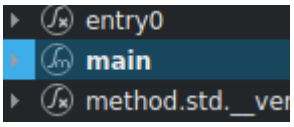
Application

On commence par installer cutter :

```
alaia@alaia-IdeaPad-Gaming-3-15ARH05:~/Téléchargements$ chmod +x Cutter*.AppImage; ./Cutter*.AppImage
```

Challenge 1

Dans cutter, on regarde la fonction main :



On l'affiche dans le décompileur :

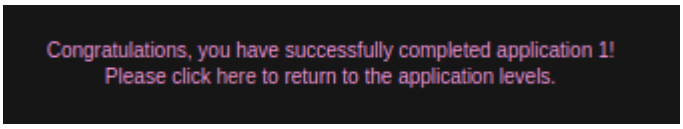
```
Décompileur (main)

// WARNING: Variable defined which should be unma

int32_t main(char **argv)
{
    undefined4 uVar1;
    undefined4 uVar2;
    int32_t iVar3;
    char *s2;
    int32_t var_2ch;
    int32_t var_28h;
    int32_t var_24h;
    int32_t var_18h;
    int32_t var_14h;
    char ***pppcStack_10;

    pppcStack_10 = &argv;
    method.std::basic_string_char__std::char_trai
    method.std::basic_string_char__std::char_trai
    method.std::string.operator__char_const(&var_
    method.std::basic_istream_char__std::char_tra
              (std::cin, &var_14h);
    uVar1 = method.std::string.c_str___const(&var
    uVar2 = method.std::string.c_str___const(&var
    iVar3 = strcmp(uVar2, uVar1);
    if (iVar3 == 0) {
        method.std::basic_ostream_char__std::char
                  (std::cout, "IVannaHackHTS");
        var_24h = 0;
```

On trouve une chaîne de caractères. Mot de passe : **IVannaHackHTS**



Challenge 2

On lance la commande strings sur l'exécutable du fichier pour voir si on trouve quelque chose d'intéressant :

```
alaia@alaia-IdeaPad-Gaming-3-15ARH05:~/Documents/Cours/M2/S3/CYBERAV/HackThisSite/Application$ strings app2win.exe
```

On découvre une requête HTTP GET :

```
Authenticate your software
Status: Connecting...
Status: Reading data...
Status: Validated
0Congratulations! The password to this level is '
Status: Serial invalid
?Sorry, you entered an incorrect serial number. Please re-enter.
Status: Sending request...
*GET /app2.php?pass=kB2F.b0-sJS,k HTTP/1.0
Host: appchall2.hts
```

Je ressens ta peine mon cher ami :

```
;-- str.Ihate_this_shit:
0x00539018          .string "Ihate this shit" ; len=16
```

On lance l'exécutable sur notre vieille machine Windows XP poussiéreuse et on intercepte le trafic avec Wireshark :

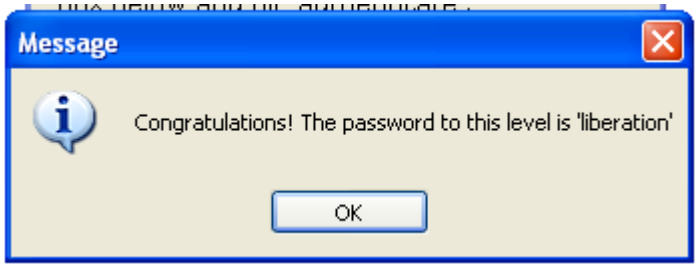
Destination	Protocc	Length	Info
137.74.187.101	HTTP	133	GET /app2.php?pass=kB2F.b0-sJS,k HTTP/1.0 Continuation
192.168.1.9	HTTP	1581	HTTP/1.1 200 OK (text/html)

