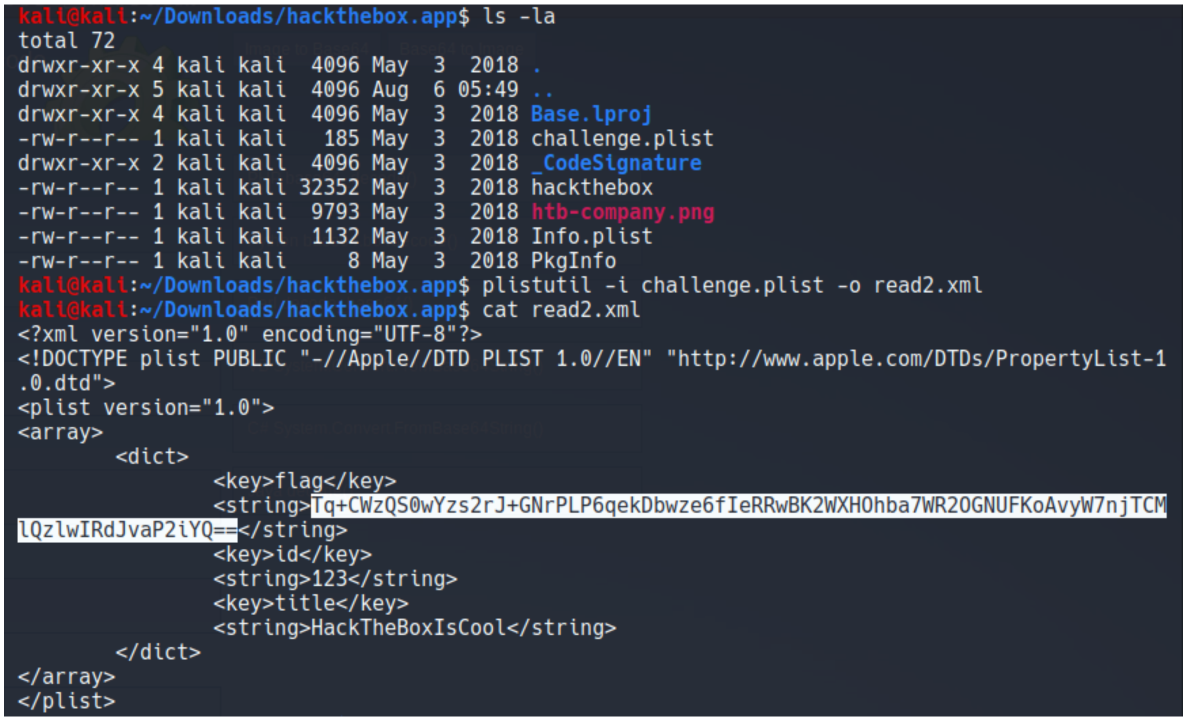
Cryptohorrific

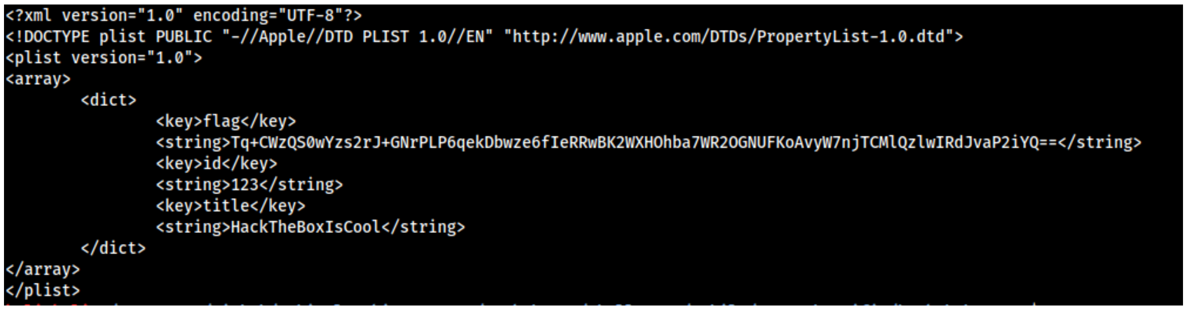
Reported by kaiUb (https://github.com/kaiUb777)

