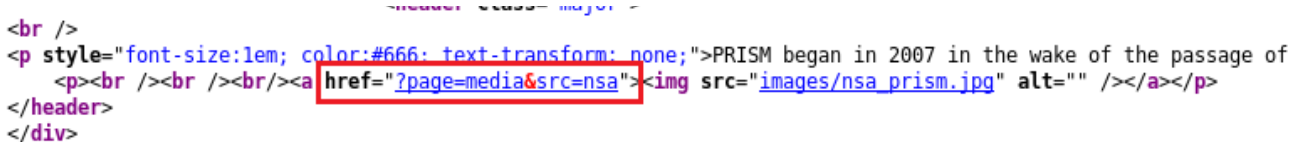
XSS via OBJECT tag

EXPLICATION

En examinant le code source de la page **index.php**, on aperçoit l'URL suivante pour l'une des images :



N'ayant pas encore examiné cette page, on va y faire un tour. On voit que lorsque le paramètre **nsa** est donné à **src**, une image s'affiche bien. Il est intéressant de remarquer que l'affichage de l'image passe par une balise HTML **OBJECT** :

Lorsqu'on essaie de manipuler le paramètre d'URL **src**, on s'aperçoit qu'aucune image n'est affichée, mais que notre input utilisateur est reflété dans l'attribut **data** du tag **OBJECT** :

En cherchant un peu, on trouve qu'il est possible d'exécuter du Javascript par le biais de l'attribut **data** d'un tag **OBJECT** :
https://html5sec.org/

En suivant les indications du lien ci-dessus, on tente l'URL suivante :

```
http://192.168.1.20/?
page=media&src=data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==
```

La valeur encodée en base64 correspond à `<script>alert(1)</script>`.
Ce qui permet bien de récupérer un **flag**.

RESSOURCES

Un script python permet d'envoyer la requête avec l'URL craftée, et d'afficher la page contenant le flag.

MITIGATION

> Never trust user input.
> En fonction du framework utilisé, il existe pas mal de XSS sanitizers permettant d'implémenter des politiques de validation de l'input inséré dans les balises HTML.