

Introduction

1 Overview

The report documents the findings of penetration testing of Anthem box that was performed on the Tryhackme platform.

The objective was to find the flag and a report that documents the main findings, the vulnerabilities that were found, and the methods that were used. The report will also include screenshots that document processes, a conclusion, and suggested fixes that the client must perform to secure the web application.

2 Scope

The “Anthem box” specified that the testing will occur only on the given box, located in room “anthem”.

Social Engineering is not included within the scope.

3 Out of Scope

The client specified that no external resource testing will be permitted, including JS codes that hold certain URLs that are not part of the domain.

4 Summary

At first, the website had to be investigated to collect all the flags. Once the first vulnerability on the website was found, more information about the perspective of the website programmer was obtained, which yielded additional findings.

Detailed Findings

Enumeration – User

System misconfiguration - Root Flag

User Flag - THM{N00T_NOOT}

Root Flag - THM{YOU_4R3_1337}

Proof of concept (with HD screenshots) –

Reconnaissance:

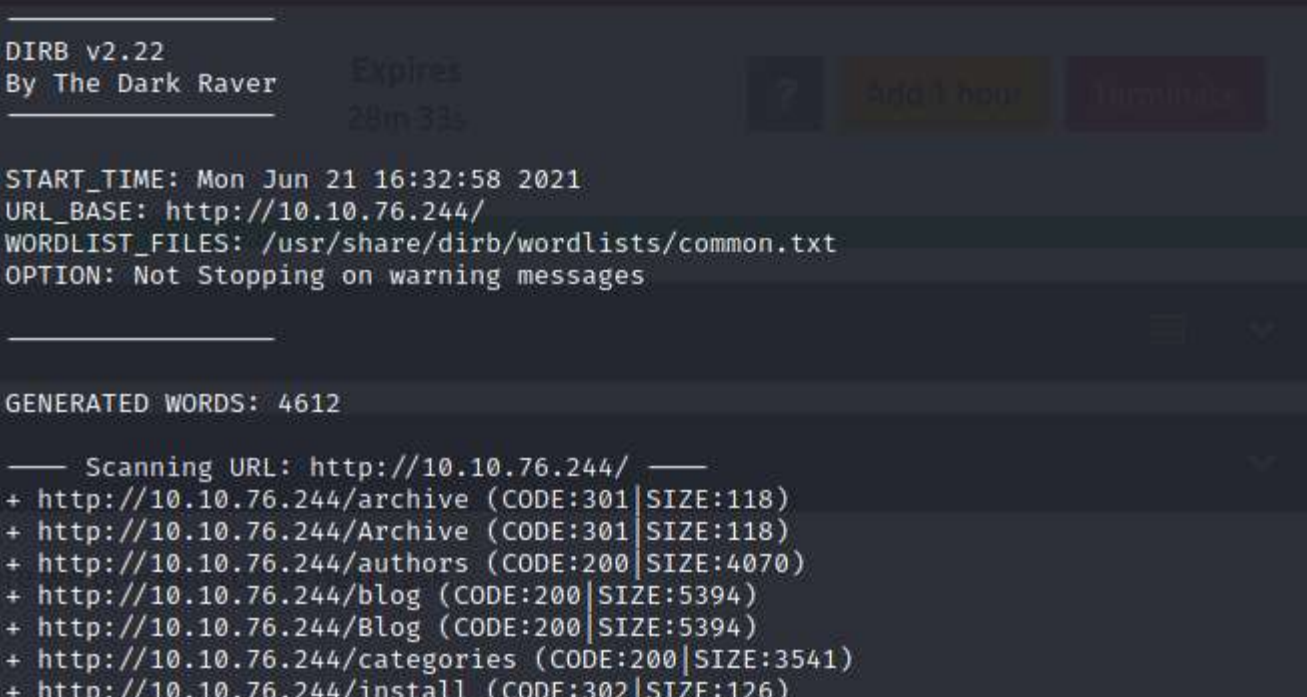
Command: nmap -sC -sV 10.10.92.201

```
root@kali:~# nmap -sC -sV -Pn 10.10.92.201
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 14:19 EDT
Nmap scan report for 10.10.92.201
Host is up (0.31s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
rdp-ntlm-info:
  Target_Name: WIN-LU09299160F
  NetBIOS_Domain_Name: WIN-LU09299160F
  NetBIOS_Computer_Name: WIN-LU09299160F
  DNS_Domain_Name: WIN-LU09299160F
  DNS_Computer_Name: WIN-LU09299160F
  Product_Version: 10.0.17763
  System_Time: 2021-06-21T18:20:33+00:00
ssl-cert: Subject: commonName=WIN-LU09299160F
Not valid before: 2021-06-20T18:10:11
Not valid after: 2021-12-20T18:10:11
ssl-date: 2021-06-21T18:21:40+00:00; +1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We see 2 services http and rdp on this server. Let's enumerate the website and see if we can find something.

Using dirb to find as many pages as we can on the website.

