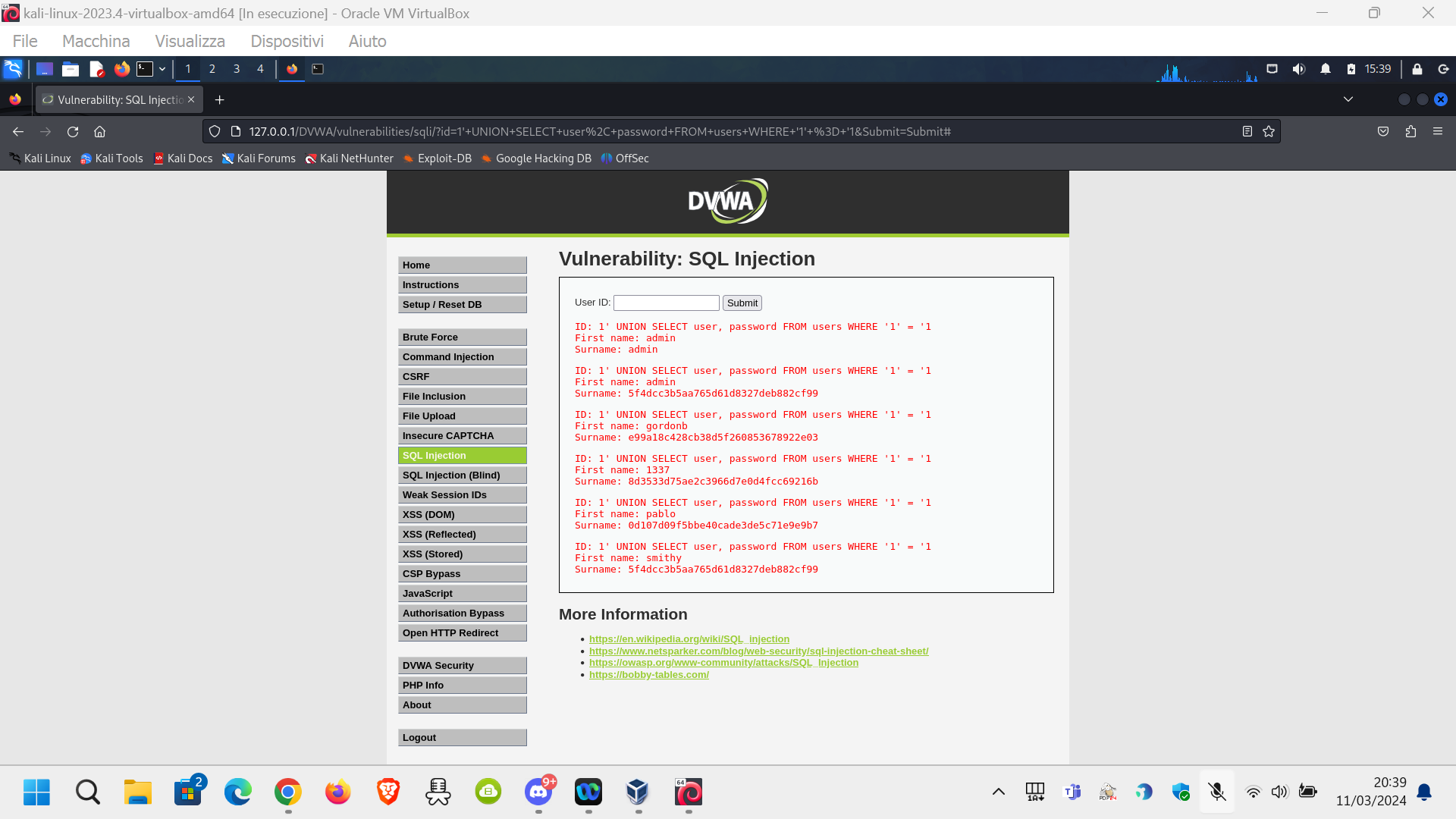
**ESERCIZIO W14D1 PRATICA 1**

**Obiettivo:** Il compito assegnato consisteva nel recuperare le password degli utenti da un sistema compromesso utilizzando un attacco di SQL injection e successivamente eseguire il cracking delle password recuperate.

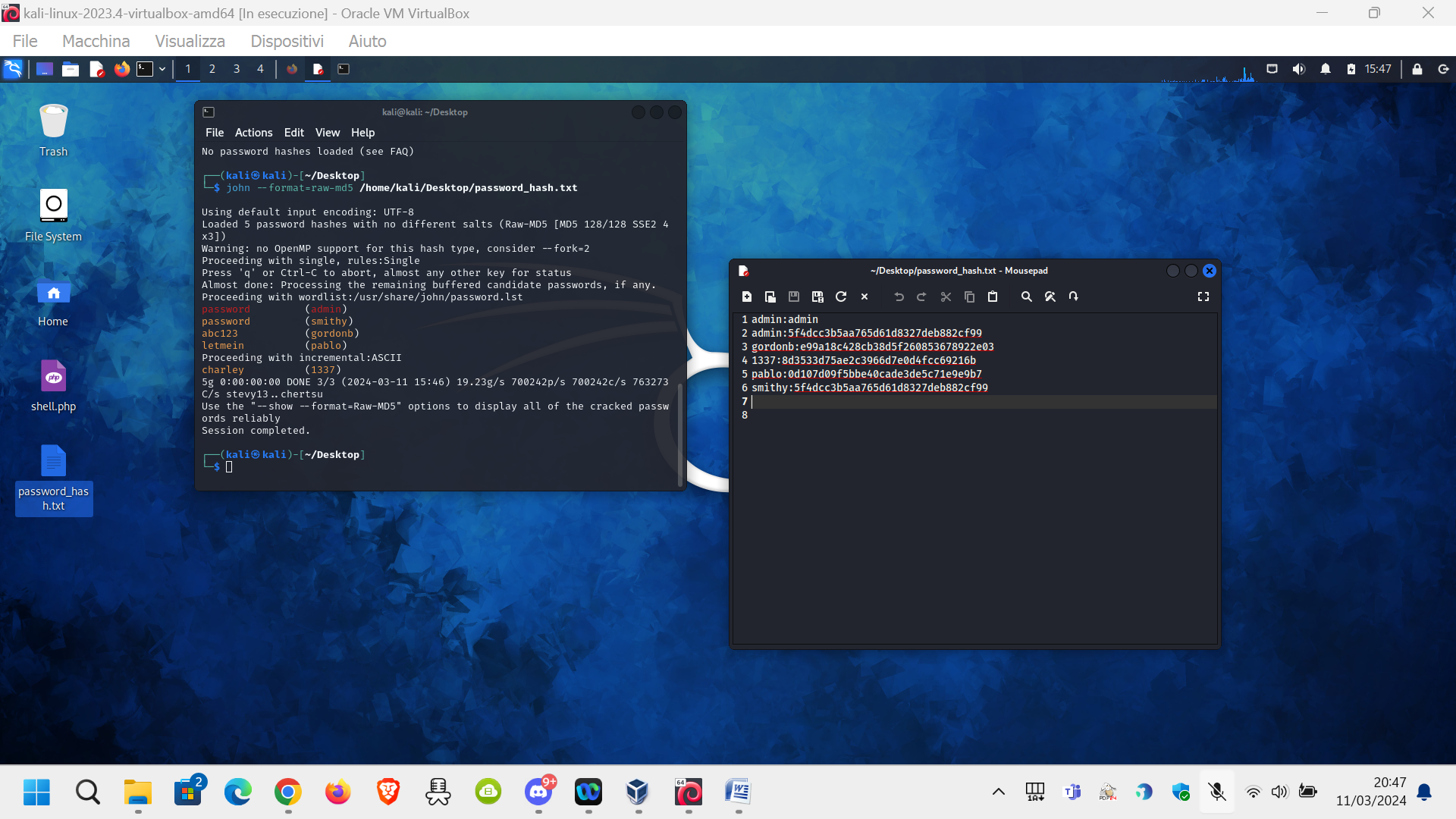
**Azioni intraprese:**

1. **Identificazione del sistema target:** Il sistema target è la DVWA
2. **Esecuzione dell'attacco SQL injection:** Utilizzando l'interfaccia web di DVWA, è stato eseguito un attacco di SQL injection inserendo una stringa di payload **UNION SELECT** nell'input del parametro della pagina.

