Anthem

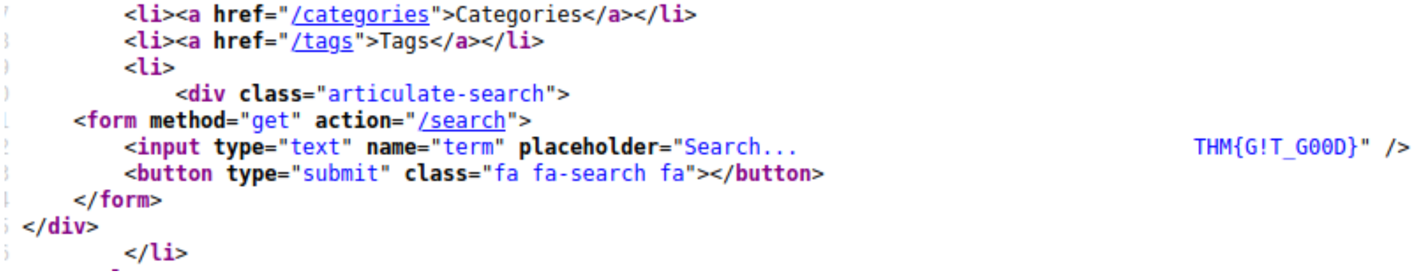
Working Theory

flag1
====
THM{L0L_WH0_US3S_M3T4}

found meta in source code
url: http://10.10.237.68/archive/we-are-hiring/

flag 2
====
THM{G!T_G00D}

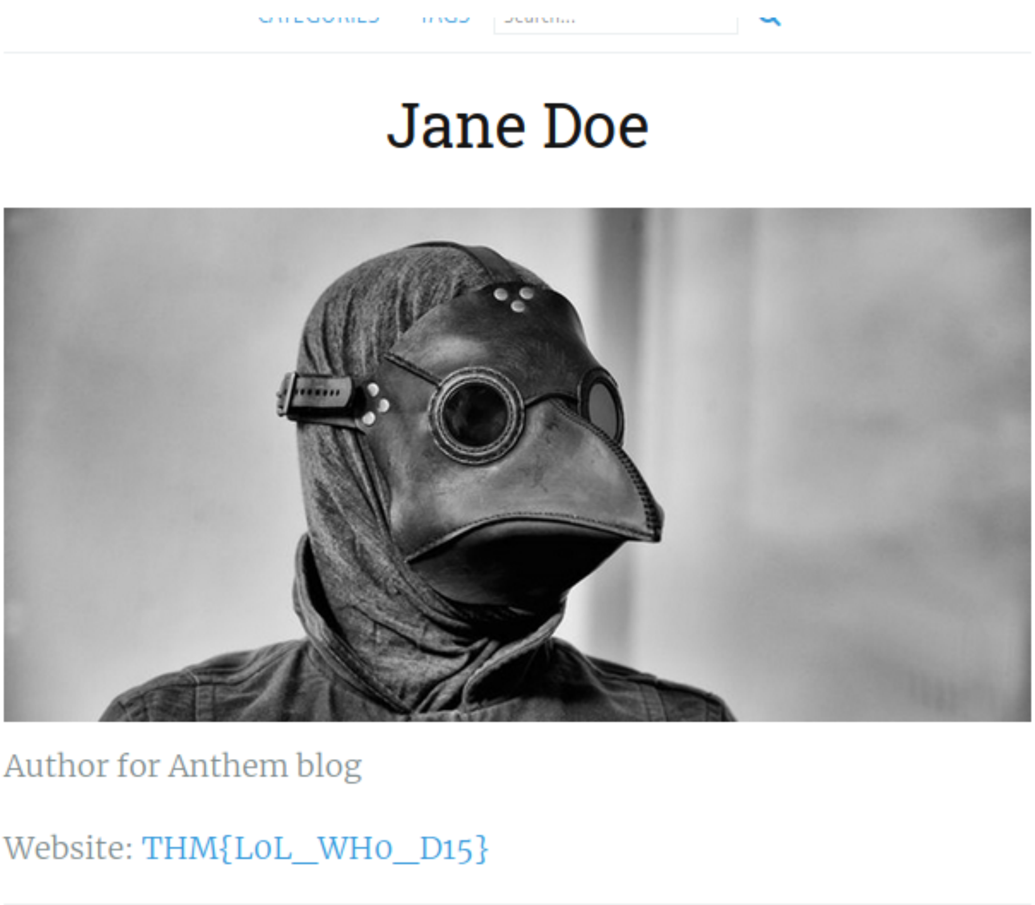
found in source code search form



```
        <li><a href="/categories">Categories</a></li>
        <li><a href="/tags">Tags</a></li>
        <li>
            <div class="articulate-search">
    <form method="get" action="/search">
        <input type="text" name="term" placeholder="Search...                                 THM{G!T_G00D}" />
        <button type="submit" class="fa fa-search fa"></button>
    </form>
</div>
        </li>
```

