

WRITE-UP

File Hunt - Web

Thomas Quadro

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.

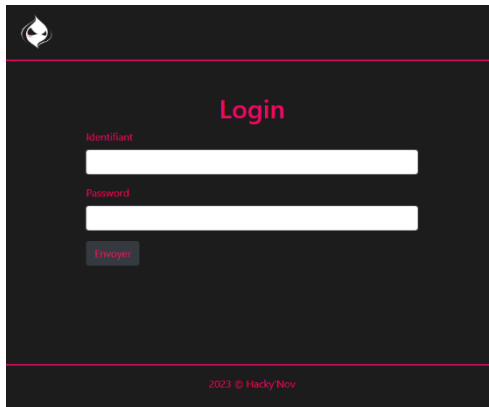
La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants,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

<https://hackynov.fr/>

Table des matières

Partie 1 : Présentation du challenge	4
Partie 2 : Sources	4
Partie 3 : Résolution.....	5

Partie 1 : Présentation du challenge



Nom du challenge : File Hunt

Domaine : Web

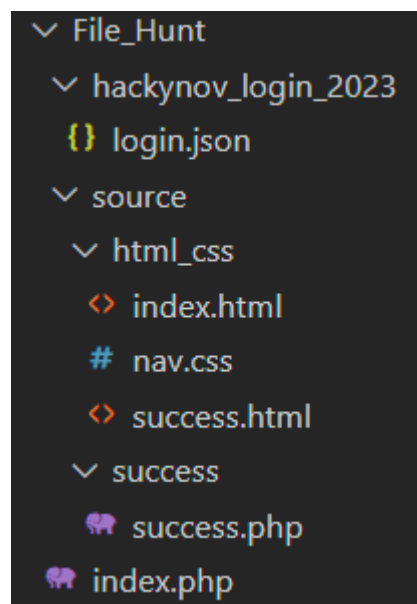
Difficulté : ★ ★ ★ ★ ★

Auteur : Thomas Quadro

Description : Hacky'Nov a mis à disposition un site web pour l'évènement. Connectez-vous au compte admin pour récupérer le flag.

Partie 2 : Sources


Le challenge comporte les fichiers suivants :



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

Partie 3 : Résolution

1. Nous arrivons sur la page de connexion, il faut trouver l'identifiant et le mot de passe.



Login

Identifiant

Password

Envoyer

2023 © Hacky'Nov

2. Pour cela, il faut aller regarder ces cookies (F12 puis Application) et trouver celui portant le nom « John » et qui est encodé en Json.

[illegible]

3. Pour décoder le message, on peut utiliser plusieurs manières :
 - Aller sur un site qui décode l'URI

- Utiliser la fonction javascript '`decodeURIComponent()`' et mettre le contenu du cookie dedans

```
> decodeURIComponent("%7B%0A%20%20%20%22identifiants%22%3A%20%22admin%22%2C%0A%20%20%20%22mot%20de%20passe%22%3A%20%22Hacky%27Nov%22%0A%7D")
< `{\\n  "identifiants": "admin",\\n  "mot de passe": "Hacky'Nov"\\n}`
```


Ensuite il faudra entrer les identifiants de connexions et un message d'erreur apparaîtra.

4. Il faudra reregarder le cookie John qui a changé, puis le décoder de la même façon qu'au point 3. Une instruction apparaîtra nous disant d'aller dans le dossier source.

John	aller%20dans%20le%20dossier%20hackynov_lo...	lo...	/	Se...	59						Medi...
Jean-Luc	U2FsdGVkX1%2BIXTTLCBx16A%2FW6hpM%2B...	lo...	/	Se...	110						Medi...
Pierre	%2BIXTTLCBx16A%2F%2B2sv4FBDkmJ%2B%3D	lo...	/	Se...	42						Medi...
Jean	U2FsdGVkX19LIsnoCniVwLdyfWigXZM%2B3tR...	lo...	/	Se...	144						Medi...
Emile	U2FsdGVkX1%2FhQh0ZF76a8c2AHMpwzU3y%...	lo...	/	Se...	131						Medi...
Bernard	U2FsdGVkX19LIsnoCniVwLdyfWigXZM%2B3tR...	lo...	/	Se...	147						Medi...

```
> decodeURI("aller%20dans%20le%20dossier%20hackynov_login_2023%20%21")
< 'aller dans le dossier hackynov_login_2023 !'
```

5. Une fois « /hackynov_login_2023 » ajouté à l'URL, il faudra aller dans le fichier « login.json »

Name	Last modified	Size	Description
Parent Directory	-	-	-
 login.json	2023-01-04 17:07	367	

Apache/2.4.54 (Win64) PHP/8.0.26 mod_fcgid/2.3.10-dev Server at localhost Port 80

```
[
  {
    "type": "admin",
    "mail": "account.admin.network@Hacky'Nov.fr",
    "mdp": "fc294a4698f9886f4d7df480442541f5"
  },
  {
    "type": "user",
    "mail": "martin.ytb@rest.fr",
    "mdp": "QwNjb3VudEBiYWVreSdOb3ZAVXN1cg=="
  },
  {
    "type": "guest",
    "mail": "gilbert46755@soap.com",
    "mdp": "QwNjb3VudEBiYWVreSdOb3ZAR3Vlc3Q="
  }
]
```

6. Il faudra ensuite déchiffrer les mots de passe « user » et « guest » en base 64 en utilisant :

- La fonction javascript « atob() »
- Aller sur un site qui déchiffre la base 64

```
> atob("QwNjb3VudEBiYWVreSdOb3ZAVXN1cg==")
< "Account@Hacky'Nov@User"
```

```
> atob("QwNjb3VudEBiYWVreSdOb3ZAR3Vlc3Q=")
< "Account@Hacky'Nov@Guest"
```

7. Après avoir fait ceci, il faudra déduire le mot de passe administrateur qui sera « Account@Hacky'Nov@Admin » puis entrer les identifiants de connexion. Vous serez redirigée vers une page où sera affiché le flag.



Le FLAG est : HN0x02{Kin0@d3r@T0t3n}