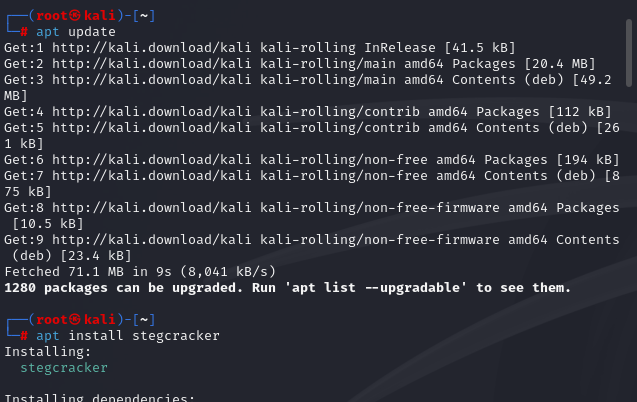
Kopatych.

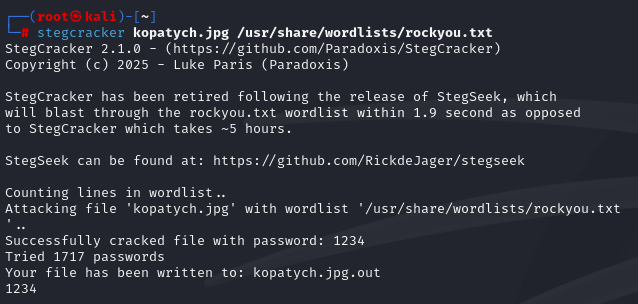
Скачиваем картинку Копатыча, и при первом анализе на сайте https://www.aperisolve.com/ в строке strings мы можем заметить, что в картинке есть зашифрованный файлик.



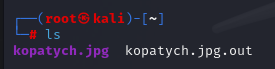
Используем инструмент stegcracker чтоб его достать. По умолчанию данного инструмента нет в образе Kali, поэтому нужно сначала его установить.



Теперь используем данный инструмент на нашей картинке. Использовать stegcracker просто, передайте ему файл в качестве первого параметра и, по желанию, передайте путь к списку слов паролей для проверки в качестве второго параметра. Если вы не укажете список слов, инструмент попытается использовать встроенный список слов rockyou.txt, который поставляется с Kali Linux. Пример использования видно на скриншоте ниже.

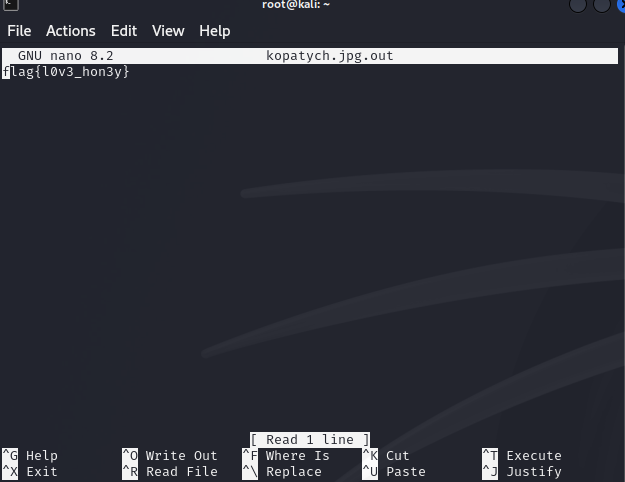


В результате мы получим вывод в виде файла kopatych.jpg.out, который сохранится в той же директории, где находилась наша картинка.



Далее нам нужно просто посмотреть что находится внутри данного файла с помощью nano, и там мы обнаружим нужный нам флаг.