```
root@kali:~# dirb http://10.10.76.244 -w /usr/share/wordlists/dirb/big.txt
```



```
DIRB v2.22
By The Dark Raver

Expires: 28m 33s
? Add 1 hour Turn off

START_TIME: Mon Jun 21 16:32:58 2021
URL_BASE: http://10.10.76.244/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

GENERATED WORDS: 4612

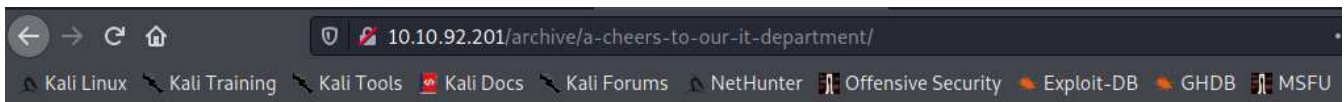
— Scanning URL: http://10.10.76.244/ —
+ http://10.10.76.244/archive (CODE:301|SIZE:118)
+ http://10.10.76.244/Archive (CODE:301|SIZE:118)
+ http://10.10.76.244/authors (CODE:200|SIZE:4070)
+ http://10.10.76.244/blog (CODE:200|SIZE:5394)
+ http://10.10.76.244/Blog (CODE:200|SIZE:5394)
+ http://10.10.76.244/categories (CODE:200|SIZE:3541)
+ http://10.10.76.244/install (CODE:302|SIZE:126)
```

Command: dirb http://10.10.92.201 -w /usr/share/dirb/big.txt

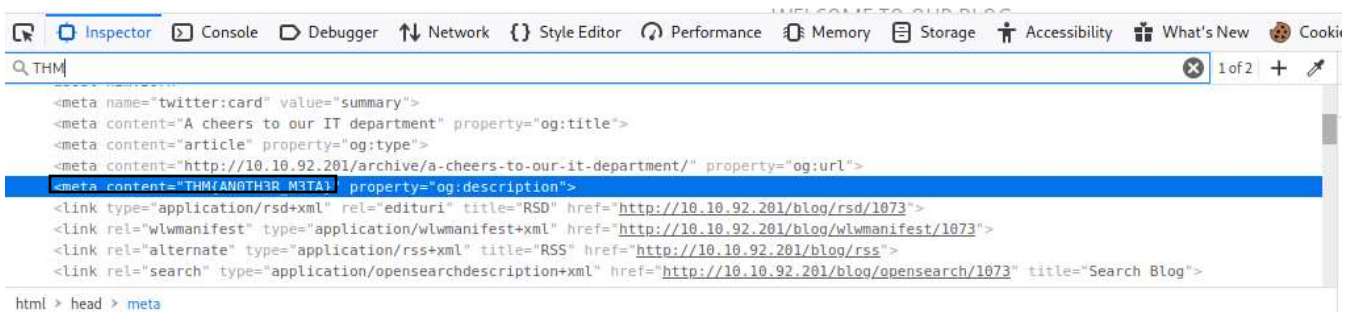
We got many more directories like archive, blog, categories so let's check them to get all we can.

