แบบฝึกหัดปริศนา

Computer Programming - ★★ **Proposer:** พี่ที่ออกโจทย์ง่ายที่สุด

มีการรายงานว่ามีแบบฝึกหัดใน Grader ข้อนึงที่น่าสงสัย โจทย์ข้อนี้ไม่ได้จัดอยู่ในหมวดใด ๆ เลย พร้อมทั้งมี Template Code มาให้ซึ่งโดยปกติแล้วจะไม่มี และคน upload โจทย์ก็ไม่ใช่คนในทีมพี่สอนด้วย

ในฐานะที่คุณเป็นฝ่าย Security ของเว็บไซต์ Grader นี้ คุณต้องวิเคราะห์โจทย์ข้อนี้ให้ได้ว่าโจทย์ข้อนี้ต้องการอะไร และส่งคำตอบกลับมาในรูปแบบ Flag

(ฟังก์ชันสร้าง Flag มีไว้ให้แล้วครับ น้องไม่ต้องกังวล 🙂)

<u>คำอธิบายโจทย์</u>

ฉันเข้ามาฝังมัลแวร์ในระบบ Grader แล้วแต่ระบบมีการป้องกันที่แน่นหนา ฉันพยายามแฮกเพื่อให้ได้รหัสผ่าน แต่มันใช้เวลานานมาก ฉันกลัวว่าคนในทีมจะรู้และจะเปลี่ยนรหัสผ่านใหม่ ฉันจึงรีบออกจากระบบมาก่อน แต่ฉันได้ข้อมูลคร่าว ๆ มาดังนี้

- ตอนที่ฉันกำลังแฮกเข้าหารหัสผ่านเข้า server ฉันพบกับไฟล์อันนึงที่มีแต่ข้อความที่ดูเหมือนถูกเข้ารหัสเต็มไปหมด**ด้วยวิธีเข้ารหัสครัวซองต์ (Croissant Encryption)** ซึ่งใช้ Key ในการเข้ารหัสโดยเป็นตัวอักษรภาษาอังกฤษตัวเล็ก 4 ตัว ฉันคิดว่าน่าจะเป็นไฟล์ที่รวมรหัสผ่านทั้งหมด โดยในนั้นมีทั้งรหัสผ่านจริงกับปลอม
- ในการ Login ใน Server ฉันพบว่าการพิมพ์รหัสผ่านจะต้องมีทั้งรหัสผ่านที่ถูกเข้ารหัสอยู่ พร้อมกับ Key ในการเข้ารหัสนั้น
- รหัสผ่านที่ถูกต้องจะมีคำว่า “ovenbreak” ***เป็นลำดับย่อย**** ของข้อความที่ถูกถอดรหัสด้วย**วิธีการถอดรหัสแบบสลัด (Salad Decryption) ซึ่งต้องใช้ Key อันเดียวกันตอนเข้ารหัสครัวซองต์**

เพื่อให้ทีมงาน Track IP เครื่องฉันไม่ได้ ฉันต้องรีบซ่อนตัวให้ได้ไวที่สุด เพราะฉะนั้นคุณต้องถอดรหัสเองเพราะฉันไม่มีเวลามาทำให้

ฉันจะส่งรายละเอียดทั้งหมดผ่านโจทย์ Grader ข้อนี้เพื่อให้ทีมงานไม่สงสัย โจทย์ข้อนี้จะมีแค่คุณที่เห็นเท่านั้น

CTF07 - แบบฝึกหัดปริศนา

ไฟล์ที่แนบมาด้วย

CTF07.zip โดยในไฟล์ zip นั้นประกอบไปด้วย

1. ไฟล์ pass.txt รวม รหัสผ่านที่ถูกเข้ารหัสทั้งหมด 500 ตัว มีเฉพาะตัวพิมพ์เล็กและแต่ละตัวมีความยาว 32 ตัวอักษร **รับประกันว่าในไฟล์ pass.txt จะมีรหัสผ่านและ Key แค่ตัวเดียวเท่านั้นที่ถูกต้อง**
2. ไฟล์ code.cpp เป็น ไฟล์ C++ ที่มีฟังก์ชันการเข้ารหัสครัวซองต์ (CroissantEncrypt) และฟังก์ชันสร้าง Flag (GenerateFlag)
    - ฟังก์ชัน main , การถอดรหัสแบบสลัด (SaladDecrypt) , ฟังก์ชันตรวจสอบรหัสผ่าน (checkPassword) ถูกเว้นว่างไว้
    - Library ที่จำเป็นทั้งหมดถูก include แล้ว
3. ไฟล์ md5.cpp และ md5.h ซึ่งจำเป็นในการสร้าง Flag
4. **ทุกไฟล์ต้องอยู่ใน folder เดียวกับ code.cpp เท่านั้น มิฉะนั้นไฟล์จะ run ไม่ได้**

รูปแบบ Flag

เป็นข้อความที่ได้จาก hash md5 ของคำตอบของโจทย์ที่ได้ โดยสามารถได้ Flag มาจากฟังก์ชัน GenerateFlag

OVB{md5}

* **หมายเหตุ:** *สำหรับข้อความ S และ T ใด ๆ เราจะกล่าวว่า S เป็น**ลำดับย่อย**ของ T ก็ต่อเมื่อเราสามารถลบตัวอักษรบางตัวของ T (หรือไม่ลบเลย) โดยที่ลำดับของตัวอักษรอื่น ๆ คงเดิม จนทำให้ข้อความ T กลายเป็น S ได้ เช่น “ace” เป็นลำดับย่อยของ “abcde” แต่ “aec” ไม่ใช่ลำดับย่อยของ “abcde”*