Разбор интересных задач CTFLEARN. Автор: Евсеев Григорий (заголовок)

Представленные ниже задачи взяты с ctflearn.com

**Web: Inj3ction Time**

I stumbled upon this website: [http://web.ctflearn.com/web8/](http://web.ctflearn.com/web8/ ) and I think they have the flag in their somewhere. UNION might be a helpful command

Решение.

В тексте есть подсказка, что UNION может быть полезной командой для решения этой задачи. UNION позволяет выполнять несколько SELECT запросов и добавлять их результаты в изначальный запрос.

INFORMATION\_SCHEMA обеспечивает доступ к метаданным о базе данных, информации о сервере MySQL, такой как название базы данных или таблицы, типе данных столбца или привилегиях доступа. Попробуем получить информацию из INFORMATION\_SCHEMA:

1 union select table\_name from information\_schema.tables

Узнаем, сколько столбцов(полей) в таблице с помощью ORDER BY:

1 order by 4

Перечисляя количество столбцов, остановились на 4, так как начиная с 5 сайт перестает выдавать результаты запроса. Теперь добавим еще 3 столбца к нашей изначальной команде, чтобы получилось 4. Получается следующее:

1 union select table\_name,2,3,4 from information\_schema.tables

Выводит список с названиями таблиц. Здесь мы находим таблицу с названием «w0w\_y0u\_f0und\_m3». Дальше будем искать в ней нужный нам столбец:

1 union select column\_name,2,3,4 from information\_schema.columns

Нашли столбец с названием «f0und\_m3». Теперь получим значения данного столбца из данной таблицы:

1 union select f0und\_m3,2,3,4 from w0w\_y0u\_f0und\_m3

Получили флаг:

abctf{uni0n\_1s\_4\_gr34t\_c0mm4nd}

**Web: Calculat3 M3**

Here! <http://web.ctflearn.com/web7/> I forget how we were doing those calculations, but something tells me it was pretty insecure.

Решение.

Мы видим калькулятор. Посмотрим, как он работает. Мы вводим пример и ответ выводится прямо в <body>. Попробуем написать команду:

;ls

Нам вывелась директория сайта. Здесь же мы нашли флаг:

ctf{watch\_0ut\_f0r\_th3\_m0ng00s3}

**Forensics: Bobby Toe's iPad**

Here is a pic of my friend Bobby Toe. while he's happy to give you his iPad, he's not as willing to give you the flag. can you get it from him? here is an image of Bobby Toe: [https://mega.nz/#!iWAm2KJL!2uRVDKrHOWryZkZNW6leV0sQMh-b0-AYQksa3i-A3Eg](https://mega.nz/" \l "!iWAm2KJL!2uRVDKrHOWryZkZNW6leV0sQMh-b0-AYQksa3i-A3Eg)

Решение.

Качаем картинку. Проверим сначала описание файла с помощью команды: file

Видим, что картинка формата .png. Проверим ее с помощью команды: zsteg – утилиты для извлечения данных из изображений формата .png и .bmp по стеганографическим алгоритмам.

Команда нашла в изображении информацию, находящуюся после конца файла IEND. Найдем конец файла утилитой bless. У .png файлов конец файла отмечен завершающим чанком IEND. Находим его с помощью утилиты и видим, что IEND находится не в конце файла. Здесь же замечаем расширение JFIF. Находим его заголовок:

FF D8 FF E0

Это начало другого файла. Разделим их. После этого снова проверим изначальное изображение: zsteg. На этот раз команда ничего не вывела. Тогда воcпользуемся командами:

zsteg-mask bobbytoesipad.png

eog bobbytoesipad\*

Появилось изображение с некоторым текстом: zpv\_tigqylhbafmeoesllpms

Теперь разберемся со вторым файлом, который мы нашли внутри первого. Он не открывается как изображение. Попробуем восстановить его. В файле не хватало байта. Восстановив его, можем открыть картинку. Видим там текст: bbbabydonthurtmewhatislove. Возможно, это пара шифртекст-ключ. Расшифруем. Получился флаг:

you\_thinkyougotskillshuh

**Cryptography: So many 64s**

Help! My friend stole my flashdrive that had the flag on it. When he gave it back the flag was changed! Can you help me decrypt it?

[https://mega.nz/#!OHhUyIqA!H9WxSdG1O7eVcCm0dffggNB0-dBemSpBAXiZ0OXJnLk](https://mega.nz/" \l "!OHhUyIqA!H9WxSdG1O7eVcCm0dffggNB0-dBemSpBAXiZ0OXJnLk)

Решение.

Нам дан файл с очень длинным текстом. Напишем программу, которая будет декодировать этот текст:

import base64

f = open(‘flag.txt’, ‘r’) – открываем файл для чтения

res = f.read() – читаем текст в переменную

while True: – выполняем бесконечно

res = base64.b64decode(res).decode(‘utf-8’) – декодируем

if ‘{‘ in res: – если находим фигурную скобку в тексте

print(res) – выводим результат

break – прекращаем цикл принудительно

Результатом выполнения программы будет флаг:

ABCTF{pr3tty\_b4s1c\_r1ght?}

**Forensics: Seeing is believing**

My colleague's an astronaut who's currently on a mission orbiting in space. Just a few hours ago, unfortunately, his communication device caught fire so he's unable to report back to base. I did, however, receive a strange file that I can't seem to open. I think it may shed some light on his situation. Can you help me save poor boy Johnny? File:

[https://mega.nz/#!LTRUTaZb!9Nh0NwDONJQiOThif3G62evP8H\_W9eIJSu0PdBQWKyg](https://mega.nz/" \l "!LTRUTaZb!9Nh0NwDONJQiOThif3G62evP8H_W9eIJSu0PdBQWKyg)

Решение.

Разархивируем файл. Посмотрим его формат с помощью команды: file. Это файл формата .ogg. Поменяем расширение файла help.me на help.ogg. Это звуковой файл. В нем ничего не слышно. Тогда проверим его программой SonicVizualizer.

В программе Layer -> Add Spectrogram. Теперь можно увидеть QR-код. Скриншотим и декодируем. Получается ссылка на сайт, где и указан флаг:

the\_flag\_is{A\_sP3c7r0gr4m?!}