

CONSEGNA [SETTIMANA 3 LEZIONE 2]

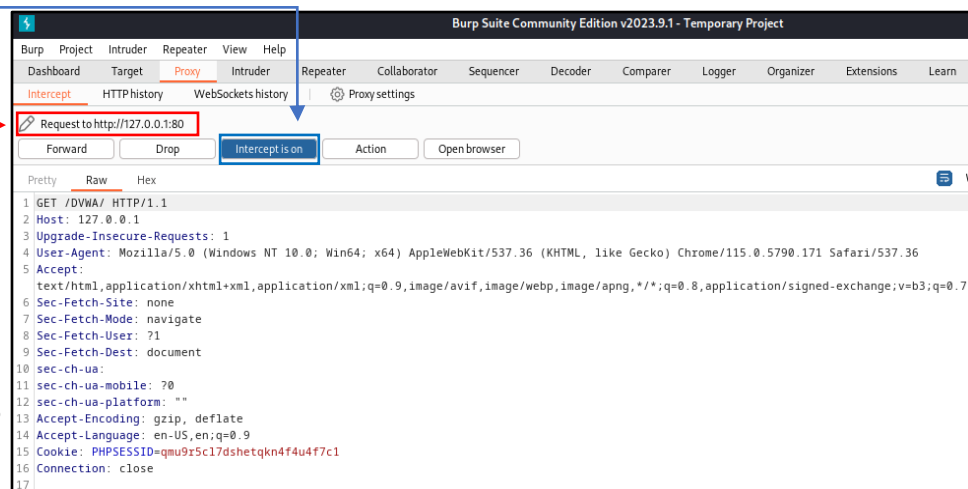
UTILIZZO DI BURP SUITE

Nella schermata qui sotto è mostrata l'applicazione *Burp Suite*, precisamente una suite contenente numerosi strumenti per la sicurezza delle applicazioni web.

In particolar modo oggi andremo ad utilizzare *Burp Suite* per intercettare le richieste dal client al sito web, potendo raccogliere così informazioni riguardanti la connessione ed eventuali dati sensibili (come password, indirizzi email ecc...).

In questa schermata, dopo aver abilitato l'intercettazione delle connessioni,

ci verranno fornite tutte le informazioni inerenti alla connessione che il client sta effettuando (nel nostro caso verso l'indirizzo **127.0.0.1/DVWA**, una web app hostata sul nostro computer utile per esercitarsi nella pratica del pentest). Possiamo quindi notare che sono elencate numerose informazioni riguardo alla connessione, come ad esempio il metodo **GET** alla riga 1 (un metodo del protocollo http che consente al client di richiedere informazioni al web server) e l'host alla riga 2 (nel nostro caso 127.0.0.1).



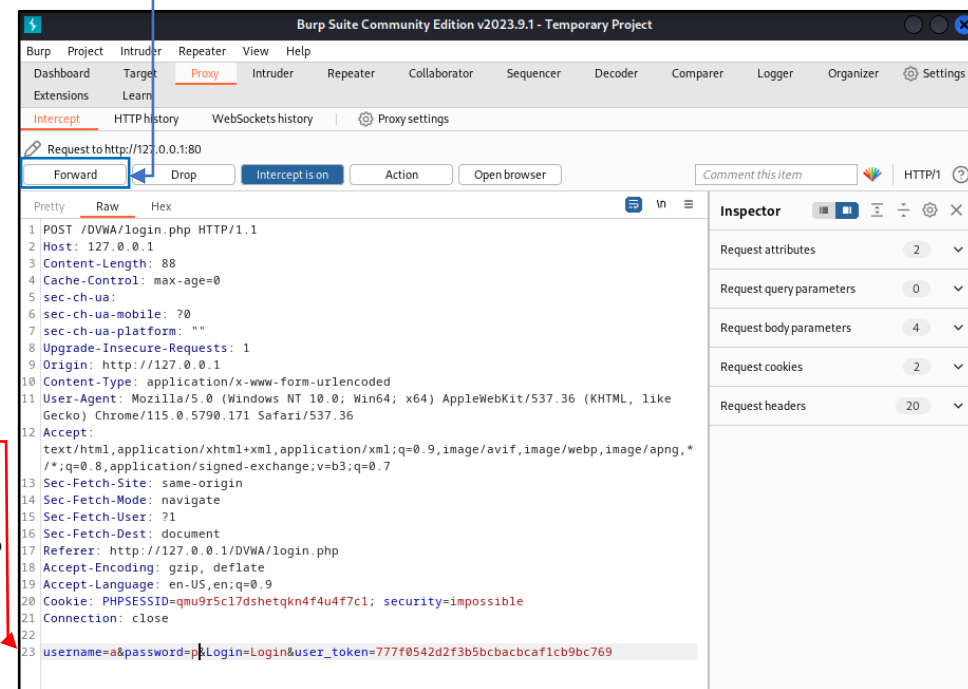
Dopo aver inviato la richiesta tramite il tasto "forward", il browser sarà in grado di mostrare la pagina di accesso dove potremo inserire le credenziali richieste.

Dopo aver inserito le credenziali e aver mandato la richiesta di login, potremo intercettarla e ricavare i dati di accesso.

Possiamo notare che in questo caso la presenza del metodo **POST** alla riga 1 (sempre un metodo del protocollo http, ma che al posto di richiedere informazioni le invia al web server).


Da questa schermata è possibile inoltre modificare il valore dei dati inseriti (nel nostro caso username e password) prima di inviare la richiesta.

Avendo modificato questi valori, noteremo che la richiesta di login sarà negata.



Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php



Username

Password

Login

Login failed