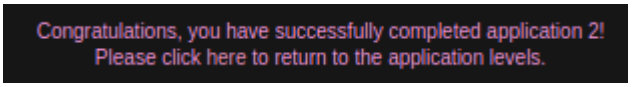
On regarde le contenu de la réponse :

```
Line-based text data: text/html
    63482-74819-88456-98378\r\n
    45910-18394-85113-51290\r\n
    10110-19101-59111-41563\r\n
    11424-74719-19578-99238\r\n
    25182-28381-85611-85258\r\n
    62351-12939-12481-58020\r\n
    63482-74819-88456-98378\r\n
    45910-18394-85113-51290\r\n
    18381-21931-98680-86523\r\n
    32910-21944-12391-51939\r\n
    12389-16781-72893-71892\r\n
    83478-91933-89823-98511\n
```

On teste un de ces codes dans l'application préhistorique :

Ça fonctionne, on obtient le mot de passe **liberation** :





Challenge 3

On regarde les strings dans le fichier :

```
alaia@alaia-IdeaPad-Gaming-3-15ARH05:~
e/Application$ strings app3win.exe
```

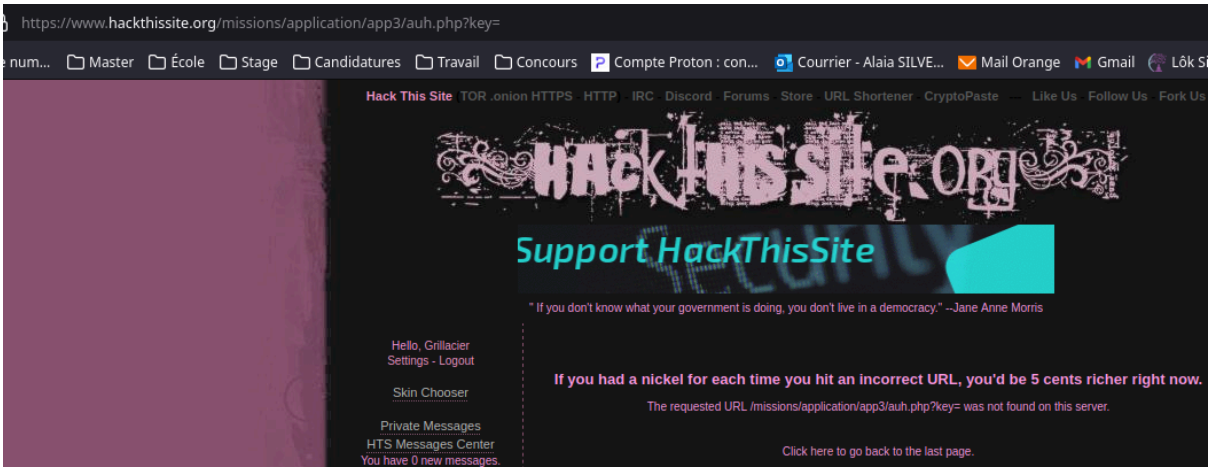
On a une requête HTTP GET :

```
Status: Validated
0Contratulations! The password to this level is '
false
Status: Serial invalid
?Sorry, you entered an incorrect serial number. Please re-enter.
Status: Sending request...
-GET /missions/application/app3/auth.php?key=
        HTTP/1.1
Host: hackthissite.org
```

Wireshark ne nous donne rien d'intéressant :

```
   HTTP      145 GET /missions/application/app3/auth.php?key=\000 HTTP/1.1
   HTTP       66 HTTP/1.0 400 Bad request  (text/html)
   HTTP      148 GET /missions/application/app3/auth.php?key=\000555 HTTP/1.1
   HTTP       66 HTTP/1.0 400 Bad request  (text/html)
```

hackthissite.org non plus :



pickle :

```
ecx = edi;
eax = FindResourceA (*(data.0052921c), 0x65, "PICKLE", edi, ecx, ebx);
```

On ouvre le fichier de l'exercice 3 avec Hex Workshop :

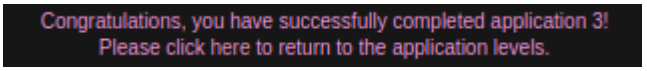
On cherche "Sorry" qui est le message renvoyé quand on essaye de rentrer un code dans l'application :

```
.....................true.........
..............Status: Validated....
......2...0.......0Contratulations!
 The password to this level is '...
.....................'.............
..........false.....................
...Status: Serial invalid.........A
...?.......?Sorry, you entered an i
```

