# **CTF Topic: PDF Analysis Using Jotti.org**



# **1. Introduction**



Capture The Flag (CTF) challenges often include tasks that require analyzing and extracting information from PDF files. PDFs can contain hidden data, embedded objects, and metadata that can be crucial in solving these challenges. This guide will introduce you to the tools and techniques used for PDF analysis in a CTF environment.

# **2. Tools and requirements**

Virus Scan

# **4. Scenario**



Imagine you are participating in a CTF challenge where you are given a suspicious PDF file. Your task is to uncover hidden information and extract data that might lead you to the next clue or the flag.

# 

# **5. Process to Perform**

Step1: Download the PDF given in the link:

<https://www.mediafire.com/file/s08mje7paavj1l7/Analysisfile.pdf/file>

Step 2: Analyze It using the Virusscan tool: <https://virusscan.jotti.org/>

Step 3: Upload the file and solve the CTF

# 

# **6. Let's Begin The Challenge**

Start by extracting the metadata from the PDF file to gather basic information about the document.

# **Question**

Flag1: What is the version used by the pdf ?

Answer: 1.5

Flag Captured

Flag2: What is the MD5 hash value ?

Answer: 880bf67206e533e271a2967542cdaeb5

Flag Captured

# **8. Hint**

