**MD2PDF\_Solution\_Documentation**

**Written by: Yuval Quina**

1. To begin with, I started with performing an Nmap port scanning:

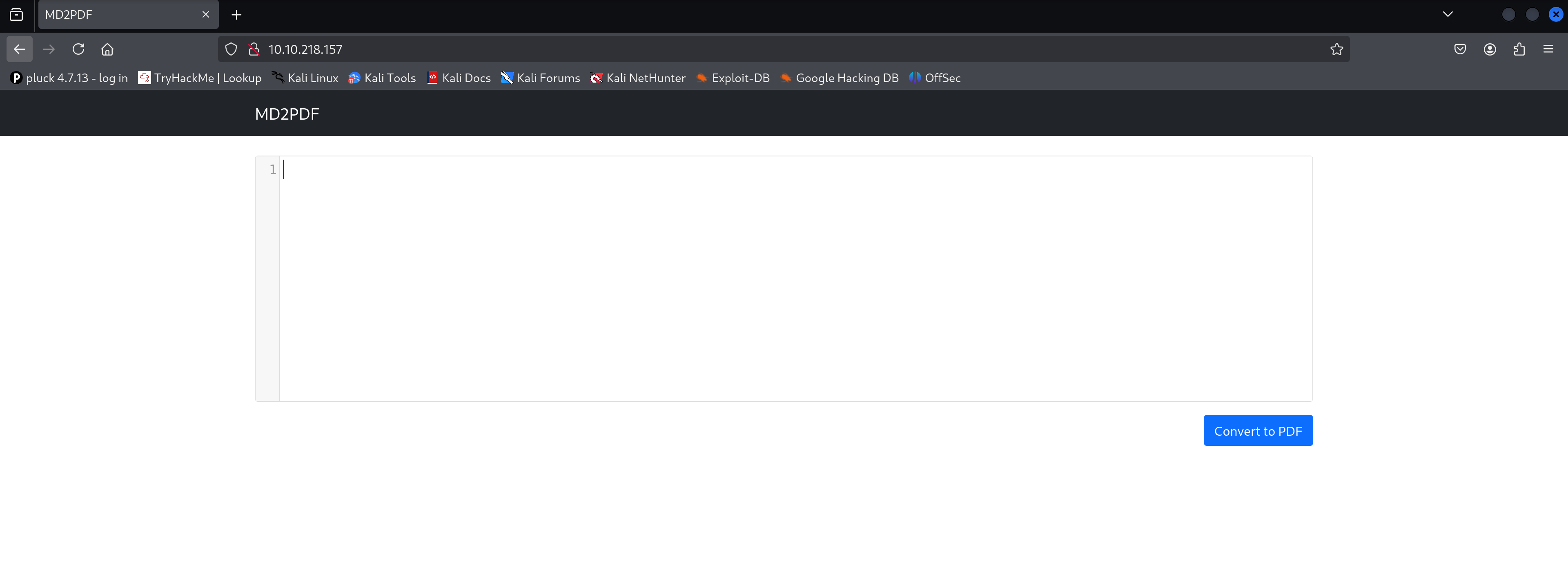


I saw an unusual port and service, the tcp 5000 & upnp, which made me research about it:

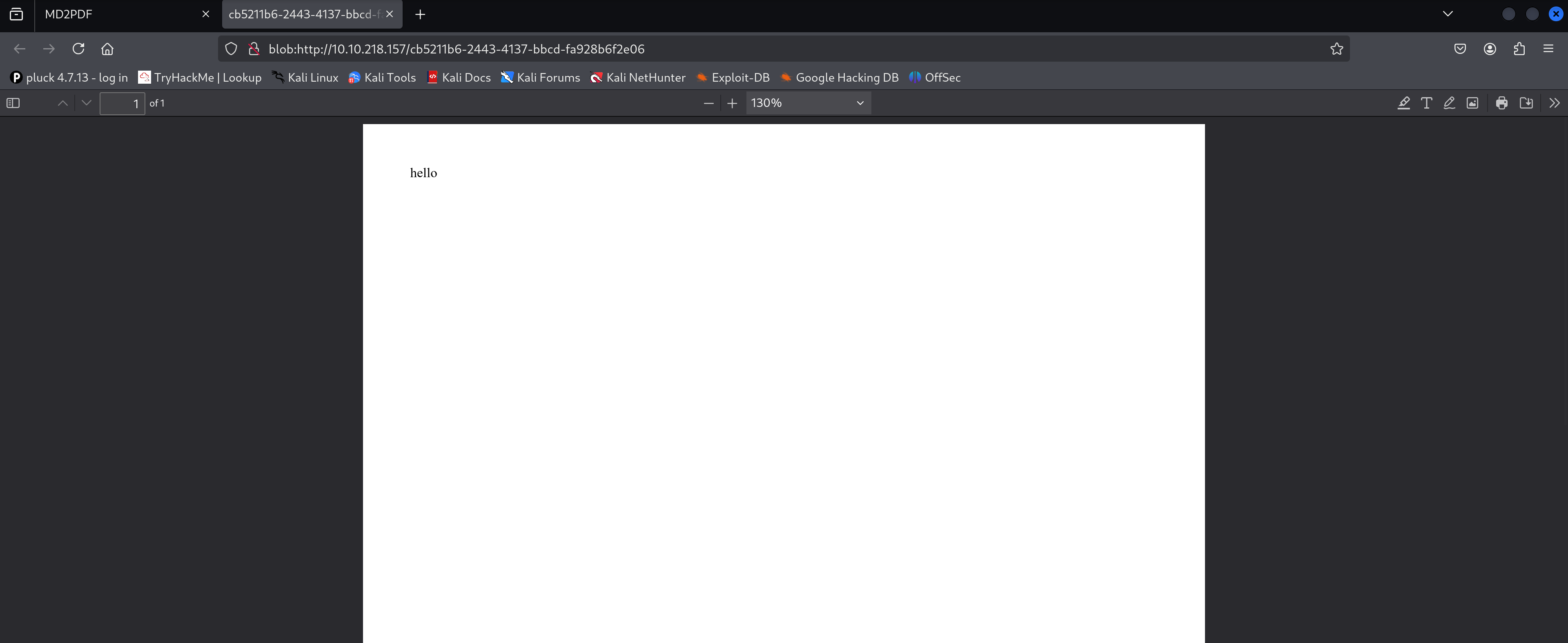
**UPnP (Universal Plug and Play)** is a network protocol that allows devices (like smart TVs, routers, game consoles, printers) to automatically discover and communicate with each other on a local network. It’s designed for ease of use, often used in home networks.

**TCP Port 5000** is often used by the UPnP SOAP service, which is part of the UPnP control protocol.

1. After I researched it, I entered the website of this target:

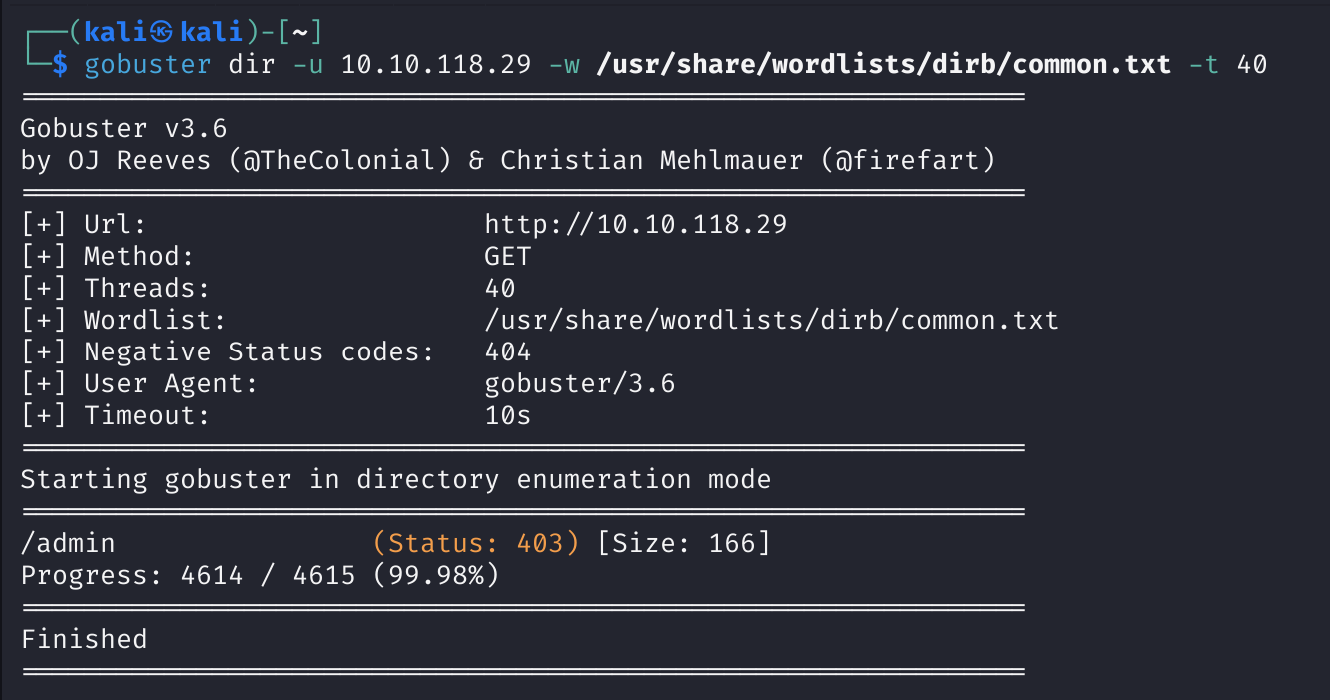


1. Immediately, I entered “hello” over the text area and clicked of the convert blue button:



1. Doing it, cause the website to convert the text to a PDF file which contains the entered text.

I thought to leave it for a moment and try enumerating directories using gosbuster:

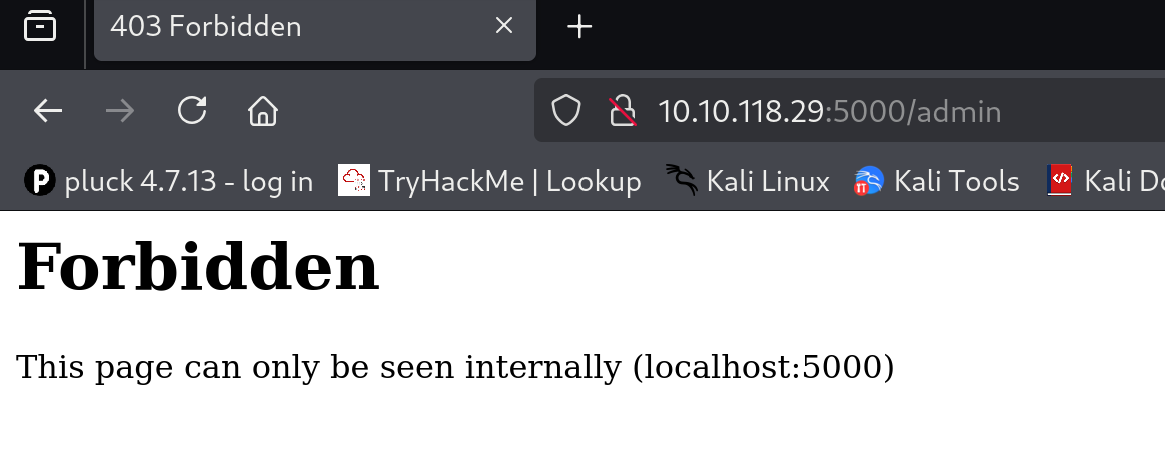


I found the directory “/admin” and when I opened it I faced with this error:

תמונה שמכילה טקסט, צילום מסך, תוכנה, תכונות מולטימדיה

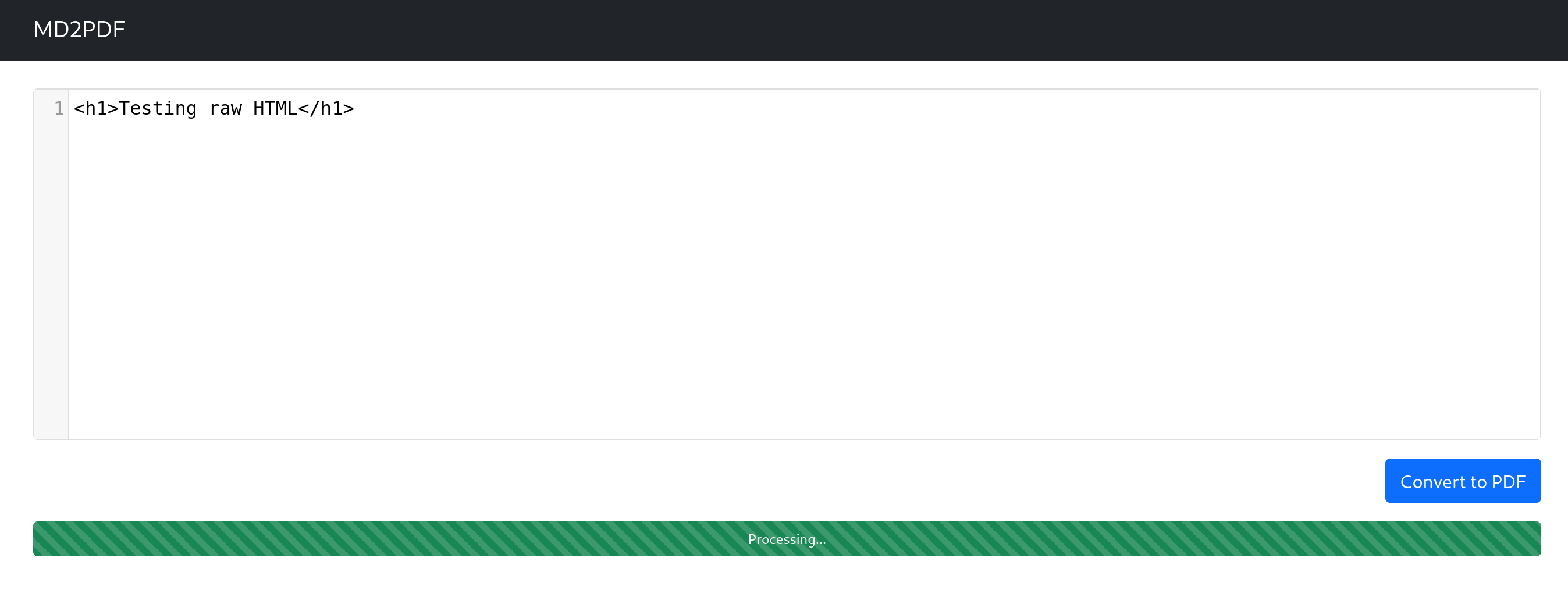
תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

