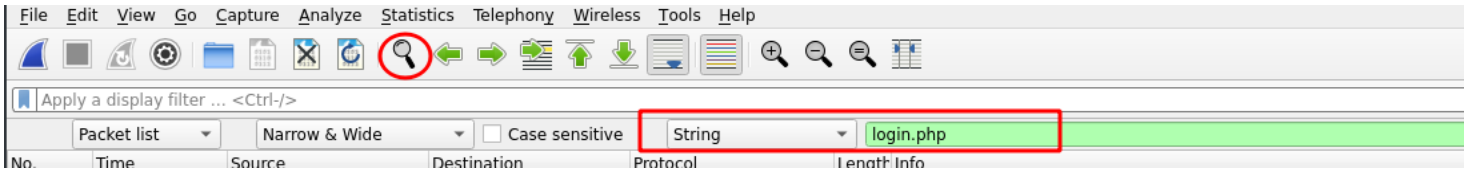
Write up - Easy Mr Tobor

Si on a déjà fait la machine Mr Robot, le CTF est de suite plus simple .

Donc tout d'abord si nous voulons nous connecter et sachant qu'il faut chercher un mot de passe de connexion nous pouvons essayer de trouver une page ressemblant à un formulaire de connexion du style login.php...



Nous pouvons constater une suite succesive de formulaire... S'agirait'il d'un brute force ?

La réponse est quasiment toujours la même pour les requêtes

```
<body class="login login-action-login wp-core-ui  locale-en-us">
<div id="login">
        <h1><a href="https://wordpress.org/" title="Powered by WordPress" tabindex="-1">user&#039;s Blog!</a></h1>
<div id="login_error"><strong>ERROR</strong>: The password you entered for the username <strong>elliot</strong> is incorrect. <a href="http://172.16.1.131/wp-login.php?action=lostpassword">Lost your password?</a><br/>

e="loginform" id="loginform" action="http://172.16.1.131/wp-login.php" method="post">
```

Mais la dernière requête, ne renvoie pas ça !
on peut filtrer sur le **tcp.stream eq 44**

```
POST /wp-login.php HTTP/1.1
Host: 172.16.1.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.1.131/wp-login.php?loggedout=true
Content-Type: application/x-www-form-urlencoded
Content-Length: 106
Origin: http://172.16.1.131
DNT: 1
Connection: close
Cookie: s_cc=true; s_fid=1205055F9F4AECE9-02754C52DF63F926; s_nr=1670748693600; s_sq=%5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+c
Upgrade-Insecure-Requests: 1

log=elliot&pwd=p4ssw0rd!&wp-submit=Log+In&redirect_to=http%3A%2F%2F172.16.1.131%2Fwp-admin%2F&testcookie=1HTTP/1.1 302 Found
Date: Sun, 11 Dec 2022 01:47:13 GMT
Server: Apache
X-Powered-By: PHP/5.5.29
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
Set-Cookie: wordpress_a18dab227d7d3edf2847c74402d3fd9a=elliot%7C1670896034%7CC5TX6F9k9coPyiosCr8bKIsm7f6byn2Pr7uXz8YZqqH%7Cb967992c83
Set-Cookie: wordpress_a18dab227d7d3edf2847c74402d3fd9a=elliot%7C1670896034%7CC5TX6F9k9coPyiosCr8bKIsm7f6byn2Pr7uXz8YZqqH%7Cb967992c83
Set-Cookie: wordpress_logged_in_a18dab227d7d3edf2847c74402d3fd9a=elliot%7C1670896034%7CC5TX6F9k9coPyiosCr8bKIsm7f6byn2Pr7uXz8YZqqH%7C
Location: http://172.16.1.131/wp-admin/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```