07/02/2023

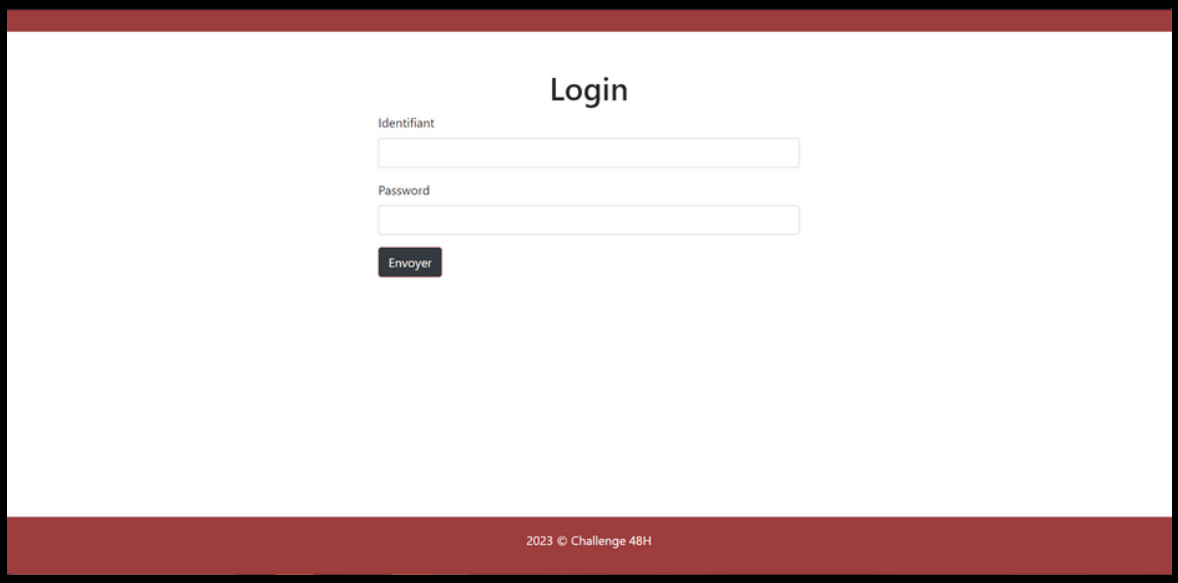
CHALLENGE 2

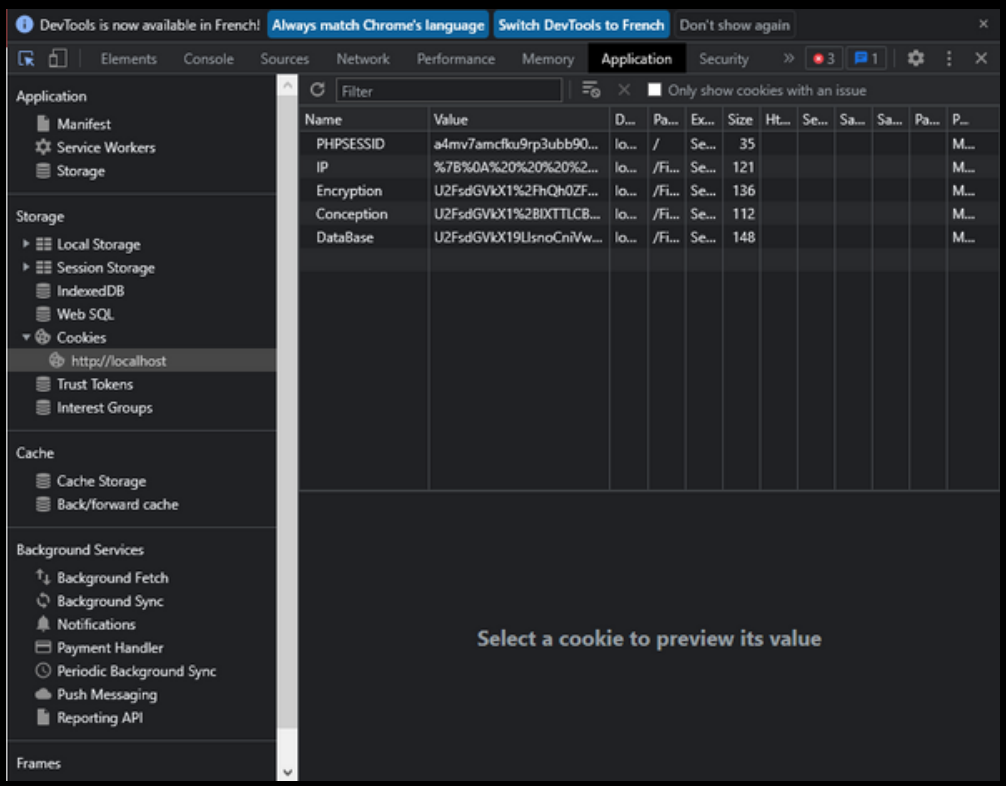
Version 1.0

Préparé par :
Thomas, Davy, Enzo, Thibo, Matt

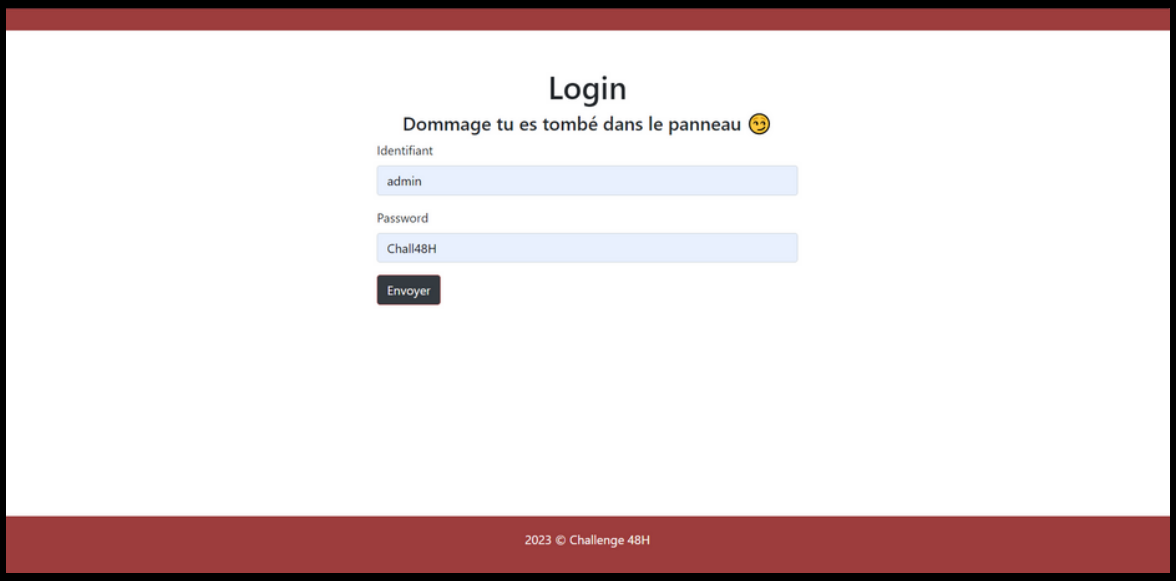
B2 et B1 Informatique Aix

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

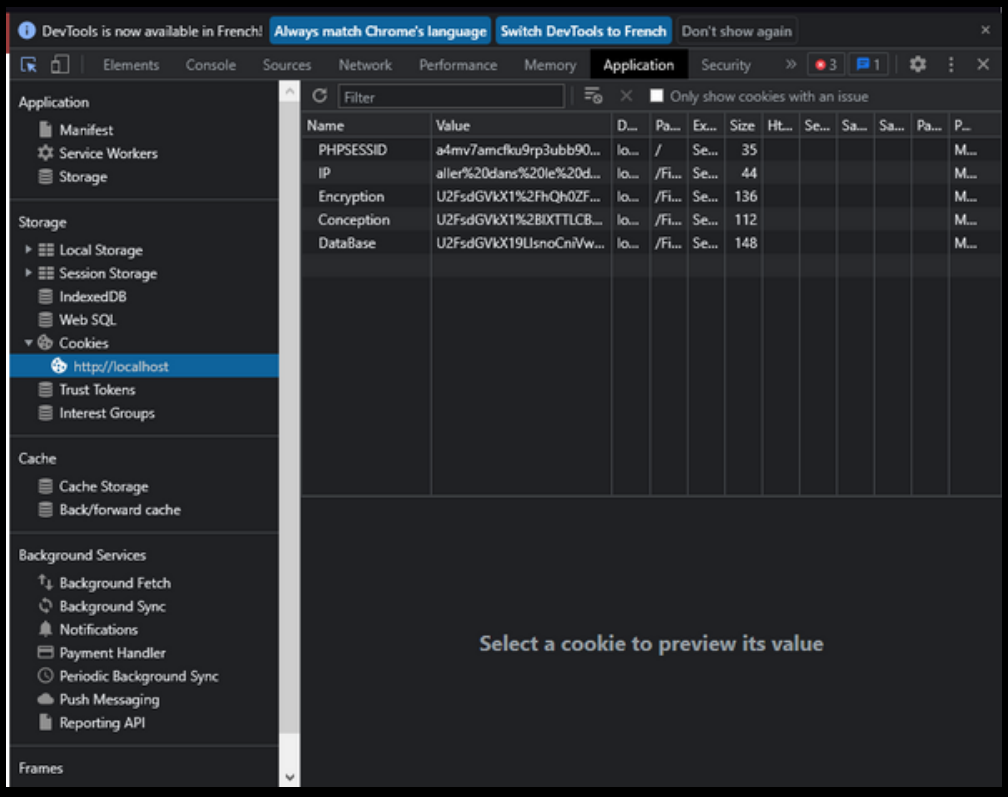




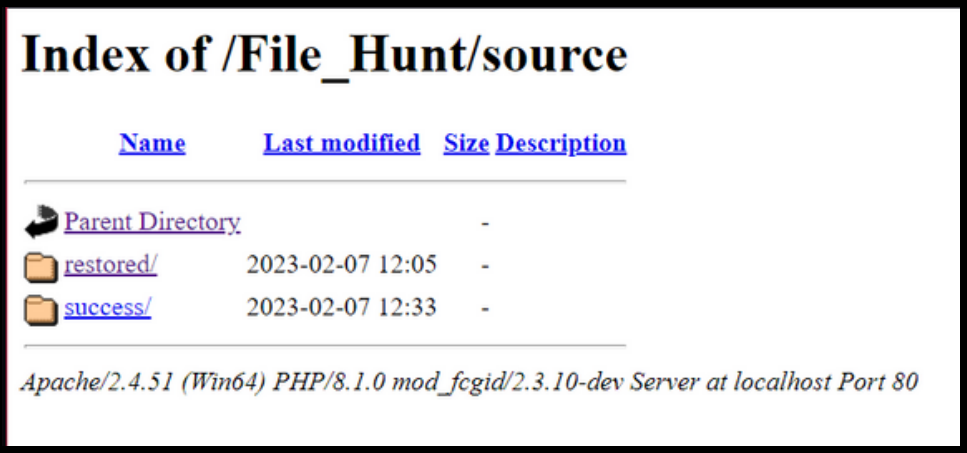
Entrez l'identifiant et le mot de passe dans le cookie ip.



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



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

