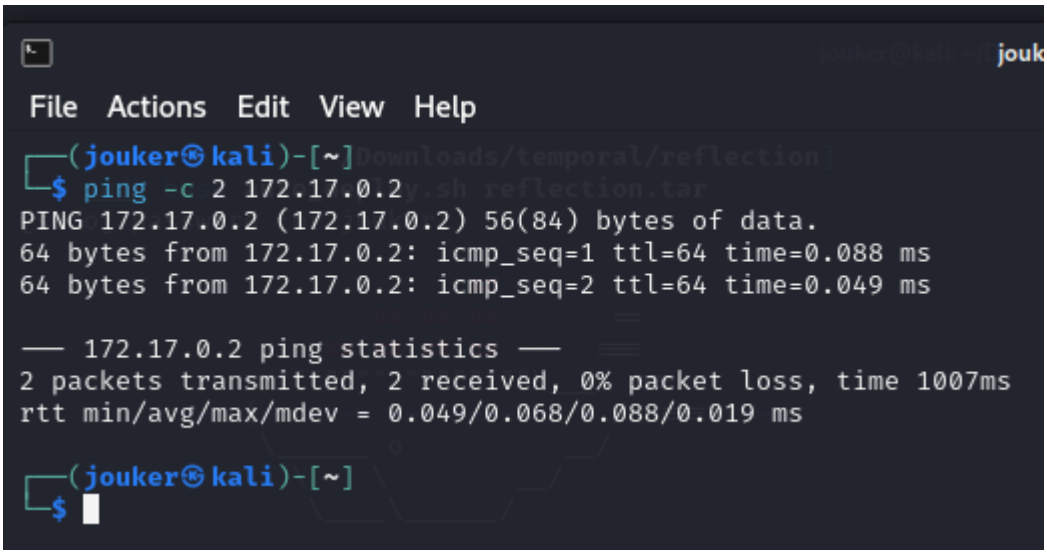
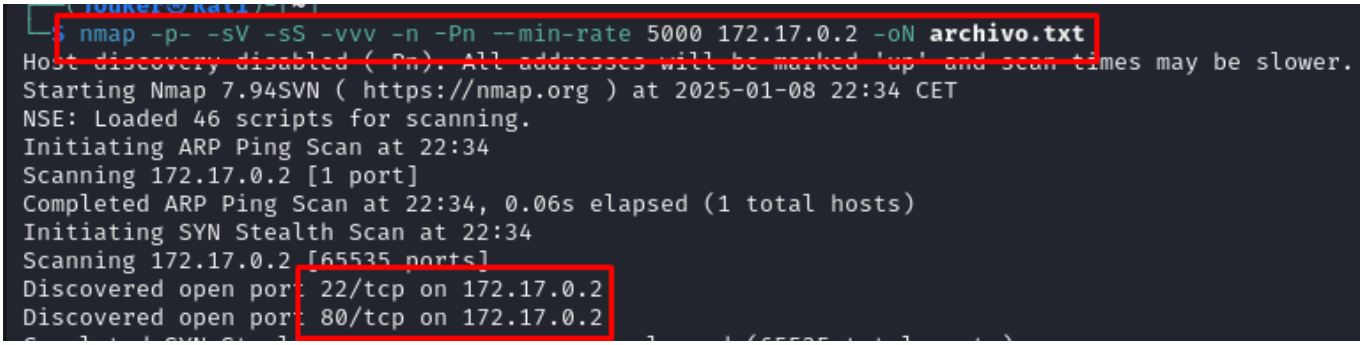
Encendemos la máquina

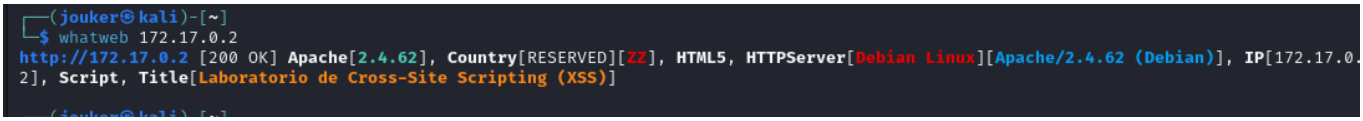
Ping activado con la victima y verificamos conectividad.