1. ***Change extension file (challenge) .plist to .xml with plistutils and see the content. Query: plistutils -i challenge.plist -o challenge.xml***



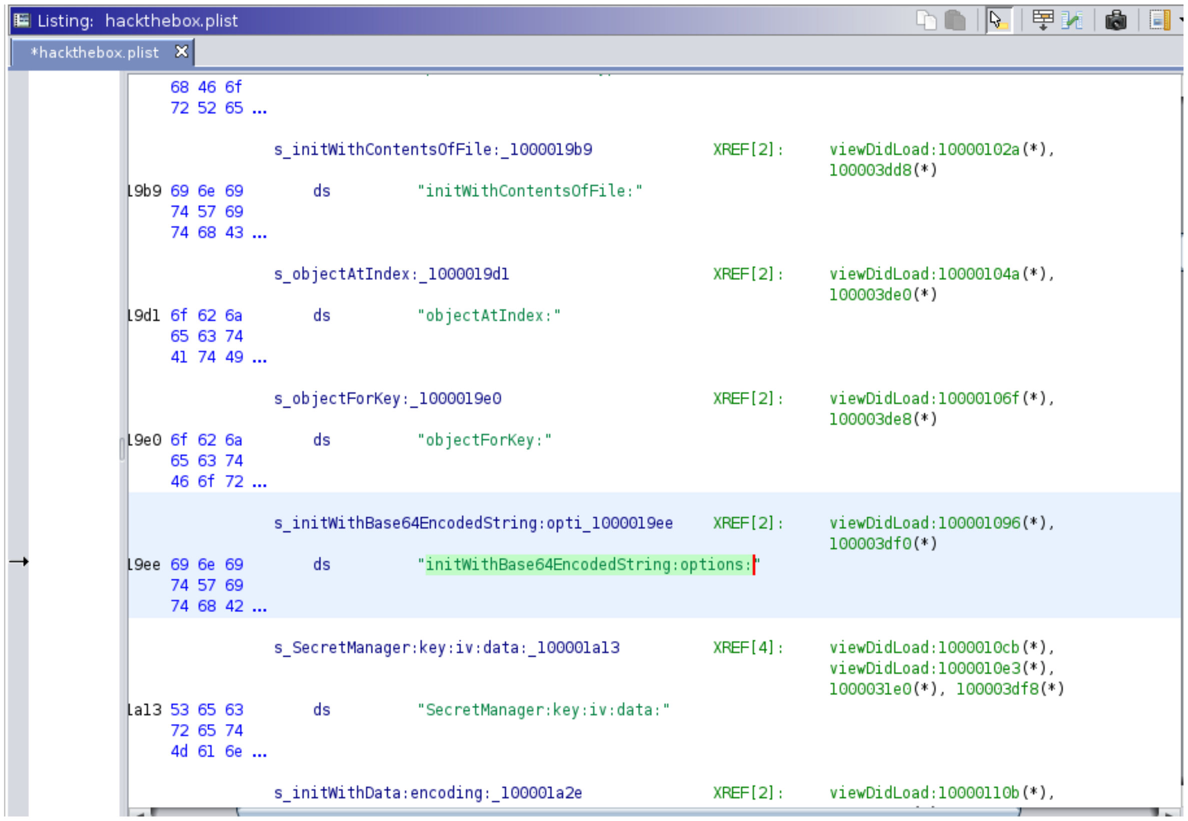
```
kali@kali:~/Downloads/hackthebox.app$ ls -la
total 72
drwxr-xr-x 4 kali kali  4096 May  3  2018 .
drwxr-xr-x 5 kali kali  4096 Aug  6 05:49 ..
drwxr-xr-x 4 kali kali  4096 May  3  2018 Base.lproj
-rw-r--r-- 1 kali kali   185 May  3  2018 challenge.plist
drwxr-xr-x 2 kali kali  4096 May  3  2018 _CodeSignature
-rw-r--r-- 1 kali kali 32352 May  3  2018 hackthebox
-rw-r--r-- 1 kali kali  9793 May  3  2018 htb-company.png
-rw-r--r-- 1 kali kali  1132 May  3  2018 Info.plist
-rw-r--r-- 1 kali kali     8 May  3  2018 PkgInfo
kali@kali:~/Downloads/hackthebox.app$ plistutil -i challenge.plist -o read2.xml
kali@kali:~/Downloads/hackthebox.app$ cat read2.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1
.0.dtd">
<plist version="1.0">
<array>
        <dict>
                <key>flag</key>
                <string>Tq+CWzQS0wYzs2rJ+GNrPLP6qekDbwze6fIeRRwBK2WXHOhba7WR2OGNUFKoAvyW7njTCM
lQzlwIRdJvaP2iYQ==</string>
                <key>id</key>
                <string>123</string>
                <key>title</key>
                <string>HackTheBoxIsCool</string>
        </dict>
</array>
</plist>
```

