consegna S6-L5

SQLI blind & XSS stored

SQLI blind

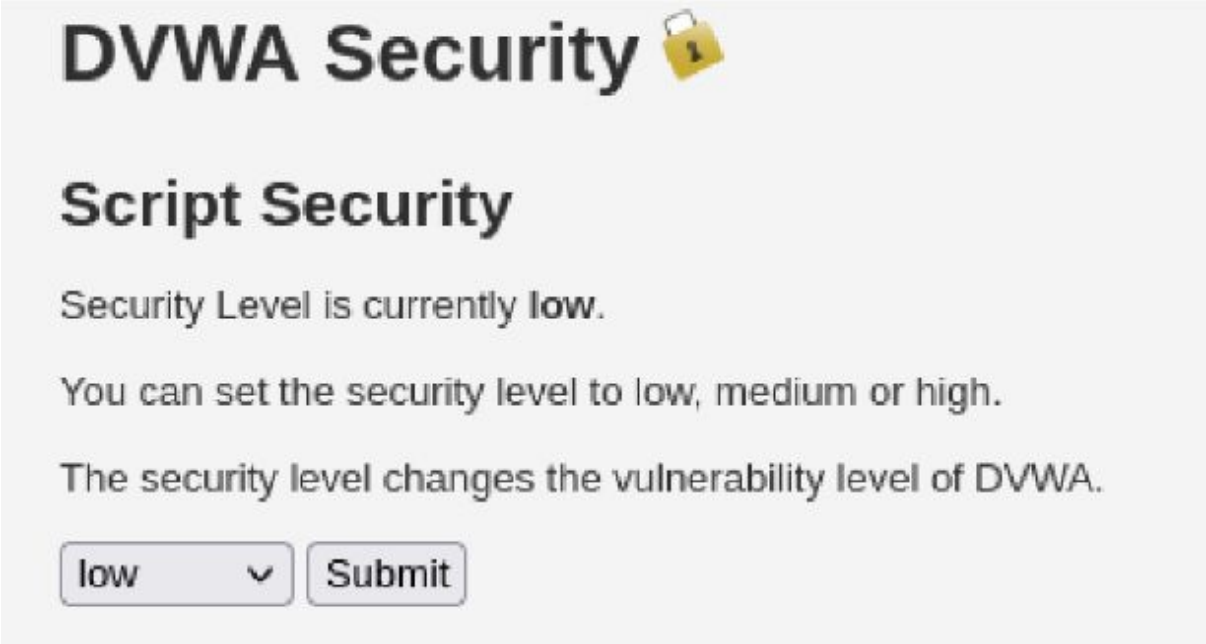
SQLi blind è una tecnica di attacco informatico in cui un attaccante inserisce un codice SQL malevolo in un'applicazione web attraverso input utente, al fine di ottenere informazioni sensibili dal database. La particolarità di SQLi blind è che l'applicazione web non restituisce direttamente i risultati dell'iniezione SQL ma l'attaccante dovrà recuperare le informazioni tramite altre tecniche