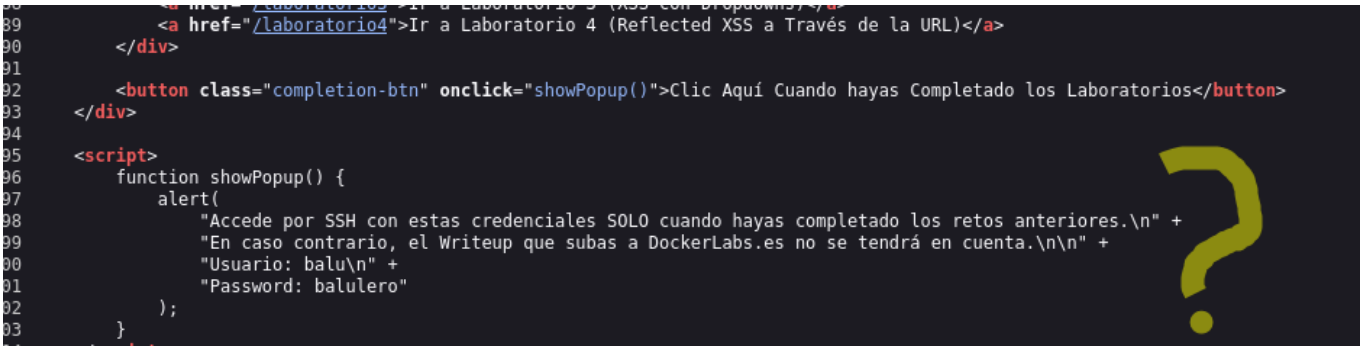
Nmap marca abiertos los puertos 22 y 80



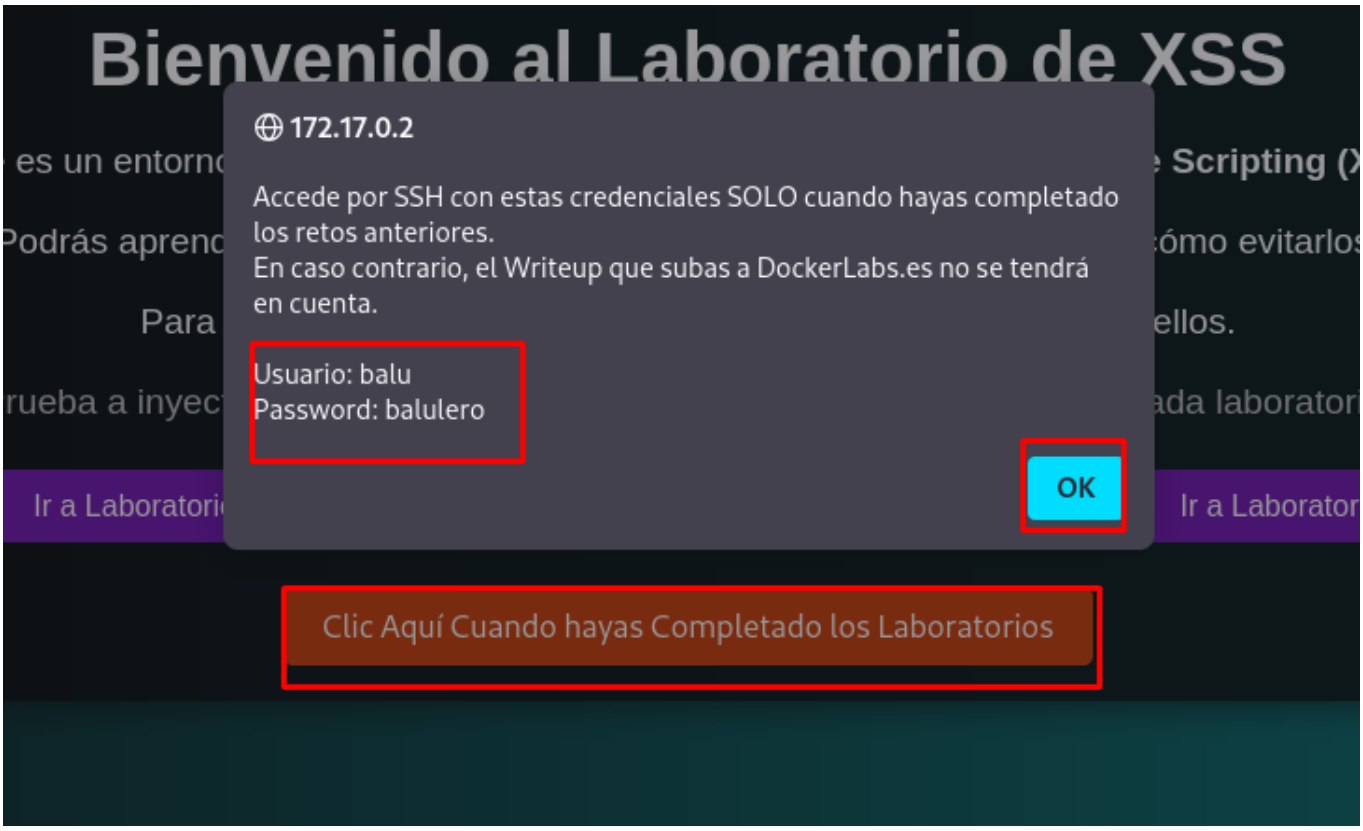
Laboratorio de XSS, tan sencillo nos dicen la vulnerabilidad a tratar?



