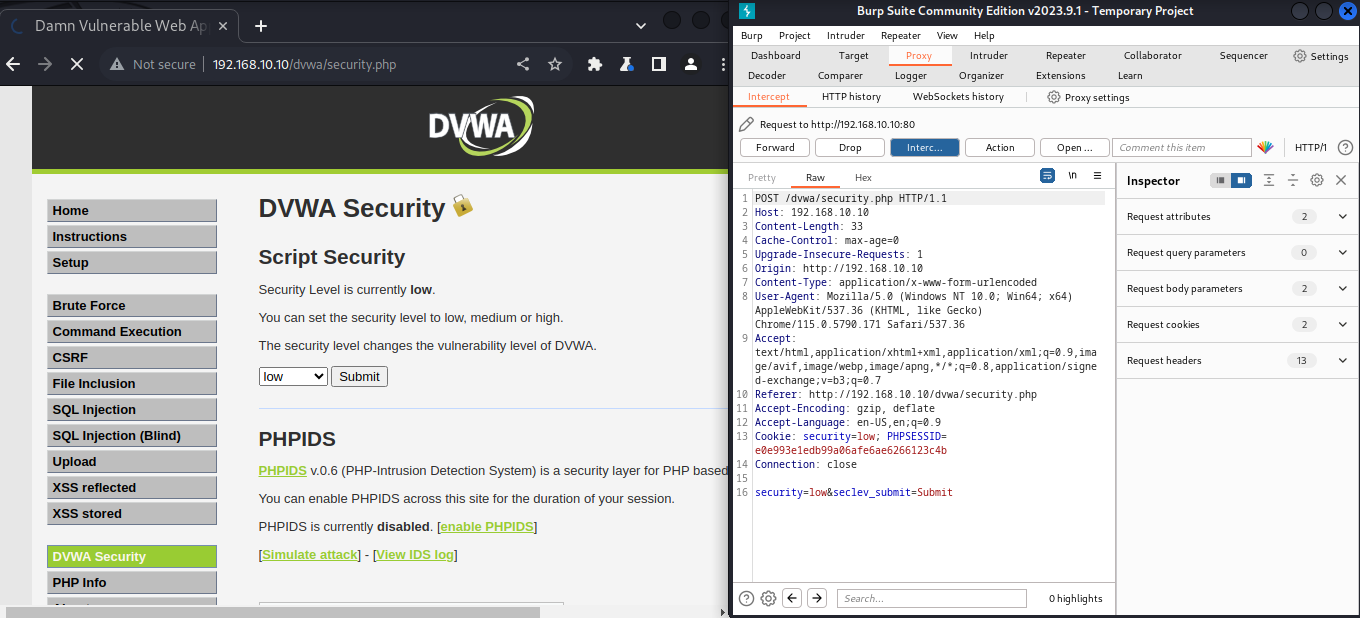
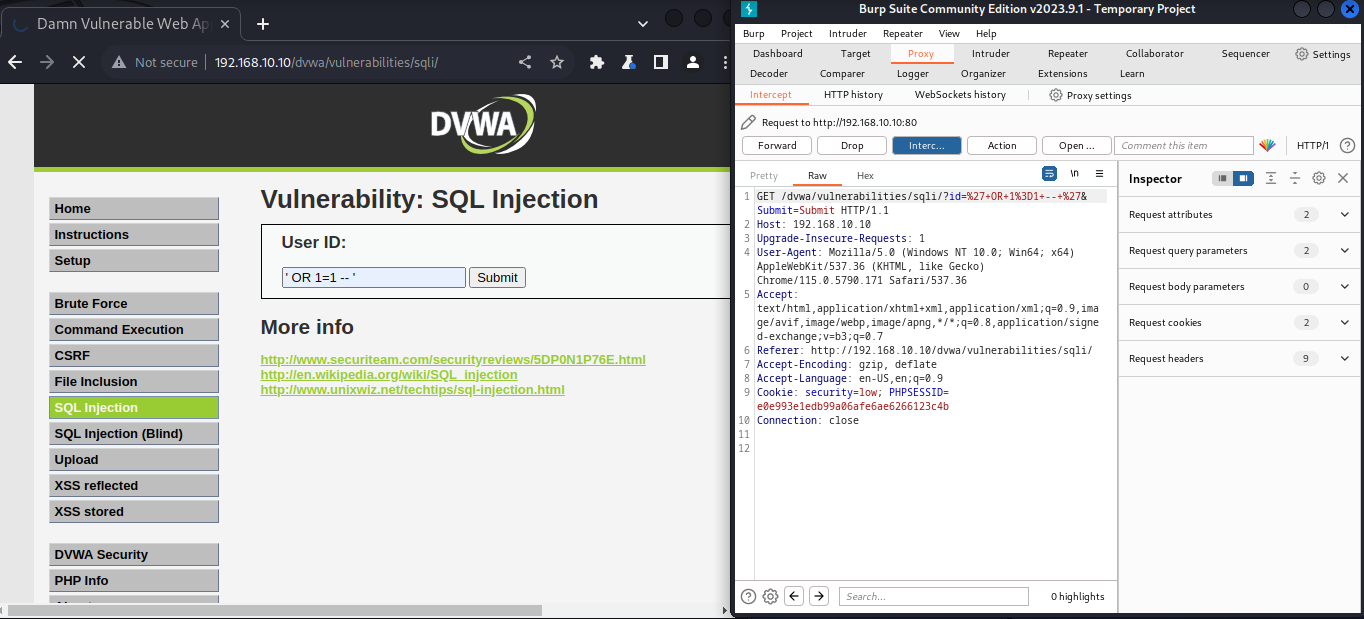
