Задачи первого отборочного этапа

1. PPC

1.1. Captcha

Балл: 1000

Условие:

Сервис VK тестирует новый вид капчи, но им нужно проверить что все ОК, поможете?

Ответ: CTF{y3p_y3p_1t$_OCR}

Решение:

Задача на OCR, пример решения:

```python
from requests import session
from re import compile
from PIL import Image
import pytesseract
import os

if not os.path.exists('./images'):
    os.mkdir('./images')

server_ip = 'localhost'
server_port = 5000
regex = compile('(static/images/(\w+\.jpg))')
flag = compile("CTF\{.*?\}")
s = session()
def read_text_from_image(image_path):
    image = Image.open(image_path)
    text = pytesseract.image_to_string(image)
    return text

while True:
    response = s.get(f"http://{server_ip}:{server_port}").text
    if "CTF" in response:
        print(flag.findall(response))
        exit(0)
    image = regex.findall(response)
    image_path = image[0][0]
    image_name = image[0][1]
    response = s.get(f"http://{server_ip}:{server_port}/{image_path}", stream=True)
    with open(f'./images/{image_name}', 'wb') as file:
        for chunk in response.iter_content(chunk_size=128):
            file.write(chunk)
    answer = read_text_from_image(f"./images/{image_name}")
    s.post(f"http://{server_ip}:{server_port}", data={"answer":answer})

```

1.2. Calc

Балл: 1000

Условие:

Проверим твои навыки математики и программирования? Все просто - тебе дают пример, надо решить и ввести ответ. И так много-много раз. А потом раз - и вот он флаг!

Ответ: CTF{C@lcuL@t3_PlupIU}
Решение:
Пример решения на python:

```python
from pwn import *
from re import compile


server_ip = 'localhost'
server_port = 7090
regex = compile(b'[\d\*\-\+\**,\/,\/\/,\%]+')

io = remote(server_ip, server_port)
response = io.recvline()
print(response)

while True:
    if b"CTF" in response:
        print(response)
        io.close()
        exit(0)
    response = regex.findall(response)
    print(response)

    response = eval(''.join(str(i.decode()) for i in response))
    print(response)
    io.sendline(str(response).encode())
    print(f"sending {response}")
    response = io.recvline()
    response = io.recvline()
    print(response)
```

1.3. 3:15
Балл: 1000
Условие:
В данной задаче вам необходимо прорешать N (N >= 100) раундов подряд такой прикладной задачи: на вход дается текст на латинице, необходимо посчитать количество гласных и количество согласных. Детальное описание задачи - на сервере
Подключайтесь к серверу по netcat и отправляйте корректные ответы. Если ответ некорректный, счетчик сбрасывается и нужно начинать сначала. Используйте python (socket, pwn) или netcat для решения задачи. Время на решение одного раунда - буквально пара секунд, то есть процесс однозначно придется автоматизировать
Ответ: CTF{9FXImUTSmlquekaYPVbf}
Решение:

```
import socket
from time import time, sleep
```

```
def count_vowels_and_consonants(message):
    vowels = "aeiouAEIOU"
    consonants = "bcdfghjklmnpqrstvwxyzBCDFGHJKLMNPQRSTVWXYZ"

    # Initializing counters
    vowel_count = 0
    consonant_count = 0

    # Counting vowels and consonants
    for char in message:
        if char in vowels:
            vowel_count += 1
        elif char in consonants:
            consonant_count += 1

    return vowel_count, consonant_count


def recvall(sock):
    # Helper function to recv n bytes or return None if EOF is hit
    data = bytearray()
    while True:
        packet = sock.recv(2048)
        # print('recv', len(packet))
        if len(packet) == 0:
            break
        data.extend(packet)
        if len(packet) < 2048:
            break
        sleep(0.1)
    return data

buffer_size = 2048

def send_length_of_input():
    # Create a socket object
    client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    server_address = ('0.0.0.0', 9001)

    exclude = [
        'Welcome to our challenge! You need to count vowels and consonants in
the messages below.',
        'Give me your answers like M:N, where M - count of vowels, N - count
of consonants. Example - 5:3'
    ]

    try:
        client_socket.connect(server_address)
        sleep(0.5)
        for i in range(101):
            print(i)
            input_data = recvall(client_socket).decode().split('\r\r\n')
```

```
            result_array = [element for element in input_data if element not
in exclude]
            # print(result_array)
            input_data = " ".join(result_array)
            v, c = count_vowels_and_consonants(input_data)
            client_socket.send(f"{v}:{c}\n".encode())
            sleep(0.2)

    except Exception as e:
        print(f"Error: {e}")

    finally:
        # Close the socket
        client_socket.close()

send_length_of_input()
```

2. Web

2.1. go go go
Балл: 1000
Условие:
Да тут все настолько просто, что мне даже описание делать лень было…
Ответ: CTF{s1mpl3_g0_$$T1}
Решение:
В исходном коде можно найти структуру:

```go
type User struct {
        ID       int
        User     string
        Password string
        GetFlag  func() string
}
```

И обработчик:

```
Hi, {{ .User }}
```

Что намекает нам на SSTI уязвимость.
Пробуем передать в параметре user payload:
`http://localhost:3000/user={{.}}`
и получаем ответ:
`[{1 admin edcb06fb87ecfe460177b32925b64fca 0x100da6450}]`
Теперь наша задача вызвать функцию GetUserFlag, сделать это можно передав следующий payload:
`http://localhost:3000/user={{call%20.GetUserFlag}}`
И получаем флаг.

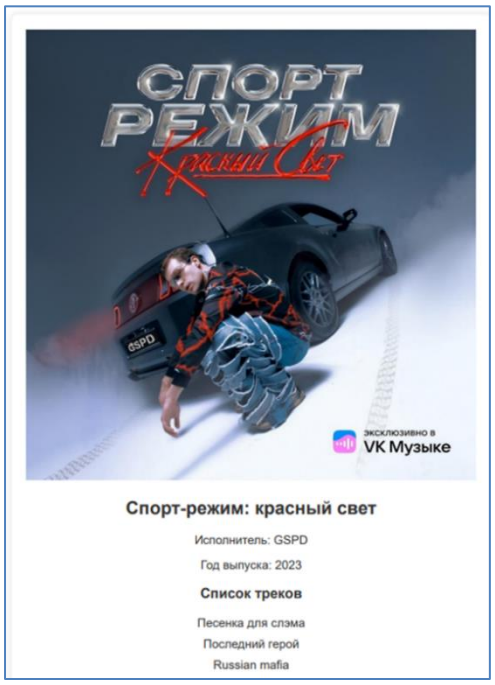
2.2. I Love PHP (NO)
Балл: 1000
Условие:
Не знаю как вы - а я обожаю PHP (нет), потому что там столько всего интересного…
P.S. флаг храниться в файле /flag.txt
Ответ: CTF{us3_pHp_an7th3r3}
Решение:
Т.к. нам даны исходники- стоит начать и их изучения. Видим, что на странице admin.php есть интересная функция `readCustomFile`. Так же замечаем интересный вызов:

```
if (isset($_GET['adminpage'])) {
                $adminpage = $_GET['adminpage'];
                $param = $_GET['param'];
                $answer = call_user_func_array($adminpage, [$param]);
                echo $answer;
            }
```

Который позволяет нам произвести вызов функции `readCustomFile`. Но для начала надо попасть на страницу.
В index.php есть простенькая sql-injection, достаточно подставить следующий запрос:
`admin' or 1=1 -123`
Теперь мы попали на страницу admin.php и можем провернуть удаленный вызов функции:
`http://localhost:5000/admin.php?adminpage=readCustomFile&param=/flag.txt`
Тем самым получив флаг.

2.3. pass by pass
Балл: 1000
Условие:
Тут кажется все просто, но что-то блокирует… Справишься?
Ответ: CTF{byp@$$_f1lter!}
Решение:
Задача на sql-injection bypass. В ходе исследования, можно понять, что блокируются следующие символы:
`['or', 'select', 'union', ' ', '--', 'OR', "SELECT", 'UNION', ';', 'Select', 'Union']`
Итоговый эксплоит выглядит так:
`admin'/**/oR/**/'1'='1`

2.4. Красный свет / зеленый свет
Балл: 1000
Условие:
Наш разработчик готовил веб-сайт к релизу нового альбома своего любимого исполнителя. Позже выяснилось, что альбома два, ну он и применил креативность свойственную гику. Теперь на сайте доступны два альбома. Но не только лишь все могут найти второй. Челендж заключается именно в этом. У меня не получилось, все методы перепробовал



Ответ: CTF{Fm5jJ9fmeDntM7mIRdLi}
Решение:
Сайт показывал одну картинку, если заходить на него стандартным способом, а также вызывать стандартными методами: 'GET', 'POST', 'PATCH', 'DELETE', 'OPTIONS', 'HEAD', 'CTF'. Если же отправить любой другой HTTP метод, то открывалась другая картинка

3. Crypto

3.1. FairPlay?
Балл: 1000
Условие:

```
Смотри что у меня есть!

|Q|W|E|R|T|
|A|B|C|D|F|
|G|H|I|J|K|
|L|M|N|O|P|
|Y|S|U|V|Z|

QCUSYWYCTRINMKRT

P.S. формат флага - ctf{some_word_here}
```

Ответ: ctf{easy_square_cipher}
Решение:
Два варианта:
- обращаем внимание на название задания - если поменять местами слова - получится playfair - шифр Плейфера. Гуглим и решаем.
- Обращаем внимание на данную нам таблицу и нехватку одной буквы (таблица 5x5, букв в алфавите 26) - идем изучать square cipher и находим шифр Плейфера.

https://www.dcode.fr/playfair-cipher

3.2. ThinkLikeAOldMan
Балл: 1000
Условие:
Вам в руки попала записка из далеких 2000-х годов, кажется, в ней что-то зашифровано. Понять бы что…
2228333{58877778_333666777_6665553}
Ответ: ctf{just_for_old}
Решение:
В задании давался намек на старые времена, а тогда телефоны были кнопочные. Вот и разгадка - текст в записке - всего лишь сообщение, набранное на кнопочном телефоне. https://www.dcode.fr/multitap-abc-cipher

3.3. UGUACUUUC
Балл: 1000
Условие:
Думаешь, что знаешь, что такое UCUCUGA? Ну тогда держи новую задачку UGUACUUC!
UGUACUUUC{GGGGAGAACGAGACAAUCUGU_AUGGAGUCGAGUGCAGGAGAG}
Ответ: ctf{genetic_message}
Решение:
Нам дана последовательность странных символов, но мы точно знаем, что UGUACUUUC — это CTF (по формату флага). Отсюда можем сделать вывод что на одну букву приходится по три символа:
UGU – C
ACU – T
UUC - F

```
Попробуем поискать в гугле подсказки, вбив туда "UGU ACU UUC", попадаем на
страничку на википедии (или любом другому ресурсе), где рассказывается про
генетический код: https://ru.wikipedia.org/wiki/Генетический_код

Дальше находим таблицу сопоставления (в примере на википедии она называется
Обратная таблица) и расшифровываем сообщение.
```

3.4. messageX
Балл: 1000
Условие:
Ну чисто по классике - один мой товарищ уверовал что он новый Брюс Шнайер и начал пилить свои "криптосистемы". Отдал на проверку одну из них вам, как быстро вы сможете доказать ему, что даже без знания ключа его система, мягко говоря, не ахти?
OFR{VGEF_PQODKBF_FTQ_YQEEMSQ!}
Ответ: CTF{JUST_DECRYPT_THE_MESSAGE!}

Решение:
1. Легкий способ.

Если бегло изучить код - можно понять, что шифр представляет из себя разновидность шифра Цезаря - и тут нам поможет любой онлайн калькулятор.

2. Сложный способ.
   Нам дан исходный код программы, остается его изучить:
   - ключ генерируется рандомно в пределах от 1 до 100
   - шифруются только буквы
   - есть смещение через ASCII число буквы 'A'
   - ключ высчитывается по длине алфавита (%26) - перебирать все 100 вариантов ключа вообще не обязательно
   - алгоритм шифрования описан одной строкой

Просто пишем обратную программу - по сути нам нужно взять все тоже самое, и поменять знак в одном месте (вместо того что бы отнимать ключ - будем его прибавлять)
Пример:

```
def decrypt(encrypted_message, key):
    decrypted_message = ""
    encrypted_message = encrypted_message.upper()

    for char in encrypted_message:
        if char.isalpha():
            ascii_offset = ord('A')
            decrypted_char = chr((ord(char) - ascii_offset - key) % 26 + ascii_offset)
            decrypted_message += decrypted_char
        else:
            decrypted_message += char

    return decrypted_message

encrypted_text = "OFR{VGEF_PQODKBF_FTQ_YQEEMSQ!}"
for i in range(1,100):
    key = i
    message = decrypt(encrypted_text, key)
    if message[0:3] == "CTF":
        print(message, key)
        exit(0)
```

4. OSINT

4.1. Чудо-остров

Балл: 1000

Условие:

Наш агент провел ночную фотосъемку, успел отправить лишь одно фото, а дальше перестал выходить на связь. Установи его последнее местоположение. Правильным ответом будет название базы отдыха, где было запечатлено это фото. Оно может состоять из нескольких слов, вводи все. На регистр мы ничего не проверяем, язык ввода – английский

Ответ: Koh Tao
Решение:
Работаем с stegSolve

4.2. Timestamp
Балл: 1000
Условие:
На фотографии изображен самый популярный цифровой актив и один из символов Италии, которым они гордятся. Что же их объединяет? В какую дату произошло то самое событие, что помогло одному человеку стать сытым, а второму - богатым?