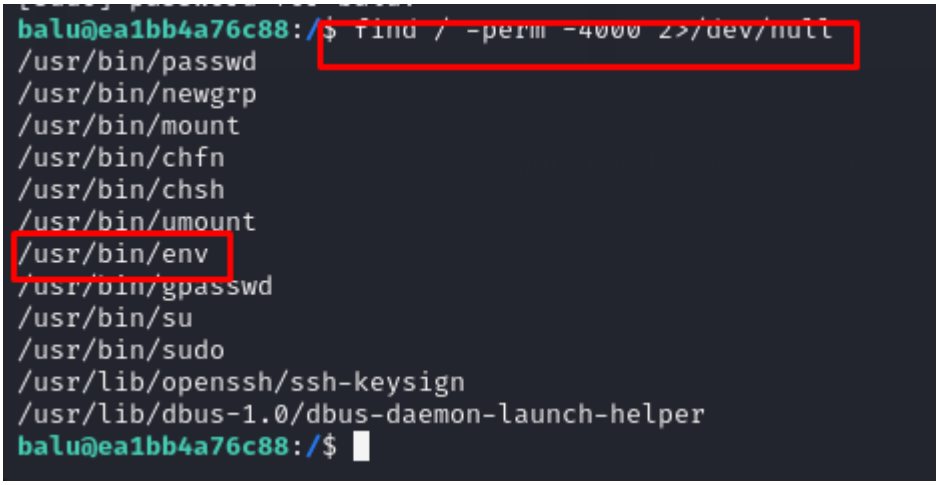
Al parecer las credenciales estan puestas tal cual dentro del código fuente de la 172.17.0.2



Tampoco estaban escondidas, el pop up lo obtenemos tan pronto como le demos a "CLIC AQUI..."