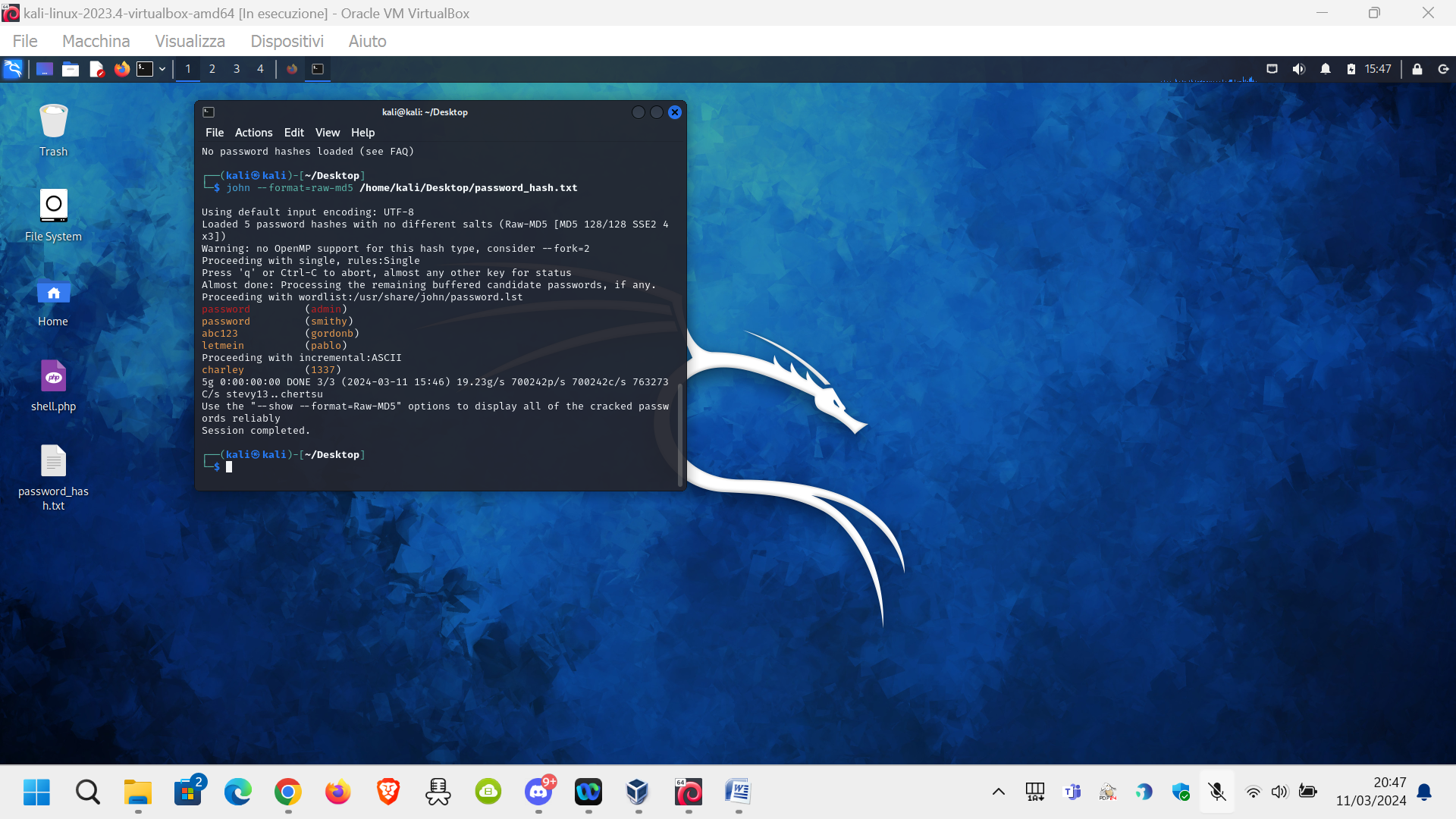
1' OR '1' = '1'; SELECT user, password FROM users WHERE password = MD5('password\_da\_ricercare')

Tramite questo comando ho trovato l’hash delle password.

1. **Recupero delle hash delle password:** Dall'output dell'attacco SQL injection, sono state estratte le hash delle password degli utenti. Le hash delle password sono state individuate seguendo il formato **nome\_utente:hash\_password**.
2. **Preparazione delle hash delle password per il cracking:** Le hash delle password sono state organizzate in un formato corretto, con ogni riga contenente il nome utente seguito da due punti e l'hash della password.

****

1. **Esecuzione del cracking delle password:** Utilizzando lo strumento John the Ripper, sono state fornite le hash delle password preparate come input per il cracking delle password. John the Ripper ha eseguito il cracking delle password utilizzando una wordlist di default e un'analisi incrementale, riuscendo a trovare diverse password.



1. **Riassunto delle password trovate:** Le password trovate da John the Ripper sono state riassunte insieme ai rispettivi nomi utente. Sono state fornite le password decifrate che possono essere utilizzate per accedere agli account nel sistema.

Di seguito sono elencate le password trovate accanto ai rispettivi nomi utente:

* Utente: admin, Password: password
* Utente: smithy, Password: password
* Utente: gordonb, Password: abc123
* Utente: pablo, Password: letmein
* Utente: 1337, Password: charley

**Conclusioni e considerazioni:** L'attacco di SQL injection è stato eseguito con successo e le password degli utenti sono state recuperate utilizzando le hash delle password trovate durante l'attacco. Il cracking delle password ha avuto successo grazie all'utilizzo di John the Ripper, che ha fornito le password in chiaro corrispondenti alle hash fornite.