Полезные ссылки:

<https://github.com/Paradoxis/StegCracker>

<https://spy-soft.net/rockyou-txt/>

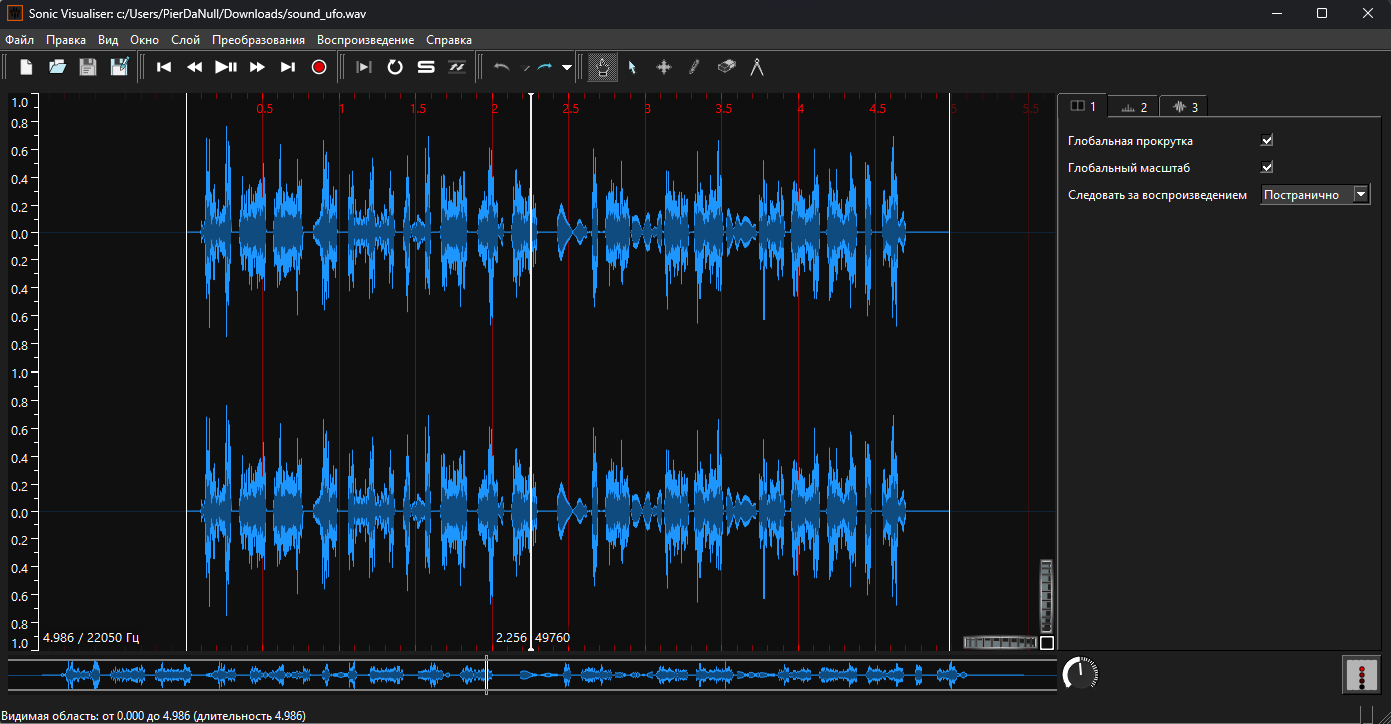
<https://www.aperisolve.com/>

UFO.

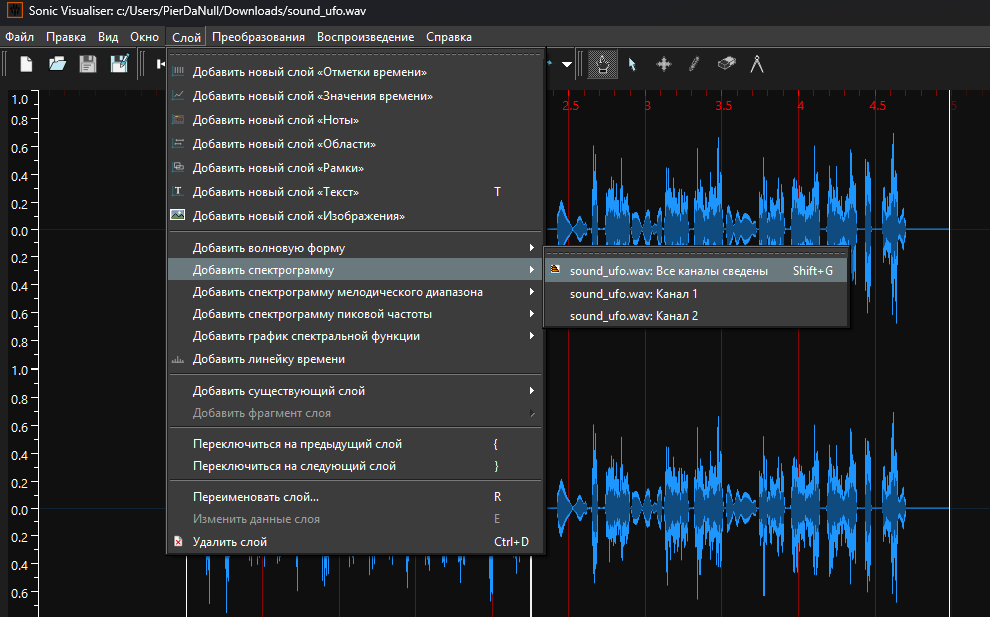
Описание: Мы получили сообщение из космоса, пока не очень понятно, что хотели сказать нам внеземные формы жизни, но может ты справишься?

