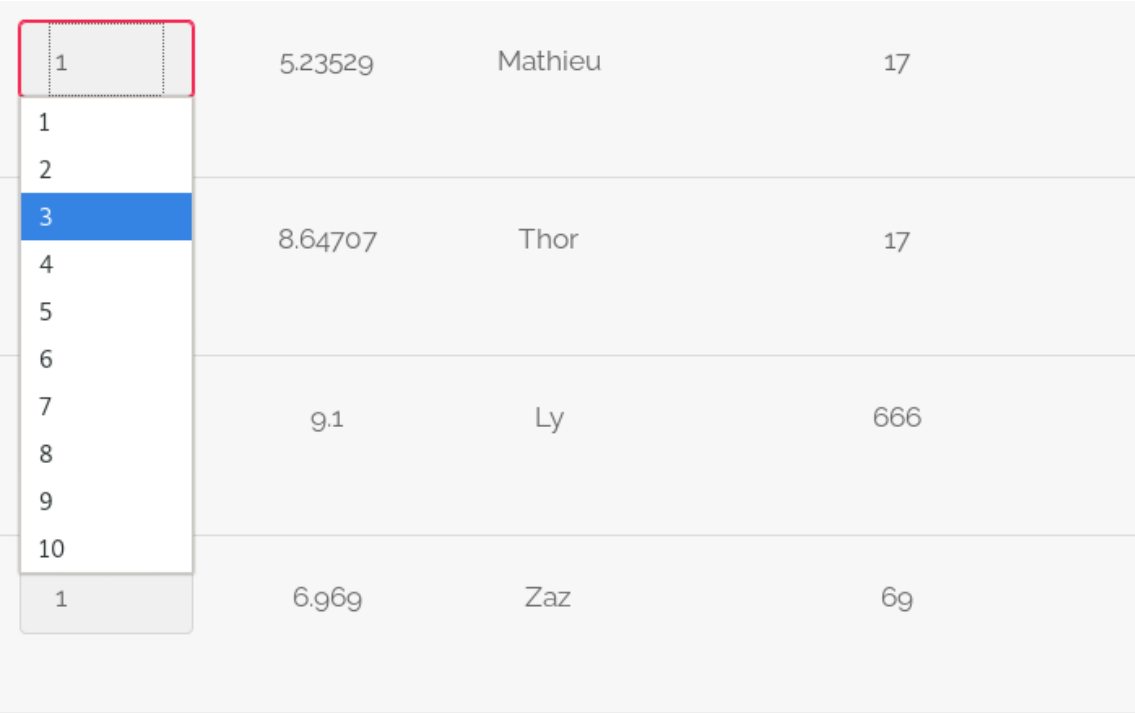
Manipulating the survey input

EXPLICATION

Comme relevé en phase d'énumération (voir ENUMERATION – partie 3), une page **survey** est disponible sur l'application. Il s'agit d'une liste de noms, que nous pouvons noter grâce à un petit menu déroulant, de 1 à 10 ; ce qui influe les colonnes **average** (moyenne des notes) et **nb of votes** :



Lorsqu'on clique sur l'un des chiffres pour noter une personne, la requête envoyée a cette forme :

```
POST /?page=survey HTTP/1.1
Host: 192.168.1.37
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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: http://192.168.1.37/?page=survey
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
Cookie: I_am_admin=68934a3e9455fa72420237eb05902327
Connection: close
Upgrade-Insecure-Requests: 1

sujet=2&valeur=3
```

On essaie alors simplement de remplacer "valeur" (un chiffre normalement entre 1 et 10) par un input arbitrairement important, comme 100 000. La requête est considérée comme valide, le vote avec la note 100 000 est pris en compte, ce qui augmente bien sûr excessivement la colonne "Average" de la personne pour laquelle on vient de voter.

Cette manipulation d'input est possible car aucune validation n'est effectuée en backend de l'input utilisateur, qui n'est naïvement que régulé par le formulaire en front.

L'envoi de la requête modifiée nous révèle un **flag**.

RESSOURCES

Un script python permet d'automatiser l'envoi de la requête modifiée, et révèle la page sur laquelle le flag est affiché.

MITIGATION

> Ne pas se fier à des mécanismes de front-end pour la validation du *user-input*. Valider et réguler le user-input directement à réception en back-end.