1. Identification de la surface d'attaque

En analysant le code source de la page (notamment le pied de page), des liens de redirection vers des réseaux sociaux ont été identifiés sous la forme : index.php?page=redirect&site=facebook. Ce type de paramètre est souvent vulnérable si le serveur ne valide pas la destination ou le protocole utilisé.

2. Test et Manipulation de paramètre

Plutôt que de fournir une URL classique (comme google.fr), le test a consisté à injecter le protocole **javascript:**. Ce protocole permet d'exécuter du code directement dans le contexte du navigateur de l'utilisateur.

3. Exploitation (Payload)

L'URL finale utilisée pour déclencher la faille a été : http://192.168.1.27/index.php?page=redirect&site=javascript:alert('XSS_Reflected').

En validant cette URL, le serveur a "reflété" le code JavaScript sans le filtrer, provoquant l'affichage d'une page de succès contenant le flag.

4. Flag obtenu

Le hash SHA256 révélé est : **B9E775A0291FED784A2D968OFCFAD7EDD6B8CDF87648DA647AAF4BBA288BCAB3**.

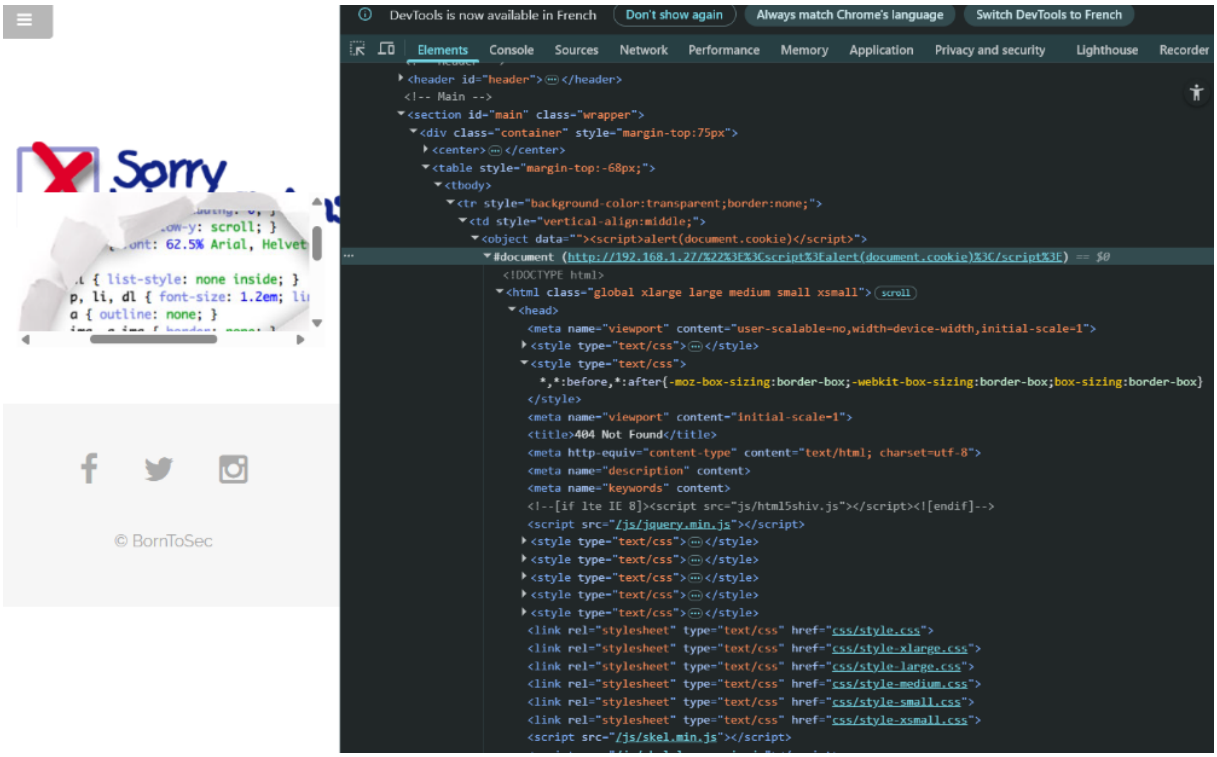
5. Remédiation

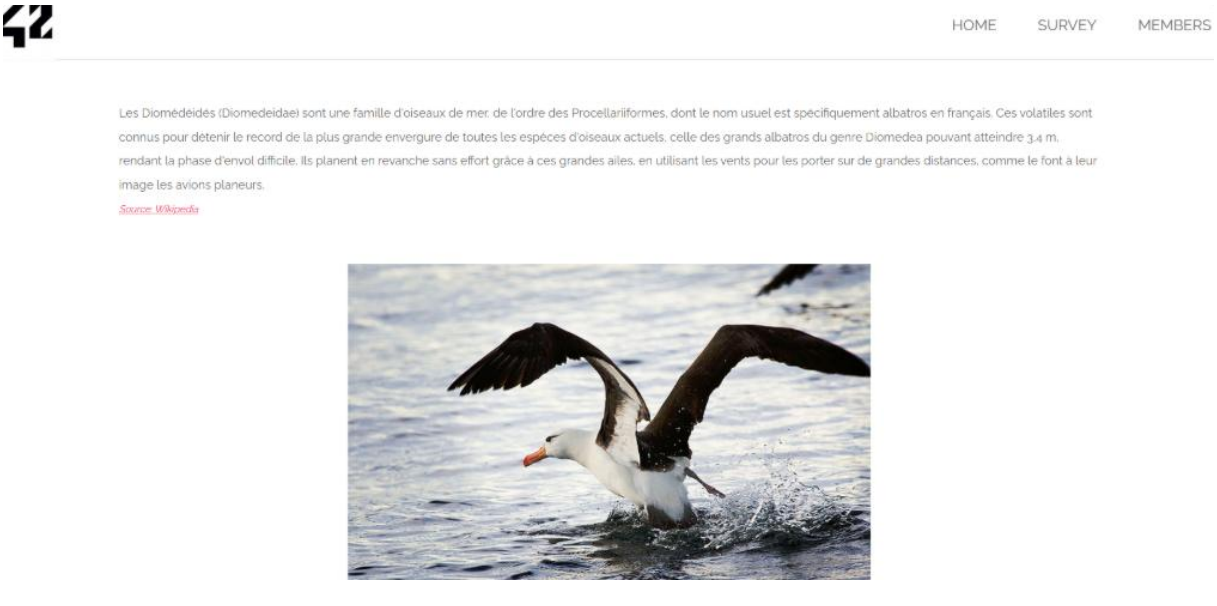
Validation de la destination : Le serveur doit uniquement autoriser une liste blanche de domaines de confiance (ex: facebook.com, twitter.com).