Скачиваем файл sound\_ufo.wav и сразу понимаем, что это какая-то звуковая запись, но прослушав услышим непонятные шумы. Первое и самое очевидное что мы можем сделать с данным waf – это посмотреть его спектрограммы. Это можно сделать разными инструментами на разных ОС, я буду использовать инструмент sonic visualiser.

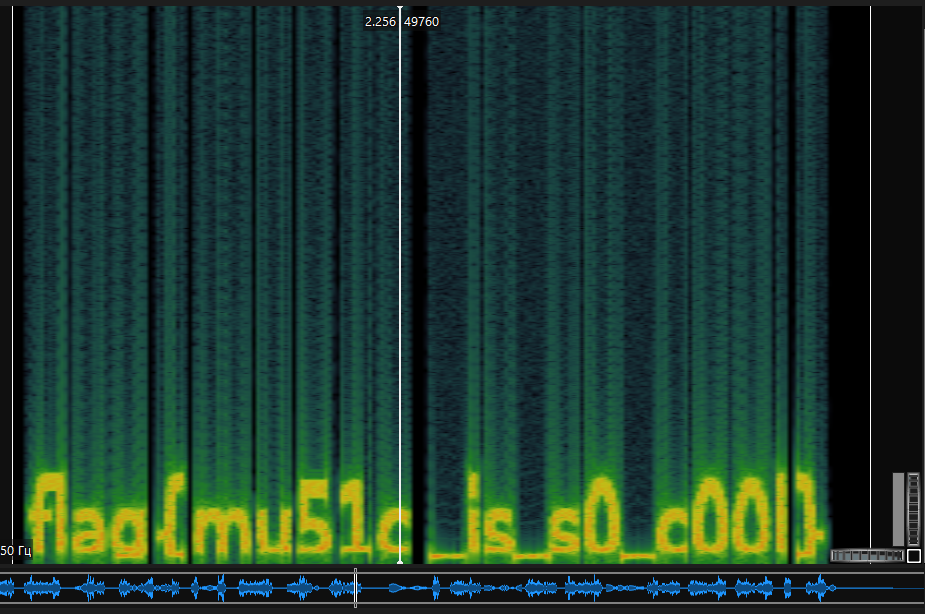
Открываем наш файл в данном инструменте.



Пока ничего не ясно и непонятно, нам нужно зайти во вкладку слой > добавить спектрограмму > все каналы сведены.



После этого немного поигравшись колесиком мыши, будет виден нужный нам флаг.



Полезные ссылки:

<https://codeby.net/threads/osnovy-steganografii-v-capture-the-flag.63200/>

<https://www.sonicvisualiser.org/>

CryptoPyc.

Описание: Атомная Станция - очень серьезный объект! Информации там много, хранить и передавать нужно!

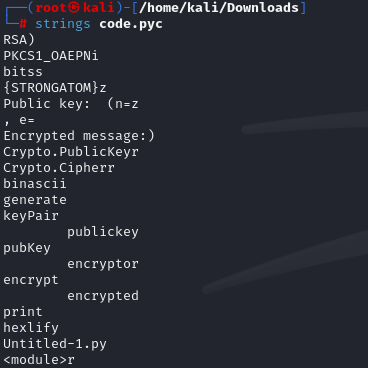
Наш программист написал приложение, которая выдает зашифрованное сообщение и какой-то ключ.

