TECNICHE DI EXPLOIT CON #XSS REFLECTED E #SQL:

#DVWA + KALI LINUX

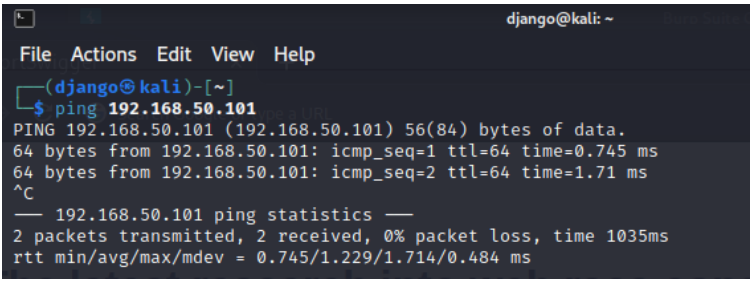
TRACCIA:
CONFIGURATE IL VOSTRO LABORATORIO VIRTUALE PER RAGGIUNGERE LA DVWA DALLA MACCHINA KALI LINUX (L'ATTACCANTE). ASSICURATEVI CHE CI SIA COMUNICAZIONE TRA LE DUE MACCHINE CON IL COMANDO PING. RAGGIUNGETE LA DVWA E SETTATE IL LIVELLO DI SICUREZZA A «LOW».
SCEGLIETE UNA DELLE VULNERABILITÀ XSS ED UNA DELLE VULNERABILITÀ SQL INJECTION: LO SCOPO DEL LABORATORIO È SFRUTTARE CON SUCCESSO LE VULNERABILITÀ CON LE TECNICHE VISTE NELLA LEZIONE TEORICA. LA SOLUZIONE RIPORTA L'APPROCCIO UTILIZZATO PER LE SEGUENTI VULNERABILITÀ:
-XSS REFLECTED
-SQL INJECTION (NON BLIND)

CONSEGNA:

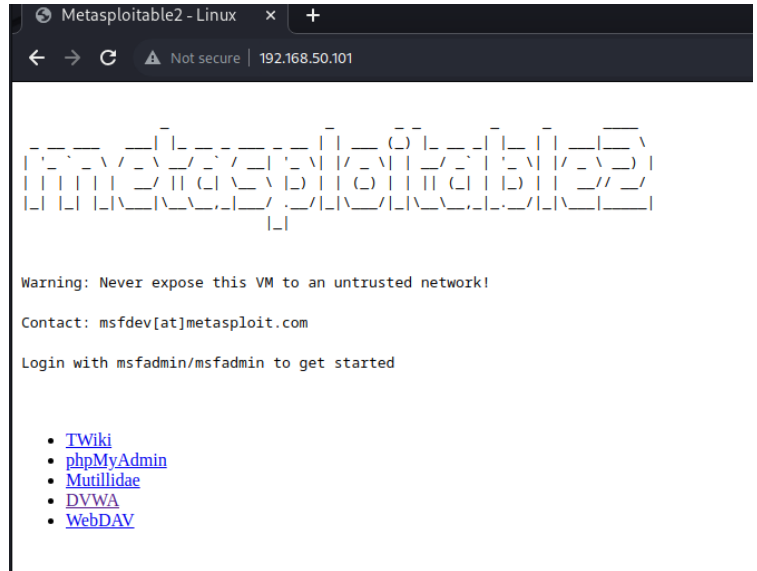
XSS
1. ESEMPI BASE DI XSS REFLECTED, I (IL CORSIVO DI HTML), ALERT (DI JAVASCRIPT), ECC
2. COOKIE (RECUPERO IL COOKIE), WEBSERVER ECC.

SQL
1. CONTROLLO DI INJECTION
2. ESEMPI
3. UNION SCREENSHOT/SPIEGAZIONE IN UN REPORT DI PDF

AL FINE DELL'ESERCIZIO È SUFFICIENTE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SULLA STESSA RETE, LASCIO QUINDI L'IP DI METASPLOITABLE SIA 192.168.50.101, MENTRE QUELLO DI KALI LINUX RESTERÀ 192.168.50.100. E FACCIO UN PING DI PROVA DA KALI.

