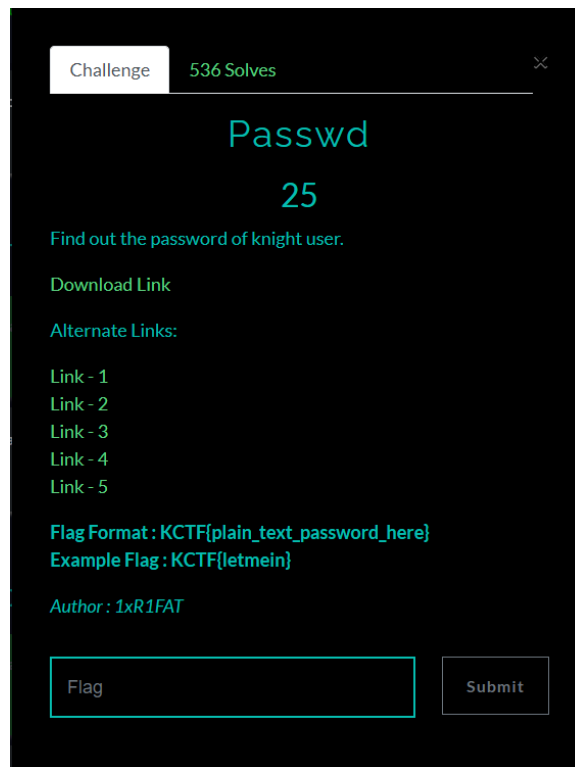


Passwd



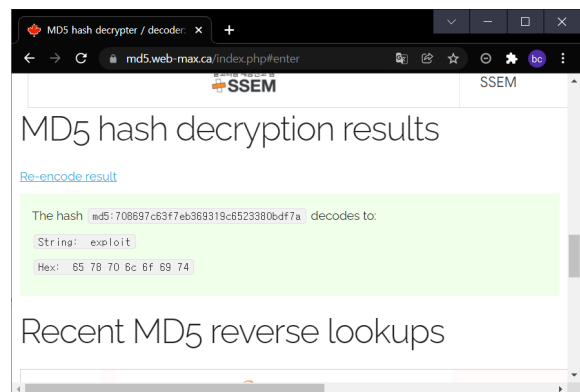
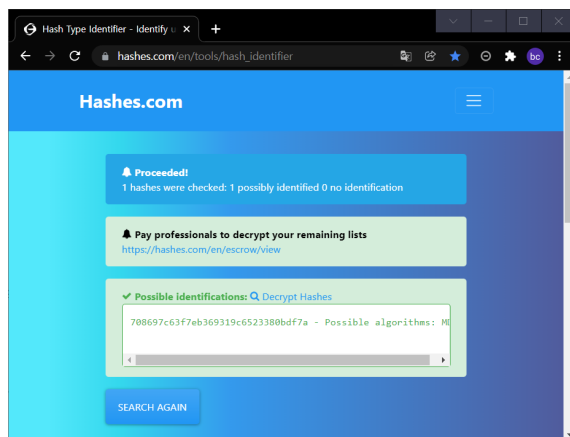
```
root:x:0:0:root:/root:/usr/bin/zsh
bin:x:1:1:/:/usr/bin/nologin
daemon:x:2:2:/:/usr/bin/nologin
mail:x:8:12:/:var/spool/mail:/usr/bin/nologin
ftp:x:14:11:/:srv/ftp:/usr/bin/nologin
http:x:33:33:/:srv/http:/usr/bin/nologin
nobody:x:65534:65534:Nobody:/usr/bin/nologin
dbus:x:81:81:System Message Bus:/usr/bin/nologin
systemd-journal-remote:x:988:988:systemd Journal Remote:/usr/bin/nologin
systemd-network:x:987:987:systemd Network Management:/usr/bin/nologin
systemd-oom:x:986:986:systemd Userspace OOM Killer:/usr/bin/nologin
systemd-resolve:x:984:984:systemd Resolver:/usr/bin/nologin
systemd-timesync:x:983:983:systemd Time Synchronization:/usr/bin/nologin
systemd-coredump:x:982:982:systemd Core Dumper:/usr/bin/nologin
uidd:x:68:68:/:/usr/bin/nologin
avahi:x:980:980:Avahi mDNS/DNS-SD daemon:/usr/bin/nologin
named:x:40:40:BIND DNS Server:/usr/bin/nologin
brltty:x:979:979:Braille Device Daemon:/var/lib/brltty:/usr/bin/nologin
colord:x:978:978:Color management daemon:/var/lib/colord:/usr/bin/nologin
cups:x:208:208:cups helper user:/usr/bin/nologin
dhcpd:x:977:977:dhcpd privilege separation:/usr/bin/nologin
dnsmasq:x:976:976:dnsmasq daemon:/usr/bin/nologin
git:x:975:975:git daemon user:/usr/bin/git-shell
mpd:x:45:45:/:var/lib/mpd:/usr/bin/nologin
nbd:x:974:974:Network Block Device:/var/empty:/usr/bin/nologin
nm-openvpn:x:973:973:NetworkManager OpenVPN:/usr/bin/nologin
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/usr/bin/nologin
openvpn:x:972:972:OpenVPN:/usr/bin/nologin
partimag:x:110:110:Partimage user:/usr/bin/nologin
polkitd:x:102:102:PolicyKit daemon:/usr/bin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/usr/bin/nologin
rtkit:x:133:133:RealtimeKit:/proc:/usr/bin/nologin
sddm:x:971:971:Simple Desktop Display Manager:/var/lib/sddm:/usr/bin/nologin
tss:x:970:970:tss user for tpm2:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/usr/bin/nologin
junior:x:1000:1000:Root@ROOT:/home/junior:/bin/zsh
knight:x:708697c63f7eb369319c6523380bdf7a:/home/junior:/bin/zsh
```

제공된 파일의 최하단을 보면

708697c63f7eb369319c6523380bdf7a

해시된 암호가 보인다.

이를 Hashes.com 사이트에 넣어보면 MD5로 암호화 되어있을 가능성을 얻을 수 있고,



복호화해보면 평문을 얻을 수 있다.

FLAG : `KCTF{exploit}`