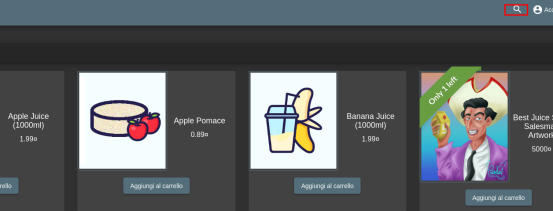
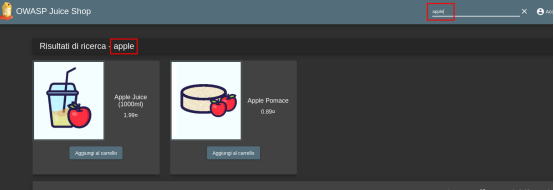
**XSS**

Reflected:

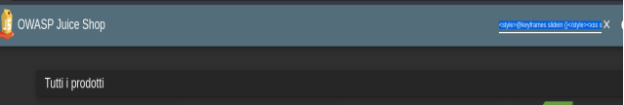
Nella pagina principale abbiamo la possibilità di fare una ricerca:



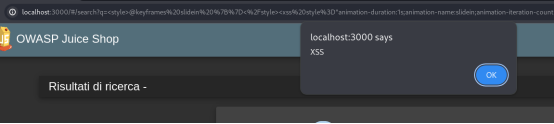
Se scriviamo qualcosa, ci viene riportato a schermo esattamente cosa abbiamo scritto:



Dopo vari tentativi, ho scoperto che inserendo un determinato comando, abbiamo una XSS Reflected:

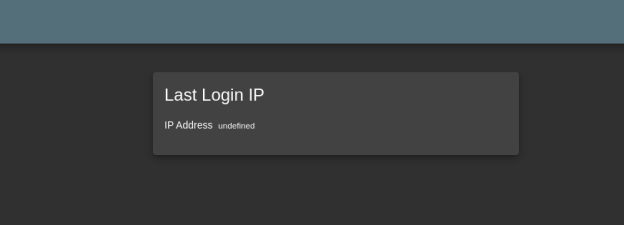
  
  
<xss onafterscriptexecute=alert(1)><script>1</script>

*localhost:3000/#/search?q=<style>@keyframes x{}<%2Fstyle><xss style%3D"animation-name:x" onanimationend%3D"alert('XSS')"><%2Fxss>*

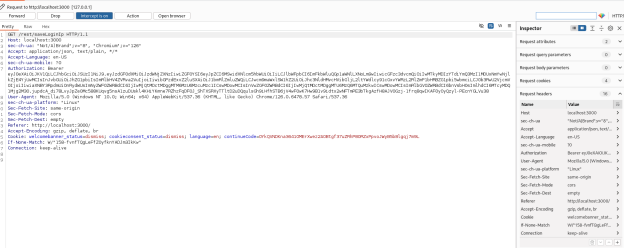


Stored:

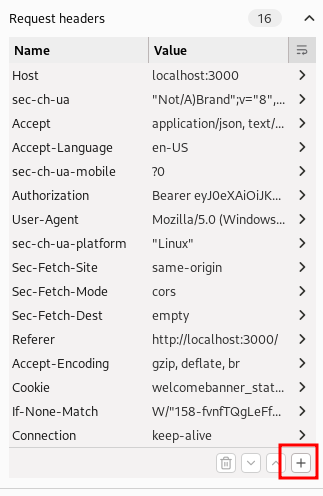
E’ possibile effettuare una Stored XSS nella pagina del “last login IP” di un qualsiasi utente tramite l'uso dell'header “True Client IP”. Questa pagina mostra l’IP da dove si è collegato l'utente e viene “Catturato” tramite l’header True Client IP che però non è sanificato.

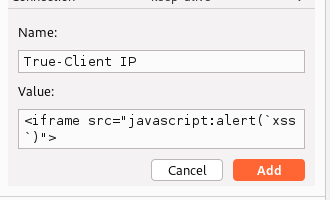


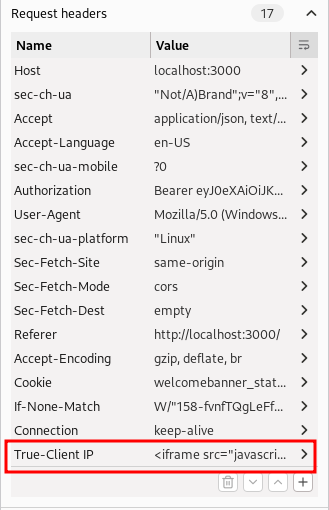
L’ip viene memorizzato quando l’utente effettua il logout, per perfezionare questa XSS dobbiamo intercettare la richiesta di logout con burp e aggiungere l’header in questione:

