

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

Задание засчитывается, если был отправлен верный ответ. Любой другой ответ приносит 0 баллов.

Победителями признаны участники, набравшие не менее 900 баллов. Призёрами II степени признаны участники, набравшие не менее 600 баллов. Призёрами III степени признаны участники, набравшие не менее 400 баллов.

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

Он так видит

Реверс-инжиниринг, 200 баллов

Художник хотел написать красивую картину, но вечно его тянет куда-то не туда. Направьте его на путь истинный.

Генератор

ucucu.ga/20s/artist/generate.py

Решение

Координаты траектории, по которой должно было путешествовать перо художника, при отрисовке грубо округлялись, и накапливалась ошибка. Требовалось убрать округление из кода и аккуратно разобрать получившиеся контуры букв.

ucucu.ga/20s/artist/WRITEUP.md

Ответ

ugra_art_is_so_jvneovpakwnvjtoalqimg_great_7bfe1cd239ab

777

Веб-технологии, 200 баллов

Новое онлайн-казино! Абсолютно честное — играйте и выигрывайте. Выплаты в Фантиках (Ф). Пока что, правда, доступна только рулетка, да и та особенная.

Генератор

ucucu.ga/20s/casino/generate.py

Решение

При падении приложения сбрасывалось состояние генератора псевдослучайных чисел. Таким образом, после восстановления результаты игр повторялись. Можно было запомнить выпадающие на рулетке числа и обыграть казино.

ucucu.ga/20s/casino/WRITEUP.md

Ответ

ugra_vulnerability_beats_probability_1fa905601f7a

Сага о резервных копиях Форензика, 200 баллов

Наш администратор регулярно делает резервные копии базы данных. Правда, когда база упала, восстановить тексты статей не получилось... На кону репутация всей компании, выручайте.

Генератор

ucucu.ga/20s/dumpster/generate.py

Решение

Требовалось найти в дампе базы данных запрос UPDATE, стиривший данные в таблице с текстами статей, и проимпортировать дампы без него.

ucucu.ga/20s/dumpster/WRITEUP.md

Ответ

ugra_mind_your_updates_a9c485519b2

Пинг

Стеганография, 200 баллов

Про нашего бывшего сисадмина можно часами рассказывать смешные истории. Например, он когда-то написал и поставил на все сервера свой ping! Теперь вы, наверное, понимаете, за что мы его уволили...

До сих пор не можем эту поделку со всех хостов удалить.

Генератор

ucucu.ga/20s/hello/generate.py

Решение

Флаг был закодирован в резервном бите протокола IPv4. По спецификации RFC этот бит всегда равен нулю, однако в приведённом фрагменте трафика это было не так.

ucucu.ga/20s/hello/WRITEUP.md

Ответ

ugra_this_bit_is_r5s5rv5d_afa53fe3db

Задача 27

Бинарная эксплуатация, 250 баллов

Не только CTF-разработчики пишут и пользуются своими велосипедами. В этот году составители ЕГЭ по информатике решили перенести приём одного из заданий в собственную проверочную систему. Даже публичное тестирование объявили...

Генератор

ucucu.ga/20s/lms/generate.py

Решение

Необходимо было выйти из песочницы, отредактировав скрипт запуска, после чего найти флаг на файловой системе.

ucucu.ga/20s/lms/WRITEUP.md

Ответ

ugra_use_well_tested_sandboxes_147

В эфире

Веб-технологии, 150 баллов

Крупнейшая районная блог-платформа была существенно переработана. Новая версия работает на современном, модном и молодёжном языке программирования TypeScript. Разработчики системы абсолютно уверены в её безопасности.

Настолько, что даже открыли её исходный код. Что ж, мы тоже в них верим, и надеемся, что наши секреты никто не прочтёт.

ucucu.ga/20s/onair/public/app.zip

Генератор

ucucu.ga/20s/onair/generate.py

Решение

В данном задании нужно было обнаружить ошибку при проверке прав — при отсутствии прав отдавалась ошибка, но запрос продолжал обрабатываться.

ucucu.ga/20s/onair/WRITEUP.md

Ответ

ugra_who_writes_so_bad_code_b0c212b93b

Напечатай это

Форензика, 100 баллов

Екатерина Павловна попросила вас распечатать странный файл, потому что у неё сломался принтер. Чем же она занималась?

Генератор

ucucu.ga/20s/printme/generate.py

Решение

Файл был сохранён в режиме отслеживания изменений: в нём сохранены сделанные правки. Каждое изменение удаляло одну букву. При прочтении этих букв в хронологическом порядке их удаления получался флаг.

ucucu.ga/20s/printme/WRITEUP.md

Ответ

ugra_slowly_losing_bits_of_sanity_176432afe1b9

Перевёртыш

Криптография, 100 баллов

Наташ, вставай, мы там всё перевернули. Вообще всё.

Генератор

ucucu.ga/20s/reverse/generate.py

Решение

Участникам был дан файл, биты которого были записаны в обратном порядке.

ucucu.ga/20s/reverse/WRITEUP.md

Ответ

ugra_deified_civic_radar_reviver_4

Камуфляж

Стеганография, 300 баллов

На этой картинке кое-что затаилось. Назовите кое-что.

Генератор

ucucu.ga/20s/uniform/generate.py

Решение

При открытии изображения в программе stegsolve в режиме случайной палитры проявлялись бледные буквы, нужно было их прочитать с помощью графического редактора.

ucucu.ga/20s/uniform/WRITEUP.md

Ответ

ugra_who_s_that_writin_john_the_revelator_56adf154c542

Вопрос на миллион

Программирование, 300 баллов

Директор магазина очень разозлился на кассиршу Зинаиду и решил её наказать. Он сказал, что не отпустит её домой, пока она не заработает на своей кассе выручку в миллион рублей!

Генератор

ucucu.ga/20s/zinaida/generate.py

Решение

Необходимо было автоматизировать считывание штрихкодов с помощью, например, библиотеки pyzbar.

ucucu.ga/20s/zinaida/WRITEUP.md

Ответ

ugra_must_be_funny_in_a_rich_man_s_world_1786ba630e17