I started with the article we-are-hiring and after checking the page I started the developer options to inspect the page and there in the meta data I found a flag

Flag 1: THM{LOL_WHO_US3S_M3T4}



Anthem.com



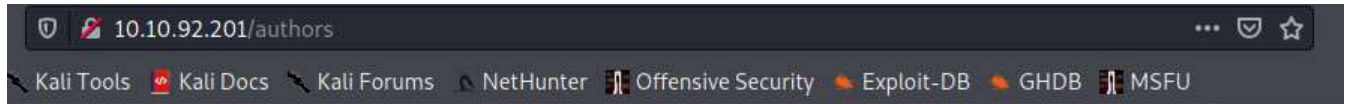
After this page I went to check the source code for this website to search for a flag or anything and there I got another flag in the comments of the html code.

Flag 2: THM{GIT_GOOD}



As I was getting these flags, I searched for each and every page and inspected those pages as well. So, after searching for the authors directory. I found another flag.

Flag : THM{LOL_WH0_D15}



Jane Doe

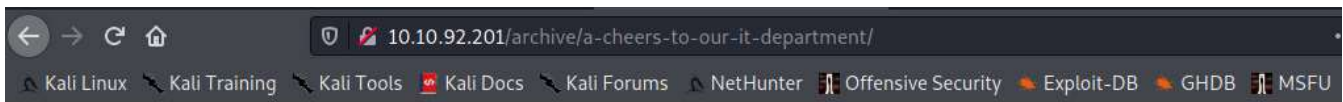


Author for Anthem blog

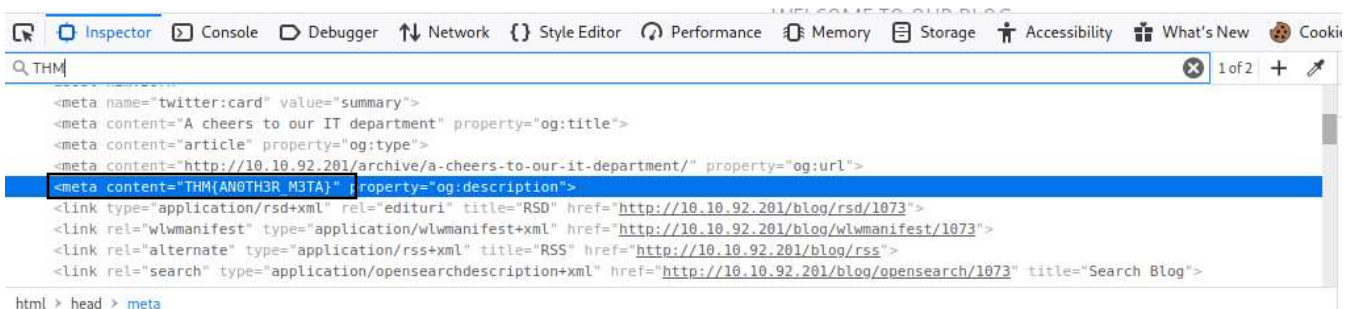
Website: [THM{LOL_WH0_D15}](#)

And lastly when inspecting the archive/a-cheer-to-our-it-department I found the final flag as well in the meta data.

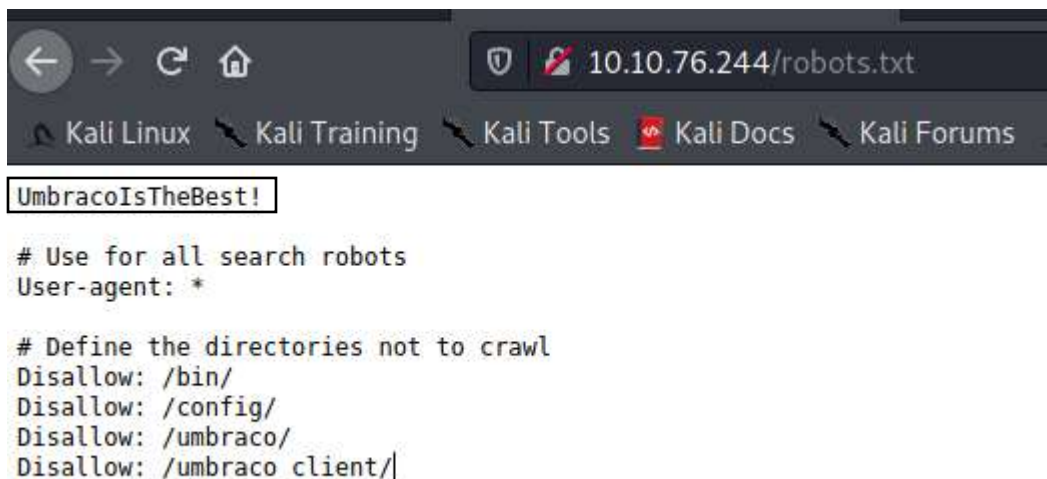
Flag 4: THM{AN0TH3R_M3TA}



Anthem.com

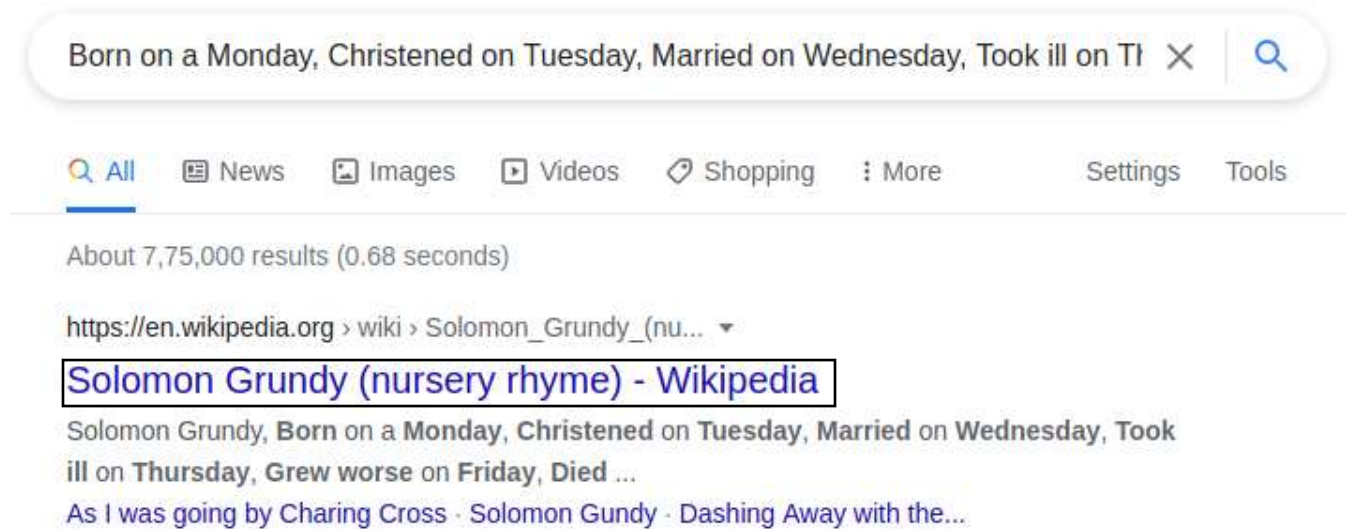


