05/Dec/2021 - 06/Dec/2021

[redacted]

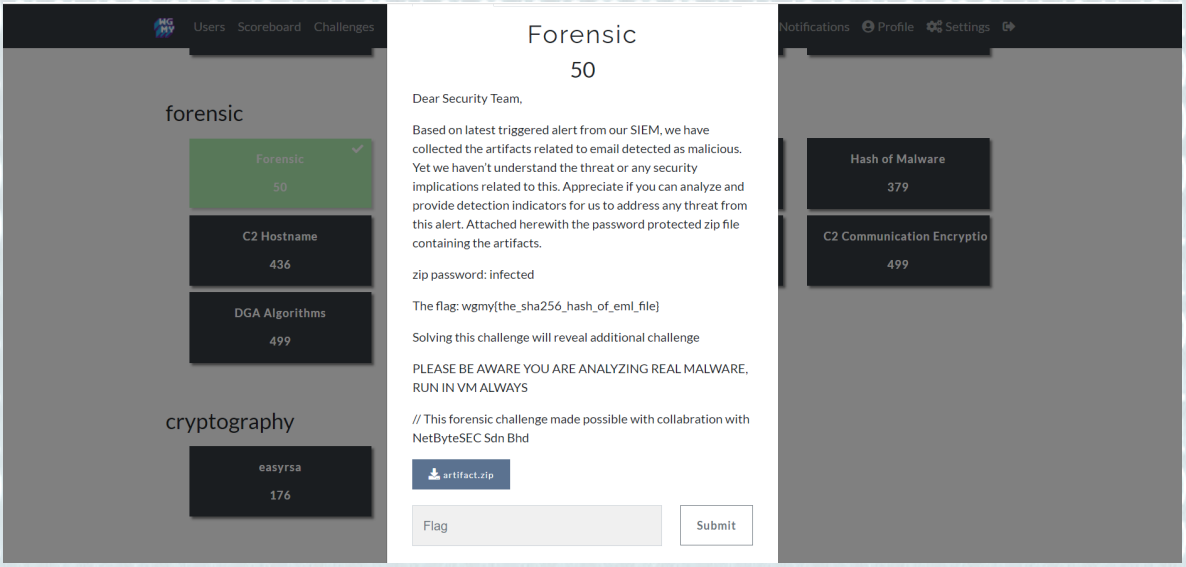
Here we present to you

HACKED

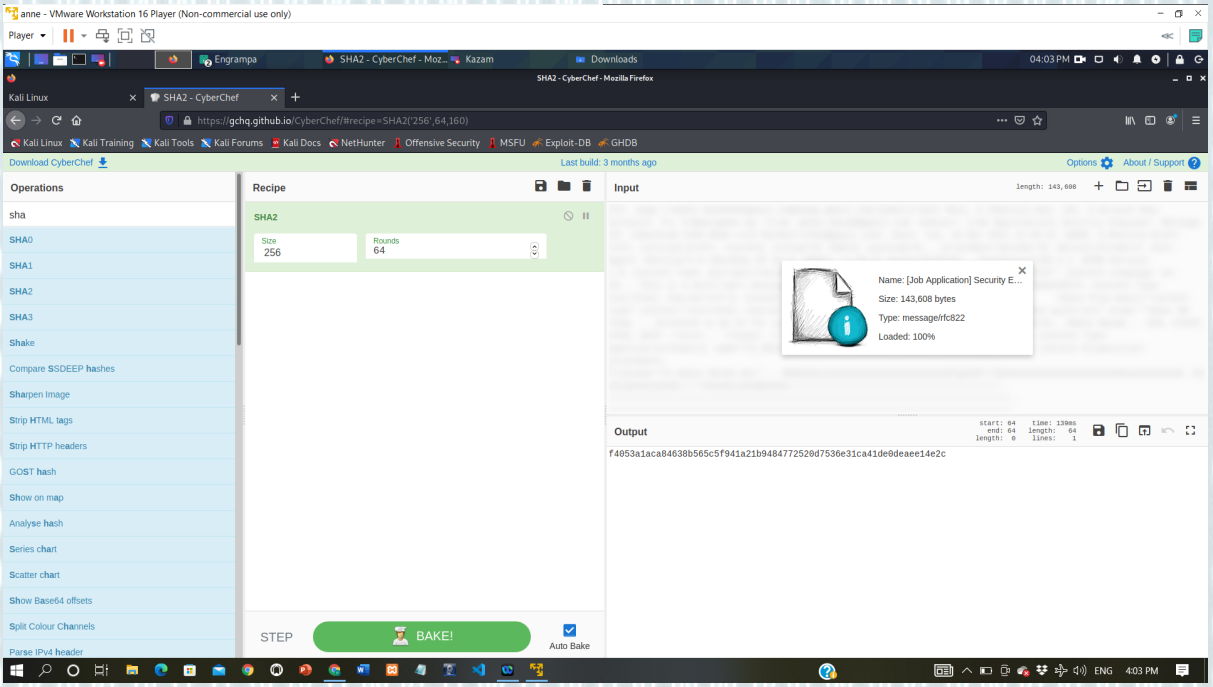
WRITE-UP

BY Dilettante

FORENSIC



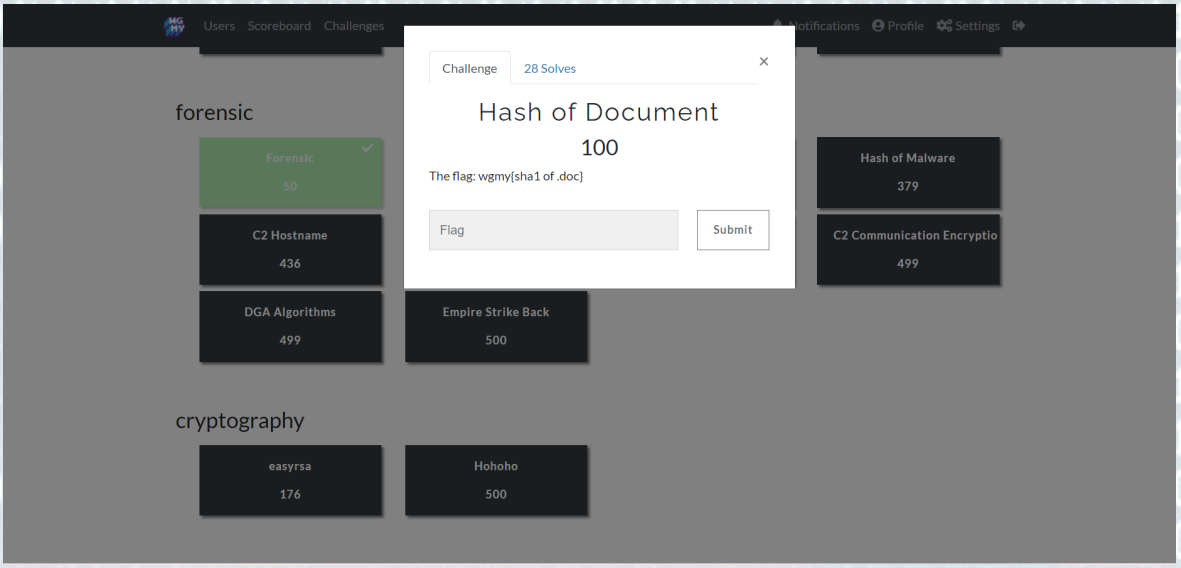
