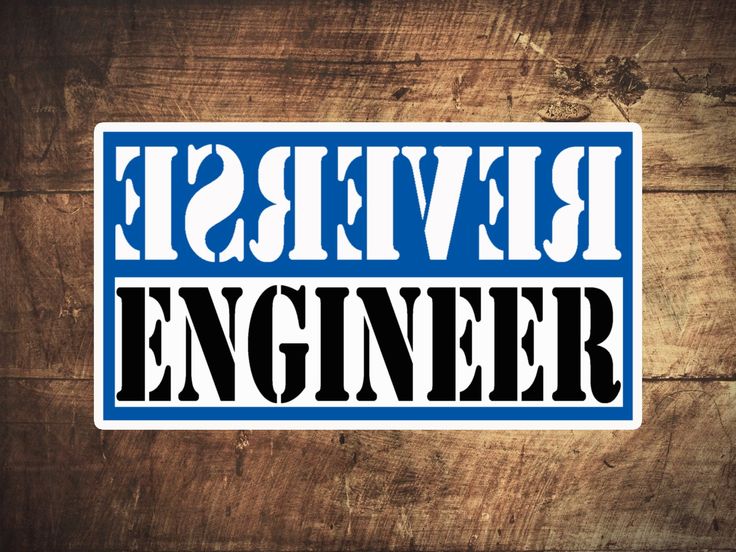
**CTF Topic: Reverse Engineering**

****

**Introduction**

Reverse engineering is the process of analysing a software application to understand its components and functionality. This is commonly used in cybersecurity to uncover vulnerabilities, understand malware behaviour, and develop patches for software applications. Reverse engineering involves several techniques such as disassembly and debugging to dissect and analyse the inner workings of a program.

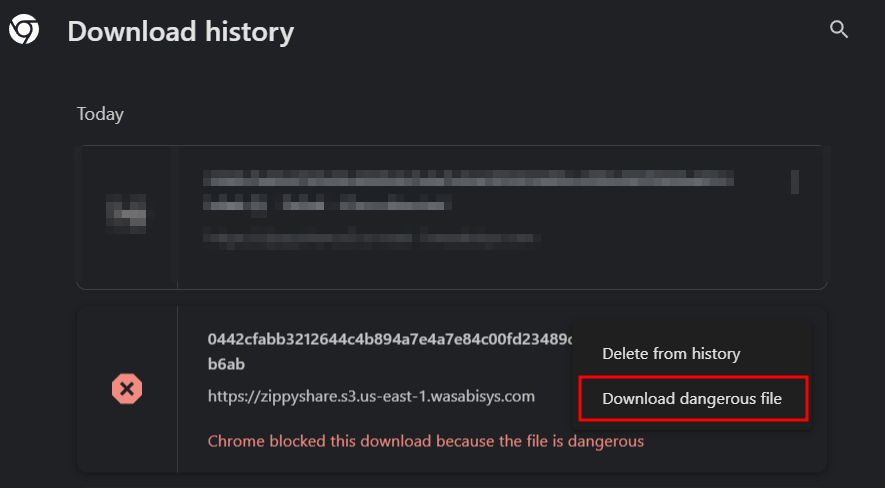


**Link**

**1.** [**https://dogbolt.org/**](https://dogbolt.org/)

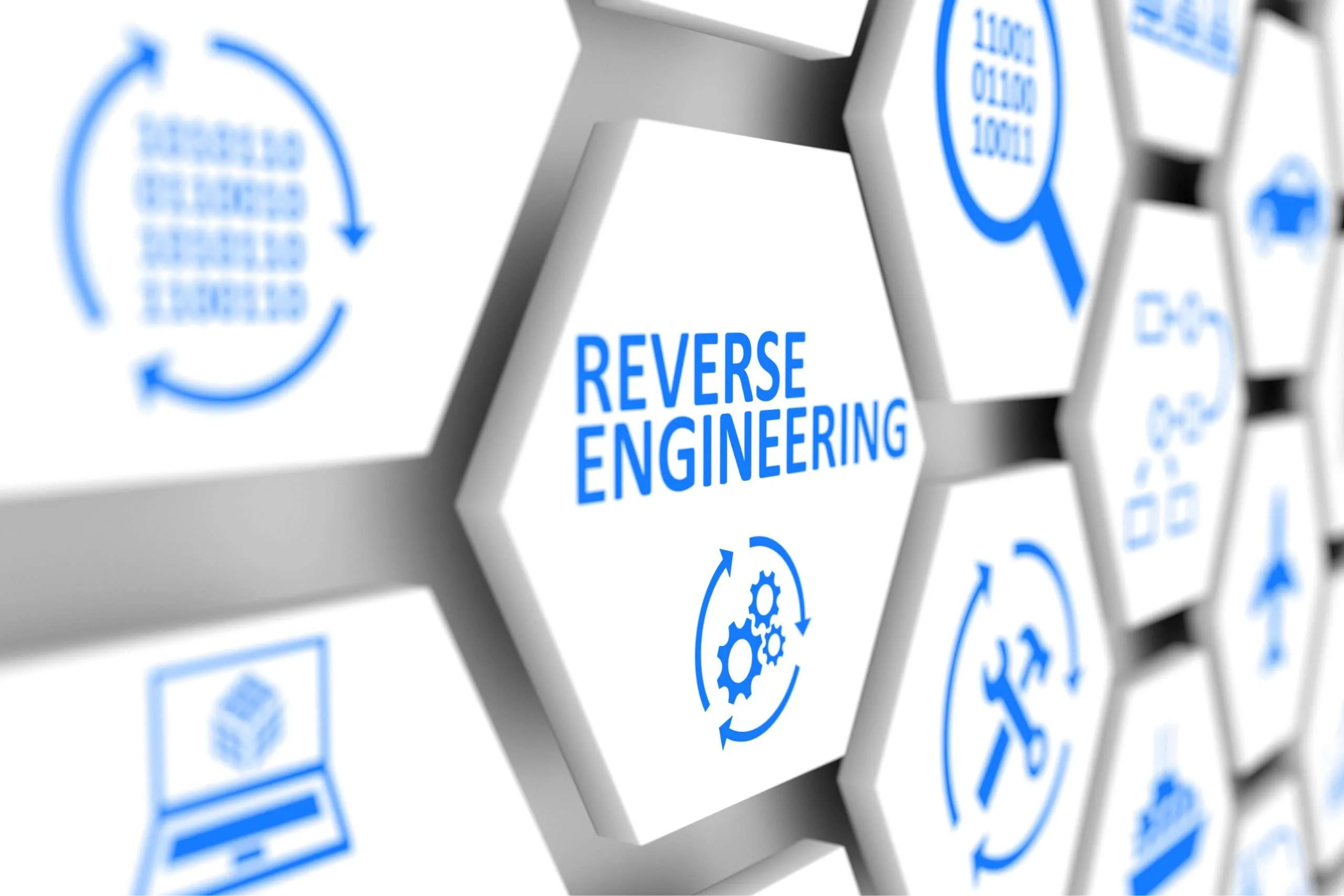
**2. Binary File Link:-** [**https://zippyshare.day/RGibKMe18O9Jcuy/file**](https://zippyshare.day/RGibKMe18O9Jcuy/file)

**Note:-** After Downloading the Binary File ,Don’t Try to Execute in your Machine.

In case chrome blocks your download. ****

**Scenario**

As a new security analyst, you are tasked with reverse engineering a basic binary file to understand its functionality and uncover any hidden features or messages.



**Process**

To begin, download the binary file and open it in your preferred disassembly tool.