Now as we have got all the 4 flags now, we have to look for the foothold. As while searching for the flags, I have already checked all the webpages in that website so I thought of checking the robots.txt.



These directories suggests that umbraco CMS is running on this website and the first string could easily be a password for a user.

After searching somemore I found a username JD@anthem.com which is an author on one of the blogs I thought of trying JD as username with the string we found earlier as password but I did not work. So, I looked a little more and there was a poem written on another blog so I thought of checking that poem on google.



And yes we got an author.

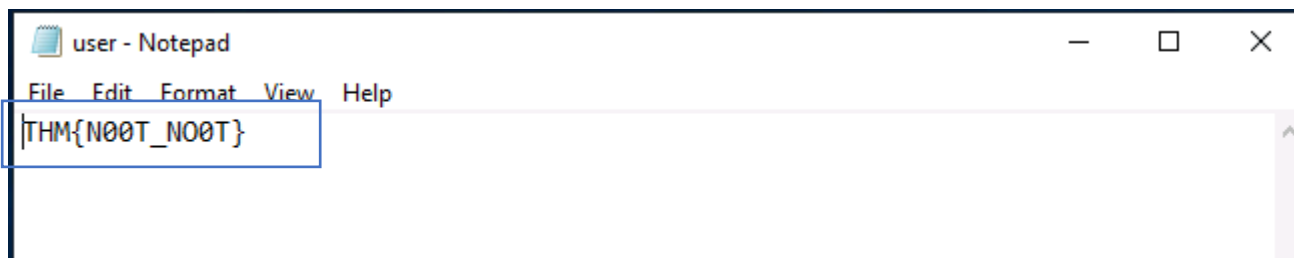
Exploits:

As earlier we got JD as username for john doe so, I thought of using SG for Solomon Grundy on the rdp and bingo we found our user and its password.

Command: `rdesktop 10.10.76.244 -u "SG" -p "UmbracoIsTheBest!" -d Anthem`