On inverse true et false :

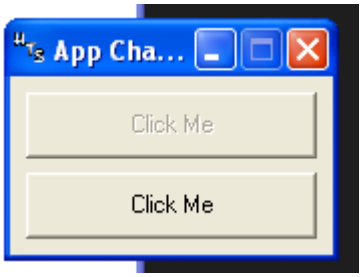
```
.....................false.........
..............Status: Validated....
......2...0.......0Contratulations!
 The password to this level is '...
.....................'.............
..........true......................
...Status: Serial invalid.........A
...?.......?Sorry, you entered an i
```

On écrit ce qu'on veut dans l'application et elle nous donne le mot de passe : **fireyourboss** :



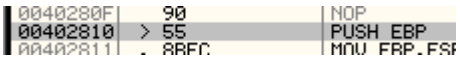
Challenge 4

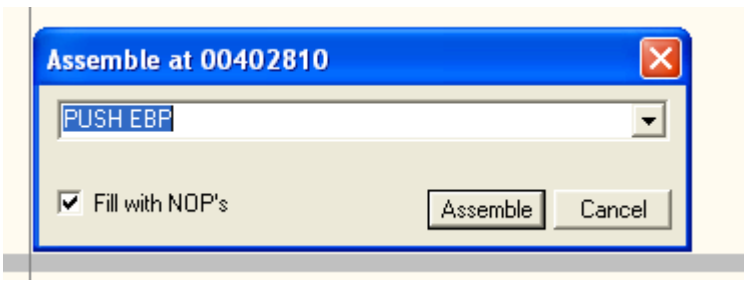
Le niveau 4 consiste en 2 boutons "Click Me", survoler un bouton le grise, le rendant impossible à cliquer :



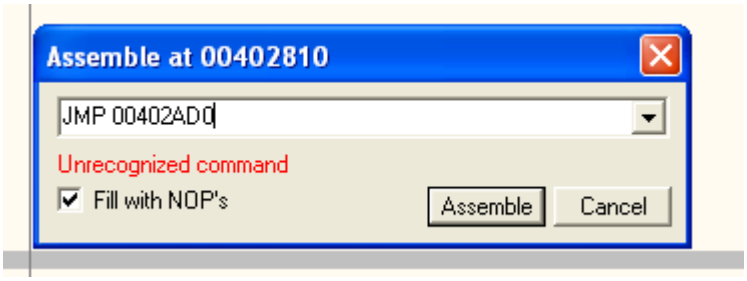
On ouvre l'application dans OllyDbg :

On va modifier l'action push de la ligne 00402810 :

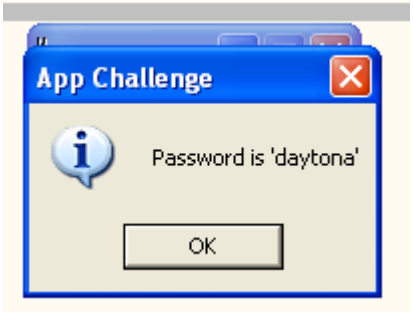




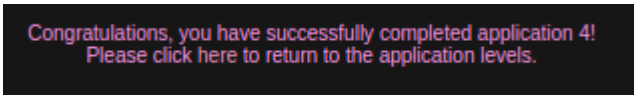
On la remplace par un jump vers la ligne 00402AD0 :



On sauvegarde et on relance l'application :



Mot de passe : **daytona**



Challenge 5

Mot de passe : **powertripping**

Challenge 6

Mot de passe : **magical**

Challenge 7

Mot de passe : **caged**

Challenge 8

Mot de passe : **2644-164-73427**

Challenge 9

Mot de passe : **SoundKing**

Challenge 10

Mot de passe : **HiddenSecrets**

Challenge 11

Mot de passe : **Search&Destroy**

Challenge 12

Mot de passe : **Creeper**

Challenge 13

Mot de passe : **537-314-137-616**

Challenge 14

Mot de passe : **ihatethereg**

Challenge 15

Mot de passe : **platform93/4**

Challenge 16

Mot de passe : **freedom**