

# Write-Up: Nwbin (Rev)

Ομάδα: mousiko\_gymsasio\_agrinou\_lt\_1 (Μουσικό Γυμνάσιο  
Αγρινίου - Λ.Τ.)  
Μαθητές/Μαθήτριες: Πέτρος Παπαθανασίου

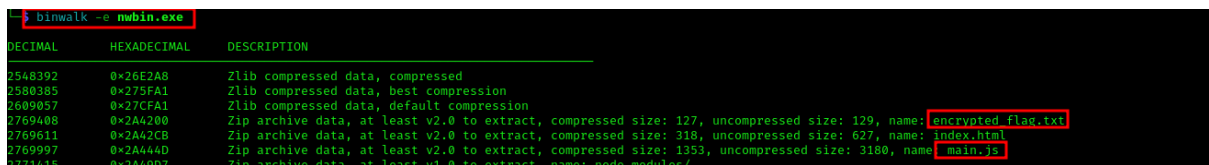
## Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα zip αρχείο που περιέχει ένα exe binary. Αναζητεί την λύση ενός γρίφου ώστε να μας δώσει την σημαία.

## Επίλυση

### Αρχική ανάλυση

Το ανοίγω με έναν hex editor και βλέπω ότι έχει μέσα κρυμμένο ένα αρχείο με όνομα encrypted\_flag.txt. Με το εργαλείο binwalk μπορώ να εξαγωγή όλα τα αρχεία που βρίσκονται πίσω από το exe. Ανάμεσα σε αυτά βρίσκεται και το encrypted\_flag.txt, όπως και το main.js.



DECIMAL	HEXADECIMAL	DESCRIPTION
2548392	0x26E2A8	Zlib compressed data, compressed
2580385	0x275FA1	Zlib compressed data, best compression
2609057	0x27CFA1	Zlib compressed data, default compression
2769408	0x2A4200	Zip archive data, at least v2.0 to extract, compressed size: 127, uncompressed size: 129, name: encrypted_flag.txt
2769611	0x2A42CB	Zip archive data, at least v2.0 to extract, compressed size: 318, uncompressed size: 627, name: index.html
2769997	0x2A444D	Zip archive data, at least v2.0 to extract, compressed size: 1353, uncompressed size: 3180, name: main.js
2771615	0x2A48D7	Zip archive data, at least v1.0 to extract, name: node_modules/

Ψάχνοντας όλα τα διαθέσιμα αρχεία, το μόνο που ήταν αναγνώσιμο ήταν το main.js, το οποίο περιείχε τον κώδικα της εφαρμογής.

### Εκμετάλλευση ευπάθειας

Από αυτόν πήρα το σωστό hash και με ένα εργαλείο όπως το CrackStation μπόρεσα να δω το σωστό κλειδί.



```
// Prompt user for input
question('Who am I? ', (userInput) => {
  var key = userInput.toLowerCase().replace(/^[^a-z]+/g, '').trim();
  var input_hash = hash(key);
  if (input_hash === '0e54775fef09e53533c4de9aa6cfbf3ade7fb444f85d2dbd41d4b421c9621058') {
    term.write('Correct!\n');
    if (debug) {
      var flag = decryptFlag(
        encrypted,
        crypto.createHash('sha256').update(key).digest(),
        Buffer.from(iv, 'base64'),
        Buffer.from(authTag, 'base64')
      );
      term.write(`${flag}\n`);
      term.write('\n');
      return;
    }
  }
})
```

# Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0e54775fe09e53533c4de9aa6cfbf3ade7fb444f85d2dbd41d4b421c9621058

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0e54775fe09e53533c4de9aa6cfbf3ade7fb444f85d2dbd41d4b421c9621058	sha256	n7js

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

Στην συνέχεια γνωρίζοντας τον σωστό κωδικό μπόρεσα να τρέξω την εφαρμογή για να δείξει την σημαία.

