UGRACTF

Материалы отборочного этапа юниорской олимпиады по информационной безопасности Ugra CTF 2019–2020 гг.

Примечание: некоторые задачи были уникальными для каждого участника и генерировались автоматически. Для таких задач нужно сгенерировать себе вариант приложенным генератором.

Гимн года I

Стеганография, 50 баллов

Вашему вниманию предлагается гимн 2020 года.

Генератор
`ucucu.ga/20q/anthem1/generate.py`

Решение
К видеоролику прилагаются субтитры на нескольких языках. В одной из версий одна строка субтитров показывается лишь на сотые доли секунды.
`ucucu.ga/20q/anthem1/WRITEUP.md`

Ответ
`ugra_do_the_guys_a_favor_b8a4c70f7`

Гимн года II

Стеганография, 300 баллов

Вашему вниманию снова предлагается гимн 2020 года. (Да, это металшутка. Нет, не надо, спасибо.)

Генератор
`ucucu.ga/20q/anthem2/generate.py`

Решение
В большинстве плееров после окончания ролик продолжает проигрываться в течение 42 часов с низким FPS. Необходимо извлечь все кадры ролика.
`ucucu.ga/20q/anthem2/WRITEUP.md`

Ответ
`ugra_like_and_subscribe_adacddfeaa`

Больше, чем RSA

Криптография, 250 баллов

Британские учёные выяснили, что RSA-512 недостаточно хорош. Мы улучшили его в 1,5 раза. Сможете теперь расшифровать?

Генератор
`ucucu.ga/20q/bestrsa/generate.py`

Решение
Модуль RSA выбран слабым, и он легко раскладывается на простые множители. Однако, один множитель составной. На самом деле, в данной задаче используется multiprime RSA.
`ucucu.ga/20q/bestrsa/WRITEUP.md`

Ответ
`ugra_3rsa_is_secure_unless_you_get_bad_primes_cd68113d87efcde6`

Без единиц

Стеганография, 250 баллов

Как вы думаете, можно ли закодировать информацию в бесконечном потоке нулевых байтов? Этим ребятам, похоже, удалось.

Генератор
`ucucu.ga/20q/devzero/generate.py`

Решение
Биты флага кодируются скоростью отдачи файла. Проанализировать её можно с помощью программы Wireshark.
`ucucu.ga/20q/devzero/WRITEUP.md`

Ответ
`ugra_did_you_ever_feel_that_clean_099b0353112e`

ЕГЭ

Программирование, 350 баллов

В наших соревнованиях участвуют старшеклассники, которым скоро предстоит преодолеть самый важный школьный экзамен. Ребята! Это задание посвящается вам. Мы попробовали подготовить тренировочный вариант, чтобы вы могли готовиться к ЕГЭ даже во время решения CTF-задач. Надеемся, что вам будет полезно.

Генератор
`ucucu.ga/20q/ege/generate.py`

Решение
Необходимо было собрать базу родов слов и написать клиента, который будет подставлять их и отвечать на вопросы.
`ucucu.ga/20q/ege/WRITEUP.md`

Ответ
`ugra_durnytsya_dribnitsya_c5550866`

Экзамен по истории

Реверс-инжиниринг, 100 баллов

На дистанционном обучении вам необходимо сдать экзамен по истории. Ваш преподаватель создал для этого специальное программное средство. Вы знаете, что Вениамин Витальевич очень требователен, и никаких ошибок допускать нельзя!

Генератор
`ucucu.ga/20q/exam/generate.py`

Решение
Ответы к тесту хранились в виде текстовых констант в приложении. Найти и извлечь их можно с помощью утилиты strings.
`ucucu.ga/20q/exam/WRITEUP.md`

Ответ
`ugra_teacher_is_so_proud_of_you_57`

Отзыв

Криптография, 50 баллов

Участники CTF-соревнований нередко оставляют отзывы. В этот раз пришло что-то совсем непонятное:

Генератор
`ucucu.ga/20q/feedback/generate.py`

Решение
Было использовано бинарное кодирование, в котором числа 0 и 1 заменены на эмодзи двух типов.
`ucucu.ga/20q/feedback/WRITEUP.md`

Ответ
`ugra_i_love_emoji_40b5c4a67657`

Турбоптица

Реверс-инжиниринг, 150 баллов

Фанаты одной известной уже-не-современной игры создали множество её клонов и модификаций. Сможете победить в нашей?