2. ***Analyze the content file (We got the flag encoded) and some possible GCM tags***



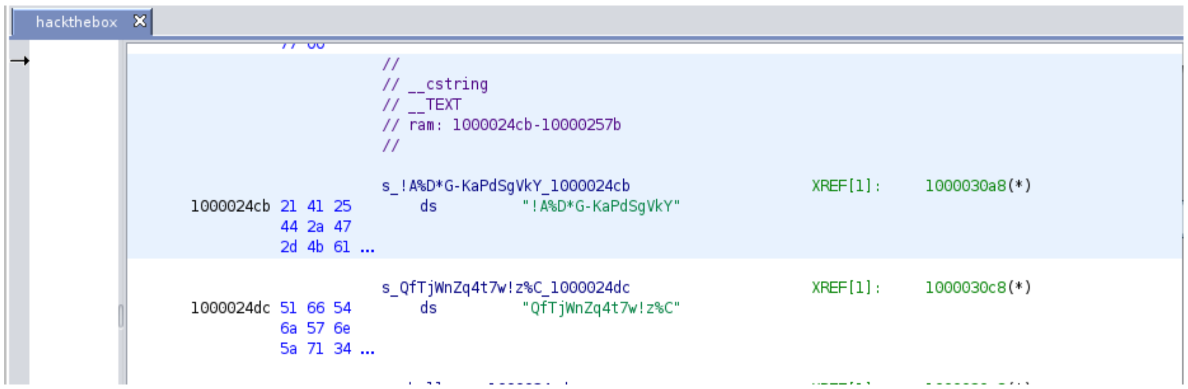
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
        <dict>
                <key>flag</key>
                <string>Tq+CWzQS0wYzs2rJ+GNrPLP6qekDbwze6fIeRRwBK2WXHOhba7WR2OGNUFKoAvyW7njTCMlQzlwIRdJvaP2iYQ==</string>
                <key>id</key>
                <string>123</string>
                <key>title</key>
                <string>HackTheBoxIsCool</string>
        </dict>
</array>
</plist>
```

3. ***After analyzing the decompiled code application (hackthebox) we see an interested function (initWithBase64EncodedString)! This is meaning our flag is encoded in base64***



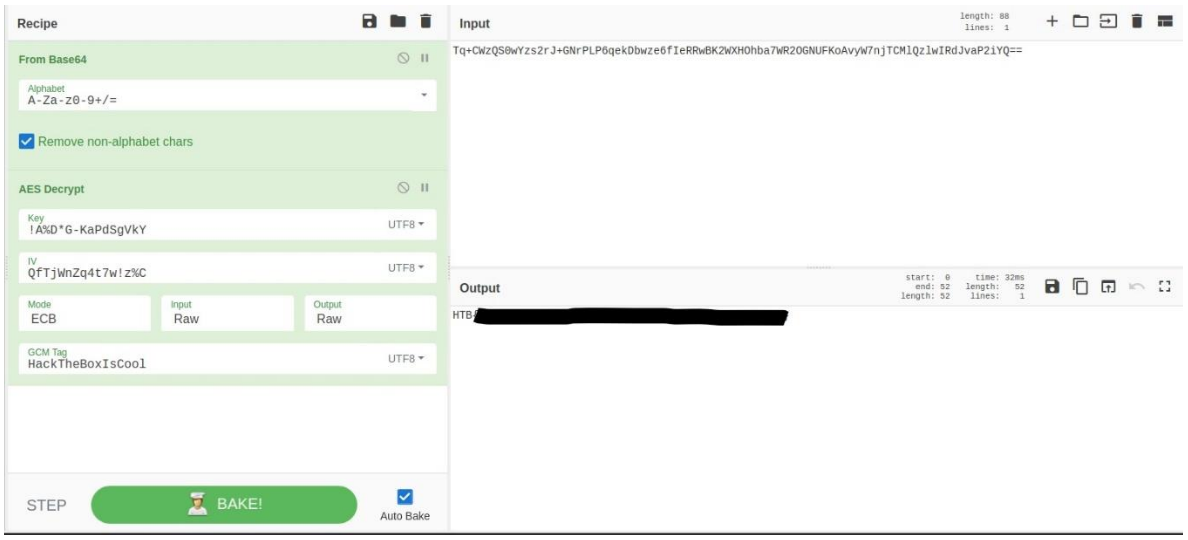
```
     68 46 6f
     72 52 65 ...