Παρατήρησα ότι εμφανίζει την λέξη “Correct”, αλλά όχι την σημαία. Αυτό συμβαίνει γιατί στην εντολή “if (debug)”, που φαίνεται πιο πάνω το debug είναι απενεργοποιημένο. Αυτό μπορούμε να το δούμε από το binary αρχείο.

```

0 74 69 66 69 61 62 69 6C 69 74 79 00 64 69 73 61  t i d i a b i l i t y . d i s a u n t 64 70744385
0 62 6C 65 64 2D 62 79 2D 64 65 66 61 75 6C 74 2D  b l e d - b y - d e f a u l t - i n t 64 70744385
0 69 64 65 6E 74 69 66 69 61 62 69 6C 69 74 79 2E  i d e n t i f i a b i l i t y . U L E B 128 101
0 68 69 67 68 5F 65 6E 74 72 6F 70 79 5F 61 70 69  h i g h _ e n t r o p y _ a p i S L E B 128 -27
0 00 64 69 73 61 62 6C 65 64 2D 62 79 2D 64 65 66  . d i s a b l e d - b y - d e f f l o a t 16 1637
0 61 75 6C 74 2D 63 63 00 64 69 73 61 62 6C 65 64  a u l t - c c . d i s a b l e d b f l o a t 16 2.703554
0 2D 62 79 2D 64 65 66 61 75 6C 74 2D 63 63 2E 64  - b y - d e f a u l t - c c d f l o a t 32 2.857284
0 65 62 75 67 00 64 69 73 61 62 6C 65 64 2D 62 79  e b u g . d i s a b l e d - b y f l o a t 64 8.480929
0 2D 64 65 66 61 75 6C 74 2D 63 63 2E 64 65 62 75  - d e f a u l t - c c . d e b u G U I D E n d o f F
0 67 2E 63 64 70 2D 70 65 72 66 00 64 69 73 61 62  g . c d p - p e r f . d i s a b A S C I I e
0 6C 65 64 2D 62 79 2D 64 65 66 61 75 6C 74 2D 63  l e d - b y - d e f a u l t - c U T F - 8 e
0 63 2E 64 65 62 75 67 2E 64 69 73 70 6C 61 79 5F  c . d e b u g . d i s p l a y _ U T F - 16 院
0 69 74 65 6D 73 00 64 69 73 61 62 6C 65 64 2D 62  i t e m s . d i s a b l e d - b G B 18030 e
0 79 2D 64 65 66 61 75 6C 74 2D 63 63 2E 64 65 62  y - d e f a u l t - c c . d e b B I G 5 e
0 75 67 2E 6C 63 64 5F 74 65 78 74 00 64 69 73 61  u g . l c d _ t e x t . d i s a S H I F T - J I S e
0 62 6C 65 64 2D 62 79 2D 64 65 66 61 75 6C 74 2D  b l e d - b y - d e f a u l t - ☒ L i t t l e E n d i a n

```

Το προφανές είναι να ενεργοποιήσουμε το debug. Όμως αφού δεν μπόρεσα να το τρέξω έτσι, δημιούργησα έναν κώδικα σε python, ο οποίος παίρνει την κωδικοποιημένη σημαία, την λέξη κλειδί και την μέθοδο κωδικοποίησης και δίνει ως αποτέλεσμα την αποκωδικοποιημένη σημαία.

```
1 from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
2 from cryptography.hazmat.backends import default_backend
3 from cryptography.hazmat.primitives import hashes
4 from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
5 import base64
6
7 # Τα δεδομένα που παρέθεσες
8 encrypted = "UcxLSyUGR7WkkPW1UtUeKFo00/wjBmvrzITDDTfS4dK2Qmb+CVgH"
9 iv = "L/gnx8voJaHR3Ye0"
10 authTag = "XGk8Kvs6lJdHIXpguds/Yw=="
11 key = "nwjs"
12
13 # Μετατροπή των δεδομένων από base64
14 ciphertext = base64.b64decode(encrypted)
15 iv_bytes = base64.b64decode(iv)
16 auth_tag = base64.b64decode(authTag)
17
18 # Δημιουργία του κλειδιού από το SHA256 του key
19 digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
20 digest.update(key.encode('utf-8'))
21 key_bytes = digest.finalize()
22
23 # Αποκρυπτογράφηση χρησιμοποιώντας το AES GCM
24 cipher = Cipher(algorithms.AES(key_bytes), modes.GCM(iv_bytes, auth_tag), backend=default_backend())
25 decryptor = cipher.decryptor()
26
27 # Αποκρυπτογράφηση του κειμένου
28 plaintext = decryptor.update(ciphertext) + decryptor.finalize()
29
30 # Εκτύπωση του αποκωδικοποιημένου μηνύματος
31 print("Αποκωδικοποιημένο μήνυμα:", plaintext.decode('utf-8'))
32
33
34
```

```
$ python3 test.py
Αποκωδικοποιημένο μήνυμα: FLAG{i_tH1nK_I_4m_uNp4cK1nG_l1KE_a_Pr0}
```

## Σημαία

Η σημαία που βρέθηκε:

FLAG{i\_tH1nK\_I\_4m\_uNp4cK1nG\_l1KE\_a\_Pr0}