

Application

Grillacier

No Avatar

Rank: Wiseman (4430 Points)

Status: Online

UserID: 2796338
Joined: 13/10/2023 11:55:17
Last Login: 09/11/2023 20:57:56
Last Active: 09/11/2023 21:42:28
Location: Not Entered
Website: <https://github.com/grillacier>
TimeZone: GMT + 1

E-mail: Hidden
IRC?: None
Discord: None
Warn Level: □□□□
Voice: Grillacier is **not muted**.

Basic: (1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11)

Realistic: (1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14) (15) (16)

Application: (1) (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14) (15) (16)

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 :

The image shows a sidebar from the Cutter decompiler. It contains three entries: 'entry0', 'main', and 'method.std.__ver'. The 'main' entry is highlighted with a blue background and a white cursor icon.

On l'affiche dans le décompilateur :

```

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**

Congratulations, you have successfully completed application 1!
Please click [here](#) to return to the application levels.

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
```

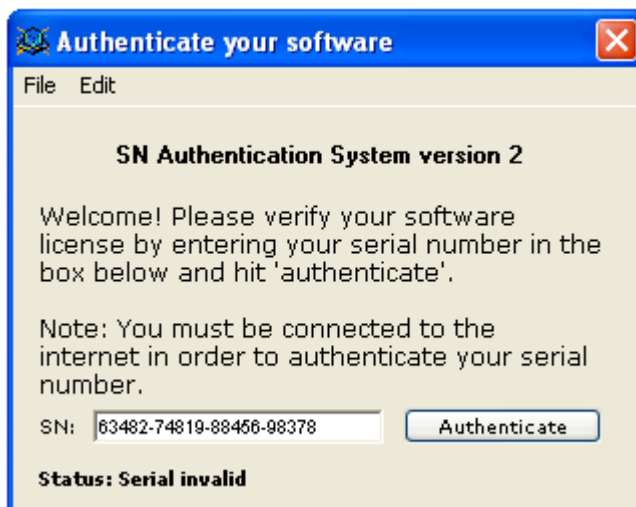
On lance l'exécutable sur notre vieille machine Windows XP poussiéreuse et on intercepte le trafic avec Wireshark :

Destination	Protocol	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)

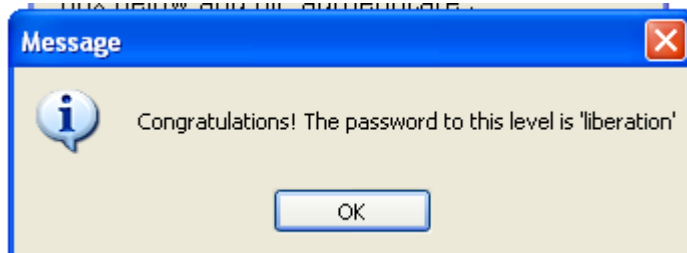
On regarde le contenu de la réponse :

```
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\r\n
```

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



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



Congratulations, you have successfully completed application 2!
Please click here to return to the application levels.

Challenge 3

On regarde les strings dans le fichier :