Генератор
`ucucu.ga/20q/flappy/generate.py`

Решение
Можно было либо пропатчить программу, задав птице правое положение, либо выяснить, что высота птицы задавалась скоростью процесса и управлять ей в DOSBox.
`ucucu.ga/20q/flappy/WRITEUP.md`

Ответ
`ugra_moore_is_flapping_in_his_dreams_365bd0c7e01414baa47423338ec`

Формулы

Реверс-инжиниринг, 150 баллов

Задания категории reverse — это всегда что-то страшное и незнакомое, а ещё очень сложное. Или нет?

Генератор
`ucucu.ga/20q/formulae/generate.py`

Решение
В столбце EE таблицы находится набор из 56 квадратных уравнений с решениями в целых числах. ASCII-символы, соответствующие ответам, являются символами флага.
`ucucu.ga/20q/formulae/WRITEUP.md`

Ответ
`ugra_school_informatics_isnt_that_useless_61eb16d744ec`

Друзья

Веб-технологии, 250 баллов

По статистике, ежедневно миллионы пользователей забывают свои пароли от различных сервисов. Разработчики пытаются решить эту проблему и создать сервисы, где для входа пароль не нужен. Но что-то всё равно идёт не так...

Генератор
`ucucu.ga/20q/friends/generate.py`

Решение
Секреты для генератора одноразовых токенов были предсказуемыми и зависели от ID пользователя. Можно было получить QR-код для администратора.
`ucucu.ga/20q/friends/WRITEUP.md`

Ответ
`ugra_oh_no_totp_secret_leaked_9e50`

Дед файл сделал

Криптография, 100 баллов

Тут дед пошёл и сделал файл, а зачем, он и не помнит уже. Кодировок современных мудрёных он не знает, по старинке действовал.

Генератор
`ucucu.ga/20q/gaffer/generate.py`

Решение
Биты файла представляли собой стандартную международную кодировку Морзе (1 — точка, 111 — тире, 0 — пауза между символами кода, 000 — между символами текста).
`ucucu.ga/20q/gaffer/WRITEUP.md`

Ответ
`ugra_my_main_backup_is_my_last_wil_f24c948f72d2`

Хай-тек I

Форензика, 100 баллов

Гражданин А. совершил тяжкое преступление: скачал новую серию Рика и Морти с нелегального торрент-трекера. Мы установили на его компьютер вирус и извлекли какой-то жесткий диск. Но торрентов там нет. Может найдете хоть что-то интересное?

Генератор
`ucucu.ga/20q/hitech1/generate.py`

Решение
На диске, помимо остальных файлов, находился временный файл восстановления редактора vim. Из него восстанавливался текст исходного файла, в котором и был флаг.
`ucucu.ga/20q/hitech1/WRITEUP.md`

Ответ
`ugra_vim_saves_the_world_e684b810b`

Хай-тек II

Сетевая разведка, 150 баллов

Мы не смогли ничего получить из данных с диска гражданина А., но наш оперативный отдел сообщил, что гражданин недавно помог провести какое-то мероприятие для одарённых детей. Сможете найти?

Решение
Файл восстановления из задания Хай-тек I содержал ещё и имя пользователя. По этому имени можно найти аккаунт в Twitter, а уже в нём — сайт мероприятия.
`ucucu.ga/20q/hitech2/WRITEUP.md`

Ответ
`ugra_we_all_make_good_websites_a87`

Хай-тек III

Сетевая разведка, 300 баллов

В наше время довольно часто происходят различные утечки — в интернет попадают данные десятков и сотен тысяч людей. Вам столько не нужно — найдите лишь пару сотен участников этого мероприятия.