Попробуйте расшифровать, что мы там спрятали. Заодно и код проверим!

Формат флага- flag{EXAMPLE}

P.S. Для работы потребуется - pip install pycryptodome.

Читаем большое описание к заданию, ничего не понимаем, и скачиваем файл code.pyc. По описанию задания и количеству баллов за него кажется, что оно очень сложное. Но самое первое что я советую делать в любой непонятной ситуации – это пройтись инструментом strings по непонятному файлу.



Видим много всего непонятного, но бросается в глаза {STRONGATOM}, буд-то это нужный нам флаг, только не хватает слова flag вначале, попробуем это ввести как флаг flag{STRONGATOM}. И да, все не так сложно, как казалось.

CryptoAtom.

Описание: Найдите ключ, которым зашифровали слово

Обернуть в flag{example} обязательно!

Для работы кода - pip install pycryptodome

Читаем описание таска, скачиваем непонятный файл code2.cpython-310.pyc, и в первую очередь как я уже говорил выше, проходимся инструментом strings.

TheBox.

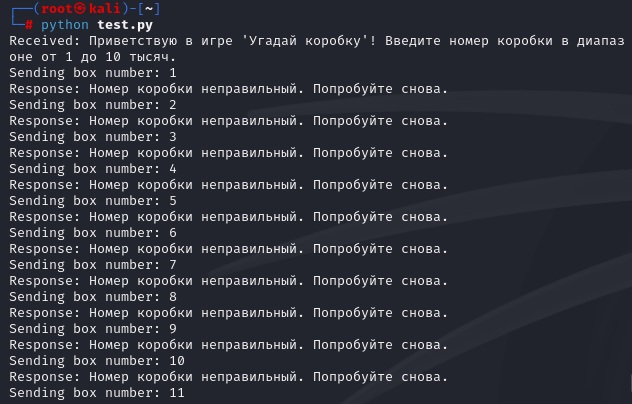
Описание: 10 тысяч коробок привезли!

Подумай только, как среди них найти нашу?

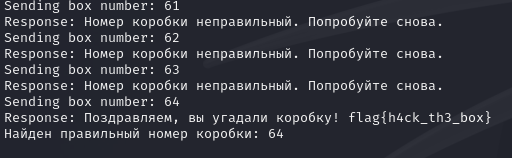
P.S. Важное уточнение - номер коробки является уникальным и после отключения от активной сессии с ботом - номер изменится. Учтите это в своих скриптах.

\*\*nc ctf.hackatom.ru 1234\*\*

Пытаемся подключиться к серверу nc ctf.hackatom.ru 1234, мы знаем что правильный номер коробки от 1 до 10000,понимаем методом тыка что мы должны угадать правильный номер коробки и у нас бесконечное количество попыток. Т.к. пользоваться ChatGPT на соревнованиях не запрещено, мы идем и просим сгенерировать код, который за нас переберет номера на сервере. Запускаем данный скрипт и просто ждем.



И спустя некоторое время скрипт угадывает правильный номер коробки, и мы получаем нужный нам флаг.



Полезные ссылки:

<https://chatgpt.com/>

бесплатный впн плагином на браузер – browsec

TheCalc.

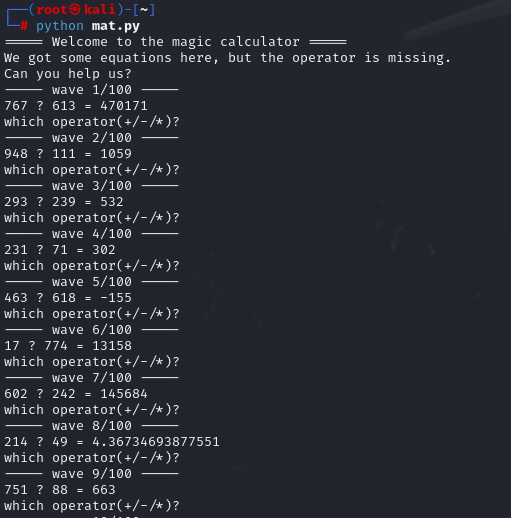
Описание: У нас есть калькулятор, но он сломался..