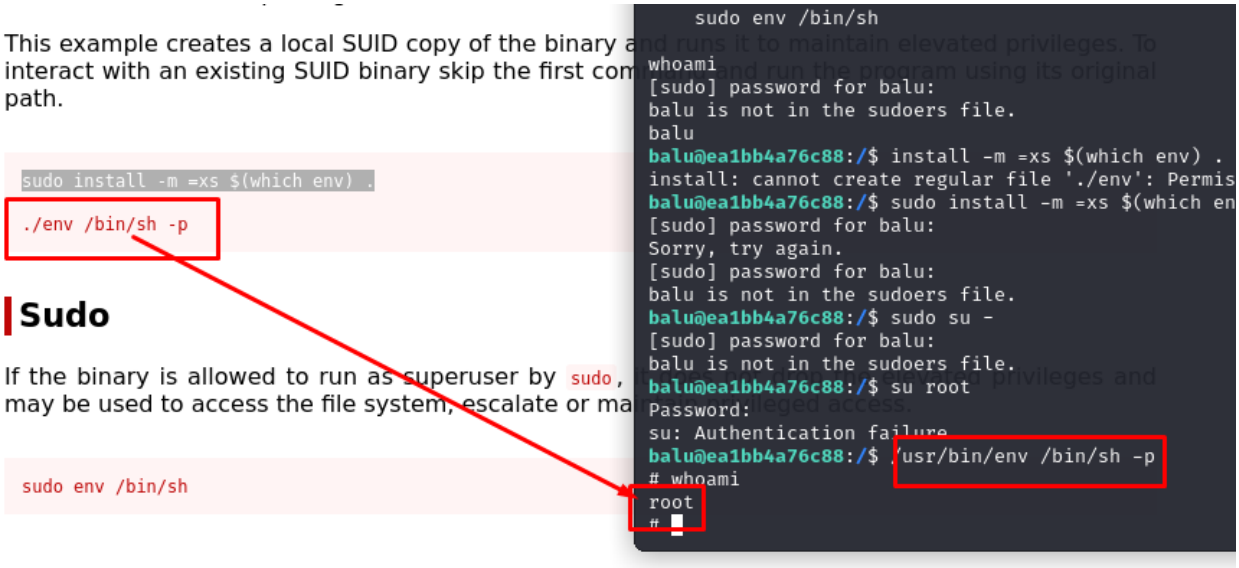


Por lo pronto voy a vulnerar primero la máquina y después me ocuparé de los laboratorios XSS internos.
Entramos con ssh y las credenciales y vemos que la escalada de privilegios es mediante find y el habitual env para escalar privilegios, si buscamos en gtfobins veremos que hay que ejecutar esta siguiente comanda



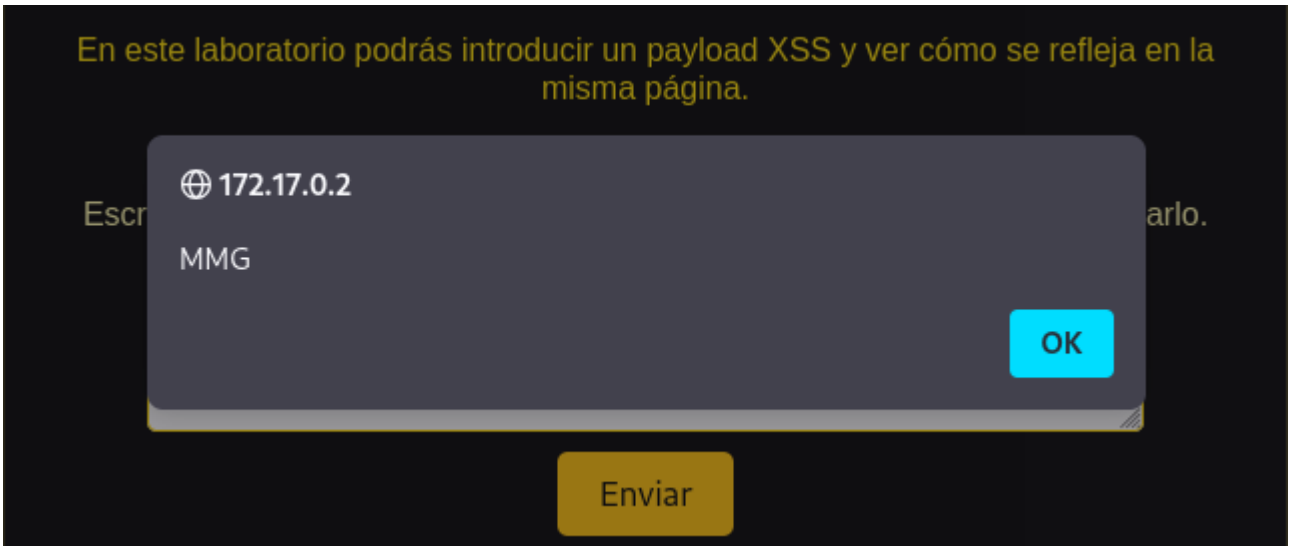
Por mucho que me hubiese gustado decir que he terminado la máquina tan solo he realizado la parte fácil, ahora me toca de verdad ponerme con el objetivo de esta máquina que es completar los

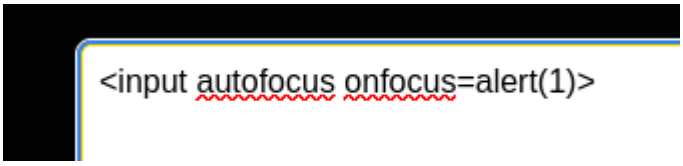
laboratorios.