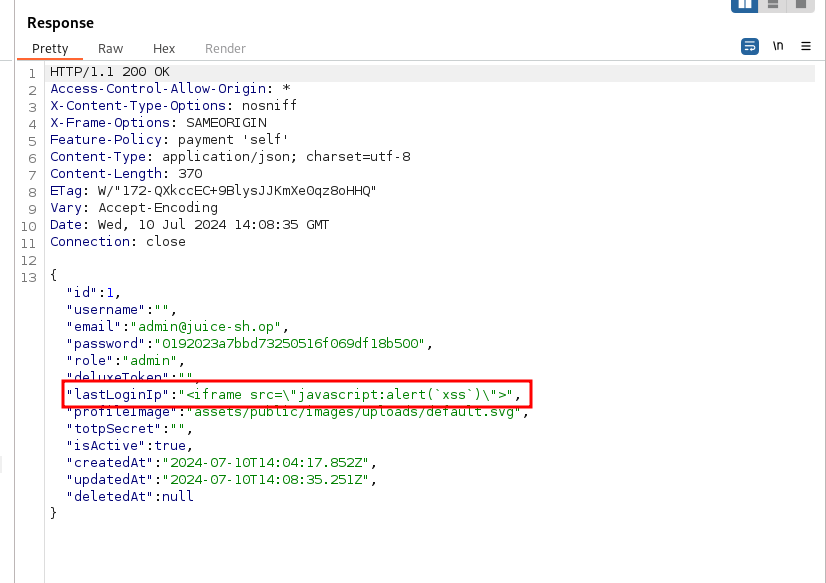


Ora aggiungiamo l’header alla logout tramite il menu request headers e cliccando sul simbolo "+”:

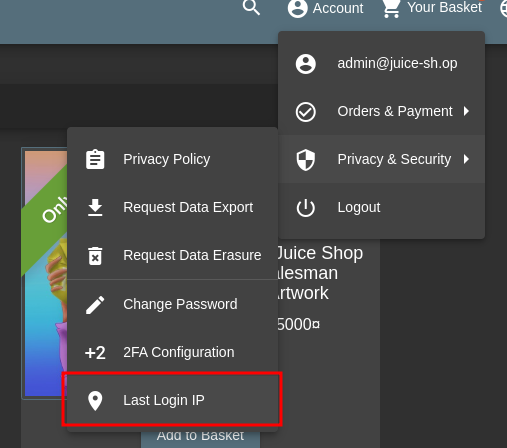


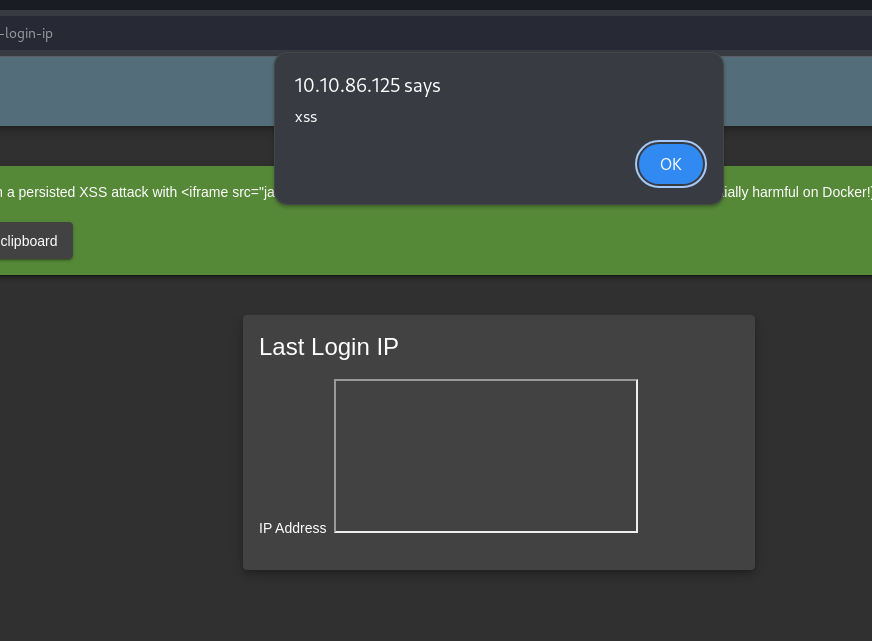




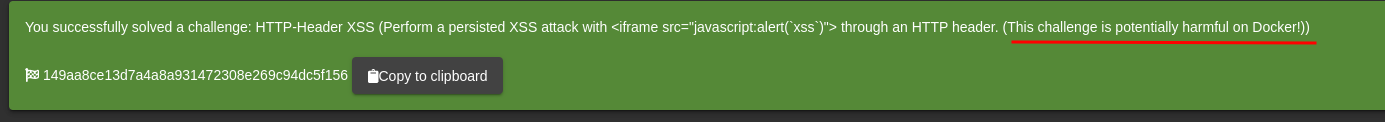


A questo punto possiamo fare il forward della richiesta e ed effettuare nuovamente la login (io sto usando l’utente admin) :





NB: Questa XSS su docker non funziona, ed essendo una challenge mi faceva un pò strano. Infatti, l'ho eseguita con il sito [tryhackme.com](https://www.tryhackme.com) attraverso la Virtual Machine e una volta risolta mi ha dato il seguente messaggio:

Probabilmente in docker è stata disattivata di proposito.