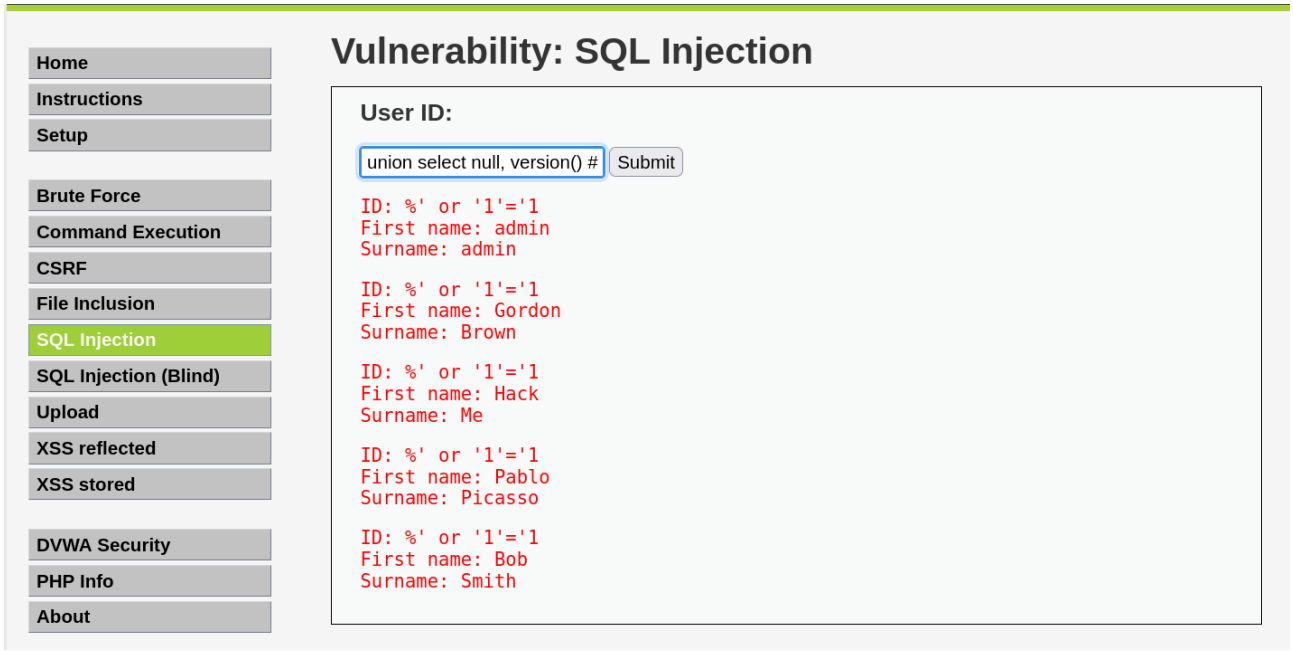
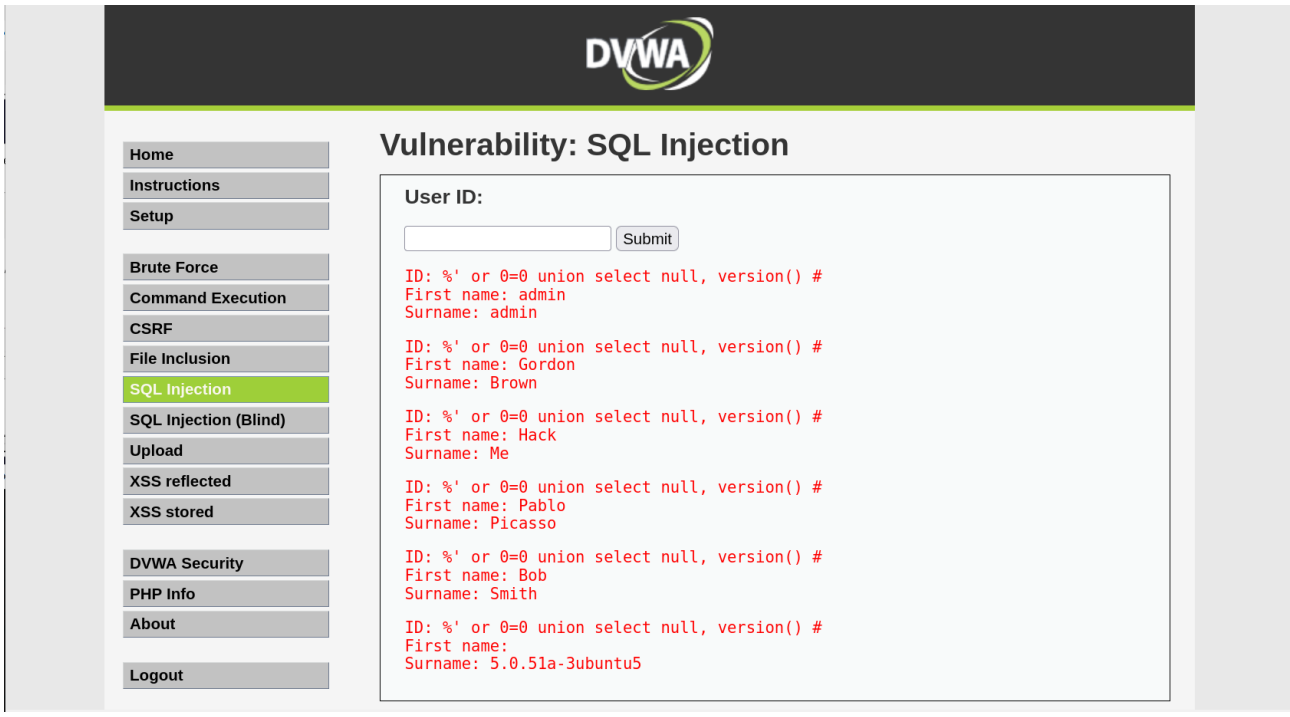
Relazione S2L2

