Sql injection(blind)

Data la problematica d'ottenere le admin password sulla dvwa impostata a livello di sicurezza low,ho optato per certificare la vulnerabilita della dvwa con sqlmap,tool con cui si otterrano anche le admin password successivamente,il tutto inizia intercettando il traffico con il tool burpsuite (proxy) con il quale ottengo cookie/PHPSESSID,ottenuti questi dati ed essendo gia' in possesso del url procedo con sqlmap.Una volta in sqlmap dopo aver inserito il comando composto da url/cookie/PHPSESSID procedero' con altri comandi come –dbs che ci dara' i database attivi che successivamente investigero' usando comandi come –D dvwa –tables –columns,dopodiche' usando –T(tables) ed –dump otterro tutto dalle "users" table.

Xss stored

Un attacco XSS stored si verifica quando l'input immesso da un utente viene archiviato (stored) e quindi visualizzato in una pagina web,grazie proprio a questa vulnerabilita' comunicando con la pagina web ho ottenuto i cookie di accesso.