

تحليل البيانات النصية

1- فك تشفير النصوص

تم فك تشفير النصوص المشفرة باستخدام تقنية Base64، وكانت النتائج كما يلي:

I. Hello! This is a secret message.

II. FLAG{Y0u_can_decode_this}

III. This is a test of emergency messages. Decode this!

2- تحليل المحتوى والأسلوب اللغوي

- الموضوع: تتعلق نوعية النصوص بالتشفير واختبار الرسائل السرية، وهي مصممة لأغراض تدريبية في مجال الأمن السيبراني.
- الأسلوب اللغوي:

- الجملة مباشرة وواضحة.
- استخدام عبارات تحفيزية مثل "Decode this!" لتشجيع القارئ على المشاركة في فك التشفير.
- النص الثاني يحتوي على FLAG{} وهو شائع في تحديات CTF (Capture The Flag) الخاصة بالأمن السيبراني.

3- تحسين أمان التشفير

Base64 ليس تقنية تشفير (Encryption) بل هو مجرد ترميز (Encoding)، مما يعني أنه غير آمن لحماية المعلومات الحساسة. لتحسين أمان التشفير، يمكن استخدام:

1. التشفير باستخدام خوارزميات قوية مثل:

○ AES (Advanced Encryption Standard)

○ RSA (Rivest-Shamir-Adleman)

2. استخدام Key و Salt قوي عند تشفير البيانات لضمان عدم القدرة على فك التشفير بسهولة.

3. استخدام Hashing مثل SHA-256 أو Argon2 إذا كانت البيانات لا تحتاج إلى فك تشفير لاحقاً.

4. دمج تقنيات مختلفة مثل Base64 مع AES بحيث يتم تشفير البيانات أولاً باستخدام AES ثم ترميزها بـ Base64 لتسهيل نقلها.

النتيجة

تم فك التشفير بنجاح وتحليل المحتوى، وتقديم اقتراحات لتحسين أمان البيانات باستخدام خوارزميات أقوى مثل AES و RSA

Zaher Al Shehri

222000935