```
root@kali:~# rdesktop 10.10.76.244 -u "SG" -p "UmbracoIsTheBest!" -d Anthem
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

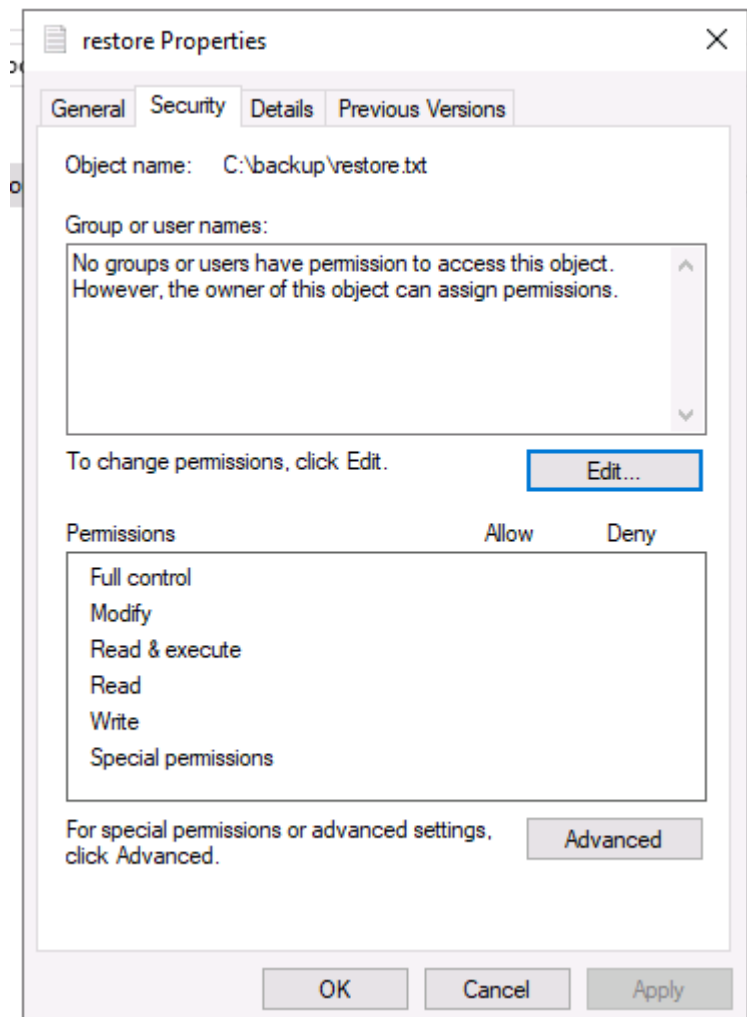
Now its time to go for user flag.



