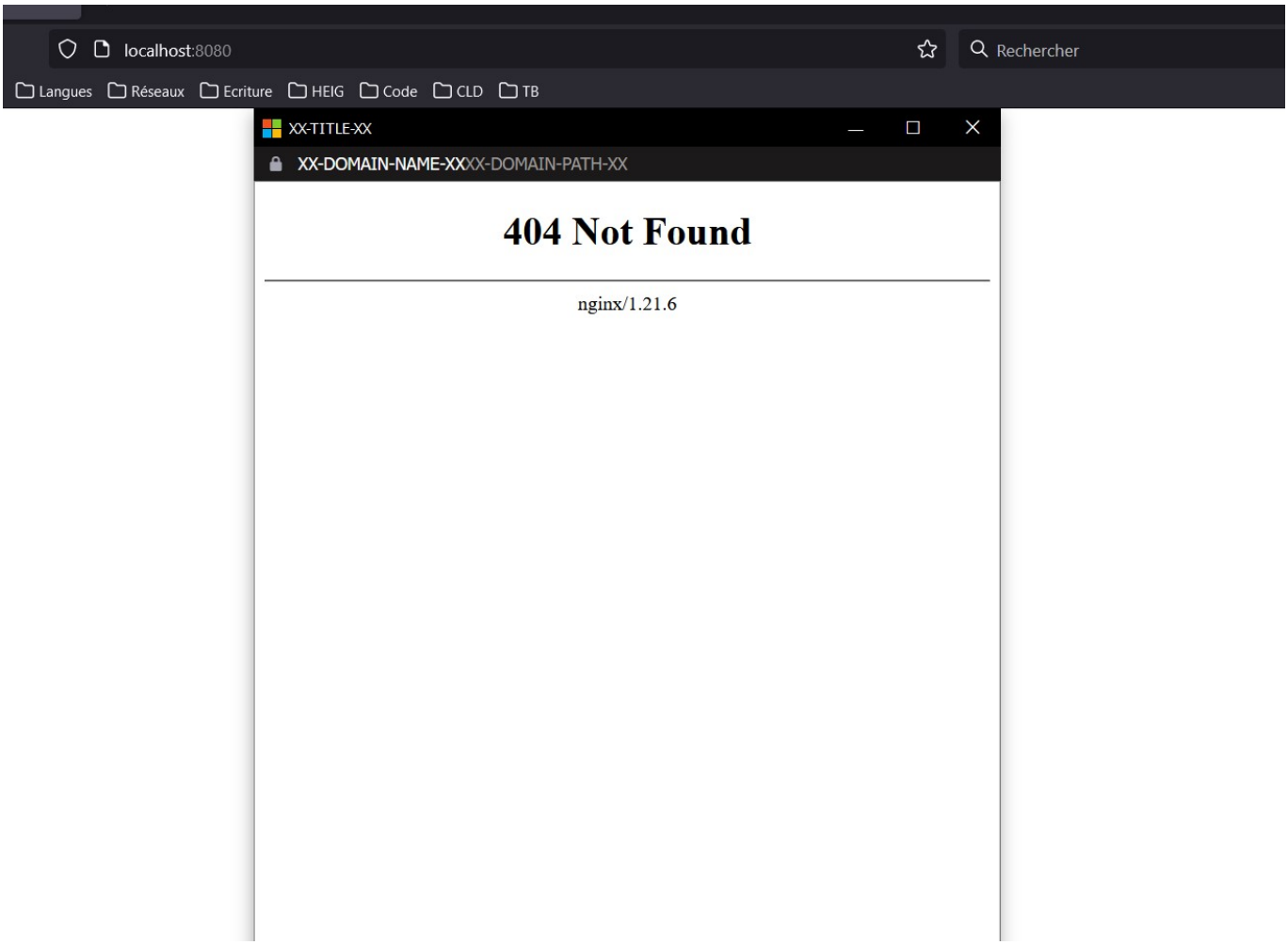
SEN Labo 3 - BITB

Ecrit par Paul Reeve

Premier BITB