In this challenge we used “foremost” to extract the artifact.zip file, then we got the .eml file. We used cyberchef to get the hash value of the file.



Flag:

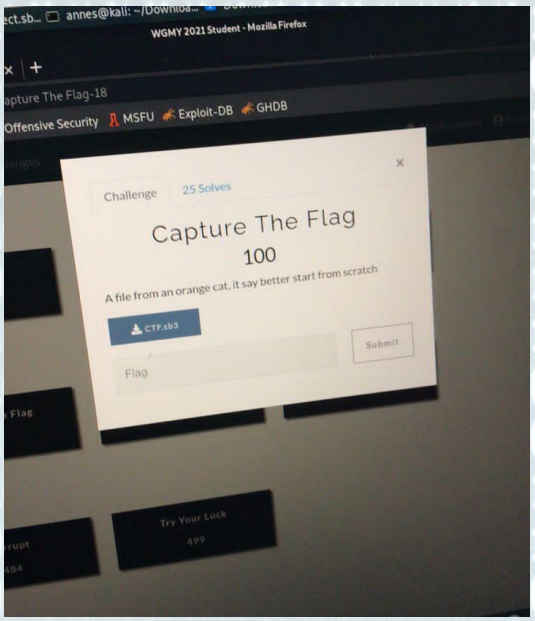
wgmy{f4053a1aca84638b565c5f941a21b9484772520d7536e31ca41de0deaee14e2c}

