

07/02/2023

CHALLENGE 2



Version 1.0

Préparé par :

Thomas, Davy, Enzo, Thibo, Matt

B2 et B1 Informatique Aix

Nous arrivons sur une page de connexion, il faudra aller voir les cookies et prendre le cookie IP .

Login

Identifiant

Password

Envoyer

2023 © Challenge 48H

DevTools is now available in French! Always match Chrome's language Switch DevTools to French Don't show again

Elements Console Sources Network Performance Memory Application Security 3 1

Application

- Manifest
- Service Workers
- Storage

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
 - http://localhost
- Trust Tokens
- Interest Groups

Cache

- Cache Storage
- Back/forward cache

Background Services

- Background Fetch
- Background Sync
- Notifications
- Payment Handler
- Periodic Background Sync
- Push Messaging
- Reporting API

Frames

Filter

Only show cookies with an issue

Name	Value	D...	Pa...	Ex...	Size	Ht...	Se...	Sa...	Sa...	Pa...	P...
PHPSESSID	a4mv7amcku9rp3ubb90...	lo...	/	Se...	35						M...
IP	%7B%0A%20%20%20%2...	lo...	/Fi...	Se...	121						M...
Encryption	U2FsdGVhX1%2FhQh0ZF...	lo...	/Fi...	Se...	136						M...
Conception	U2FsdGVhX1%2BIXTLCB...	lo...	/Fi...	Se...	112						M...
DataBase	U2FsdGVhX19LIsnoCniVw...	lo...	/Fi...	Se...	148						M...

Select a cookie to preview its value

Entrez l'identifiant et le mot de passe dans le cookie ip.

Login

Domage tu es tombé dans le panneau 😊

Identifiant

Password

Envoyer

2023 © Challenge 48H

Allez dans le cookies et regarder encore celui avec le nom IP.

DevTools is now available in French! Always match Chrome's language Switch DevTools to French Don't show again

Elements Console Sources Network Performance Memory Application Security

Application

- Manifest
- Service Workers
- Storage

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
 - http://localhost
 - Trust Tokens
 - Interest Groups

Cache

- Cache Storage
- Back/forward cache

Background Services

- Background Fetch
- Background Sync
- Notifications
- Payment Handler
- Periodic Background Sync
- Push Messaging
- Reporting API

Frames

Filter

Only show cookies with an issue

Name	Value	D...	Pa...	Ex...	Size	Ht...	Se...	St...	St...	Pa...	P...
PHPSESSID	a4mv7amcku9rp3ubb90...	lo...	/	Se...	35						M...
IP	aller%20dans%20le%20d...	lo...	/Fi...	Se...	44						M...
Encryption	U2FsdGVhX1%2FhQh0ZF...	lo...	/Fi...	Se...	136						M...
Conception	U2FsdGVhX1%2BIXTTLCB...	lo...	/Fi...	Se...	112						M...
DataBase	U2FsdGVhX19LlsoCniVw...	lo...	/Fi...	Se...	148						M...

Select a cookie to preview its value

Allez dans le cookies et regarder encore celui avec le nom IP. Suivez l'instruction du cookie (allez dans le dossier source).