flag 3
====
THM{L0L_WH0_D15}

url: http://10.10.140.106/authors/jane-doe/



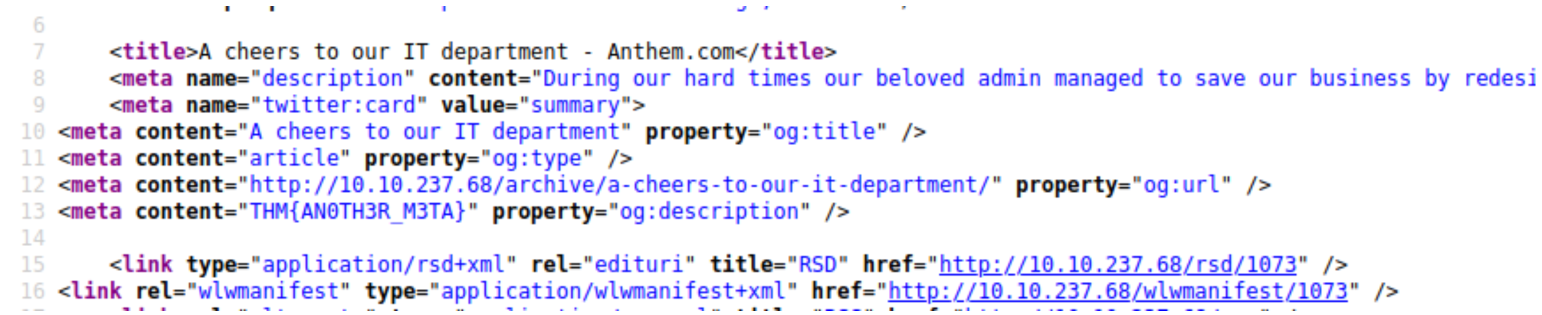
Jane Doe

Author for Anthem blog

Website: THM{L0L_WH0_D15}

flag 4
====
THM{AN0TH3R_M3TA}

found in another meta in source code
url: http://10.10.237.68/archive/a-cheers-to-our-it-department/



```
    <title>A cheers to our IT department - Anthem.com</title>
    <meta name="description" content="During our hard times our beloved admin managed to save our business by redesi
    <meta name="twitter:card" value="summary">
<meta content="A cheers to our IT department" property="og:title" />
<meta content="article" property="og:type" />
<meta content="http://10.10.237.68/archive/a-cheers-to-our-it-department/" property="og:url" />
<meta content="THM{AN0TH3R_M3TA}" property="og:description" />

    <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.237.68/rsd/1073" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.237.68/wlwmanifest/1073" />
```

enumeration

tools

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 00:55 +08
Nmap scan report for 10.10.140.106
Host is up (0.19s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
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: 2020-05-19T16:56:01+00:00
| ssl-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2020-04-04T22:56:38
|_Not valid after:  2020-10-04T22:56:38
|_ssl-date: 2020-05-19T16:56:46+00:00; +5s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4s, deviation: 0s, median: 4s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-19T16:56:06
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 96.06 seconds
```

services

http port 80

```
Potential Users
=========
Email
------
Jane Doe:  JD@anthem.com
Solomon Grundy: SG@anthem.com
```

robots.txt

```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

# Define the directories not to crawl
Disallow: /bin/
Disallow: /config/
Disallow: /umbraco/
Disallow: /umbraco_client/
```

post exploitaiton

privilege escalation

creds

```
Umbraco
======
SG@anthem.com:UmbracoIsTheBest!

RDP
===
SG:UmbracoIsTheBest!
```