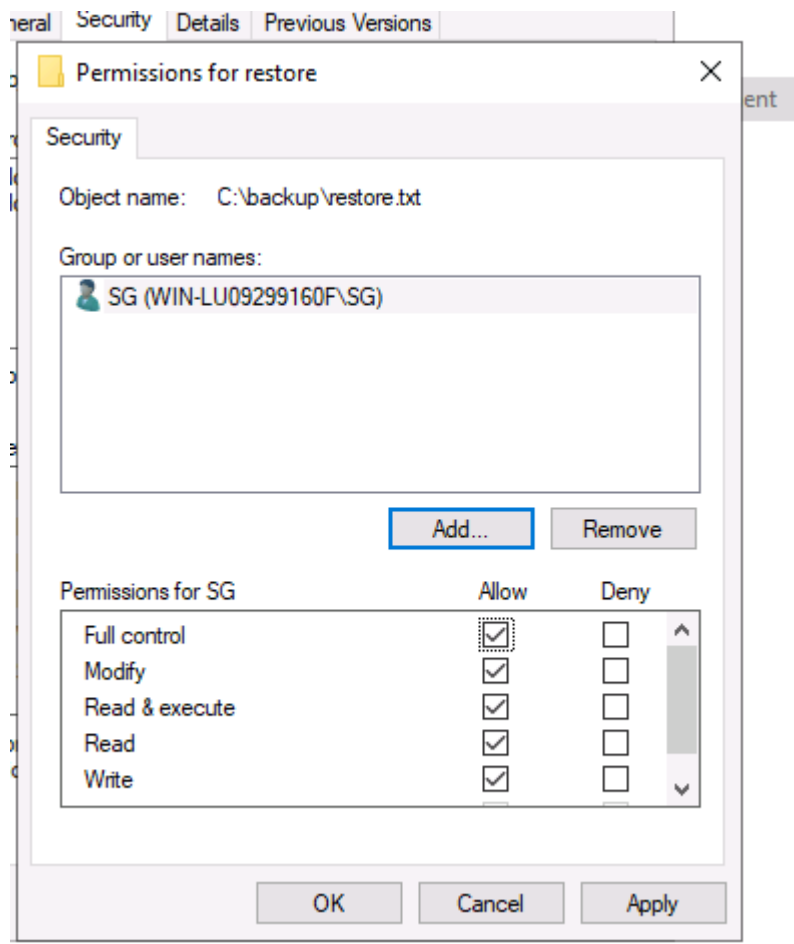
User Flag: **THM{N00T_NO0T}**

We successfully got the User flag and now let's go for the root flag.

I started to look for every file and folder including the hidden one on this machine and found a hidden directory "backup". Inside this directory there is file named restore. But wasn't able to open due to permissions.



But looking for these permissions I found that we can change these permissions as well.



So, I gave SG user full control for this file and was able to read.

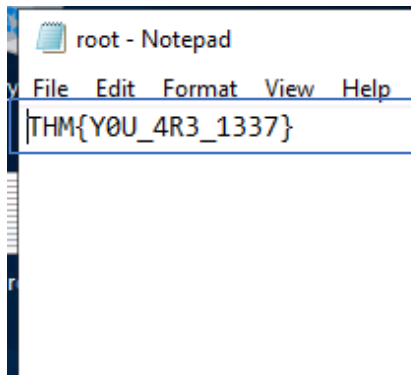


It looks like it's the password for admin user so let's try it.

Command: rdesktop 10.10.76.244 -u "administrator" -p "ChangeMeBaby1MoreTime" -d Anthem

```
root@kali:~# rdesktop 10.10.76.244 -u "administrator" -p "ChangeMeBaby1MoreTime" -d  
Anthem  
Autoselecting keyboard map 'en-us' from locale  
Core(warning): Certificate received from server is NOT trusted by this system, an e  
xception has been added by the user to trust this specific certificate.  
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?  
Core(warning): Certificate received from server is NOT trusted by this system, an e  
xception has been added by the user to trust this specific certificate.  
Connection established using SSL.  
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
```

And yes we got the admin account access. Now lets get the root flag.



Root Flag: **THM{Y0U_4R3_1337}**