Mobile Challenges

Cryptohorrific

IhSanSencan
www.ihsan.net
https://www.hackthebox.eu/profile/100992

🏆 [40 Points] Cryptohorrific [by bsecure] [832 solvers] 263 👍 22 👎 Difficulty:

🔥 First Blood: yuntao

Secure coding is the keystone of the application security!

⬇ Download   Zip Password: hackthebox sha256: c2b5854f2bf3e22978e2a40cf04f92e130db97c744334755ee050c2b2066ffb3

✔ Complete

---

root@ihsan: /Cryptohorrific/hackthebox.app

Dosya   Düzenle   Görünüm   Ara   Uçbirim   Yardım

```
root@ihsan:/Cryptohorrific/hackthebox.app# ls
Base.lproj        _CodeSignature    htb-company.png   PkgInfo
challenge.plist   hackthebox        Info.plist
root@ihsan:/Cryptohorrific/hackthebox.app# strings challenge.plist
bplist00
TflagRidUtitle_
XTq+CWzQS0wYzs2rJ+GNrPLP6qekDbwze6fIeRRwBK2WXHOhba7WR2OGNUFKoAvyW7njTCMlQzlwIRdJ
vaP2iYQ==S123_
HackTheBoxIsCool
root@ihsan:/Cryptohorrific/hackthebox.app#
```

Also for windows https://www.icopybot.com/plist-editor.htm

```
__objc_methname:00000001000024B8                                           ; __objc_const:
__objc_methname:00000001000024C3 aWindow_0         db '_window',0          ; DATA XREF: __
__objc_methname:00000001000024C3 __objc_methname ends
__objc_methname:00000001000024C3
__cstring:00000001000024CB ; ========================================================
__cstring:00000001000024CB
__cstring:00000001000024CB ; Segment type: Pure data
__cstring:00000001000024CB __cstring         segment byte public 'DATA' use64
__cstring:00000001000024CB                   assume cs:__cstring
__cstring:00000001000024CB                   ;org 1000024CBh
__cstring:00000001000024CB aADGKapdsgvky     db '!A%D*G-KaPdSgVkY',0 ; DATA XREF: __cfstri
__cstring:00000001000024DC aQftjwnzq4t7wZC   db 'QfTjWnZq4t7w!z%C',0 ; DATA XREF: __cfstri
__cstring:00000001000024ED aChallenge        db 'challenge',0        ; DATA XREF: __cfstri
__cstring:00000001000024F7 aPlist            db 'plist',0            ; DATA XREF: __cfstri
__cstring:00000001000024FD aFlag             db 'flag',0             ; DATA XREF: __cfstri
__cstring:0000000100002502 aHash_0           db 'hash',0             ; DATA XREF: __objc_c
__cstring:0000000100002502                                          ; __objc_const:000000
__cstring:0000000100002507 aTqR              db 'TQ,R',0             ; DATA XREF: __objc_c
__cstring:0000000100002507                                          ; __objc_const:000000
__cstring:000000010000250C aSuperclass_0     db 'superclass',0       ; DATA XREF: __objc_c
__cstring:000000010000250C                                          ; __objc_const:000000
__cstring:0000000100002517 aTR               db 'T#,R',0             ; DATA XREF: __objc_c
__cstring:0000000100002517                                          ; __objc_const:000000
__cstring:000000010000251C aDescription_0    db 'description',0      ; DATA XREF: __objc_c
```

```php
1  <?php
2  //Ihsan Sencan
3  //Mobile Challenges / Cryptohorrific
4  $imputText = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx="; //88 characters
5  $imputKey = "xxxxxxxxxxxxxxxx"; // 16 characters
6  $blockSize = 128; // 192, 256
7  $aes = new AES($imputText, $imputKey, $blockSize);
8
9  $enc = $aes→decrypt();
10 $aes→setData($enc);
11 $dec=$aes→decrypt();
12 echo "Decryption: ".$enc."<br/>";
13
14
15 class AES {
16
17     const M_CBC = 'cbc';
18     const M_CFB = 'cfb';
19     const M_ECB = 'ecb';
20     const M_NOFB = 'nofb';
21     const M_OFB = 'ofb';
22     const M_STREAM = 'stream';
23
24     protected $key;
25     protected $cipher;
26     protected $data;
```

```
INT          ⊖  ⊕    SQL BASICS⌄    UNION BASED⌄    ERROR/DOUBLE Q
  Load URL   http://localhost/ihsan.php
  Split URL
  Execute

  ☐ Post data  ☐ Referrer  ◄  0xHEX  ⇒    ◄   %URL  ⇒
```

Decryption: HTB{%SoC00l_H4ckTh3b0xbyBs3cur31stCh4ll3ng3!!Cr