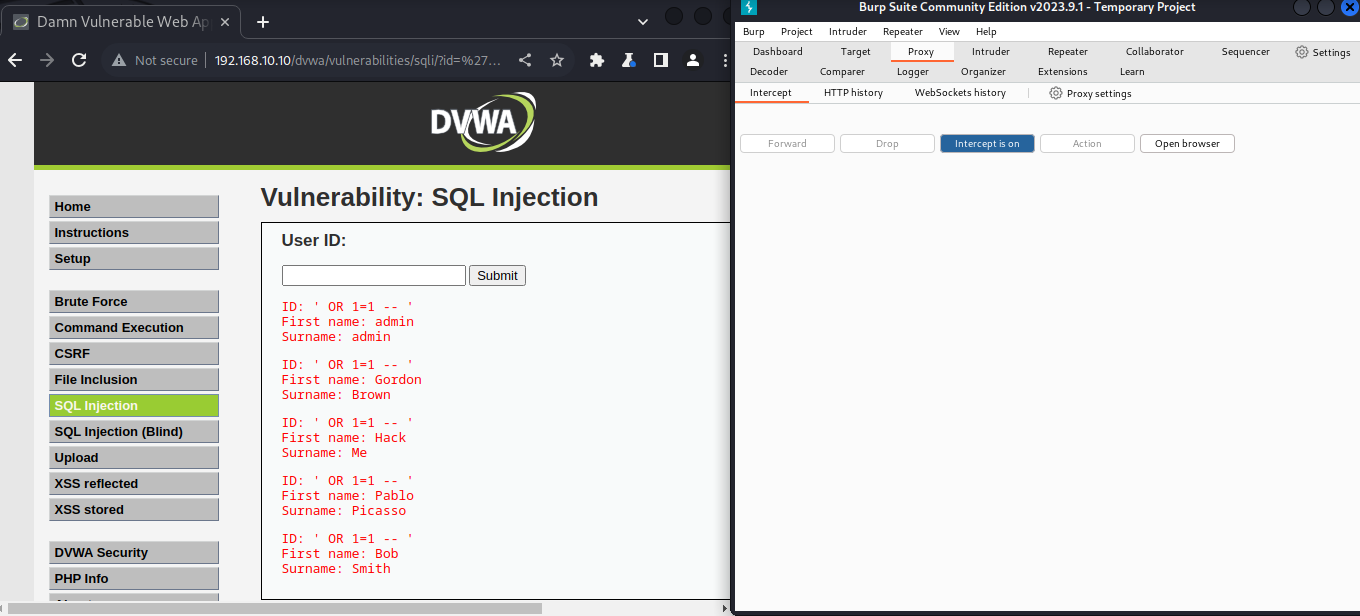
**Traccia:**

