WRITE-UP

Limited Time

Balatre Grégory

Hacky'Nov Aix-en-Provence
2022 - 2023

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

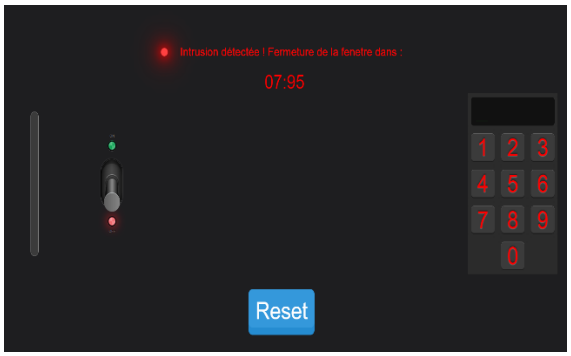
La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge



Nom du challenge : Limited Time

Domaine : Web

Difficulté : ★ ★ ★ ★ ★

Auteur : Balatre Grégory

Description : Le temps presse ! Un de nos agents infiltré dans un réseau de cybercriminel vient de se faire griller.

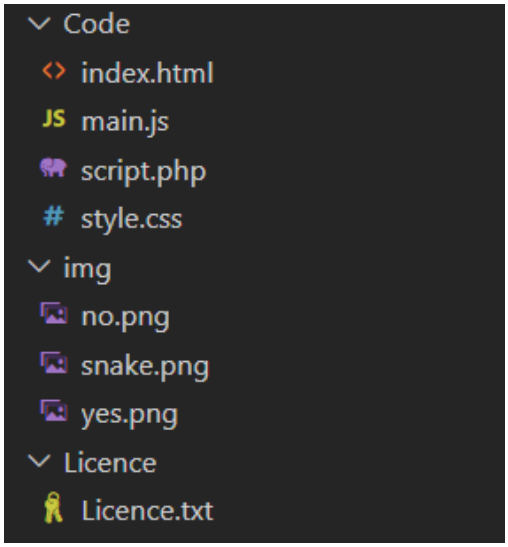
Il est pris en otage par l'ennemi et a été forcé de donner les codes d'accès au projet FEUR (un virus visant à interdire une blague bien trop évidente).

Nous arrivons à avoir une connexion stable mais le système nous bloque au bout de quelques secondes, on dirait qu'une sorte de chronomètre nous empêche de réinitialiser le système.

Vous devez empêcher coute que coute ce virus d'atteindre le système central où alors le monde risque d'être changé à jamais.

Partie 2 : Sources

Le challenge comporte les fichiers suivants :

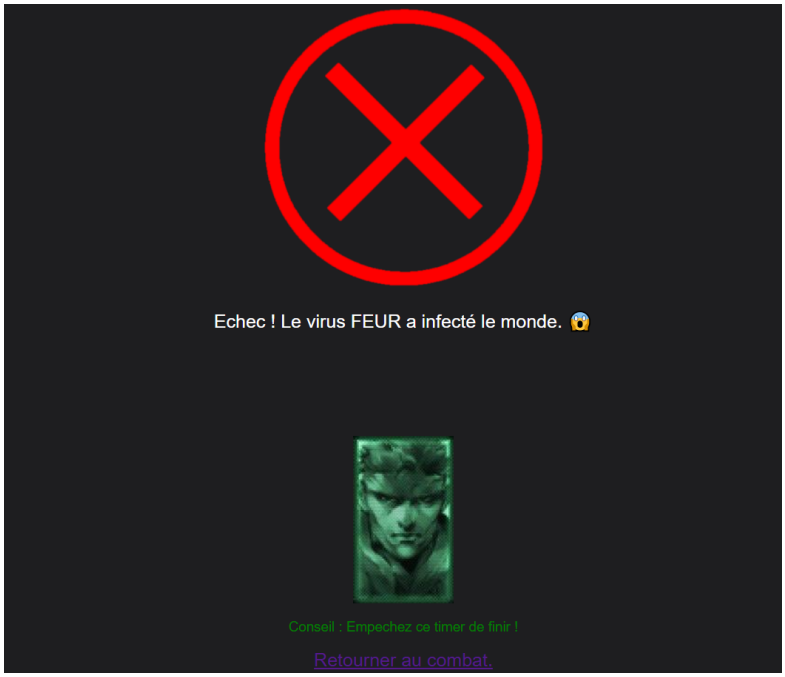


Tous les fichiers du challenge sont disponibles dans le même dossier que le write-up.

Partie 3 : Résolution

Une limite de temps en haut de l'écran nous empêche de redémarrer le système. Ce dernier mettant plus de temps que la limite affichée.

Une fois le temps passé à 0, nous sommes redirigé sur une page nous indiquant que nous avons échoué avec un indice nous demandant de trouver un moyen d'arrêter le chronomètre.