## **Steps**

* Download the Binary File: [**https://zippyshare.day/RGibKMe18O9Jcuy/file**](https://zippyshare.day/RGibKMe18O9Jcuy/file)
* Upload the downloaded file in the link [**https://dogbolt.org/**](https://dogbolt.org/). Sample portions should remain empty.
* Wait until it loaded on the all portion

**Questions**

**Flag 1: What is the address of the main function given on line 6 of binaryNinja?**

**Answer: 0x80004002**

**Flag Captured.**

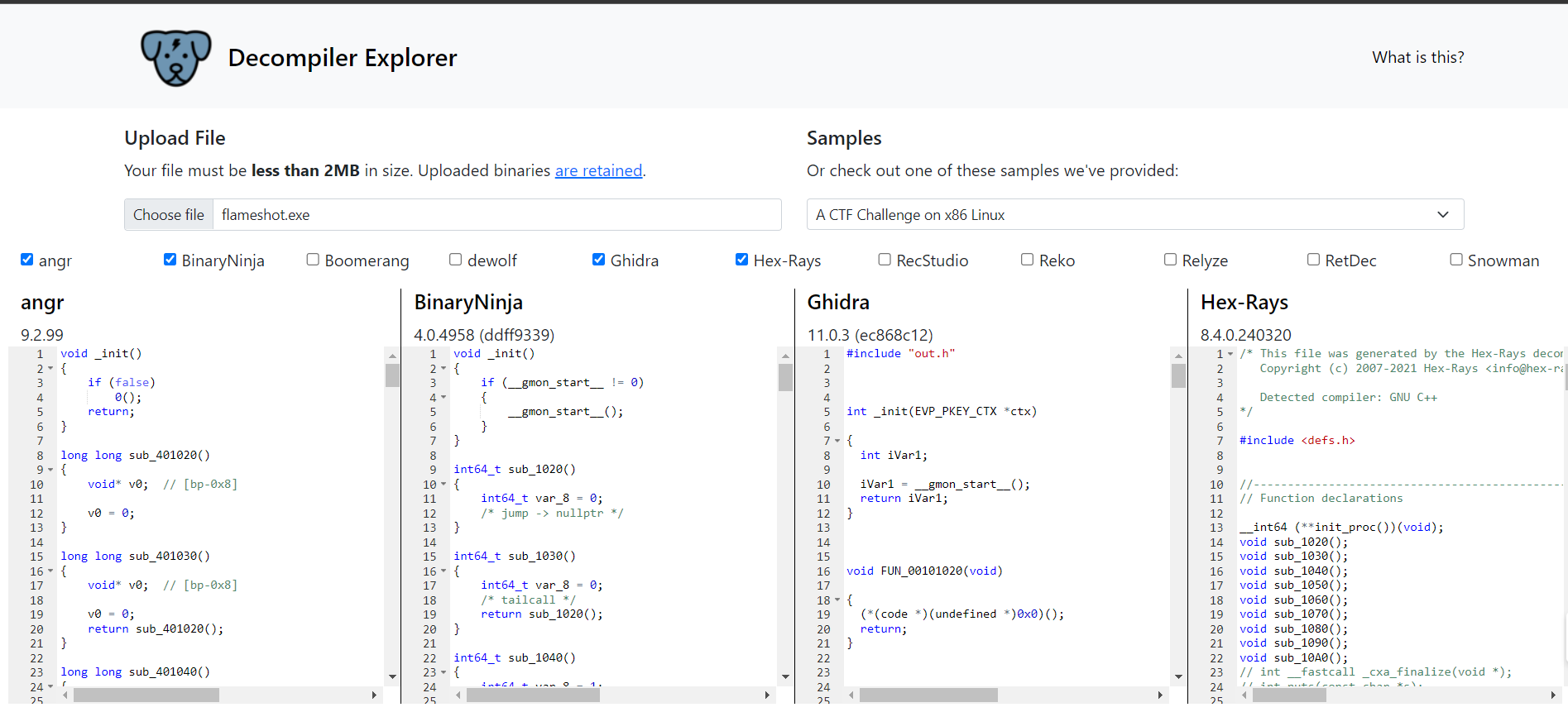
**Flag 2: What is the correct password required by the binary?**

**Answer: No Password Required.**

**Flag Captured.**

**Hint**

Use the strings command or the string search feature in your disassembly tool to quickly find readable text within the binary. This will help you identify messages and passwords used by the program.

****