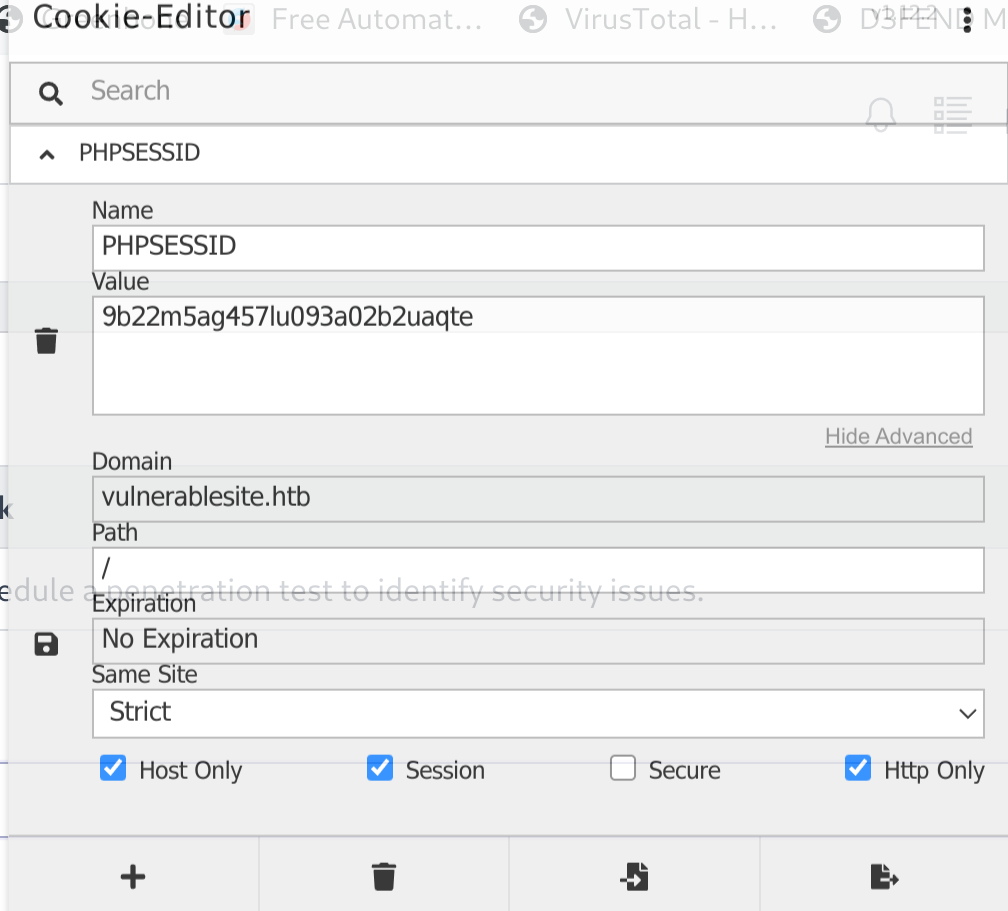
## SameSite = Strict bypass (Example)

In a HTB challenge we have found that SameSite=Strict

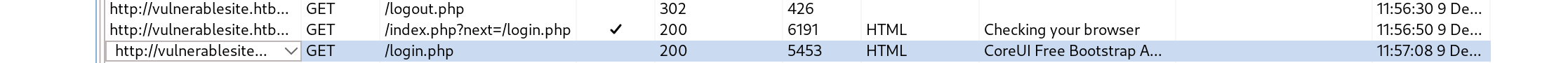


This mean the cookie will not be passed in any cross-origin request (if we will pass our code from an external exploit server it will fail as soon the victim will get it, because will not pass the cookie and login to portal will be lost).

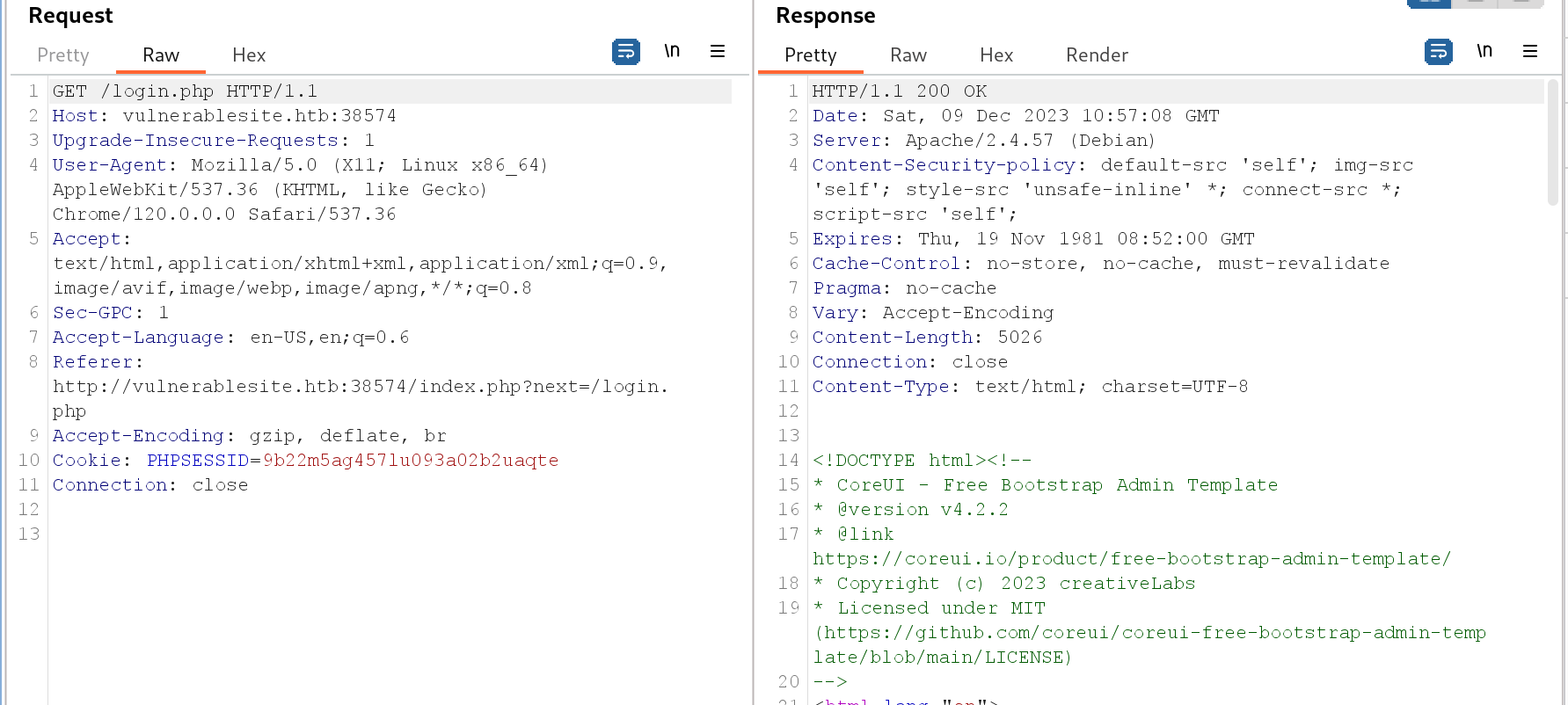
# How to Bypass?

To bypass this we need to find a vulnerable endpoint that perform a HTTP 2xx client redirect (aka via meta tag in HTML) where defacto the browser will perform the redirect without doing a page refresh.

In the challenge we found out that as soon we logout(request performed to /logout.php) the website perform a HTTP 3xx redirect aka Serverside but next a index.php is doing a HTTP 2xx (client redirect) back to /login.php:



As you see here after the index.php calls the /login.php it is performed via HTTP 200:



Now we know that is enought to promote our user by just sending a GET request to /users.php?userid=3

Then taking into consideration what we learned from HTB Accademy we could send the following JS to the victim:

***<script>***

***document.location = "http://vulnerablesite.htb/index.php?next=/users.php%3Fuserid=3";***

***</script>***

Here basically we are using the vulnerability in index.php to call users.php via ClientRedirect(HTTP 2xx) and already giving the parameters to perform a Promoting: users.php?userid=3 is users.php%3Fuserid=3 with HTML encoding.