# SECO TP 1

Nicolas Vadkerti

29 janvier 2020

https://github.com/SlaynPool/CR_SECO/

## 1 Attaques hors ligne

### 1.1 AP HTTP

On recupere le fichier .ino disponible sur moodle, on modifie les parametres de l'application comme ceci :

```
code$ head -n15 AP_HTTP.ino
#include <WiFi.h>
#include <WebServer.h>
#define CHANNEL 5
const char *ssid="NicolasV";
const char *pass="87654321";
const char *www_realm="Authentification ESP32";
const char *www_username="Toto";
const char *www_password="Totoro";
IPAddress ip(192,168,42,1);
IPAddress gateway(192,168,42,254);
IPAddress subnet(255,255,255,0);
WebServer server(80);

void wifiAPSetup() {
  Serial.println("wifiAPSetup...");
.................
```

Listing 1 – Modification du .ino

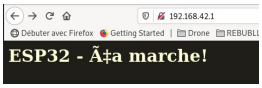


FIGURE 1 – Premier Page


FIGURE 2 – Connection


FIGURE 3 – Reussite

### 1.2 Fouille du .bin de mon voisin

Buddy ma fourni son binaire qui tourne sur son ESP. Grace à Hexdump nous avons converti le binnaire en caractère lisible :

```
code$ hexdump -C AP_HTTP-Buddy.ino.bin  --length 200
00000000  e9 06 02 2f b0 1e 08 40  ee 00 00 00 00 00 00 00  |.../...@........|
00000010  00 00 00 00 00 00 00 01  20 00 40 3f 7c 65 02 00  |........ .@?|e..|
00000020  c6 95 0d 40 42 95 0d 40  a0 95 0d 40 c6 95 0d 40  |...@B..@...@...@|
00000030  e9 95 0d 40 0c 96 0d 40  0c 96 0d 40 0c 96 0d 40  |...@...@...@...@|
00000040  0c 96 0d 40 66 95 0d 40  b2 95 0d 40 c6 95 0d 40  |...@f..@...@...@|
00000050  e9 95 0d 40 5d 9e 0d 40  da 9d 0d 40 38 9e 0d 40  |...@]..@...@8..@|
00000060  5d 9e 0d 40 81 9e 0d 40  a4 9e 0d 40 a4 9e 0d 40  |]..@...@...@...@|
00000070  a4 9e 0d 40 a4 9e 0d 40  fe 9d 0d 40 49 9e 0d 40  |...@...@...@I..@|
00000080  5d 9e 0d 40 81 9e 0d 40  00 00 00 00 00 00 00 80  |]..@...@........|
00000090  00 00 00 a0 00 00 00 c0  00 00 00 e0 14 14 14 07  |................|
000000a0  07 82 06 75 05 68 04 4e  03 34 02 27 01 1a 00 0d  |...u.h.N.4.'....|
000000b0  02 04 0b 16 03 00 00 00  01 00 00 00 00 00 00 00  |................|
000000c0  20 00 00 00 02 03 01 00                           | .......|
000000c8
code$ hexdump -C AP_HTTP-Buddy.ino.bin |grep SSID
00001110  3a 20 25 73 0d 0a 00 42  53 53 49 44 3a 20 25 73  |: %s...BSSID: %s|
```

Listing 2 – traduction

On voit que quand je cherche le mot SSID, il me repond que ce mots existe à la ligne 00001110. Nous regardons donc a cette ligne pour voir si il ya pas des mots de passes à proximité de la déclaration du SSID et :

```
00001110  3a 20 25 73 0d 0a 00 42  53 53 49 44 3a 20 25 73  |: %s...BSSID: %s|
00001120  0d 0a 00 57 45 42 20 73  65 72 76 65 72 20 73 65  |...WEB server se|
00001130  74 75 70 2e 2e 2e 00 2f  6c 6f 67 69 6e 00 57 45  |tup..../login.WE|
00001140  42 20 73 65 72 76 65 72  20 72 75 6e 6e 69 6e 67  |B server running|
00001150  2e 2e 2e 00 53 65 74 75  70 20 64 6f 6e 65 2e 00  |....Setup done..|
00001160  39 38 37 36 35 34 33 32  00 62 75 64 64 79 00 41  |98765432.buddy.A|
00001170  75 74 68 65 6e 74 69 66  69 63 61 74 69 6f 6e 20  |uthentification |
00001180  45 53 50 33 32 00 32 33  34 35 36 37 38 39 00 63  |ESP32.23456789.c|
00001190  65 73 74 71 75 6f 69 6c  65 63 6f 64 65 00 25 30  |estquoilecode.%0|
000011a0  32 58 3a 25 30 32 58 3a  25 30 32 58 3a 25 30 32  |2X:%02X:%02X:%02|
000011b0  58 3a 25 30 32 58 3a 25  30 32 58 00 00 00 00 00  |X:%02X:%02X.....|
000011c0  00 00 00 00 7c 1b 0d 40  98 1b 0d 40 0c 45 14 40  |....|..@...@.E.@|
```

Listing 3 – On a trouvé !

On comprend rapidement que le premier mots de passes que l'on semble voir est le mots de passes de l'authentification WEB, notament car "buddy" n'est pas le SSID que je vois depuis ma carte Wifi mais plutot "cestquoilecode" Donc on déduis grâce au binaire que on pourra passer l'authentification Web grâce au couple User/PWD : buddy/98765432
Et le Mot de passe du reseau Wifi : 23456789