Index of /File_Hunt/source

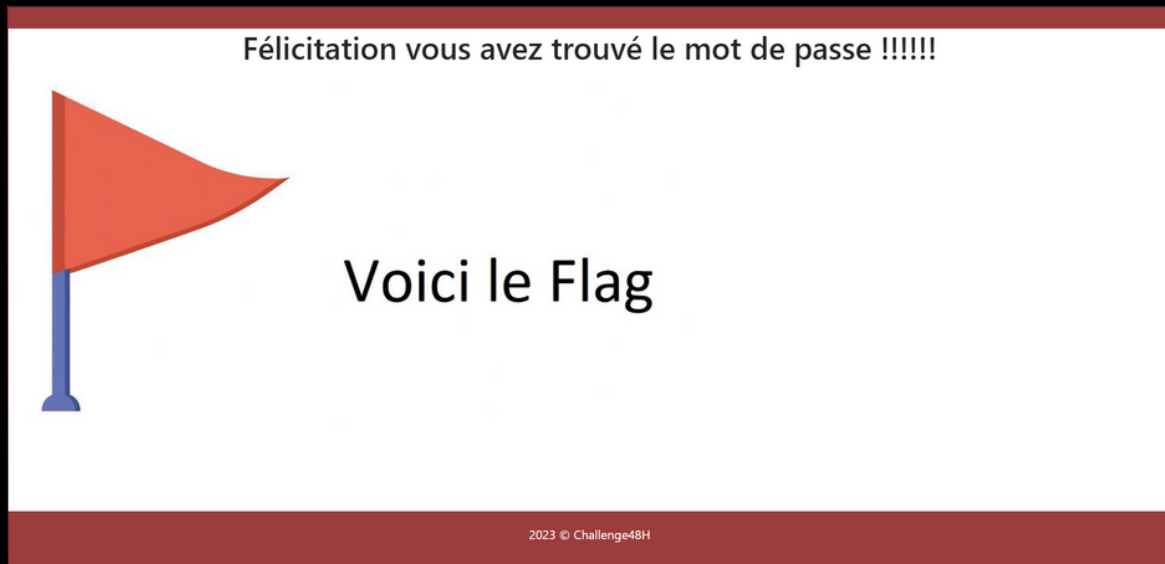
Name	Last modified	Size	Description
 Parent Directory		-	
 restored/	2023-02-07 12:05	-	
 success/	2023-02-07 12:33	-	

Apache/2.4.51 (Win64) PHP/8.1.0 mod_fcgid/2.3.10-dev Server at localhost Port 80

Allez dans le dossier restored, puis explorer le fichier login.json, il faudra déchiffrer en base 64 principalement l'utilisateur guest et user. Il faudra deviner le mot de passe admin qui est Chall_48h@Admin. Entrer ensuite les identifiants du compte admin.

```
[
  {
    "type": "admin",
    "mail": "admin.ynov@chall48.fr",
    "mdp": "f6a3789b9b925aad214332eb949eb181"
  },
  {
    "type": "ynov",
    "mail": "fabienolicart@snibel.com",
    "mdp": "QWNjb3VudEBDaGFsbGVuZ2U0OEhAWU5PVg=="
  },
  {
    "type": "ytrack",
    "mail": "ynov.campus.fr",
    "mdp": "bGVzIGNoYXVzc2V0dGVzIGRlIGwnYXJjaGkgZHVjaGVzc2Ugc29udCB1bGxlcYBzw6hjaGVz"
  },
  {
    "type": "user",
    "mail": "user.ynov@chall48.fr",
    "mdp": "Q2hhbGxfNDhoQFVzZXI="
  },
  {
    "type": "win",
    "mail": "account.admin.network@Challenge48H.fr",
    "mdp": "aHR0cHM6Ly93d3cueW91dHVlZS5jb20vd2F0Y2g/dj05TTJDZTUwSGx1OA=="
  },
  {
    "type": "loose",
    "mail": "fake.account.logique@loose.fr",
    "mdp": "YmllbnZlbnVlIGRhbngbGGEgbWF0cm1jZQ=="
  },
  {
    "type": "guest",
    "mail": "guest.ynov@chall48.fr",
    "mdp": "Q2hhbGxfNDhoQEdlZXN0"
  }
]
```

Une image avec le flag apparait !



Il faudra ensuite retrouver le fichier texte caché dans cette image (télécharger l'image) en utilisant des logiciels faits exprès (steghide).

Si vous utilisez steghide, il faudra faire cette commande :
`steghide extract -sf flags.jfif`

Un fichier texte apparaîtra, il faudra déchiffrer le message d'abord en binaire puis ensuite en hexadécimal. Le flag est `FLAG{2023@Challenge!48?h++Finì}`

P.S: des easter eggs ont été dissimulés dans le ctf mais il ne permettent pas de le résoudre !

Merci d'avoir lu ce
rapport