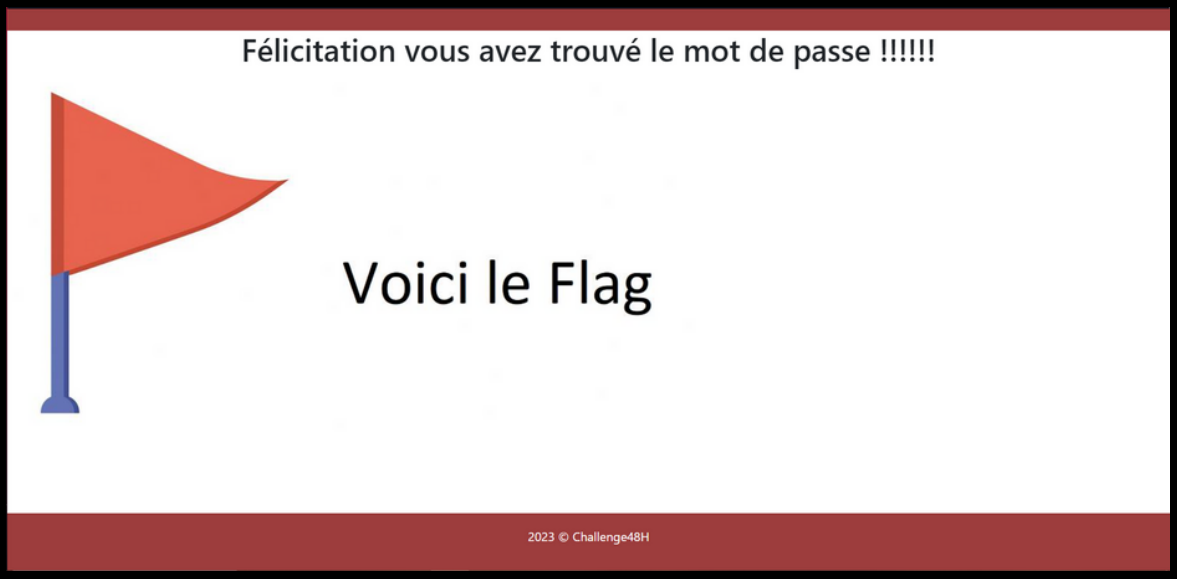
Name	Last modified	Size	Description
Parent Directory		-	
restored/	2023-02-07 12:05	-	
success/	2023-02-07 12:33	-	

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 dechiffrer 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": "bGVzIGNoYXVzc2V0dGVzIGRlIGwnYXJjaGkgZHVjaGVzc2Ugc29udCBlbGxlcyBzw6hjaGVz"
  },
  {
    "type":"user",
    "mail": "user.ynov@chall48.fr",
    "mdp": "Q2hhbGxfNDhoQFVzZXI="
  },
  {
    "type":"win",
    "mail":"account.admin.network@Challenge48H.fr",
    "mdp":"aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj05TTJDZTUwSGxlOA=="
  },
  {
    "type":"loose",
    "mail":"fake.account.logique@loose.fr",
    "mdp":"YmllbnZlbnVlIGRhbnMgbGEgbWF0cmljZQ=="
  },
  {
    "type":"guest",
    "mail": "guest.ynov@chall48.fr",
    "mdp": "Q2hhbGxfNDhoQEd1ZXN0"
  }
]
```

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 apparaitra, il faudra déchiffrer le message d'abord en binaire puis ensuite en hexadécimal. Le flag est FLAG{2023@Challenge!48?h++Fini}

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