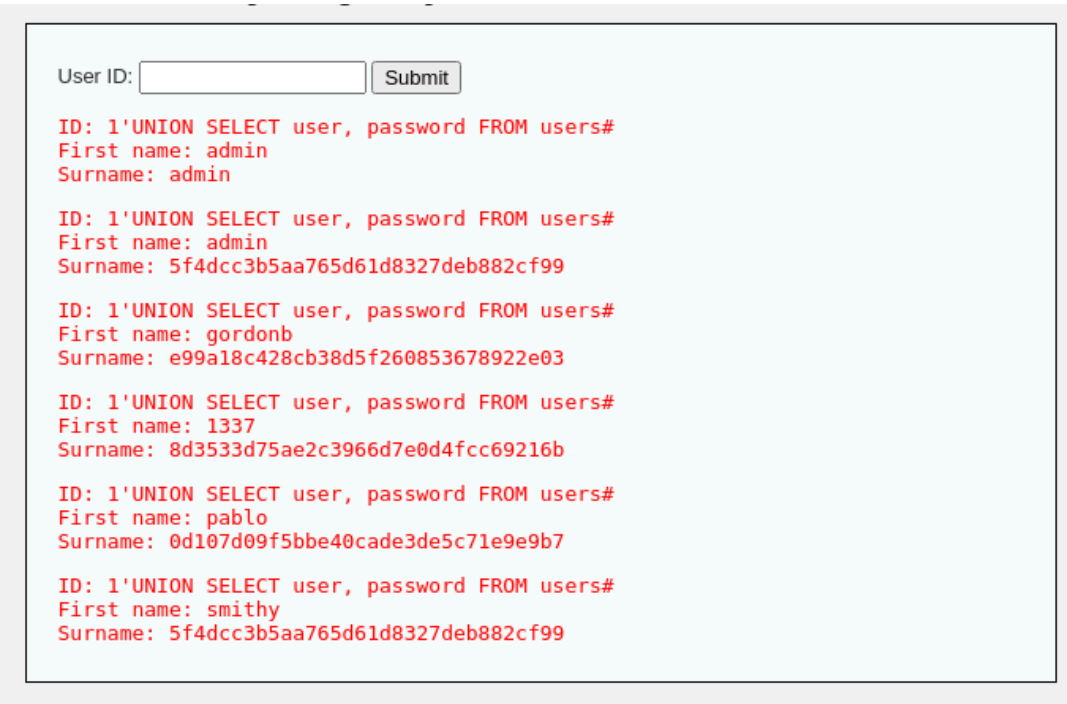
W14D1  Traccia:password cracking




Screenshot del risultato SQL Injection con relativi First name e relative password in MD5.

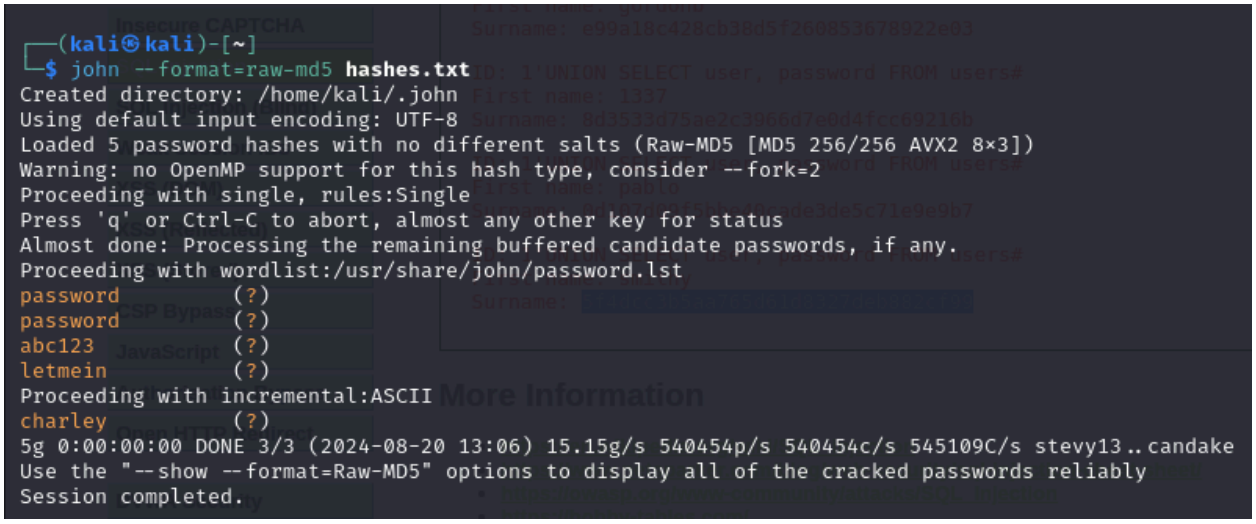
Per poter decriptare le password ho utilizzato il tool **John the Ripper** su Kali Linux.

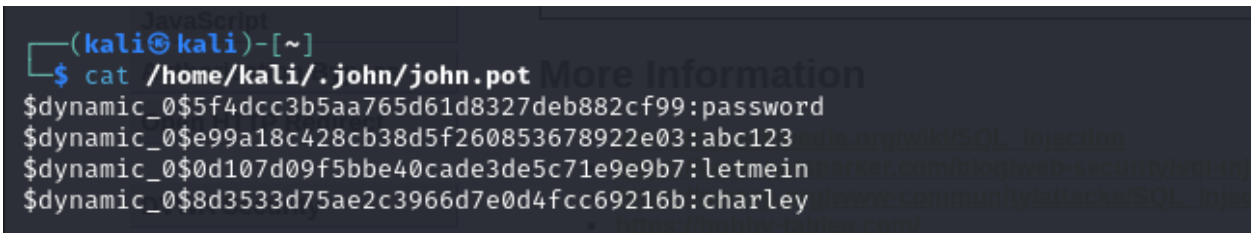
**John The Ripper** è un software libero che semplifica le attività di cracking delle password: partendo dagli hash è possibile provare a risalire alle **password in chiaro**.Una caratteristica interessante di John The Ripper è che il software può rilevare automaticamente l'**algoritmo crittografico** utilizzato per generare gli hash di ciascuna password.
La stessa utilità è in grado di tentare il **password cracking** usando un "dizionario" di parole utilizzate comunemente dagli utenti per proteggere i loro account. Conoscendo gli hash di ciascun elemento del dizionario, John The Ripper può risalire alle password originali anche per quegli algoritmi di hashing che non soffrono di alcuna vulnerabilità.

Prima di procedere con l'utilizzo del tool è stato creato un file chiamato 'hashes.txt' in cui sono state inserite le password precedentemente trovate.

**Successivamente si procede:**

- Aprendo la shell
- Digitare il comando:  john --format=Raw-MD5 hashes.txt




Nella prima immagine viene riportato il risultato del comando precedentemente scritto.

Nella seconda immagine sono riportate le varie password criptate con le relative password in chiaro.