Writeup - CyberPol API

---

1. GetYourKey

Para obter a primeira flag, o atacante deve acessar o diretório oculto na rota `/debug`.

```
b550bed920bf51ddfa0e7fd5e3cbe7846409889625861de6407825727ed14590
```

2. ExternalArea

Para obter a segunda flag, o atacante precisa:

- Utilizar o token obtido na rota anterior
- Acessar a rota `/auth`
- Usar o header HTTP `X-Forwaded-For: 127.0.0.1`

```
178596985a70e8444d8a05ed4cab977c0283d122a8e4c511485e299cce04615d
```

3. LogHere

Para obter a terceira flag, o atacante deve:

1. Acessar o documento PDF indicado anteriormente
2. Decodificar a mensagem encontrada no fim do arquivo, seguindo estes passos:

- Transformar todas as letras A em 0
- Transformar todas as letras Z em 1
- Converter o código binário resultante para ASCII

1. Após decodificar a mensagem, o atacante terá acesso ao segundo documento
2. Encontrar a terceira flag registrada na seção de **logs** do documento

```
6a731f23e72e9d00f9bc4c8e5835cf163f0fd00fc59edffa948e70dc8d64ba12
```

4. SOSLetter

Para obter a quarta e última flag, o atacante precisa:

1. Descriptografar a mensagem final encontrada no segundo arquivo PDF
2. Observar que a mensagem está criptografada usando a cifra simétrica AES
3. Localizar a chave e o vetor IV disponibilizados no próprio arquivo, na seção que descreve um *malware* fictício
4. Escrever um código para descriptografar a mensagem

- Aqui está um exemplo de código em *Python* capaz de realizar este processo:

```
import base64
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

def decrypt_data(encrypted_text):
    key = b'a1b2c3d4e5f60718293a4b5c6d7e8f90'
    iv = b'\x00' * 16
    ciphertext = base64.b64decode(encrypted_text)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)
```

```
    return decrypted_data.decode('utf-8')

if __name__ == "__main__":
    encrypted_text = input("Enter the encrypted text: ")
    try:
        decrypted_text = decrypt_data(encrypted_text)
        print("Decrypted text:", decrypted_text)
    except Exception as e:
        print("Decryption failed:", e)
```

5. Após descriptografar o valor, o atacante obterá a rota final para o terceiro e último arquivo, que conterá a quarta flag

```
a54c9a95799b797f2a2586f4f9269c83e898bc7cf8e217c26edda1e1f4b793cc
```