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

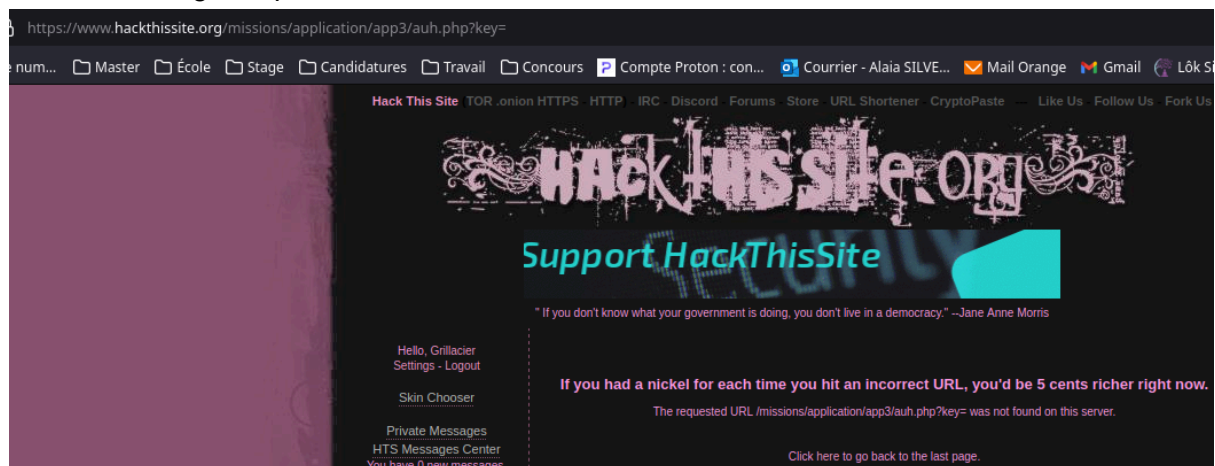
On a une requête HTTP GET :

```
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);  
hResInfo = eax;
```

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

```
Hex Workshop - [C:\Documents and Settings\Administrateur\Bureau\Application\app3win\app3win.exe]
```

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
nvalid serial number. Please re

```

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
nvalid serial number. Please re

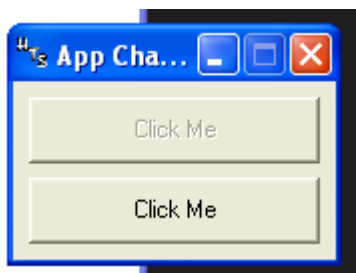
```

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

Congratulations, you have successfully completed application 3!
Please click here to return to the application levels.

Challenge 4

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

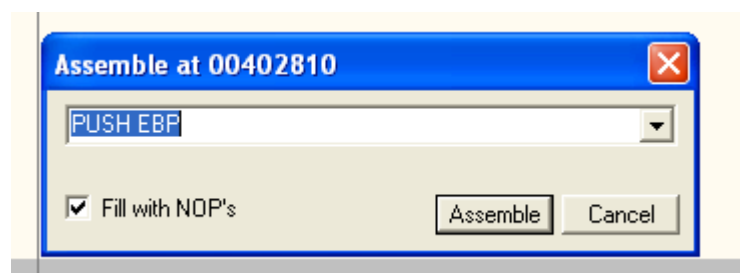


On ouvre l'application dans OllyDbg :

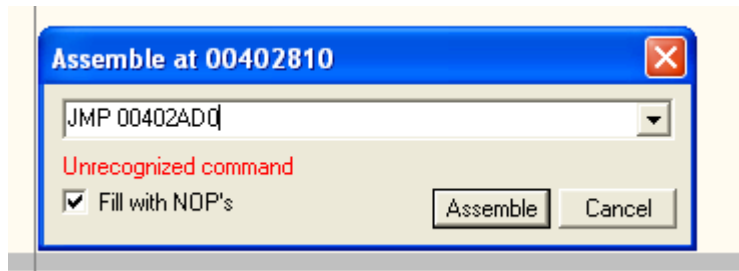
OllyDbg - app4win.exe - [CPU - main thread, module app4win]

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

0040280F	90	NOP
00402810	> 55	PUSH EBP
00402811	. 8BFC	MOV EBP,ESI



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

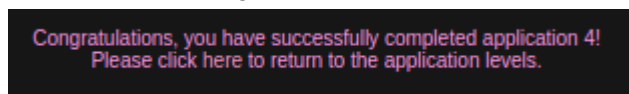


90	NOP
E9 BB020000	JMP app4win.00402AD0
90	NOP
68 16114000	PUSH <JMP.&MSUBUM60...
64:A1 00000000	MOV EAX,DWORD PTR FS:[0]

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**