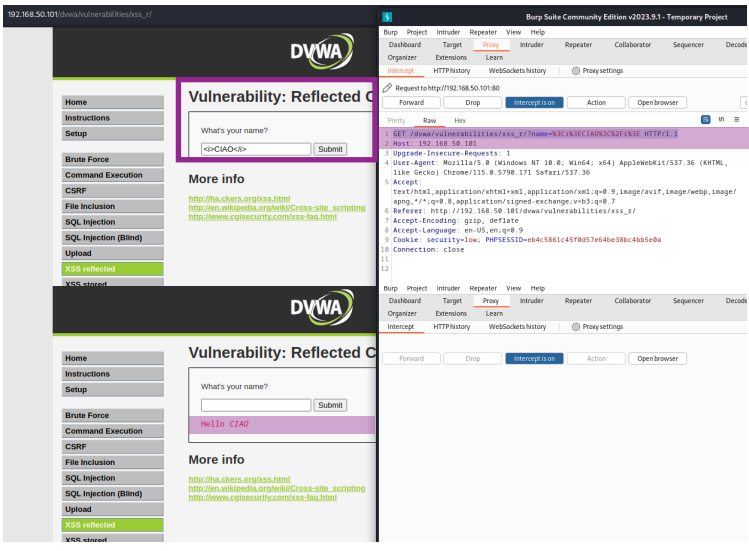


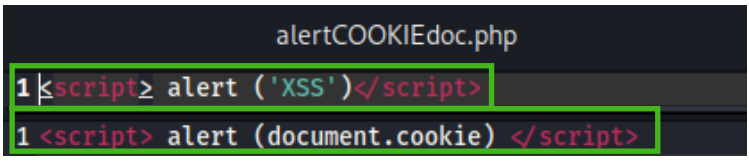
IN SEGUITO MI CONNETTO DA CHROMIUM DI BURPSUITE ALL'APP VULNERABILE INSTALLATA SU METASPLOITABLE TRAMITE IL SUO INDIRIZZO IP E MANTENENDO LA SICUREZZA SU LOW PROCEDO AGLI EXPLOIT



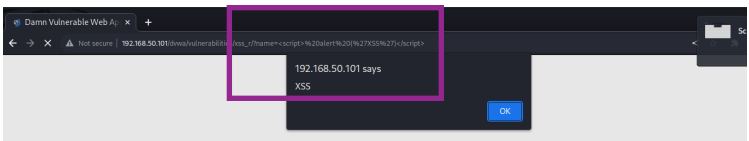
#XSS REFLECTED:

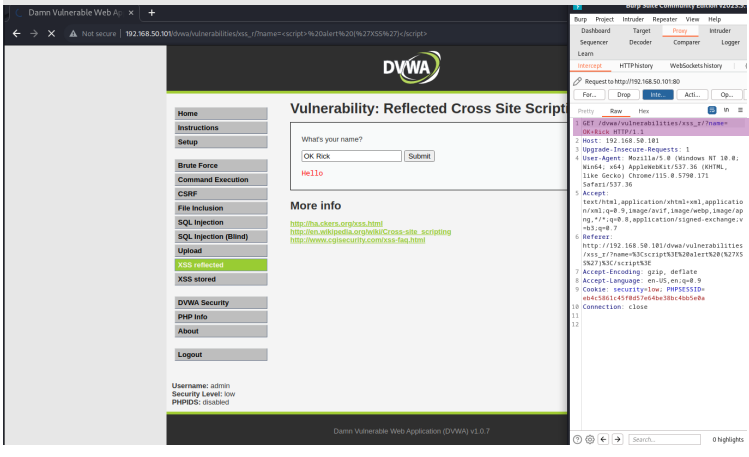
PROVIAMO ANCHE QUESTO TIPO DI ATTACCO, DOVE È SUFFICIENTE ANDARE AD INSERIRE LO SCRIPT NEL CAMPO DI INPUT DELLA PAGINA. NE HO SCELTI DUE (DI CUI UNO PRESENTATO NELLE SLIDE DURANTE IL CORSO) CHE PRESENTANO DUE TIPI DI ATTACCO E OBIETTIVI DIVERSI.
IL PRIMO VISUALIZZA NEL CAMPO IL TESTO DESIDERATO.
IL SECONOD RESTITUISCE L'ID DELLA SESSIONE UTENTE. IL LINK MALEVOLO VA INVIATO TRAMITE L'UTILIZZO DI TECNICHE SOCIAL ENGINEERING ALL'UTENTE BERSAGLIO PER COMPLETARE L'ATTACCO.
LA VERIFICA DELLA POSSIBILITÀ DI UN ATTACCO XSS REFLECTED PUÒ ESSERE FATTA INIZIANDO AD IVIARE UN SEMPLICE TEST PER VEDERE SE LA PAGINA RESTITUISCE UNA SCRITTA IN CORSIVO CON `<i>CIAO</i>`



