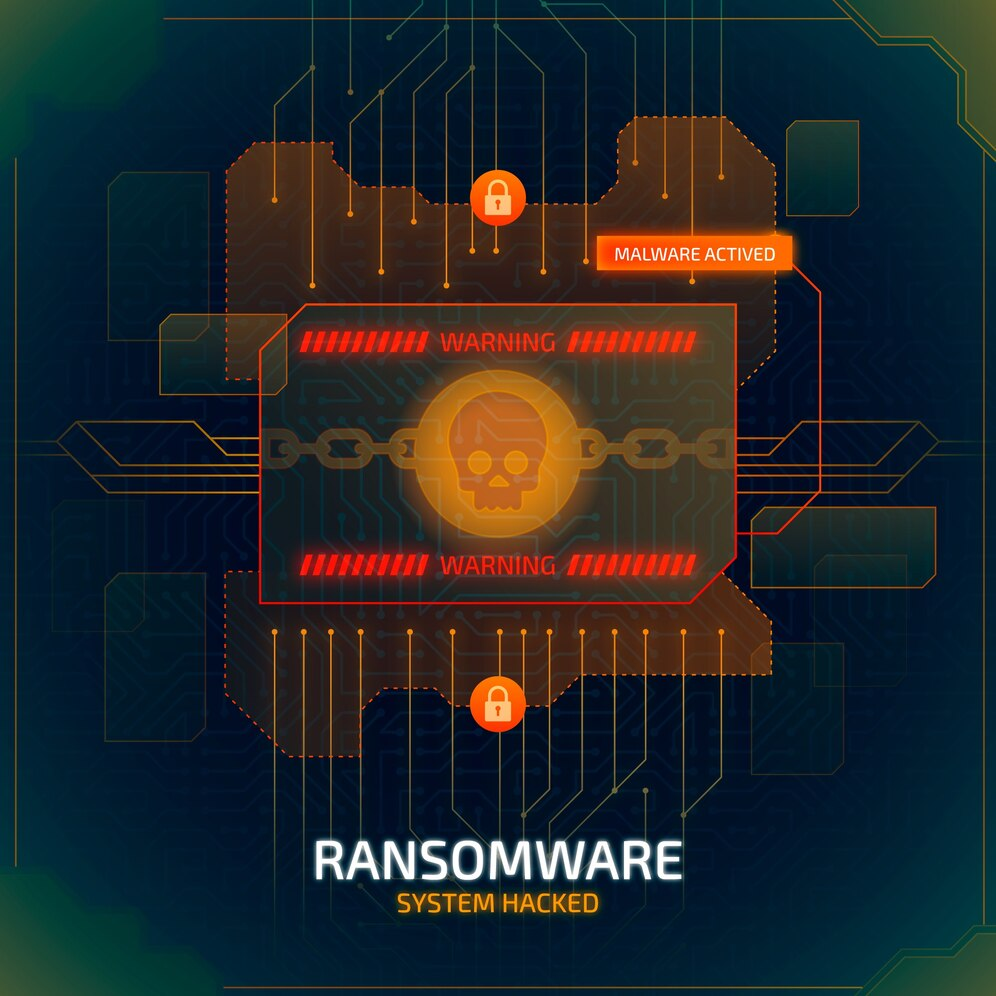
**Ransomware Basics**

**Introduction**

****

Ransomware is malicious software that encrypts a victim's files and demands a ransom to restore access. Understanding how ransomware operates and how to detect, analyze, and mitigate it is crucial for cybersecurity professionals. This Capture the Flag (CTF) scenario introduces beginners to the basics of ransomware analysis using simple, online-based tools.