Решение
На сайте мероприятия есть фотографии, встроенные с популярного фотохостинга Imgur. Можно было найти пользователя, загрузившего фотографии. В аккаунте было фото с крупным экраном, на котором открыто окно браузера. В нём — адрес админ-панели и авторизационные данные в GET-параметрах.
`ucucu.ga/20q/hitech3/WRITEUP.md`

Ответ
`ugra_querystring_is_the_new_cookie_e73a2fcb986d`

Домашняя страница

Веб-технологии, 50 баллов

Оказалось, что ещё в прошлом веке один известный человек создал свою домашнюю страничку. Она доступна сразу на нескольких языках мира. Говорят, что в одной из версий что-то спрятано. Сможете найти?

Генератор
`ucucu.ga/20q/homepage/generate.py`

Решение
Сайт отдаёт различные языковые версии в зависимости от заголовка Accept-Language. Можно логически выбрать нужную языковую версию, которая отличается от других.
`ucucu.ga/20q/homepage/WRITEUP.md`

Ответ
`ugra_what_is_your_erdos_number_58b`

Домофон

Сетевая разведка, 100 баллов

Ваши друзья-философы пригласили вас на постмодерн вечеринку.

Генератор
`ucucu.ga/20q/intercom/generate.py`

Решение
Данный домофон открывается стандартными мастер-кодами, которые можно найти по его марке.
`ucucu.ga/20q/intercom/WRITEUP.md`

Ответ
`ugra_pati_na_hate_4c7a348a63fd`

Кто

Веб-технологии, 100 баллов

«В хозяйстве пригодится!» — подумал я и добавил этот сайт в закладки.

Генератор
`ucucu.ga/20q/iswho/generate.py`

Решение
Сайт использовал утилиту whois, передая аргументы небезопасным образом. Требовалось проэксплуатировать уязвимость Remote Code Execution.
`ucucu.ga/20q/iswho/WRITEUP.md`

Ответ
`ugra_good_languages_do_not_force_you_to_rely_on_bash_2bc3a57a2afd`

Праздник в Японии

Сетевая разведка, 200 баллов

Раз в несколько лет, а если повезёт, то и дважды в год, 1 января или 1 июля японцы празднуют это.
Чтобы тоже стать причастным к празднику, вам нужно заполнить форму.

Генератор
`ucucu.ga/20q/japclock/generate.py`

Решение
По описанию видеоролика и с помощью уличных панорам можно найти требуемые часы. Ответ необходимо вводить японскими полноширинными цифрами в соответствии с инструкцией в задании.
`ucucu.ga/20q/japclock/WRITEUP.md`

Ответ
`ugra_arubaito_toranpu_pasokon_1807`

Самый короткий анекдот

Стеганография, 300 баллов

Название этого файла — самый короткий из известных анекдотов, и лет ему больше, чем всем нам. Времена сейчас, впрочем, другие, и распаковать этот архив не должно составить труда. Может, вы даже ничего и не заметите.
Вам будет полезно знать, что архив создан версией RAR 5.50.

Генератор
`ucucu.ga/20q/jk/generate.py`

Решение
Приведенный RAR-архив поврежден, однако содержимое можно восстановить, используя Recovery Record. Флаг можно получить, рассмотрев, какие именно биты архива были испорчены.
`ucucu.ga/20q/jk/WRITEUP.md`

Ответ
`ugra_when_i_was_this_small_it_already_had_a_beard_that_long_d9b26c81`

Melodrama I

Бинарная эксплуатация, 150 баллов

Твиттер-газета Melodrama выходит в свет с 1997 года. Огромную популярность издание завоевало благодаря фирменным коротким заметкам — их длина ограничена 140 символами. Все статьи перед публикацией проходят жёсткий контроль с помощью специального приложения, исходный код которого нам удалось достать. Недавно стало известно, что сотрудники топ-менеджмента Мелодрамы тайно писали заметки для другого СМИ. Сможете выяснить, что там было?