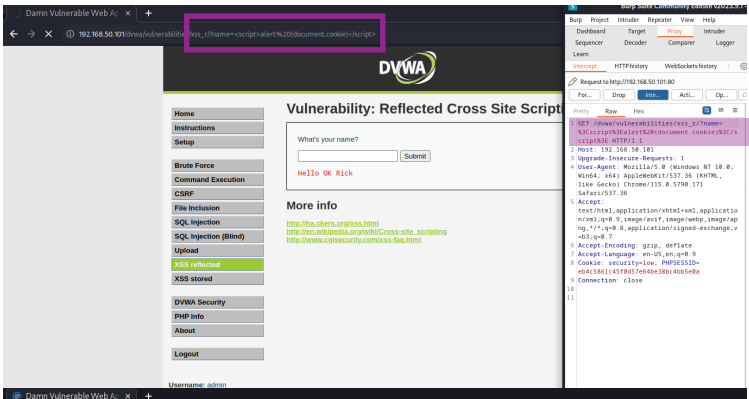


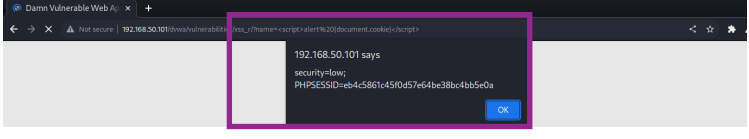
#ALERT 'XSS' / HELLO RICK





#DOCUMENT.COOKIE





#SQL INJECTION:

INIZIO OTTENENDO L'ELENCO COMPLETO DEGLI UTENTI PRESENTI NEL DB.
UTILIZZANDO UN'INGANNEVOLE STRINGA COME ' OR'a'='a OPPURE %' or '0'='0 IL SITO TROVERÀ UNA VARIABILE SEMPRE VERA QUANDO ANDRÀ A CONTROLLARE CHE L'userID COMBACI.

IN SEGUITO GRAZIE ALL'UTILIZZO DEL COMANDO UNION NELLA STRINGA 1'UNION SELECT user,password FROM users# PROVVEDO A RECUPERARE NOMI UTENTE E PASSWORD IN FORMATO HASH E PER SICUREZZA ME LI COPIO/INCOLLO E SALVO SU UN FILE .TXT CHE AD ESEMPIO CHIAMERÒ PWD.TXT
QUESTO FILE POTRÀ SUCESSIVAMENTE ESSERE CRACCATO CON L'AIUTO DEL TOOL JOHN THE RIPPER.

PER CONCLUDERE ESEGUO UN COMANDO UTILE %' and 1=0 union select null, table_name from information_schema.tables # CHE MI RESTITUISCE TUTTE LE TABELLE PRESENTI NELL'INFORMATION_SCHEMA: IN ESSO SONO MEMORIZZATE TUTTE LE INFORMAZIONI RIGUARDO LE TABELLE, E TUTTI GLI ALTRI DATABASE GESTITI DA MYSQL. SALVO I DATI SU UN ALTRO FILE .TXT.