**Tools and Requirements**

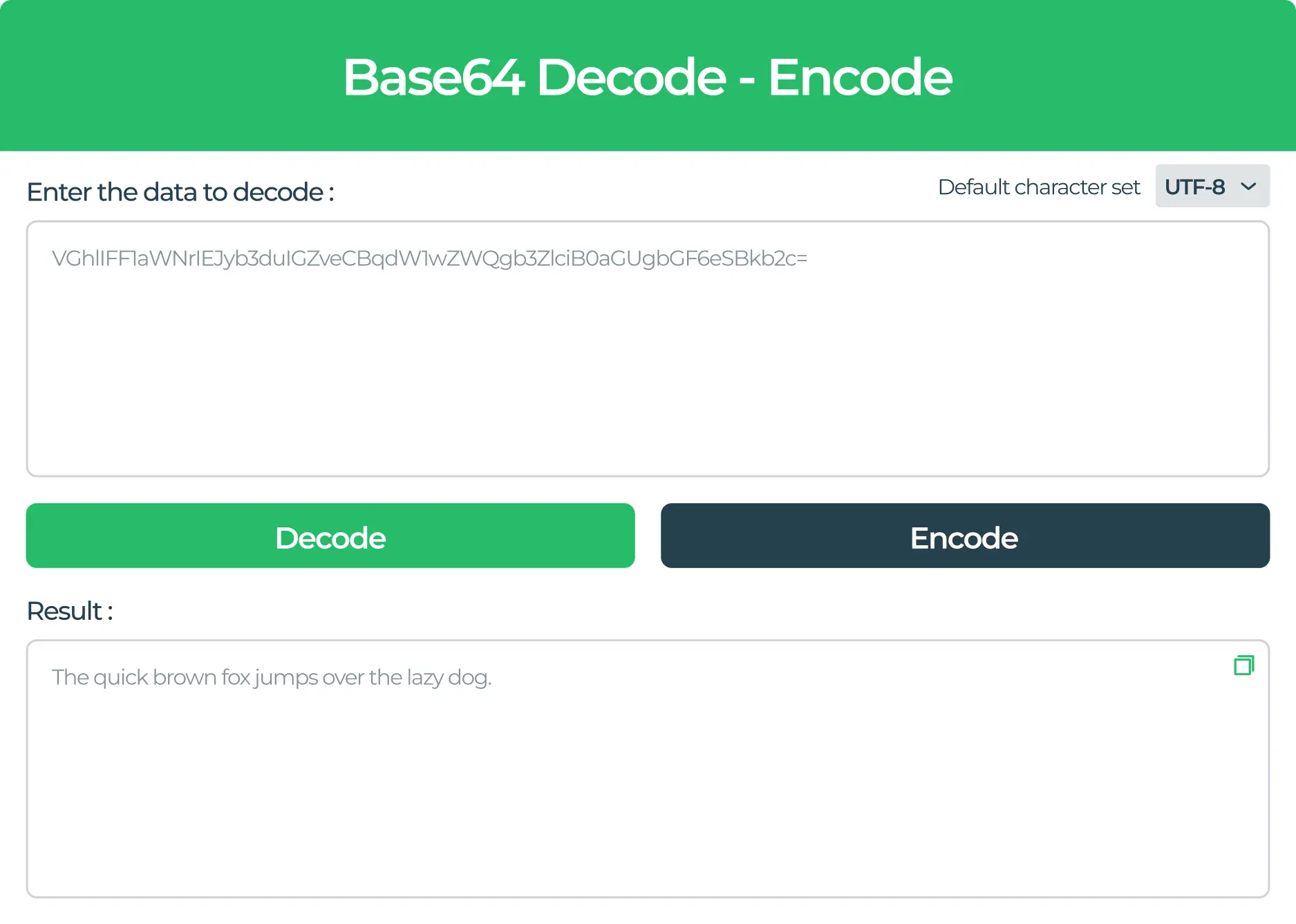
* Base64 Decode: Decode Base64 encoded strings.

Link: <https://www.base64decode.org/>

**Scenario**

In this scenario, you will simulate the analysis of a hypothetical ransomware attack. Your tasks include identifying ransomware behavior, decoding ransom notes, gathering information about malicious IP addresses, and understanding basic ransomware mitigation techniques.

**Begin**

****

To start, familiarize yourself with the online tools listed above. Use these tools to solve the challenges and capture the flags.

**Questions**

**Flag 1: Decode a Ransomware Note Using Base64 Decode**

Task: Use Base64 Decode to decode a Base64 encoded ransomware note.

Hypothetical Encoded Note:

‘WW91ciBmaWxlcyBoYXZlIGJlZW4gZW5jcnlwdGVkLiBQYXkgMSBCaXRjb2luIHRvIHRoZSBmb2xsb3dpbmcgYWRkcmVzcy4=’

Question: What is the decoded message in the ransomware note?

Hint: Use the Base64 Decode tool to decode the message.

Answer: Your files have been encrypted. Pay 1 Bitcoin to the following address.

Flag Captured.

**Flag 2: Decode a Base64 Encoded URL Using Base64 Decode**

Task: Use Base64 Decode to decode a Base64 encoded URL provided by ransomware.

Hypothetical Encoded URL: aHR0cDovL3JhbnNvbXdhcmUtZXhhbXBsZS5jb20=

Question: What is the decoded URL?

Hint: Copy the encoded string and use the decode function.

Answer: http://ransomware-example.com

Flag Captured.

**Hint**

For example, as mentioned in the question you should visit the online tool with the help of the link provided and do what is said. You can see flag 1 has been done for you.