1. I understood that there is something interesting there, so I tried unsuccessfully, using port 5000, accessing this page using the port 5000 so it failed again:



1. Here I realized that I would be able to access this page internally using a SSRF on the converter itself:

Firstly, I tried to use html to check if the converter can run raw html commands:

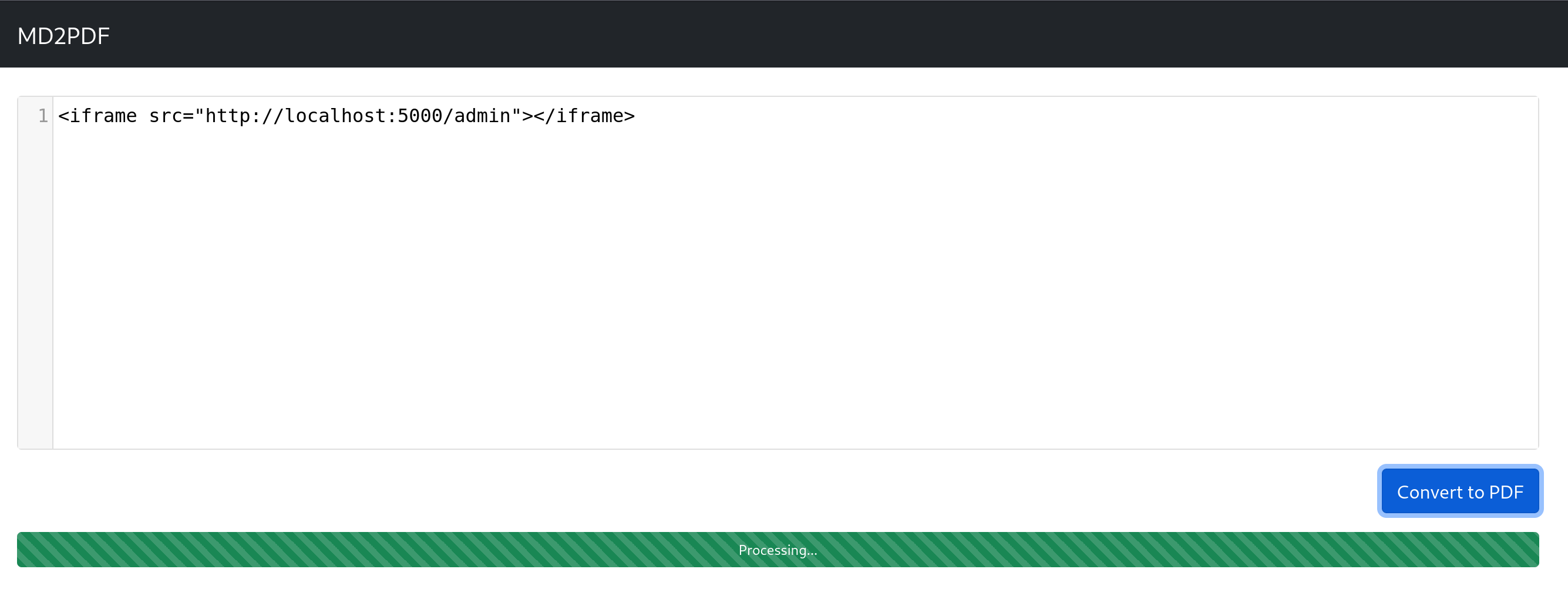


And the result showed me that it was possible:

תמונה שמכילה צילום מסך, טקסט, תוכנה, מחשב

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

Therefore, I tried to run an iframe tag that will load the “/admin” page using the port 5000 and the localhost:



and it gave me the flag:

תמונה שמכילה טקסט, צילום מסך, תוכנה

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.