XSS stored

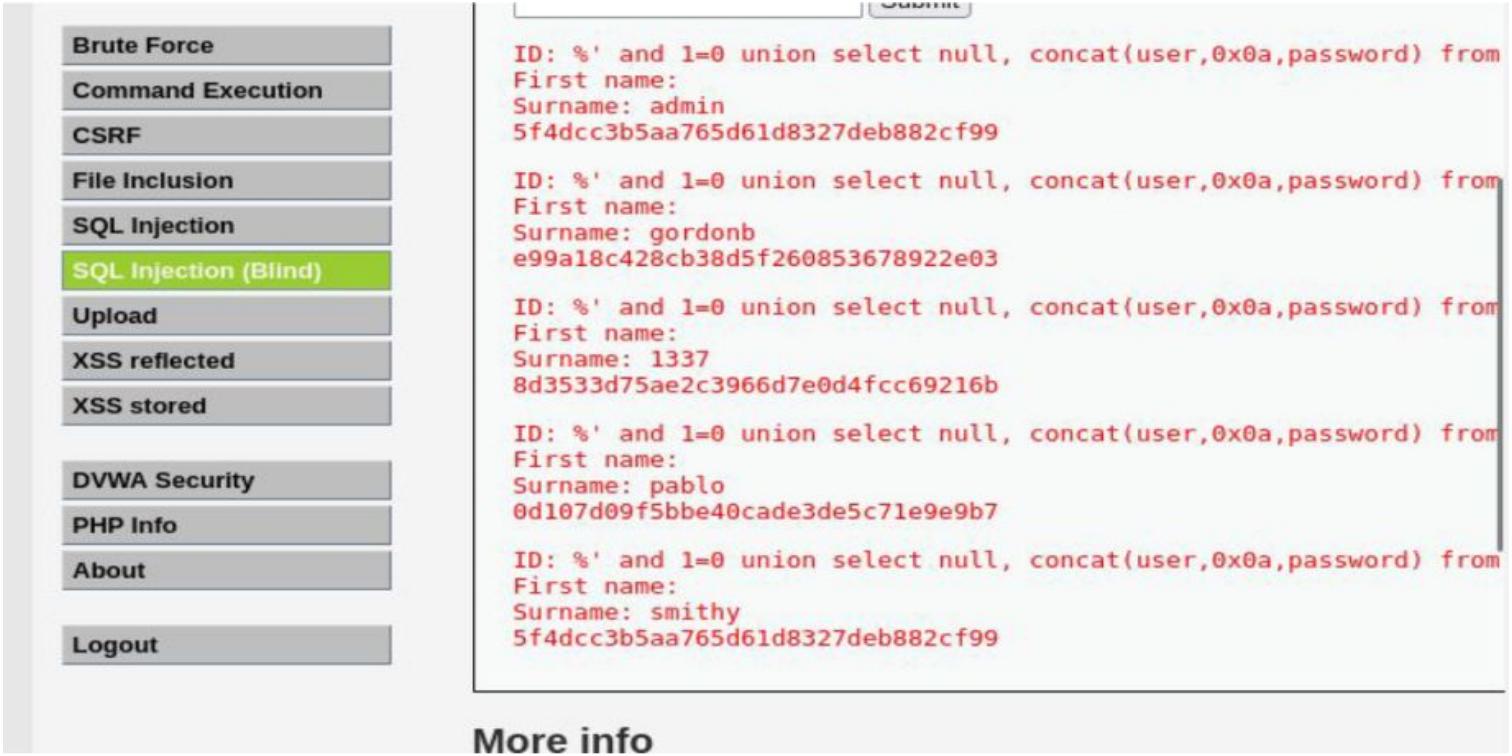
XSS Stored (Cross-Site Scripting Stored) è una vulnerabilità di sicurezza web in cui un attaccante inserisce script malevoli all'interno di dati immagazzinati su un server web consentendo all'attaccante di eseguire azioni dannose o di rubare informazioni sensibili

set up ambiente

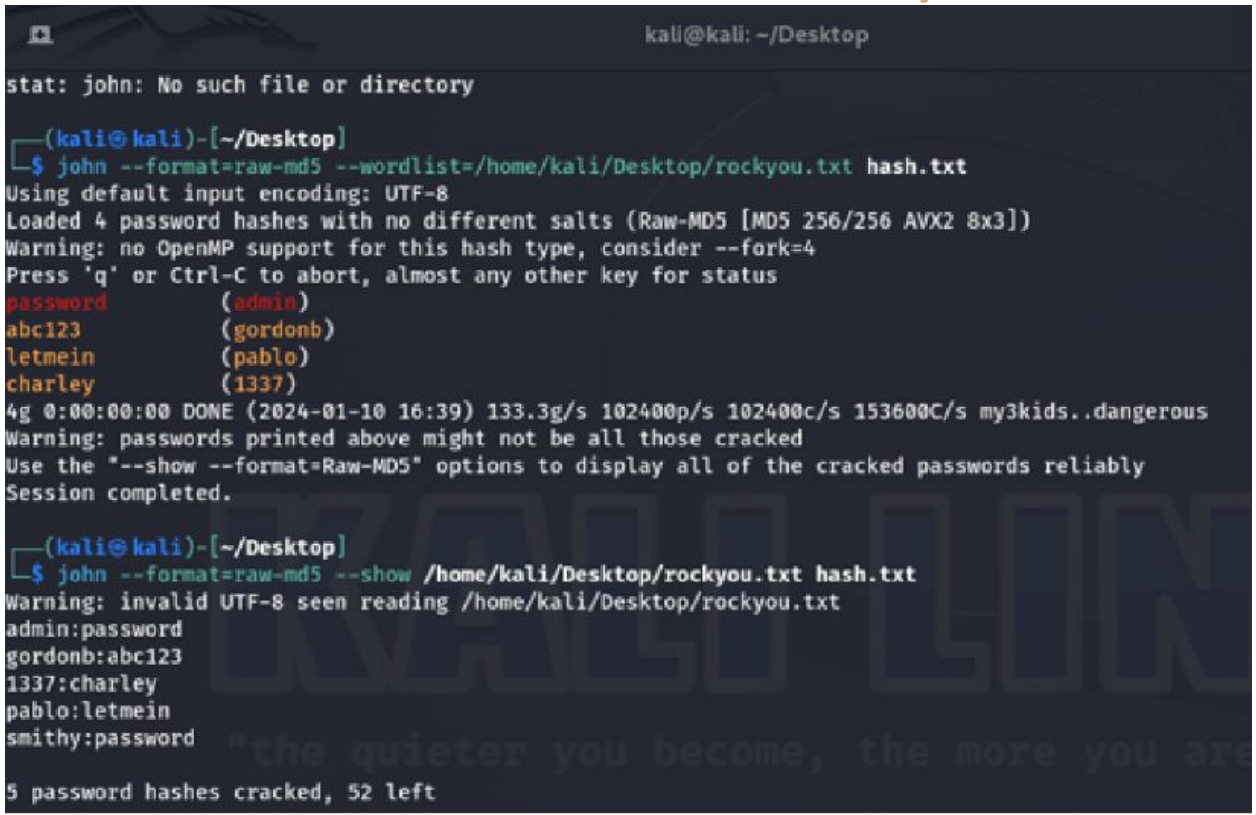
essendo che la consegna di oggi richiedeva di eseguire due attacchi su DVWA settiamo la sicurezza su “low” per iniziare ad impostare il nostro ambiente



