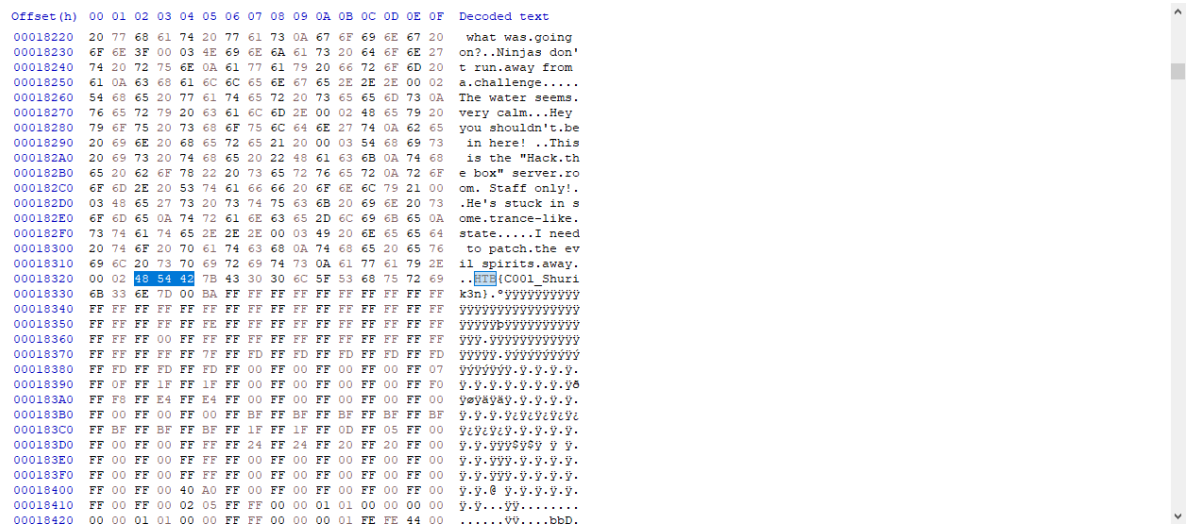
What is it?

We are provided with a GameBoy ROM that we are supposed to reverse engineer in order to obtain the flag. The game is a simple map where access to a building is locked off, and the goal is to patch the game to let you in to the restricted area.

How to solve it?

I opened the file in Ghidra expecting to patch a few things here and there. My first idea was to see if certain strings that are printed to the user during gameplay can be found in memory, and by finding them I could find the functionality that checks whether you can clip into the restricted area.

Funnily enough (as opposed to my expectations) the flag was stored in plaintext in the file itself, so by using a hex editor we could just extract it.



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00018220  20 77 68 61 74 20 77 61 73 0A 67 6F 69 6E 67 20   what was.going
00018230  6F 6E 3F 00 03 4E 69 6E 6A 61 73 20 64 6F 6E 27  on?..Ninjas don'
00018240  74 20 72 75 6E 0A 61 77 61 79 20 66 72 6F 6D 20  t run.away from
00018250  61 0A 63 68 61 6C 6C 65 6E 67 65 2E 2E 2E 00 02  a.challenge.....
00018260  54 68 65 20 77 61 74 65 72 20 73 65 65 6D 73 0A  The water seems.
00018270  76 65 72 79 20 63 61 6C 6D 2E 00 02 48 65 79 20  very calm...Hey
00018280  79 6F 75 20 73 68 6F 75 6C 64 6E 27 74 0A 62 65  you shouldn't.be
00018290  20 69 6E 20 68 65 72 65 21 20 00 03 54 68 69 73   in here! ..This
000182A0  20 69 73 20 74 68 65 20 22 48 61 63 6B 0A 74 68   is the "Hack.th
000182B0  65 20 62 6F 78 22 20 73 65 72 76 65 72 0A 72 6F  e box" server.ro
000182C0  6F 6D 2E 20 53 74 61 66 66 20 6F 6E 6C 79 21 00  om. Staff only!.
000182D0  03 48 65 27 73 20 73 74 75 63 6B 20 69 6E 20 73  .He's stuck in s
000182E0  6F 6D 65 0A 74 72 61 6E 63 65 2D 6C 69 6B 65 0A  ome.trance-like.
000182F0  73 74 61 74 65 2E 2E 2E 00 03 49 20 6E 65 65 64  state.....I need
00018300  20 74 6F 20 70 61 74 63 68 0A 74 68 65 20 65 76   to patch.the ev
00018310  69 6C 20 73 70 69 72 69 74 73 0A 61 77 61 79 2E  il spirits.away.
00018320  00 02 48 54 42 7B 43 30 30 6C 5F 53 68 75 72 69  ..HTB{C00l_Shuri
00018330  6B 33 6E 7D 00 BA FF FF FF FF FF FF FF FF FF FF  k3n}.ºÿÿÿÿÿÿÿÿÿÿ
00018340  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00018350  FF FF FF FF FF FE FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿþÿÿÿÿÿÿÿÿÿÿ
00018360  FF FF FF 00 FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿ.ÿÿÿÿÿÿÿÿÿÿÿÿ
00018370  FF FF FF FF FF 7F FF FD FF FD FF FD FF FD FF FD  ÿÿÿÿÿ.ÿýÿýÿýÿýÿý
00018380  FF FD FF FD FF FD FF 00 FF 00 FF 00 FF 00 FF 07  ÿýÿýÿýÿý.ÿ.ÿ.ÿ.ÿ.
00018390  FF 0F FF 1F FF 1F FF 00 FF 00 FF 00 FF 00 FF F0  ÿ.ÿ.ÿ.ÿ.ÿ.ÿ.ÿ.ÿð
000183A0  FF F8 FF E4 FF E4 FF 00 FF 00 FF 00 FF 00 FF 00  ÿøÿäÿäÿ.ÿ.ÿ.ÿ.ÿ.
000183B0  FF 00 FF 00 FF 00 FF BF FF BF FF BF FF BF FF BF  ÿ.ÿ.ÿ.ÿ¿ÿ¿ÿ¿ÿ¿ÿ¿
000183C0  FF BF FF BF FF BF FF 1F FF 1F FF 0D FF 05 FF 00  ÿ¿ÿ¿ÿ¿ÿ.ÿ.ÿ.ÿ.ÿ.
000183D0  FF 00 FF 00 FF FF FF 24 FF 24 FF 20 FF 20 FF 00  ÿ.ÿ.ÿÿÿ$ÿ$ÿ ÿ ÿ.
000183E0  FF 00 FF 00 FF FF FF 00 FF 00 FF 00 FF 00 FF 00  ÿ.ÿ.ÿÿÿ.ÿ.ÿ.ÿ.ÿ.
000183F0  FF 00 FF 00 FF FF FF 00 FF 00 FF 00 FF 00 FF 00  ÿ.ÿ.ÿÿÿ.ÿ.ÿ.ÿ.ÿ.
00018400  FF 00 FF 00 40 A0 FF 00 FF 00 FF 00 FF 00 FF 00  ÿ.ÿ.@ ÿ.ÿ.ÿ.ÿ.ÿ.
00018410  FF 00 FF 00 02 05 FF FF 00 00 01 01 00 00 00 00  ÿ.ÿ...ÿÿ........
00018420  00 00 01 01 00 00 FF FF 00 00 00 01 FE FE 44 00  ......ÿÿ....bbD.
```

FLAG: HTB{C00l_Shurik3n}