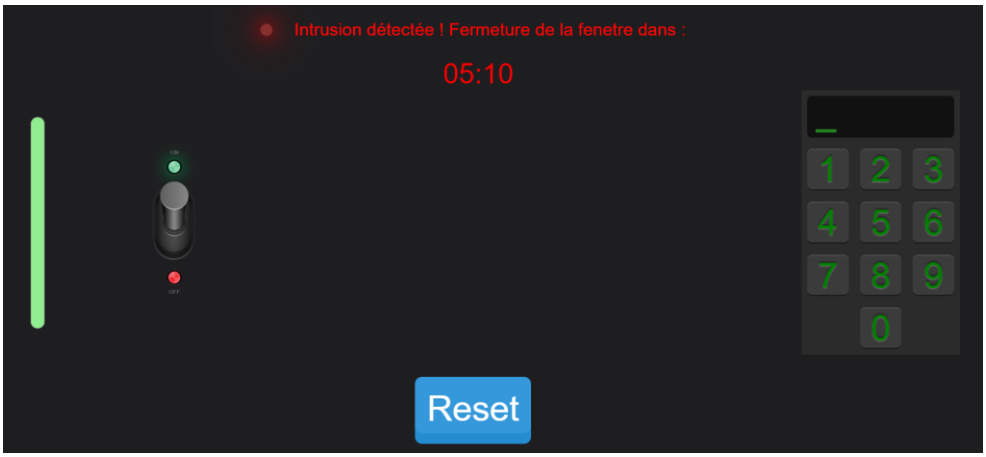
En regardant les fichiers, on voit que le chronomètre est fait en Javascript et si l'on se penche un peu sur le fonctionnement de ce dernier, on remarque une fonction « Timer » qui arrête le temps si le password est égal à une certaine valeur.

```
if (pass == atob("ZGVjb2RlVVJJKCJTdHJpbmcuZnJvbUNoYXJDb2RlJTI4NjksMTIwLDExNiwxMDEsMTEwLDEwMCw4NCwxMDQsMTAxLDg0LDEwNSwxMDksMTAx

    //Stop the time
    document.getElementById("Step1").value = pass;

    return true;
```

Du coup, nous pouvons faire un F12 pour copier cette valeur et la coller dans une console pour savoir qu'elle est sa valeur. Réalisons la manipulation 3 fois pour enfin trouver le mot « ExtendTheTime ».

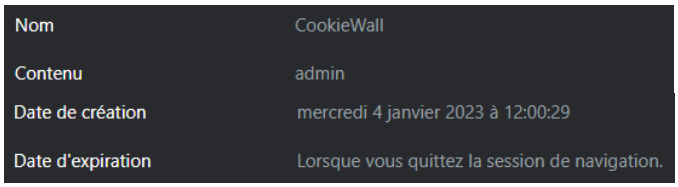
```
> atob("ZGVjb2RlVVJJKCJTdHJpbmcuZnJvbUNoYXJDb2RlJTI4NjksMTIwLDExNiwxMDEsMTEwLDEwMCw4NCwxMDQsMTAxLDg0LDEwNSwxMDksMTAxJTI5Iik=")
< 'decodeURI("String.fromCharCode%2869,120,116,101,110,100,84,104,101,84,105,109,101%29")'
> decodeURI("String.fromCharCode%2869,120,116,101,110,100,84,104,101,84,105,109,101%29")
< 'String.fromCharCode(69,120,116,101,110,100,84,104,101,84,105,109,101)'
> String.fromCharCode(69,120,116,101,110,100,84,104,101,84,105,109,101)
< 'ExtendTheTime'
```

Le chronomètre étant mal géré en Javascript, ce dernier est sensible à une injection de JS. Rentrons donc la commande suivante dans l'url : javascript:clock = timer("ExtendTheTime");



On remarque que le temps s'arrête et que la sécurité du digicode s'est désactivée. En regardant une fois de plus le code, on remarque une variable égale à 2580 et un reverse() par la suite, nous indiquant de tester le code à l'envers : 0852 => Success !

Pour terminer, inspectons les cookies. Nous possédons un cookie admin mais dont la date d'expiration est passé.



En regardant comment les cookies sont utilisés dans le code, nous trouvons une fonction qui va faire une vérification au moment où nous pressons le bouton Reset.

```
document.getElementById("button").addEventListener("click", function(){

  EventDate = new Date("April 1, 2023 00:00:00");

  if (+time === +EventDate) {
    document.getElementById("Step3").value = time;
  }
})

creerCookie(Date.now());
```

Il faut donc changer la date de ce dernier par la date de l'évènement à minuit grâce à une injection de JS : javascript:creerCookie("April 1, 2023 00:00:00");

Nous pouvons désormais cliquer sur le bouton de Reset pour arrêter le processus et obtenir le flag.