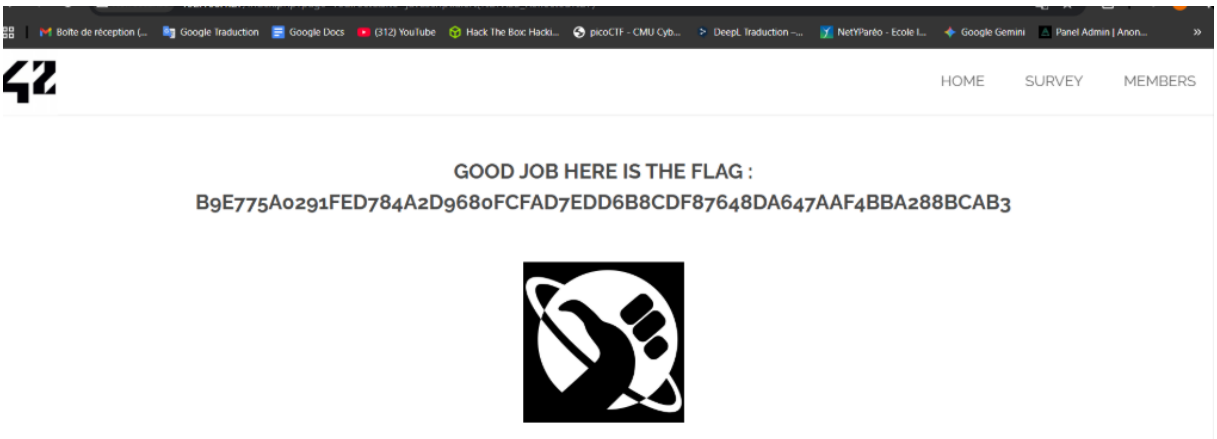
Filtrage du protocole : Interdire l'utilisation du protocole javascript: dans les paramètres de redirection.

Nettoyage des sorties : Utiliser la fonction PHP htmlspecialchars() pour neutraliser toute tentative d'injection de scripts avant l'affichage ou le traitement du paramètre.

Capture d’écran


DevTools is now available in French
Don't show again
Always match Chrome's language
Switch DevTools to French
Elements
Console
Sources
Network
Performance
Memory
Application
Privacy and security
Lighthouse
Recorder
Sorry
© BornToSec


HOME
SURVEY
MEMBERS
Les Diomédéidés (Diomedeidae) sont une famille d'oiseaux de mer de l'ordre des Procellariiformes, dont le nom usuel est spécifiquement albatros en français. Ces volatiles sont connus pour détenir le record de la plus grande envergure de toutes les espèces d'oiseaux actuels, celle des grands albatros du genre Diomedea pouvant atteindre 3,4 m, rendant la phase d'envol difficile. Ils planent en revanche sans effort grâce à ces grandes ailes, en utilisant les vents pour les porter sur de grandes distances, comme le font à leur image les avions planeurs.
Source: Wikipedia


HOME
SURVEY
MEMBERS
GOOD JOB HERE IS THE FLAG :
B9E775A0291FED784A2D9680FCFAD7EDD6B8CDF87648DA647AAF4BBA288BCAB3