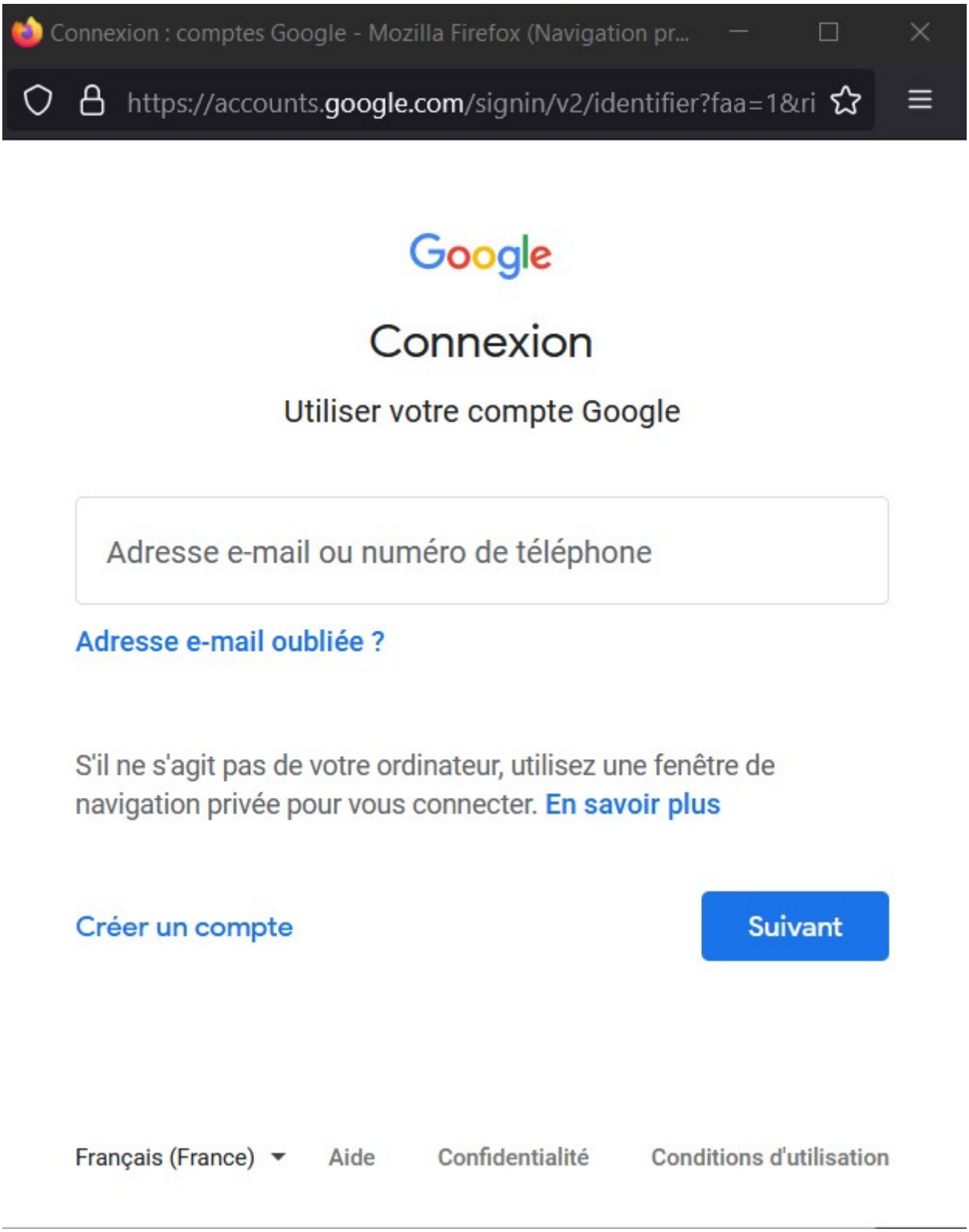
En utilisant le thème `Windows-Chrome-DarkMode`