Нам срочно нужно решить 100 примеров, ошибешься хоть на один....

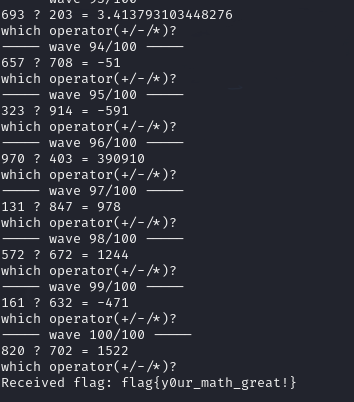
Всему прогрессу - конец!

\*\*nc ctf.hackatom.ru 10001\*\*

Аналогично таску TheBox подключаемся к серверу nc ctf.hackatom.ru 10001, узнаем подробно условия задачи, и просим ChatGPT сгенерировать нам код, который решит за нас все примеры и выведет флаг. Запускаем скрипт.



Получаем нужный нам флаг.



Полезные ссылки:

<https://chatgpt.com/>

бесплатный впн плагином на браузер – browsec

D-Link.

Описание: Хочу следить за тем, что там мой друг смотрит в интернете...

Не спрашивай зачем, ведь как говорила моя подруга из Канады - "Люди могут простить почти всё - не прощают лишь тем, кто не интересуется чужими делами".

А я хороший друг...

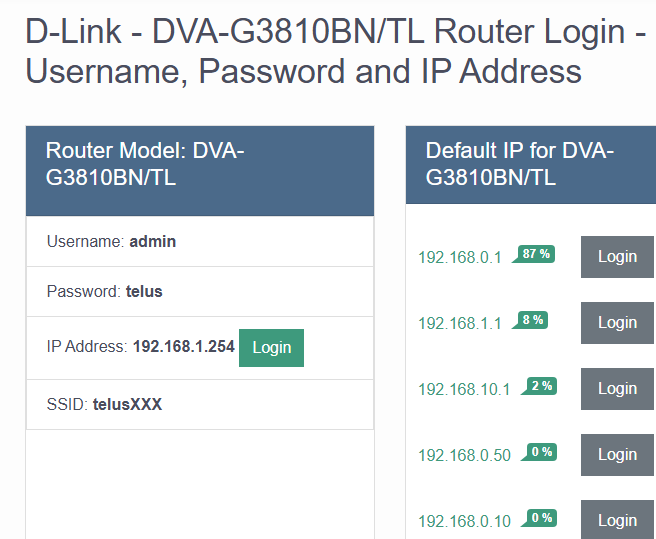
http://ctf.hackatom.ru:3001/

Описание таска нам ни о чем не говорит, поэтому мы сразу переходим на сайт <http://ctf.hackatom.ru:3001/> . Видим страничку входа в админ панель роутера D-Link.



В первую очередь нужно попробовать зайти под заводским пользователем.

Слева сверху м видим модель роутера, попробуем поискать в интернете, какие логин с паролем у заводского пользователя данной модели.



Пытаемся ввести найденные логин с паролем на нашу страничку авторизации. Успешно входим и видим нужный нам флаг.