Primer LAB:

El primero no ha funcionado, adjunto captura del segundo que si que ha funcionado, con su respectivo payload

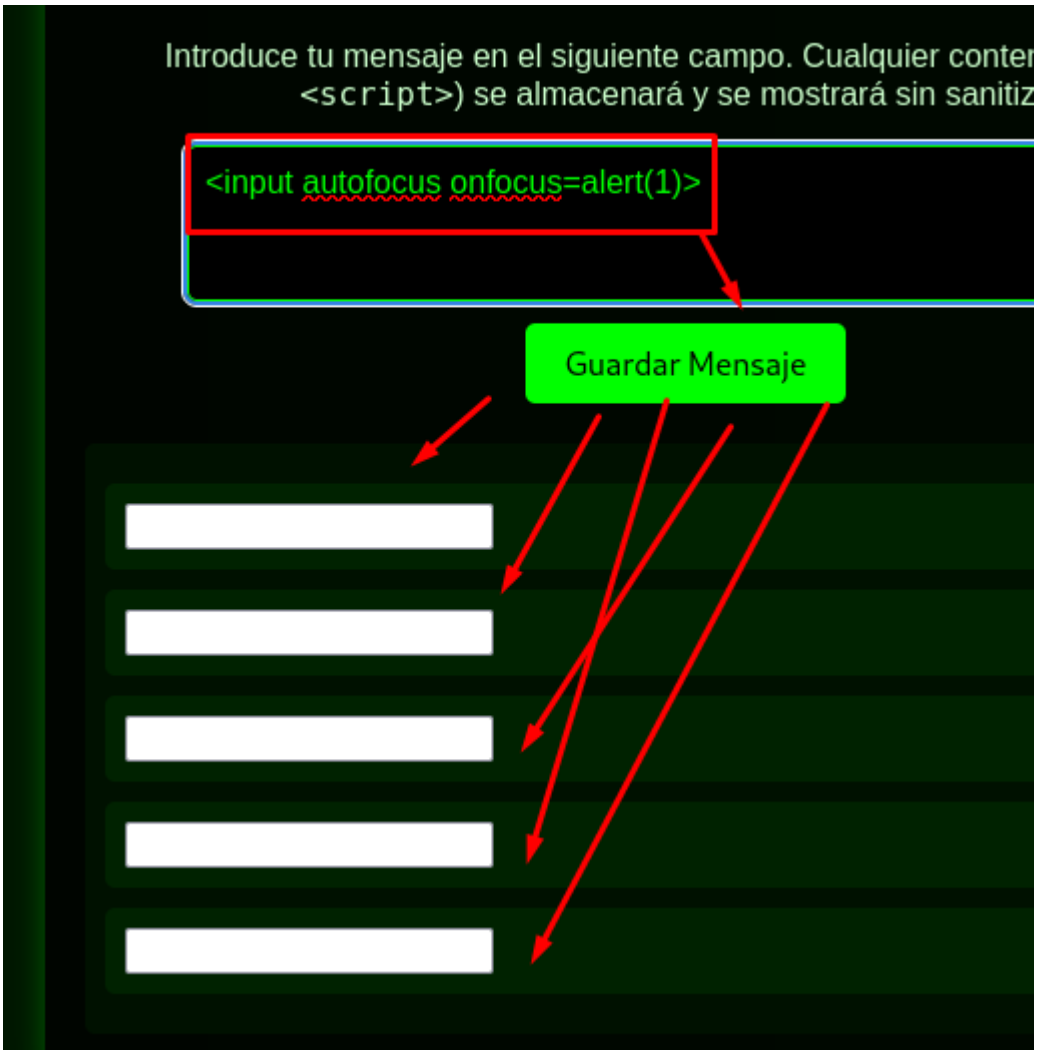

En este laboratorio podrás introducir un payload XSS y ver cómo se refleja en la misma página.
Escr
arlo.
172.17.0.2
MMG
OK
Enviar