Utilizzando l’attacco SQL Injection (non blind), andare a compromettere il database di DVWA.

Accediamo a BurpSuite e alla nostra DVWA. Impostiamo il livello di sicurezza su low e procediamo all’attacco SQL Injection:



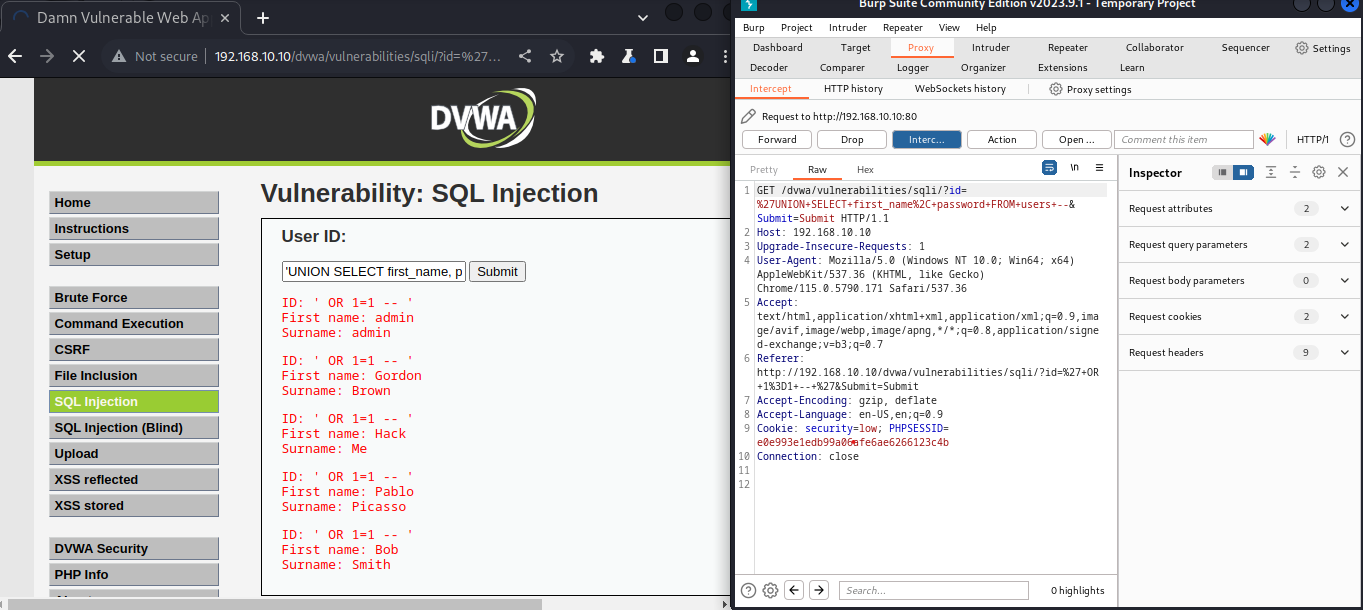


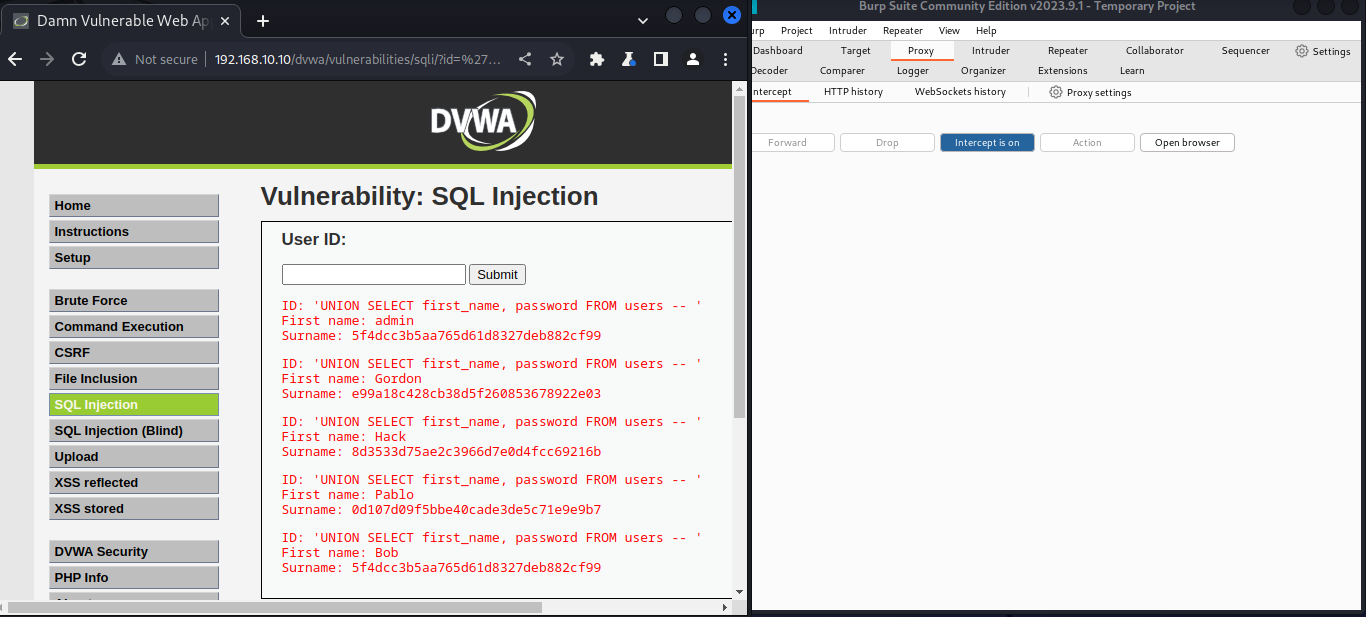


* **‘OR 1=1 –’** 🡪 Con questo primo attacco siamo andati ad estrapolare le informazioni utente corrispondenti a nome e cognome.

Questo può portare ad attacchi molto più pericolosi che ad esempio possono portare un malintenzionato a conoscere le password di tutti gli utenti. Infatti se alla query originale aggiungiamo:

* **‘UNION SELECT first\_name, password FROM users – ‘** 🡪si può risalire alle password (criptate in hash) degli utenti, che poi tramite tool come Hashcat o JTR (John the ripper) possiamo craccare e vedere in chiaro.





Utilizzando il tool John The Ripper cracchiamo le password hash. Come si può vedere (in arancione) le password sono state “tradotte” in chiaro:

