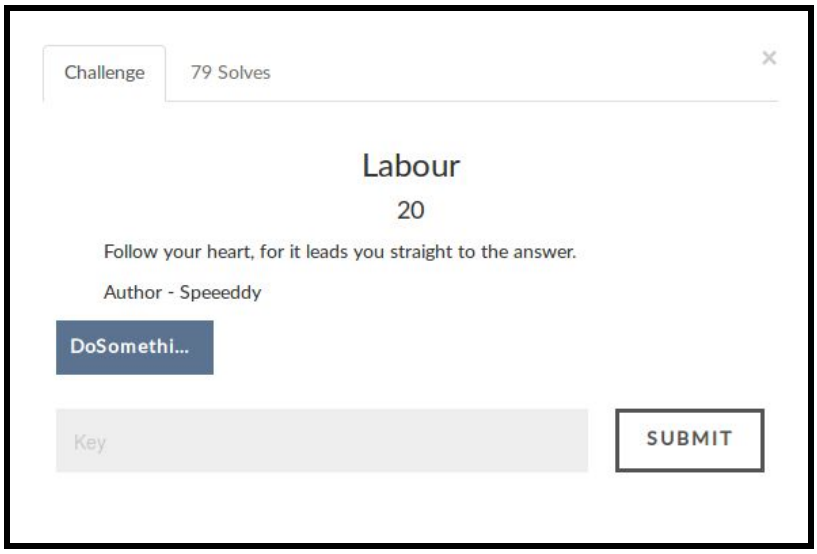
BITSCTF Misc Labour (20 points)

Author: Brandon Everhart

Date: Feb 2017

First off, I consider what type of challenge we are trying to solve. Whether the challenge is forensics, pwn, cryptography, reverse engineering, or web hacking, makes a big difference in how we should approach it. Here our challenge is in the miscellaneous category so…. no real help there. Therefore all we have to go on is the challenge itself. In this situation neither the name of the file, “DoSomethingWithThis" or the hint were helpful to me. My next step was to find out what kind of file I am working with. To find out information about a file in linux, such as file type, we can use the command ‘file *filename*’.




```
brandon@BlueBerry:~/ctf/bitsctf$ file DoSomethingWithThis
DoSomethingWithThis: XML 1.0 document, ASCII text, with CRLF, LF line terminators
```

The main thing I noticed here is that it is a XML file and also that it is made up of ascii text. With that description, the file should be very readable so let’s take a look at it. There are many ways to look at this file, I chose to use the command ‘strings *filename*’.

```
brandon@BlueBerry:~/ctf/bitsctf$ strings DoSomethingWithThis
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<gpx version="1.1" creator="BITSCTF" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
si:schemaLocation="http://www.topografix.com/GPX/1/1 http://www.topografix.com/GP
<!--Use appropriate brackets and underscores to separate words if you succeed-->
```

Above is a cropped screenshot from the ‘strings’ output. In this section we see an interesting note “<!--Use appropriate brackets and underscores to separate words if you succeed - -> this gives a hint to the flag format. The image on the right, while only a subset of the strings output, shows what else was interesting in the file. It is latitude and longitude coordinates! My first guess as to where the flag would be is that I would connect all the points on a map and find my flag drawn on the screen, like geospatial connect the dots. So I get all of the points listed and plot them on a map using an online tool.

```
23.71697, 89.45508
22.82885, 80.79786
39.88276, 58.81642
15.43674, 27.65039
12.69179, 17.50781
14.91081, 100.47656
45.9267, 2.21484
4.11852, 102.19922
34.85709, 65.84765
28.89086, 68.30859
39.20502, 31.92187
47.24344, 19.8457
25.30828, 29.84765
18.97119, -72.28521
-13.61609, 17.68359
33.84122, 102.23438
46.89624, 69.53907
```

Well, those points are not going to draw out the flag for me. After looking at the file more I noticed the points in the file were given names such as WP01, WP02… so I guessed that the ordering was significant. As I plotted the points one by one, this time I noticed how each one was in a different country and the countries seemed to have no relation. Could the points be random? Very unlikely that one could generate 17 random lat long coordinate pairs and have none of them land in an ocean, therefore I think the placement of the coordinates is significant. Considering the order and the placement of each point, I started writing down the first letter of the country that contains the point and what do you know the result was: **BITSCTFMAPTHEHACK.** This seemed to be the flag but it is not in a standard flag format. Hmm…. wait! We had a hint about what to do when we succeed given to us in the file! Using that hint I formated my list of letters to form the correct flag: **BITSCTF{MAP_THE_HACK}** !!