This is the super sensitive, confidential document that was affected by the ransomware. Congratulations on the bruteforce!

You can paste your bruteforce script in the box below:

|  |
| --- |
| '''  Forage AIG Cybersecurity Program  Bruteforce starter template  '''  *from* zipfile *import* ZipFile, BadZipFile  *import* sys  # *Function to attempt to extract the zip file with a given password*  def *attempt\_extract*(zf\_handle, password):  *try*:          zf\_handle.extractall(pwd=password.strip())          print(f"[+] Password found: {password.decode().strip()}")  *return* True  *except* (RuntimeError, BadZipFile):  *return* False  def *main*():      print("[+] Beginning brute-force")  *with* ZipFile('enc.zip') *as* zf:  *with* open('rockyou.txt', 'rb') *as* f:  *for* line *in* f:                  password = line.strip()  *if* attempt\_extract(zf, password):  *return*  # *Exit if password is found*      print("[+] Password not found in list")  *if* \_\_name\_\_ == "\_\_main\_\_":      main() |