Write-Up: Defaced (Web)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει να τρέξουμε έναν server, ο οποίος μας εμφανίζει το μήνυμα “DEFACED by S0URC3 EXPL0IT3R5”.Σκοπός μας είναι να ψάξουμε την ιστοσελίδα για να βρούμε κάπου την σημαία.

Επίλυση

Αρχική ανάλυση

Αμέσως από το μήνυμα “We read the source” κατάλαβα ότι η δοκιμασία θα ασχολείται με τον κώδικα source. Η σημαία λογικά θα βρίσκεται σε σχόλια μέσα στον κώδικα html και οποιονδήποτε άλλο τρέχει ο server.

Εκμετάλλευση ευπάθειας

Από την επιθεώρηση κώδικα:

Για το πρώτο μέρος της σημαίας πάτησα view page source και είδα τον html κώδικα της ιστοσελίδα

Για το δεύτερο μέρος της σημαίας πάτησα ctrl+shift+I και είδα τον style editor της ιστσελίδαας

Για το τρίτο μέρος της σημαίας πάτησα ctrl+shift+E και άνοιξα το αρχείο scipt.js

Σημαία

Η σημαία που βρέθηκε:

```
FLAG{p4rT_1_iN_HTml_th3_2ND_fl4g_pARt_in_Cs5_anD_th3_3Rd_paRT3_IN_Js}
```