Генератор
`ucucu.ga/20q/melodrama1/generate.py`

Решение
Функция memset при удалении заметки применялась некорректно, позволяя читать удаленные заметки.
`ucucu.ga/20q/melodrama1/WRITEUP.md`

Ответ
`ugra_nullptr_is_a_zero_ab198875fc7`

Melodrama II

Бинарная эксплуатация, 250 баллов

Твиттер-газета Melodrama выходит в свет с 1997 года. Огромную популярность издание завоевало благодаря фирменным коротким заметкам — их длина ограничена 140 символами. Все статьи перед публикацией проходят жёсткий контроль с помощью специального приложения, исходный код которого нам удалось достать. Говорят, у нового главного редактора такая интересная подпись, но я её не видел. Может быть вам удастся заполучить автограф?

Генератор
`ucucu.ga/20q/melodrama1/generate.py`

Решение
При добавлении содержимого в заметку длина вычислялась некорректно, можно было переполнить буфер записи и, удалив нулевой байт, считать подпись.
`ucucu.ga/20q/melodrama2/WRITEUP.md`

Ответ
`ugra_zerobyte_does_not_count_9b0da`

Сапёр-неудачник

Реверс-инжиниринг, 200 баллов

Компания-издатель ООО «АгроГеймДев» выпустила новую захватывающую игру про войну. Тем, кто сможет её преодолеть, было обещано вознаграждение — но пока что никому это не удавалось.

Генератор
`ucucu.ga/20q/mines/generate.py`

Решение
Игра хранила число мин в реестре Windows — поменяв значение ключа на 0, можно было убрать все мины.
`ucucu.ga/20q/mines/WRITEUP.md`

Ответ
`ugra_avoid_the_mines_eeec71da5183a`

Мнистерство статистики

Программирование, 350 баллов

Тётенька из бухгалтерии очень долго старалась и переписывала цифры, чтобы незаметно вынести из мнистерства статистики важнейший секретный файл. Сможете его восстановить? Лучше обучите нейронную сеть. Нет, серьёзно. Размер цифр — 28×28, это неспроста.

Генератор
`ucucu.ga/20q/mnist/generate.py`

Решение
Как и сказано в условии, необходимо было обучить нейронную сеть и распознать цифры. После чего получался файл, байты которого записаны в десятичной форме.
`ucucu.ga/20q/mnist/WRITEUP.md`

Ответ
`ugra_apply_now_for_senior_ai_researcher_3493f0ce89`

Мой Кирпич

Веб-технологии, 200 баллов

Одна известная строительная компания создала социальную сеть для всех строителей мира. Всё анонимно: нет ни регистрации, ни авторизации, а старые посты и вовсе исчезают бесследно.
Присоединяйтесь!

Генератор
`ucucu.ga/20q/mybrick/generate.py`

Решение
Форма поиска была подвержена NoSQL-инъекции, благодаря чему можно было извлечь все новости.
`ucucu.ga/20q/mybrick/WRITEUP.md`

Ответ
`ugra_escape_not_only_sql_48ae250f3`

noteasy$_5$

Криптография, 150 баллов

Генератор
`ucucu.ga/20q/noteasy5/generate.py`

Решение
В задании описан шифр простой замены для алфавита мощностью 25, необходимо было применить его к строке.
`ucucu.ga/20q/noteasy5/WRITEUP.md`

Ответ
`ugra_rituals_may_vary_and_so_do_quirks_eecbedfcffab`

Менеджер паролей

Веб-технологии, 300 баллов

Компания All Secure System выпустила собственный парольный менеджер. Отзыв клиента epicleeter: Наконец-то я смог сохранить все свои пароли в одном месте — компания All Secure Systems создала свой надёжный и безопасный менеджер паролей. Действительно ли это реальный пользователь сайта или отзыв фейковый?