Hash of Document

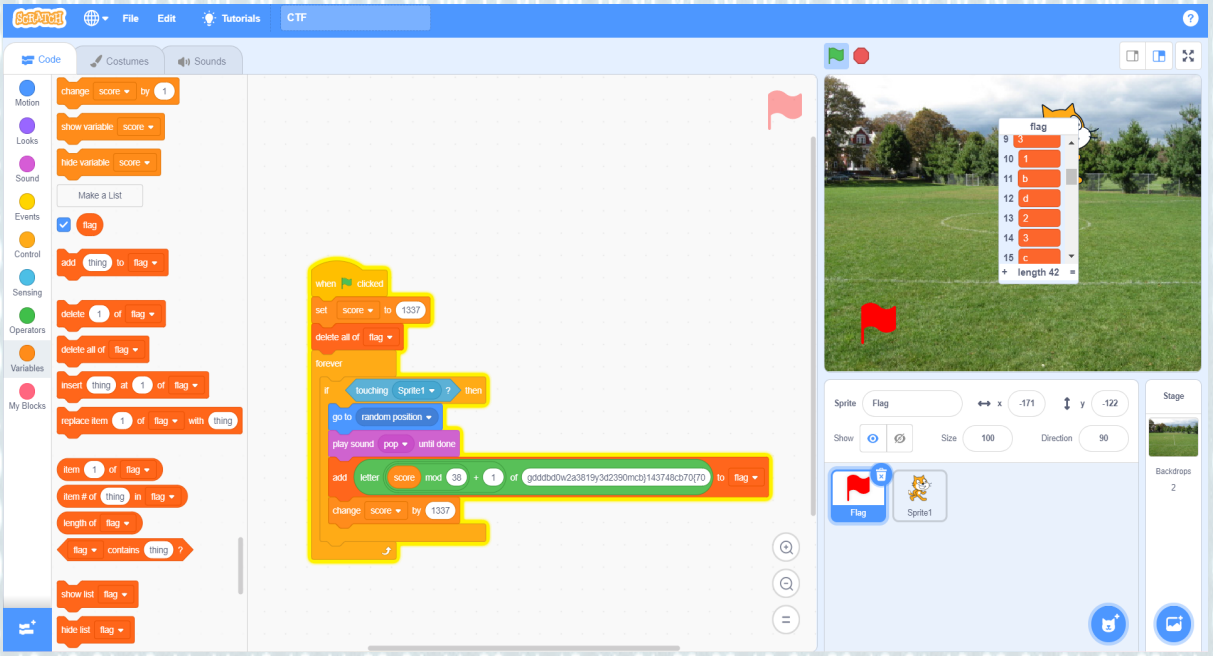


We opened and saved the doc file.
Then, we used cyberchef to hash the doc file using SHA-1 hash.
Flag: **wgmy{706301fc19042ffcab697775c30fe7dd9db4c5a6}**

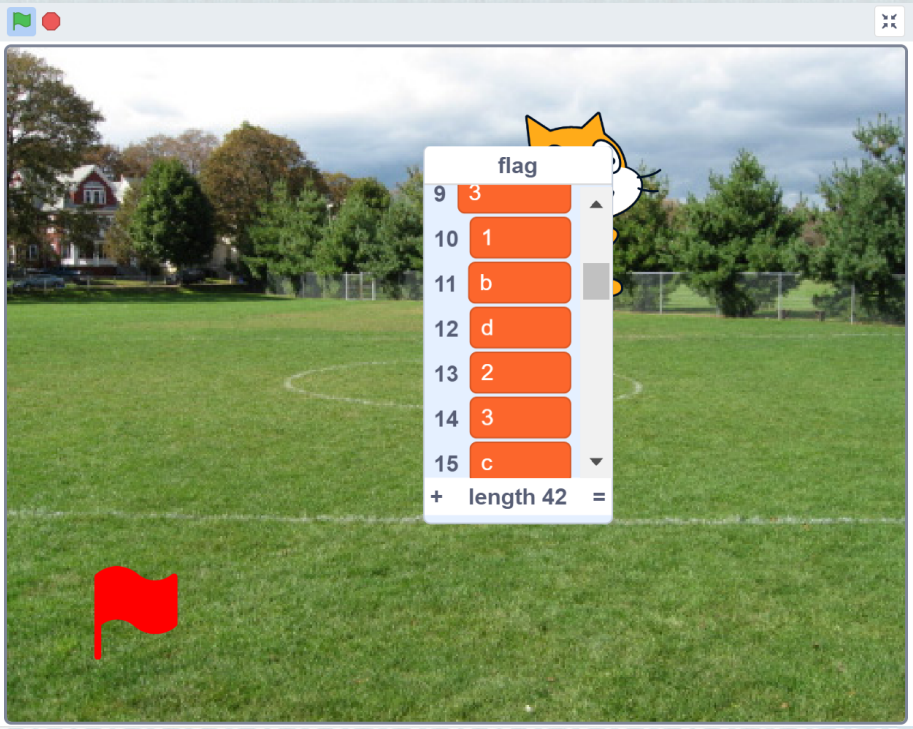
Capture The Flag



The file above is a Scratch file.



When we opened the file in Scratch, it displayed like this. In the Code tab, we clicked on the Variable and checked at ‘flag’. Then we could see a table named flag pops up.



When we moved the cat around to get the flag, the scores were entered in the flag table. There , we got the answer.

Flag: **wgmy{78b13db324cd79174adbd089030d023c}**