Come primo step ci spostiamo nella pagina SQLI blind ed eseguiamo il seguente comando “union SELECT group_concat(user),grou_concat(password) FROM users– -” il quale ci permettera’ di ricevere username e password della web app sotto forma di hash

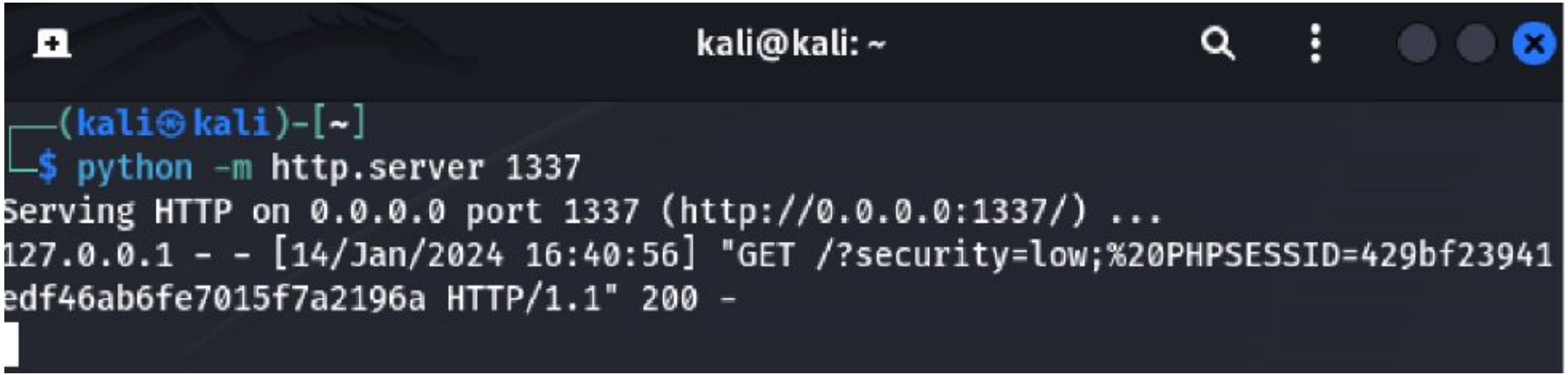


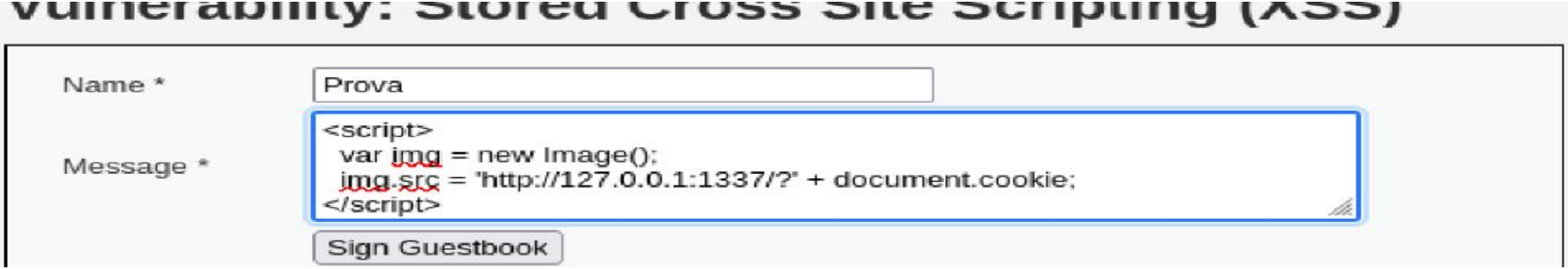
utilizzando john the ripper tramite il comando “jhon --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt hash.txt” trasformiamo in chiaro i risultati salvati precedentemente nel file “hash.txt” e le mostriamo tramite il comando “john --format=raw-md5 --show”



XSS stored

impostiamo il server in ascolto sulla porta 1337 ci spostiamo poi su DVWA per inserire lo script in figura che ci permetterà di raccogliere i cookie di sessione dal web server





come si puo' notare siamo riusciti a recuperare tutti i cookie di sessione raggiungedo cosi' il nostro obbiettivo