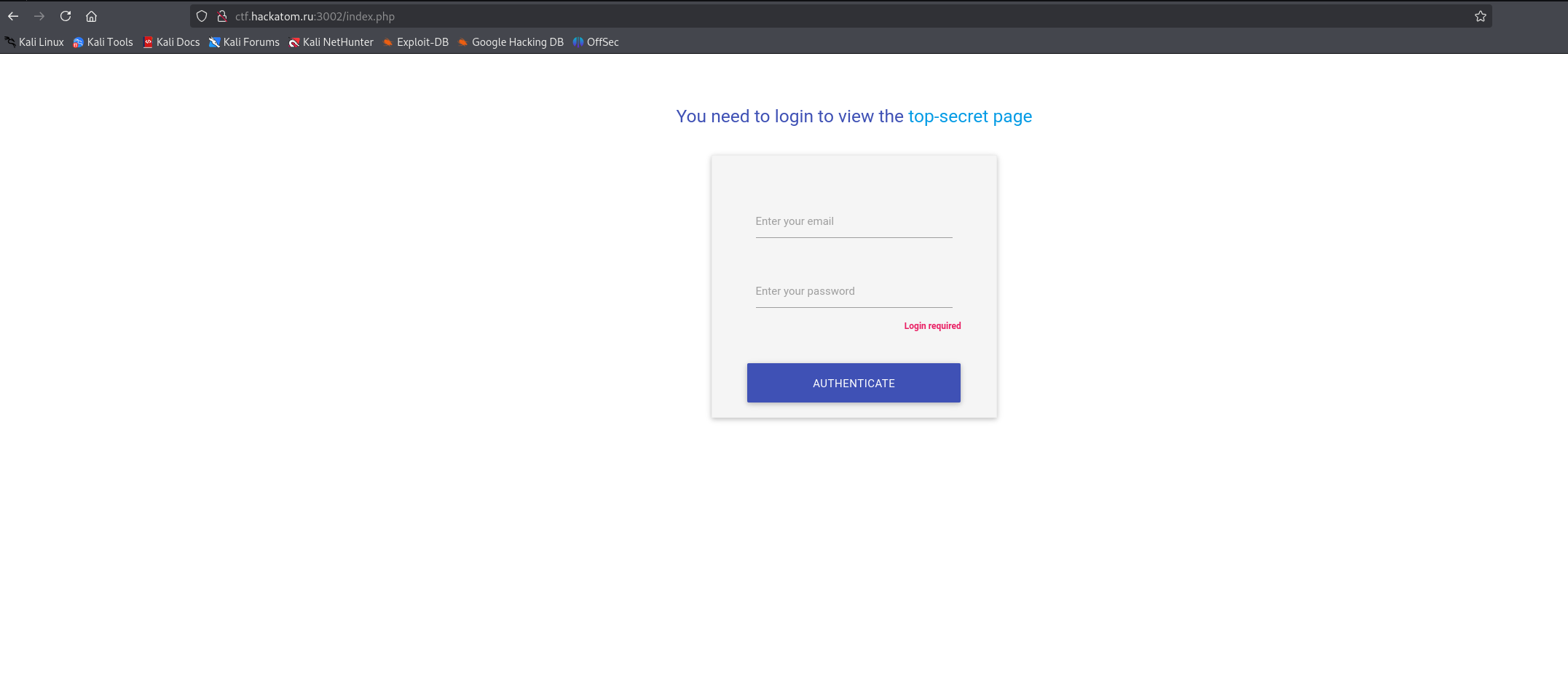
Таск решен. Все очень просто.

TopSecret.

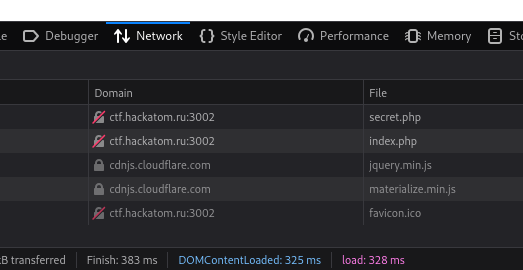
Описание: Слушай, я тут супер важный сайт хочу ломануть - <http://ctf.hackatom.ru:3002/index.php>

Может ты сможешь оттуда что-нибудь достать?

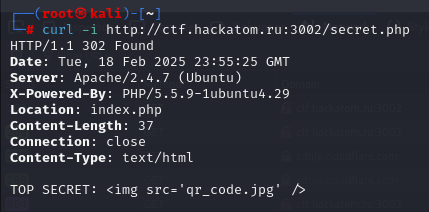
Читаем описание, из описания ничего непонятно, поэтому сразу переходим на сайт <http://ctf.hackatom.ru:3002/index.php>. Попытаемся ввести разные данные, но ни к чему нас это не приведет. Еще мы видим надпись You need to login to view the top-secret page, где top-secret page является гиперссылкой.