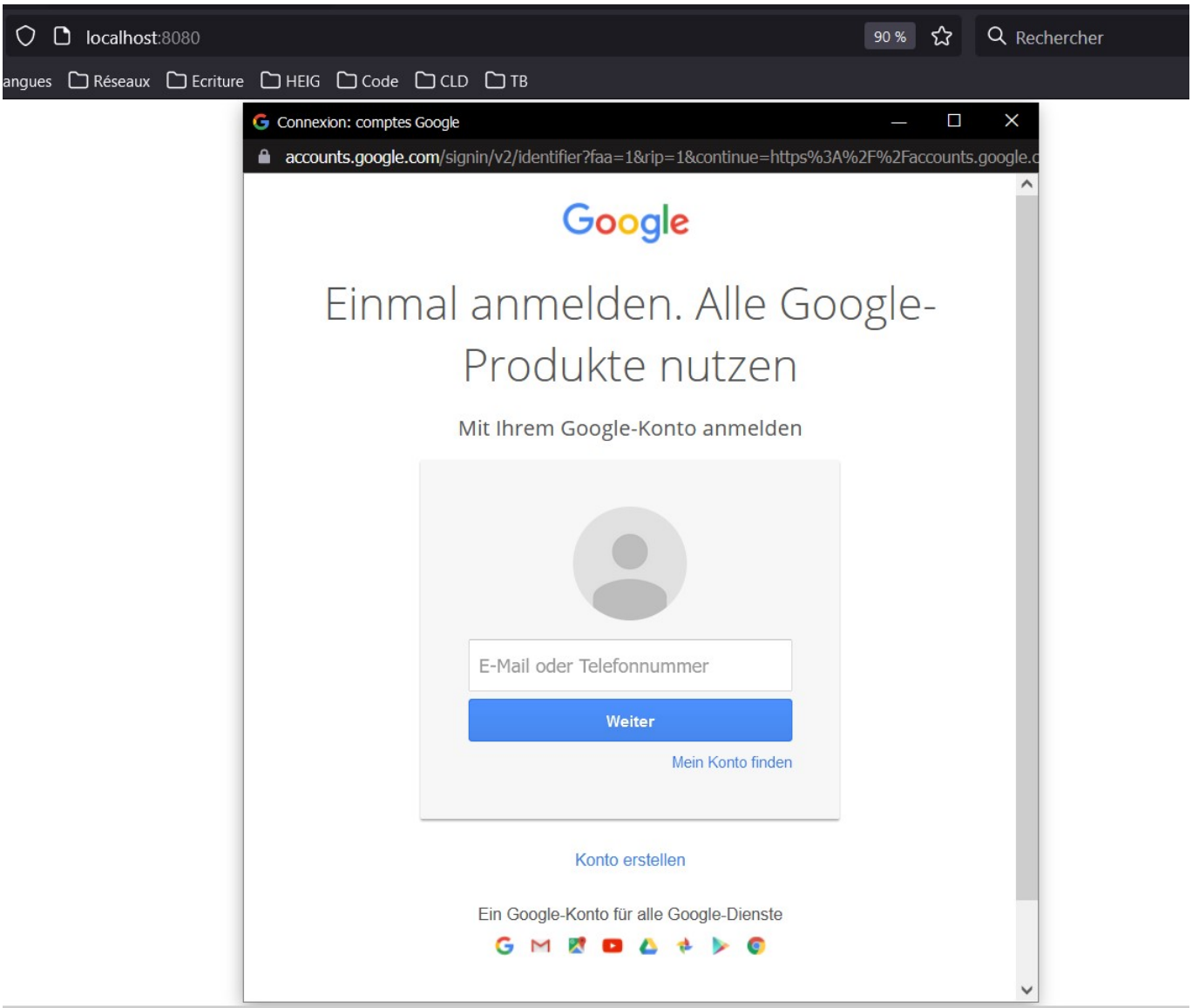
Copie d'une fenêtre d'authentification

J'ai décidé de copié la fenêtre d'authentification pour un compte Google. J'ai récupéré cette fenêtre avec twitter qui accepte la connexion avec un compte google

- Réelle fenêtre d'authentification



- Fausse fenêtre avec le thème `Windows-Chrome-DarkMode`



Valeurs des paramètres

- XX-TITLE-XX: `Connexion: comptes Google`
- XX-DOMAIN-NAME-XX: `accounts.google.com`
- XX-DOMAIN-PATH-XX: `/signin/v2/identifier?faa=1&rip=1&continue=https%3A%2F%2Faccounts.google.com%2Fgsi%2Fselect%3Fclient_id%3D49625052041-kgt0hghf445lmcmhijv46b715m2mpbct.apps.googleusercontent.com%26ux_mode%3Dpopup%26ui_mode%3Dcard%26as%3Dv6YcRX1nW718IF%252Ba96LatQ%26channel_id%3D6b516f926dbce0872008808de759f413ffa0bac2e24f5899c443d8dcf99af8bb%26origin%3Dhttps%3A%2F%2Ftwitter.com&flowName=GlifWebSignIn&flowEntry=ServiceLogin`
- XX-PHISHING-LINK-XX: `./fake_google.html` AKA le chemin local vers le fichier html qui contient le contenu de la page cloné

Différences vraie site et faux site

Langue

Le faux site est en allemand tandis que le vrai est en français. A mon avis celà est du au fait que la page html de login doit détecter le pays de mon ordinateur (la Suisse donc) mais pas la langue de mon navigateur. Ainsi

le faux site se retrouve en allemand, langue par défaut de la Suisse mais n'arrive à détecter la langue du système contrairement au vrai site

Apparence générale

L'apparence générale de la fenêtre est aussi sensiblement différente. Dans le faux site on a par exemple une icône de photo de profil qu'on ne retrouve pas dans le vrai, c'est aussi le cas d'icônes des divers services google qui ici n'apparaissent que sur le faux site.

Le vrai site est au final plus épuré que le faux site. Peut-être y'a-t'il certains mécanismes mis en place par le vrai site pour cacher certains éléments de la page html de base auquel le faux site n'a pas accès.

Il y a aussi le fait que le vrai formulaire de login Google se décompose en 2 parties. On rentre son email puis on clique sur suivant pour avoir un champ où rentrer le mot de passe. Le faux site n'arrive pas à répliquer ce principe

Clonage du site

J'ai utilisé un logiciel de clonage de site nommé HttTrack . Le processus a été relativement simple, j'ai donné au logiciel l'URL du vrai site au logiciel et il m'a téléchargé la page html du login que j'ai ensuite référencé dans l'index du BITB.

Conclusion

On voit qu'il est assez facile de faire un clonage de surface d'un formulaire de login, par contre le répliquer à la lettre est un peu plus compliqué notamment pour ce qui est de la langue et du double formulaire (email puis mot de passe). Mais au final pour un utilisateur peu habitué à ces fenêtres de login, le rendu peut être assez convainquant pour le piéger...