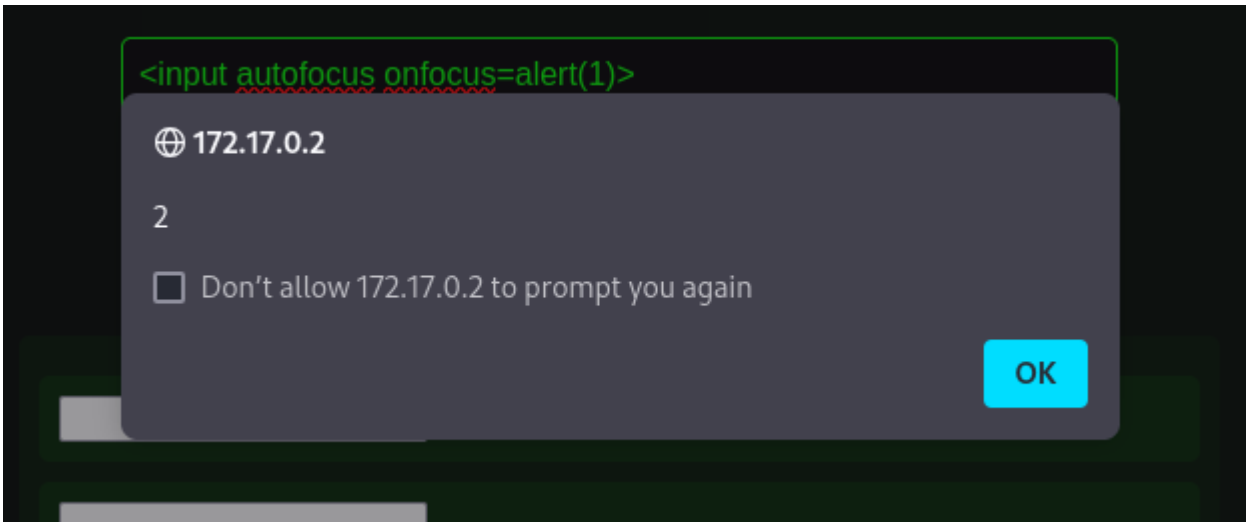

<input autofocus onfocus=alert(1)>


Laboratorio de XSS Reflejado
En este laboratorio podrás introducir un payload XSS y ver cómo se refleja en la misma página.
Esc
arlo.
172.17.0.2
1
OK
Enviar
ipt>alert('XSS')ipt>

Lab 2:

Al hacer clic a guardar mensaje en vez de mostrartelo directamente cuando lo ejecutas, lo almacena. Cuando lo almacena y le haces clic se activa el payload XSS



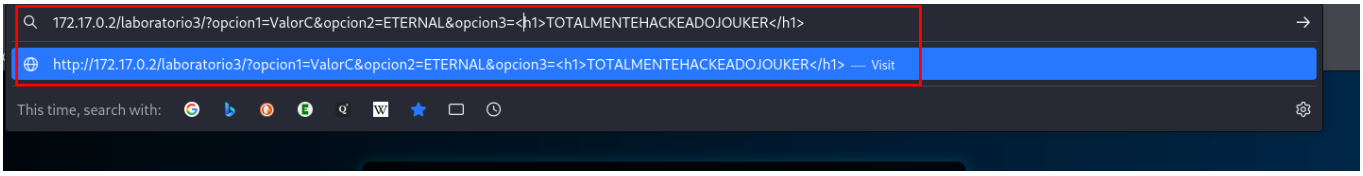


Máquina 3:

En esta máquina nos manda a sacar de paseo el burpsuite, y nos comenta que intentemos el XSS intentado interceptarlo con el burpsuite, pero al parecer por lo que veo realmente no hace falta

Esta es la imagen del laboratorio de forma normal:

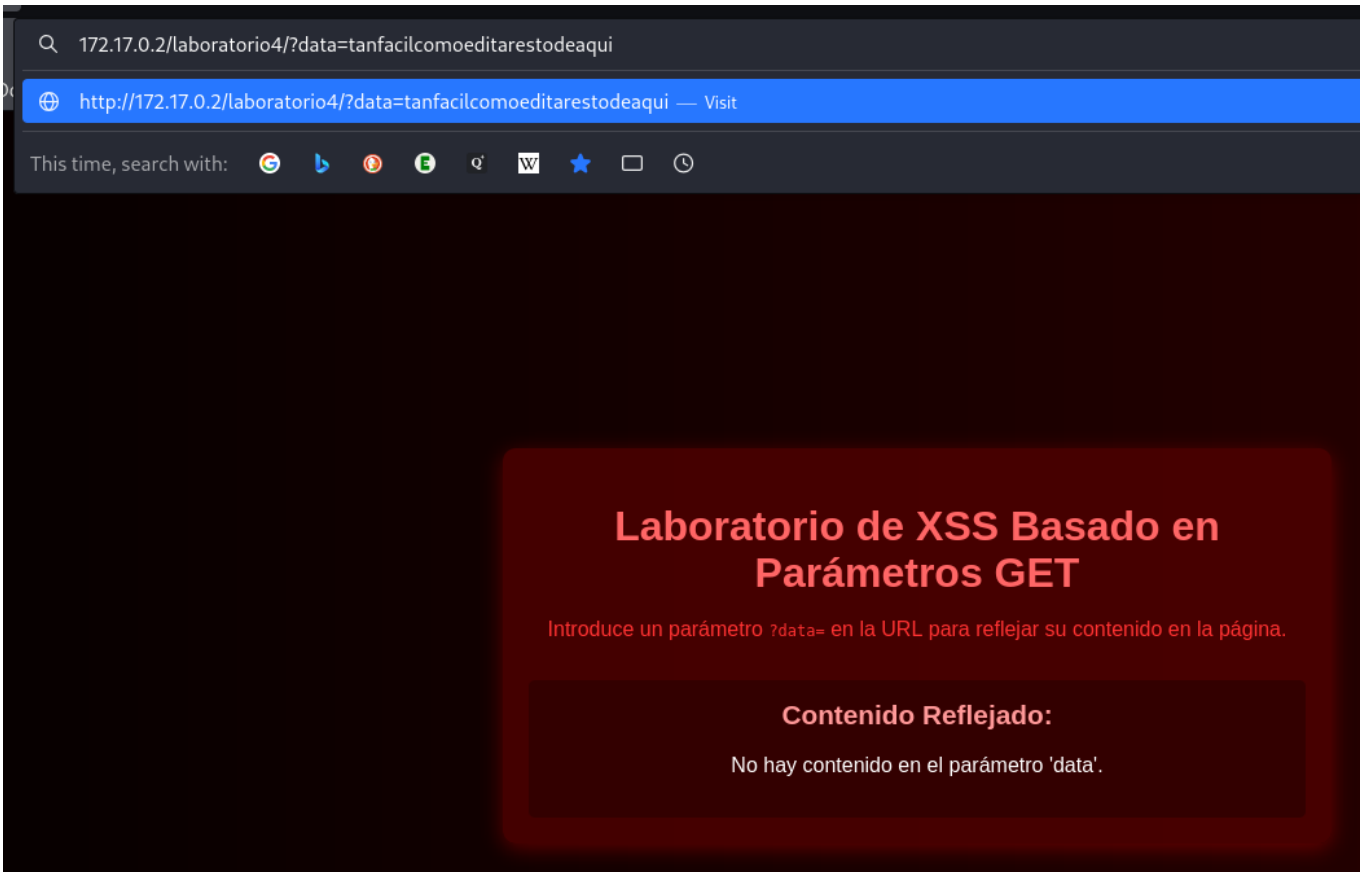
Pero el hecho de que este editado para que podamos modificarlo por burpsuite, también lo ha habilitado que se pueda modificar desde la URL.



Pasamos al lab 4 y supuestamente el más difícil.

Lab 4:

Al parecer el enunciado ya nos da la pista de poner un ?data= en la URL sin necesidad de fuzzing para inyectar el codigo que nosotros consideremos necesario, voy a probar si es tan fácil como parece



Efectivamente era tan fácil como te lo marcaba la propia máquina, no requería de dificultad adicional. Muy buena máquina para

practicas el XSS ya que no es algo que veamos de forma habitual en los CTF y siempre viene bien practicarlo