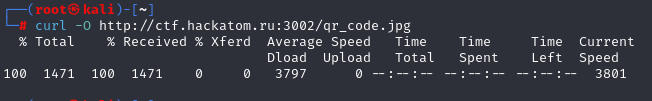
Пытаемся кликнуть по top-secret page но нас редиректит обратно на ту страницу, где мы находимся. Попробуем зайти в инструменты анализа в браузере, во вкладку Network и видим там упоминание о secret.php.



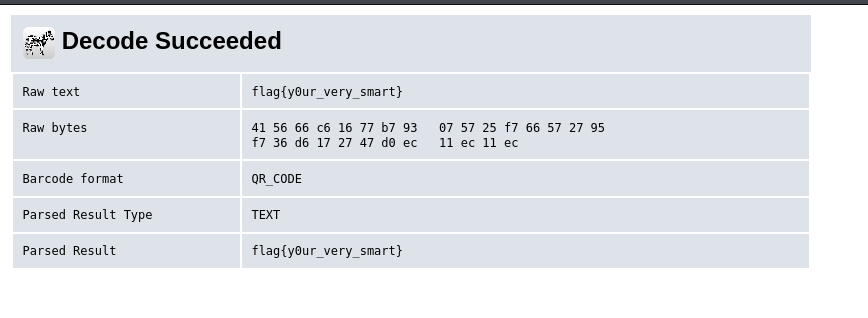
Так как с браузера нас всегда редиректит на index.php, мы попытаемся узнать подробности редиректа с помощью инструмента curl. Используем curl с ключом -i, чтоб узнать что происходит до редиректа.



В последней строке видим упоминание какой-то картинки с названием qr\_code.jpg. Скачаем данный файл.



Видим, что это какой-то qr-код, расшифруем его в онлайн декодере qr-кодов.



Поздравляю! Мы получили нужный нам флаг, таск решен.

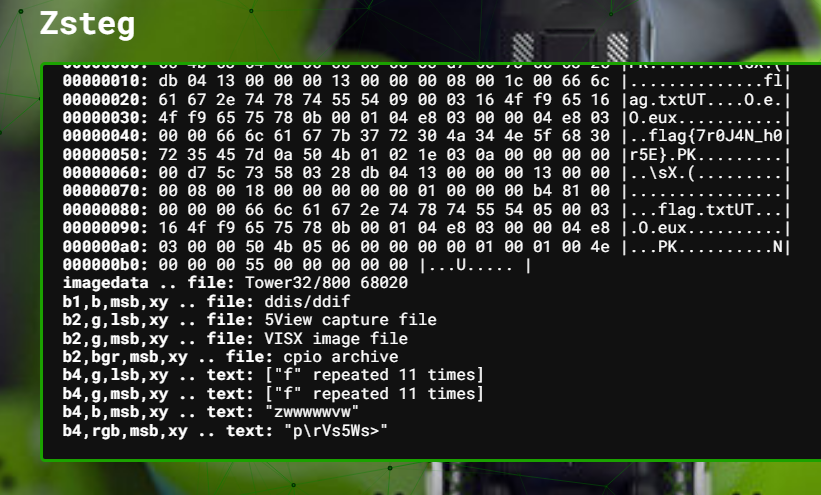
Полезные ссылки:

<https://zxing.org>

<https://www.kali.org/tools/curl/>

Horse.

Скачиваем картинку, и сразу загружаем ее на сайтик aperisolve.com.



Во вкладке Zsteg видим нужный нам флаг. Таск решен.

Полезные ссылки:

<https://www.aperisolve.com/>

KidsToy.

Описание: "Это как та детская игрушка, где нужно было повторять то, что светится, только это

какая-то подделка, которую наверняка купили в магазине «всё по пятьдесят»"

1. Программа при подключении указывает цвет, что он выбрала.

2. Используя логику программы, описанную ниже. Создайте код, который её решит. В ответ программа вас наградит!

Известно, что программка иногда "сбоит" и меняет свою логику по ходу вашего прохождения. Вы выиграете компьютер, если правильно ответите на 1000 вопросов.

