Lab 8 - Nbobw Cjmblijb (MB)

password: `swrdfish` saved as `t x s e g j t i` in the encrypted form in `passwdmemdump.txt`

Resources used:

- First I translated the code line by line using http://mipsconverter.com/instruction.html and https://www.eg.bucknell.edu/~csci320/mips_web/ . This gave me a pretty good idea of of whta the code looked like but the converters I was using, was getting confused between j and jal instructions and the memory address it was jumping or jal to.
- I commented out the first 9 lines of the translated code as I realized that these lines are the default lines that qtspim adds to each and every program.
- To solve this issue, I used https://blog.loadzero.com/blog/announcing-mipsdis/ to further disassemble the code by mapping the correct j or jal statements and their correct memory addresses at the correct lines.
- Next, I manually added labels once I had the correct memory addresses.
- After adding the labels, I realized that the first jr $ra is the routine where user input is taken and after the second jr $ra is where where the input password is matches with the actual password
- This then pointed me to the encryption algorithm which was the next immediate value of a given input. by incrementing its ascii value.
- now I went to the memory dump and isolated the password carrying zone in the following manner

```
h e G l o b a l F o u n d r
i e s M a i n f r a m e :
P l e a s e e n t e r
r o o t p a s s w o r d :
 I r e a d :

h o n e y p o t p a s s w o r
d s e c r e t a s d f g u
e s s f o o r o o t
t x s e g j t i    t e r p
s i c o r e a s t a s j w y
p a q j f r o d o b p l 3 3
t s 4 u c 3

t r y a g a i
 n   w e l c o m e !
```

- I knew that the password is held within lines that do not make sense thereby isolating lines 8-14
- I used the decryption algorithm i.e. manually subtracting 1 from ascii value of each character which gave me

```
h o n e y p o t p a s s w o r
d s e c r e t a s d f g u
e s s f o o r o o t
t x s e g j t i    t e r p
s i c o r e a s t a s j w y
p a q j f r o d o b p l 3 3
t s 4 u c 3

g n m d x o n s o z r r v p q
c r d b q d s z r c e f t
d r r e n n q n n s
s w r d f i s h    s d q o
r h b n q d z r s b r i v x
o z p i e q n c n a o k 2 2
s r 3 t b 2
```

After this I thought of 2 possible passwords, `s r 3 t b 2` because of its alphanumeric nature but I was disappointed by the fact that the password was not a strong password and it was what I feared `s w r d f i s h.`

POP CULTURE REFERENCE: Swordfish - 2001 movie starring Hugh Jackman, John Travolta. Involves some serious hacking.