                    s_initWithContentsOfFile:_1000019b9          XREF[2]:     viewDidLoad:10000102a(*),
                                                                              100003dd8(*)
19b9 69 6e 69       ds          "initWithContentsOfFile:"
     74 57 69
     74 68 43 ...

                    s_objectAtIndex:_1000019d1                   XREF[2]:     viewDidLoad:10000104a(*),
                                                                              100003de0(*)
19d1 6f 62 6a       ds          "objectAtIndex:"
     65 63 74
     41 74 49 ...

                    s_objectForKey:_1000019e0                    XREF[2]:     viewDidLoad:10000106f(*),
                                                                              100003de8(*)
19e0 6f 62 6a       ds          "objectForKey:"
     65 63 74
     46 6f 72 ...

                    s_initWithBase64EncodedString:opti_1000019ee XREF[2]:     viewDidLoad:100001096(*),
                                                                              100003df0(*)
19ee 69 6e 69       ds          "initWithBase64EncodedString:options:"
     74 57 69
     74 68 42 ...

                    s_SecretManager:key:iv:data:_100001a13       XREF[4]:     viewDidLoad:1000010cb(*),
                                                                              viewDidLoad:1000010e3(*),
                                                                              1000031e0(*), 100003df8(*)
1a13 53 65 63       ds          "SecretManager:key:iv:data:"
     72 65 74
     4d 61 6e ...

                    s_initWithData:encoding:_100001a2e           XREF[2]:     viewDidLoad:10000110b(*),
```

4. ***If you search more in the decompiled code we see two interested strings, probably one is the key and iv in aes encryption***



```
                         //
                         // __cstring
                         // __TEXT
                         // ram: 1000024cb-10000257b
                         //

                         s_!A%D*G-KaPdSgVkY_1000024cb                 XREF[1]:     1000030a8(*)
        1000024cb 21 41 25     ds          "!A%D*G-KaPdSgVkY"
                  44 2a 47
                  2d 4b 61 ...

                         s_QfTjWnZq4t7w!z%C_1000024dc                 XREF[1]:     1000030c8(*)
        1000024dc 51 66 54     ds          "QfTjWnZq4t7w!z%C"
                  6a 57 6e
                  5a 71 34 ...
```

5. ***Go to cyberchef, decode and decrypt the flag!***



From Base64
Alphabet: A-Za-z0-9+/=
✓ Remove non-alphabet chars

AES Decrypt
Key: !A%D*G-KaPdSgVkY (UTF8)
IV: QfTjWnZq4t7w!z%C (UTF8)
Mode: ECB
Input: Raw
Output: Raw
GCM Tag: HackTheBoxIsCool (UTF8)

Input (length: 88, lines: 1)

```
Tq+CWzQS0wYzs2rJ+GNrPLP6qekDbwze6fIeRRwBK2WXHOhba7WR2OGNUFKoAvyW7njTCMlQzlwIRdJvaP2iYQ==
```

Output (start: 0, end: 52, length: 52; time: 32ms, length: 52, lines: 1)

```
HTB{[redacted]
```