Lo scopo di questo esercizio è quello di provare l'SQL query injection e l'XSS reflected sul sito di dvwa.

Con l'sql injection sono riuscito ad ottenere i dati delle tabelle del database:





Le due queries che abbiamo eseguito sono:

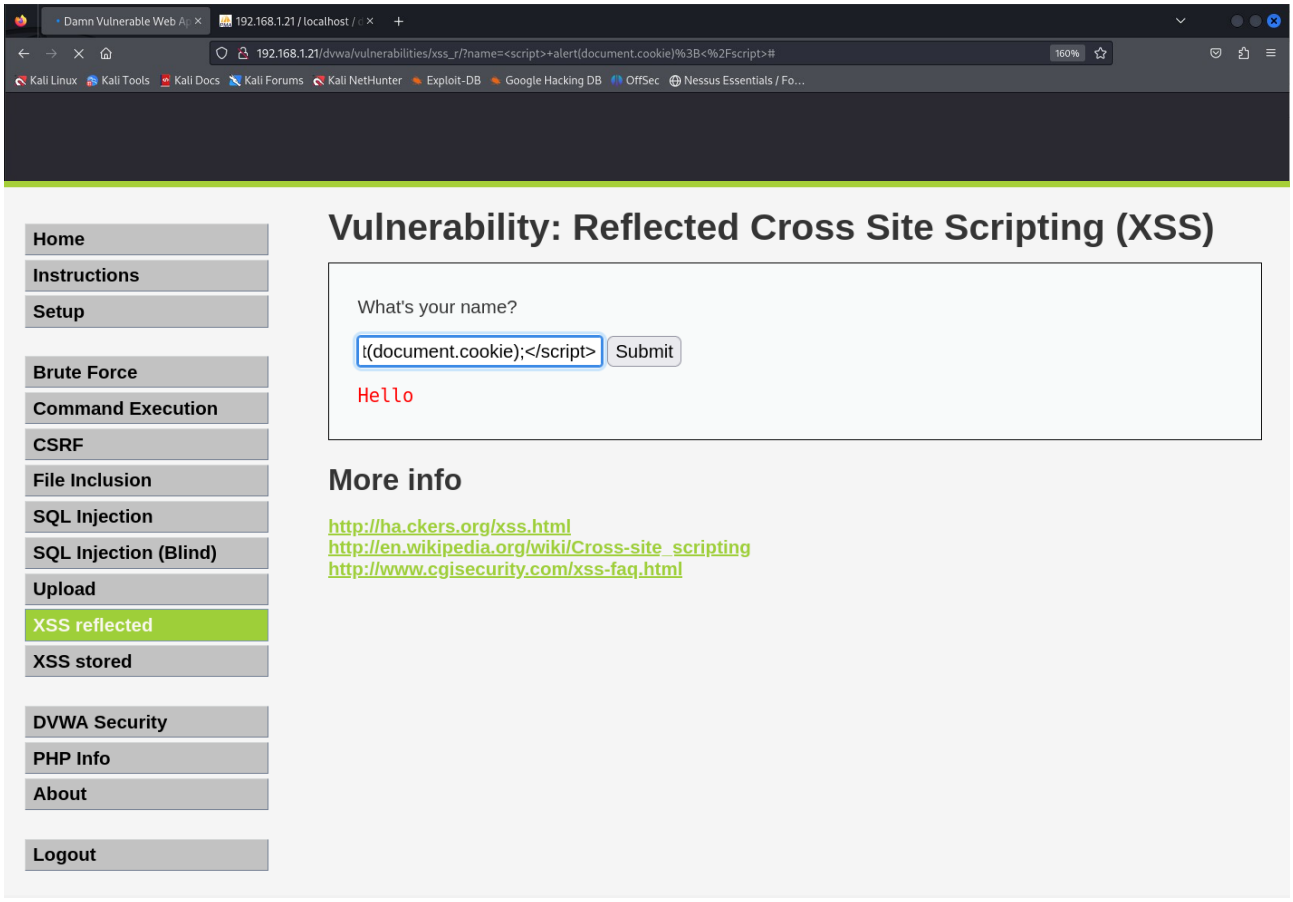
%' or '1'='1

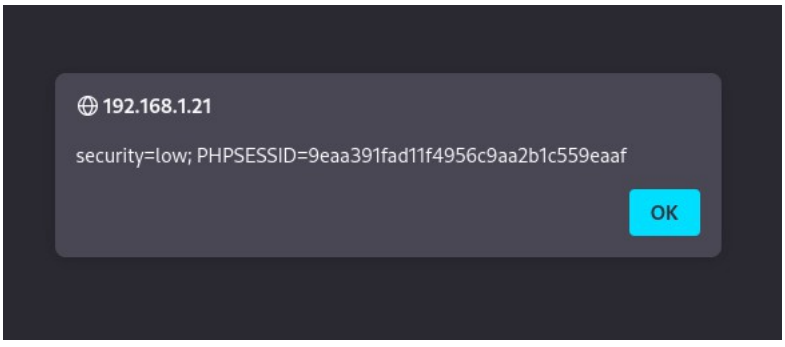
%' or 0=0 union select null, version() #

La prima dà come parametro % che non corrisponde a nulla e mette la condizione OR per dire che

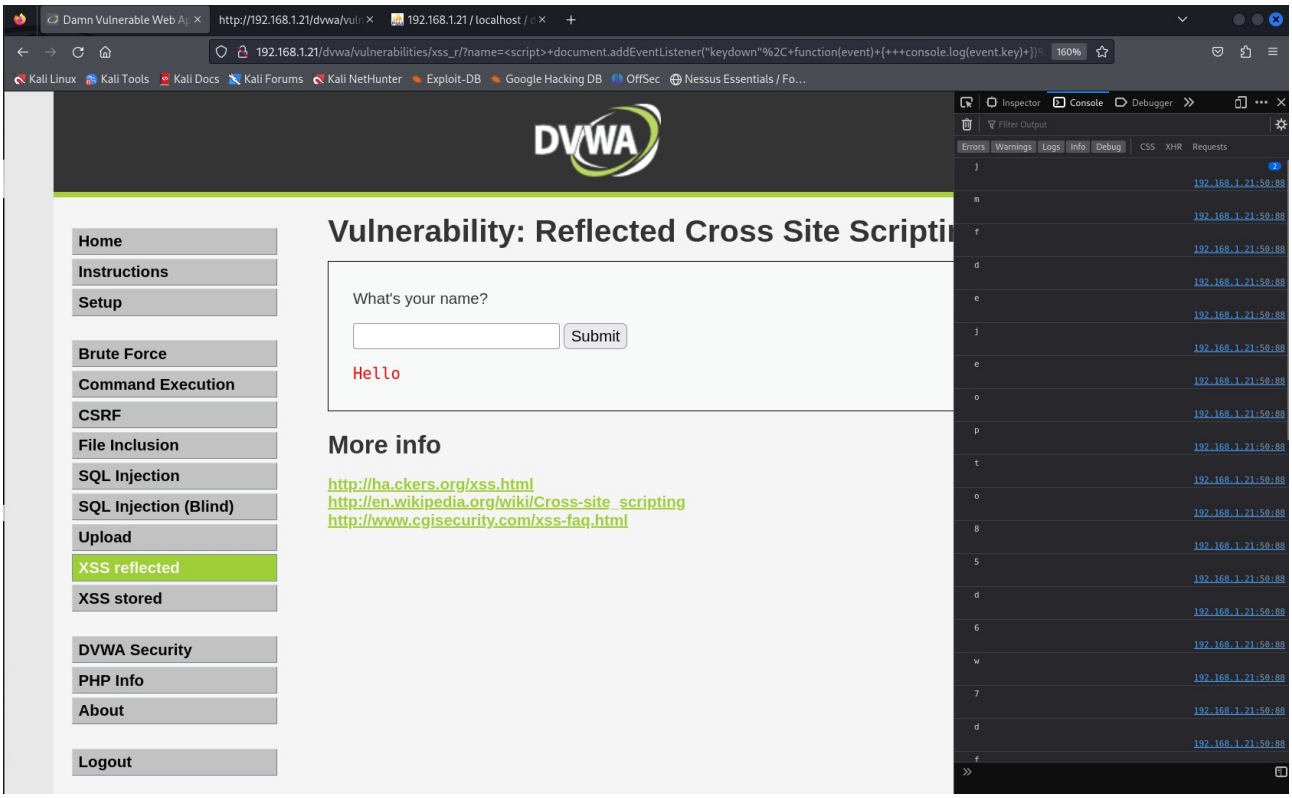
se non trova nulla con quello allora deve confrontare 1 con 1 che sarà sempre vero. In questo caso quindi avremo in output tutta la lista dei records della tabella users.
La seconda query invece fa la stessa cosa della prima e in più usa l'operatore UNION per effettuare un'altra query dove seleziona null e la versione del database. In questo modo quando finiranno i records verrà mostrata la versione.

Per quanto riguarda l'XSS reflected invece ho fatto qualche prova ed ho ottenuto i seguenti risultati:





Qui ad esempio mostriamo i cookie con un alert




```
<script>
document.addEventListener("keydown", function(event) {
  console.log(event.key)
});
</script>
```

Mentre qui invece con un semplice script vediamo in console tutti i tasti della tastiera che l'utente preme mentre rimane sulla finestra.

Davide Lecci