Генератор
`ucucu.ga/20q/passman/generate.py`

Решение
Сессионный cookie зависел от имени пользователя и была зашифрована алгоритмом XOR с постоянным ключом. Можно было легко сконструировать поддельный cookie.
`ucucu.ga/20q/passman/WRITEUP.md`

Ответ
`ugra_lets_forget_xor_forever_2ff93`

Самый важный таск

Бонус, 25 баллов баллов

В этот раз мы не смогли организовать площадки, и сделать хорошие фотографии не получится. Поэтому мы поручаем эту миссию вам! Сделайте фотографию вашей команды, выложите в любую социальную сеть с хештегом #ugractf и отправьте ссылку боту @ugractfbot.

Решение
`ucucu.ga/20q/promotion/WRITEUP.md`

Ответ
`ugra_thanks_for_good_photo_e17911d`

Великий математик

Реверс-инжиниринг, 150 баллов

Научная лаборатория по решению NP-неполных задач максимально близка к получению нового гранта. Не хватает лишь одного отчёта. Величайший математик уже месяц работает над ним, но результат найти никак не удаётся. Он написал программу для вычисления секретной строки, а она не работает... Учёный не хочет делиться с нами своими научными открытиями, мы смогли достать лишь один файл. Поможете?

Генератор
`ucucu.ga/20q/pycfail/generate.py`

Решение
В задании дан байт-код CPython, выполнение которого приводит к превышению стека рекурсии. Можно было либо декомпилировать и переписать алгоритм, либо увеличить лимит рекурсии перед запуском.
`ucucu.ga/20q/pycfail/WRITEUP.md`

Ответ
`ugra_weird_gcd_calculation_a95eb29`

Святая простота

Стеганография, 150 баллов

Простые задачи требуют простых решений. Надо лишь добавить немного красок в нашу серую действительность.

Генератор
`ucucu.ga/20q/sancta/generate.py`

Решение
Было закодировано чёрно-белое изображение: оттенок серого был простым, если бит исходного изображения черным, и составным — если белым.
`ucucu.ga/20q/sancta/WRITEUP.md`

Ответ
`ugra_no_firewood_required_for_now_e684b810bef5`

Расширение сознания

Реверс-инжиниринг, 350 баллов

Научная лаборатория по решению NP-неполных задач очень нервничает в связи с последними событиями. Настолько нервничает, что её сотрудники взяли — и написали... психотерапевта. Если вы ещё не нервничаете, поговорите с ним.

Генератор
`ucucu.ga/20q/shrink/generate.py`

Решение
В файле — исходный код на Emacs Lisp. Как и указано, он имитирует работу психотерапевта. Флаг выдаётся при упоминании нужной темы некоторое количество раз.
`ucucu.ga/20q/shrink/WRITEUP.md`

Ответ
`ugra_shrunk_the_shrink_18a284eb06b`

IBM Selectric

Криптография, 200 баллов

Электрическая печатная машинка IBM Selectric была большим прорывом для своего времени — россыпь вечно заедающих молоточков с буквами заменил небольшой шарик. Его легко можно было заменить, что позволяло печатать на печатной машинке различными шрифтами и на различных языках — достаточно было найти и установить подходящий шарик.
Нам попался вот такой замечательный экземпляр. Какой-то он подозрительный, вам не кажется?

Генератор
`ucucu.ga/20q/selectric/generate.py`

Решение
Каждый символ встречался на шаре ровно один раз. Первые символы флага встречаются на расстоянии в 3, 5, 8, 13, 21 символов — это числа Фибоначчи. Выписав все символы с соответствующими отступами, можно получить флаг.
`ucucu.ga/20q/selectric/WRITEUP.md`

Ответ
`ugra_does_one_like_new_3d_episodes_099bcf288`

Запросы

Форензика, 300 баллов

Этот пользователь отправляет весьма странные запросы. Нет ли в них чего-нибудь подозрительного?

Генератор
`ucucu.ga/20q/subdomain/public/dump.pcap`

Решение
В предоставленной записи сетевого трафика приведен пример работы DNS-туннеля iodine. Необходимо было реализовать декодер протокола и найти HTTP2-трафик внутри.
`ucucu.ga/20q/subdomain/WRITEUP.md`

Ответ
`ugra_http2_is_nice_but_better_with_iodine_15af90c465128359`