2021 하계 해킹캠프 CTF

You know about USO? write up

by arrester (Demon Team)

작성자: 김주원(arrester)

arresterloyal@gmail.com

https://github.com/Demon-KR

https://blog.naver.com/lstarrlodyl

목 차

2021 하계 해킹캠프 CTF

Ⅰ 문제 개요 및 목표

Ⅰ-1. 문제 개요

문제 제목: You know about USO?

문제 내용:

UFO - 미확인 비행 물체

USO - 미확인 수중 물체

해킹캠프가 진행되고 있는 서울 바로 밑 깊은 해저에 USO가 숨어있었다.

USO는 해킹캠프 참가자들이 풀어서 얻어야 할 flag를 암호화하는데...

해결 과정으로 암호문과 암호화한 과정만 남겨두고 갔다. 참가자들은 문제를 풀었는데 또 풀어야 하는 상황이다.

[암호화 과정]

1. 원래 flag 값 + 주어진 string_key.png 값 각 자리 별 add
2. encrypt = 위 1번 + 임의 key 값

*key 값은 1~23중 하나

문제 출제자: arrester

Ⅰ-2. 문제 목표

string_key.png QR 코드 복원 후 복호화 시도

2021 하계 해킹캠프 CTF

Ⅱ 문제 풀이

Ⅱ-1. string_key.png

그림 1 string_key.png

주어진 파일들을 정리하면 아래와 같다.

1. uso_encrypt.txt
2. string_key.png

여기서 2번인 string_key.png 파일을 열어 보면 QR Code가 있다. 그런데 QR Code가 깨진 상태라 해당 상태로는 Scan이 불가능하다. 즉, 복원이 필요하다.

복원 과정은 그림판 혹은 관련한 도구를 사용하면 되는데 풀이 보고서에서는 간편하게 그림판을 사용한다.

그림 2 그림판을 통한 복원

그림판으로 간단하게 패턴을 그려준다.

그림 3 QR Scan

복원한 string_key.png로 QR Code Scan을 진행하면 "happy_Hacking_Camp_good"이라는 문자열을 얻

을 수 있다. 해당 Scan 사이트는 https://webqr.com/index.html 여기다.

Ⅱ-2. 복호화

암호화 과정을 제공했기 때문에 해당 과정을 반대로 진행하면 복호화할 수 있다.

[암호화 과정]

1. 원래 flag 값 + 주어진 string_key.png 값 각 자리 별 add

2. encrypt = 위 1번 + 임의 key 값

*key 값은 1~23중 하나

암호화 과정을 다시 보면 1번은 아래와 같다.

uso_encrypt.txt에 있는 flag 값: ¼°½ÉÕæ©À¾ÖçßÔ×»æØáãÜîií

string_key.png QR Code 복원으로 얻은 happy_Hacking_Camp_good

각 자리 별 add

즉, uso_encrypt[0] + string_key[0], uso_encrypt[1] + string_key[1], uso_encrypt[2] + string_key[2]

이렇게 각 자리마다 더하면 된다.

그리고 2번은 임의 key 값이 1~23 중 하나를 더하기 한 값이라고 되어 있기 때문에 1~23 만큼 반복문을 작성하면 된다.

그러면 복호화 과정으로 더하기 대신 빼기를 진행하면 된다.

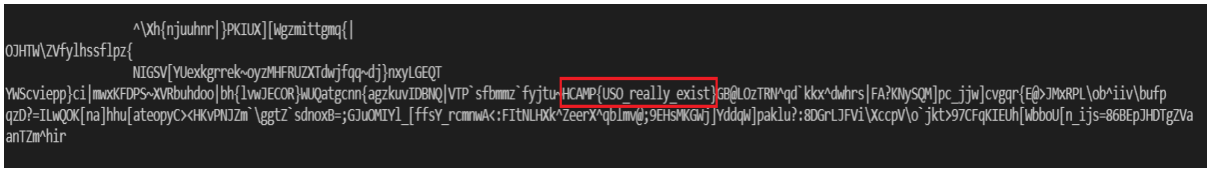
(uso_encrypt – string_key) – key

식은 위와 같으며 이 과정을 코드로 작성한다.

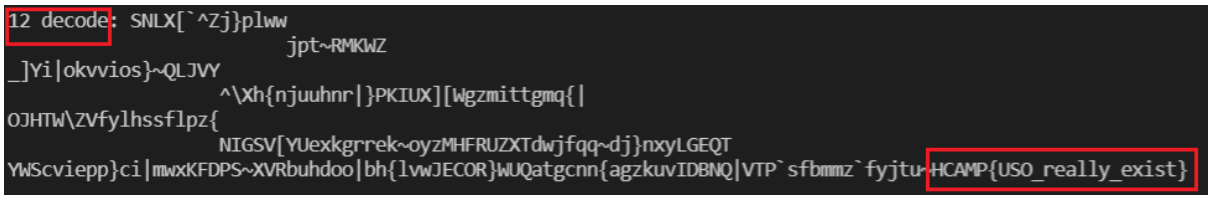
```
string_key = list("happy_Hacking_Camp_good")
encrypt_value = list("¼°½ÉÕæ©À¾ÖçßÔ×»æØáãÜîií")
key = 0
decode = ""

for key in range(1, 24):
    for i in range(0, 23):
        decode += chr(ord(encrypt_value[i]) - ord(string_key[i]) - key)

    print(str(key)+" decode: " + decode + "\n\n")
```

코드는 python으로 작성했다.

결과는 아래와 같다.



23까지 반복해서 출력하도록 작성되었기 때문에 바로 flag를 확인할 수 있다.



key 값은 12다.

flag: HCAMP{USO_really_exist}

2021 하계 해킹캠프 CTF

Ⅲ 결론

프로그래밍 작성 능력을 높일 수 있도록 만든 간단한 암호 문제입니다.

by. Demon Team arrester