Ответ в формате unix timestamp с точностью до секунды, например 1234567898. Без обертки CTF
Ответ: 1274552191
Решение:
время покупки пиццы за 10000 BTC

5. Stego

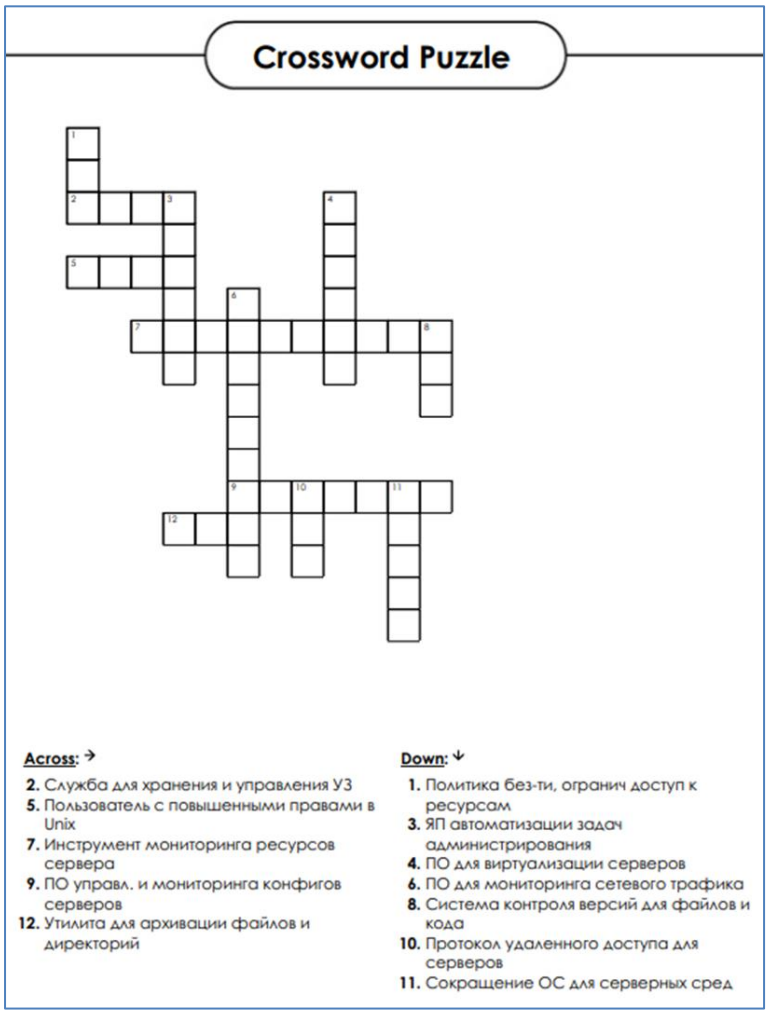
5.1. Залив
Балл: 1000
Условие:
На данном фото изображена звездная ночь (вы, кстати, могли уже встречаться с этой картинкой). Приглядитесь, может ваш глаз и не отличит ничего, но здесь явно что-то скрыто. Используйте свой арсенал для определения секретного послания, зашитого в картинку

Ответ: 7jZvRXILAQxBJ7gDAus2

Решение:
Стандартная фотография картинка в картинке, разбиваем на две и получаем флаг

6. Admin

6.1. Кроссворд
Балл: 1000
Условие:
Что должен знать самый лучший системный администратор в мире? Правильно - команды в консоли и кучу теории, а также софта. Вот мы это и проверим. Реши кроссворд, последовательно собери ключевое слово из клеток, которые помечены цифрами, и получай очки рейтинга! И да пребудет с тобой Ctrl+Alt+Delete



Ответ: ALPVRWMGASLT

Решение:

Необходимо отвечать на задачи, отмеченные в кроссворде для решений