ETAPA 2

- “En criptografía, un ataque de relleno de oráculo es un ataque que utiliza la validación de relleno de un mensaje criptográfico para descifrar el texto cifrado. En criptografía, los mensajes de texto plano de longitud variable a menudo tienen que rellenarse (expandirse) para que sean compatibles con la primitiva criptográfica subyacente. El ataque se basa en tener un "oráculo de relleno" que responde libremente a las consultas sobre si un mensaje está correctamente rellenado o no. Los ataques de relleno de Oracle se asocian principalmente con el descifrado en modo CBC utilizado dentro de los cifrados de bloque ”(Wikipedia).

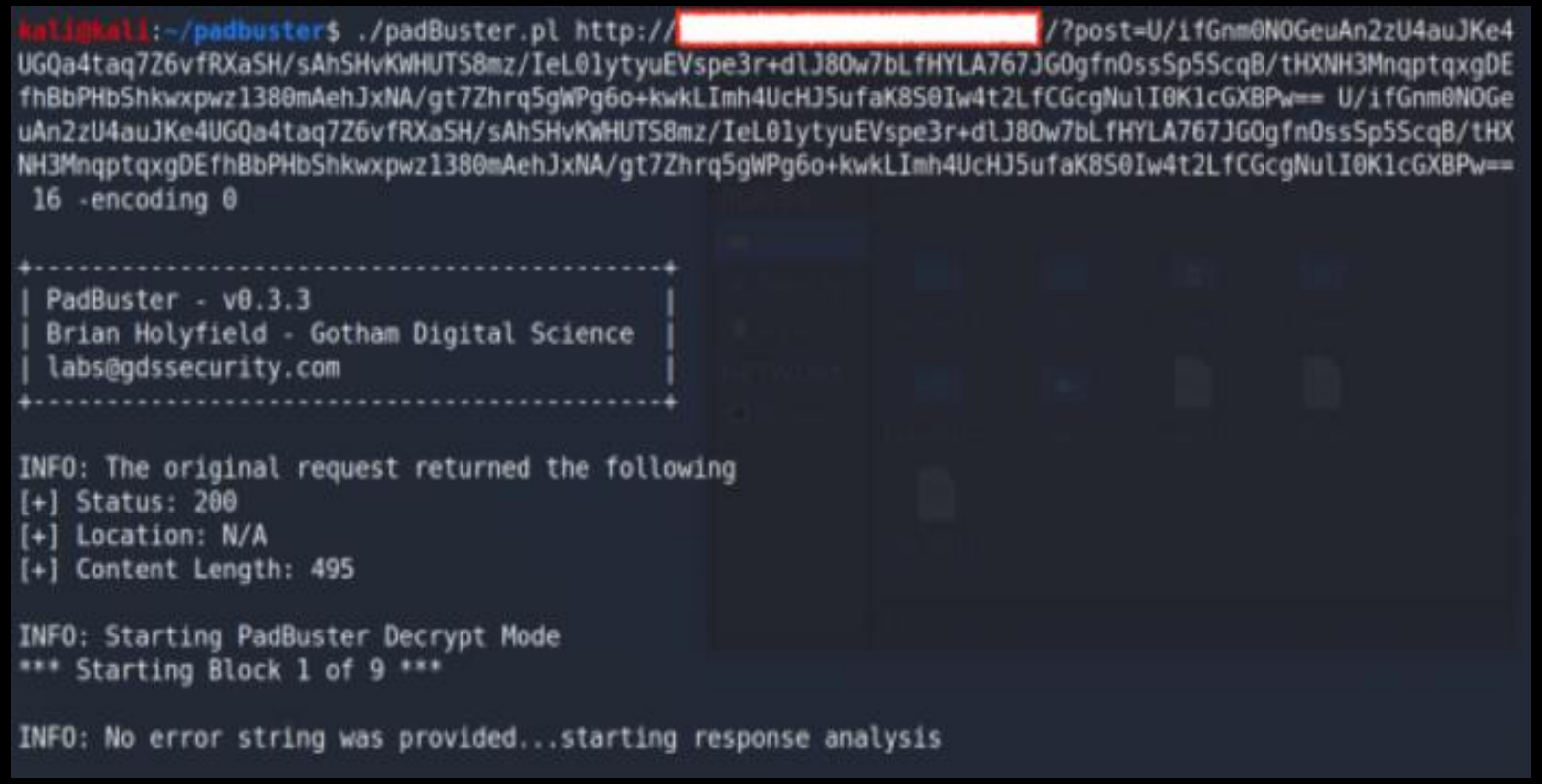
Después de leerlo y usar PadBuster, pude descifrar el valor cifrado y obtener la bandera deseada.

PoC:

- Descargar /clone PadBuster.pl from this Github repositorio en:
  - https://github.com/AonCyberLabs/PadBuster.

Forma de Usar : padBuster.pl URL EncryptedSample BlockSize [options]

Exploiting:



Como puede ver, ingresé la URL completa, que contiene el valor cifrado del parámetro de publicación, seguido del valor cifrado en sí, el tamaño del bloque (que ya sabemos que es 16) y una especificación de cómo se codifica la muestra cifrada, en este caso - encoding 0 es Base64 (que también es la predeterminada). Después de un tiempo, obtuvimos un texto sin formato de la bandera y la clave:

```
** Finished ***

[+] Decrypted value (ASCII): {"flag": "^FLAG^[redacted]
[redacted]$FLAG$", "id": "3", "key": "[redacted]"}
```