Первые 249 попыток -

Если программа говорит green, вы вводите yellow

Если программа говорит yellow, вы вводите blue

Если программа говорит blue, вы вводите red

Если программа говорит red, вы вводите green

Начиная с 250 до 499 логика изменится -

Если программа говорит green, вы вводите green

Если программа говорит yellow, вы вводите blue

Если программа говорит blue, вы вводите yellow

Если программа говорит red, вы вводите red

Начиная с 500 до 749 логика вернется -

Если программа говорит green, вы вводите yellow

Если программа говорит yellow, вы вводите blue

Если программа говорит blue, вы вводите red

Если программа говорит red, вы вводите green

И далее с 750 до 1000 логика -

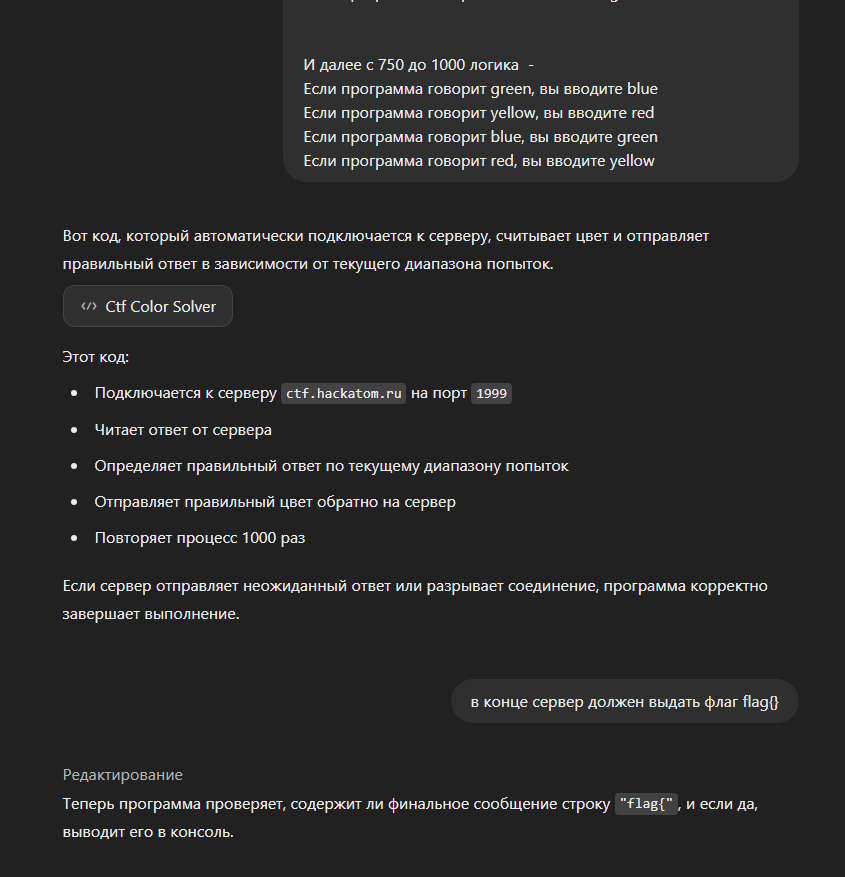
Если программа говорит green, вы вводите blue

Если программа говорит yellow, вы вводите red

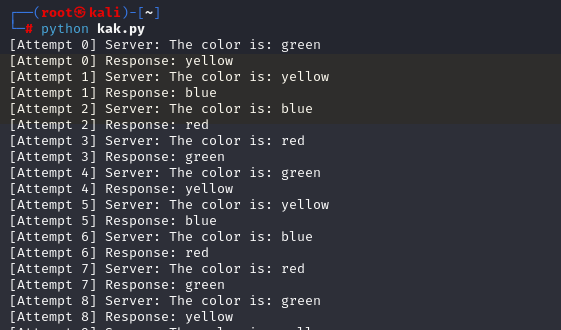
Если программа говорит blue, вы вводите green

Если программа говорит red, вы вводите yellow

Копируем условия задачки и идем к ChatGPT просить сгенерировать код, который решит нам задачу за нас.



После этого запускаем наш код и ждем.



В конце получаем нужный нам флаг flag{do\_it\_like\_me}.

Полезные ссылки:

<https://chatgpt.com/>

бесплатный впн плагином на браузер – browsec