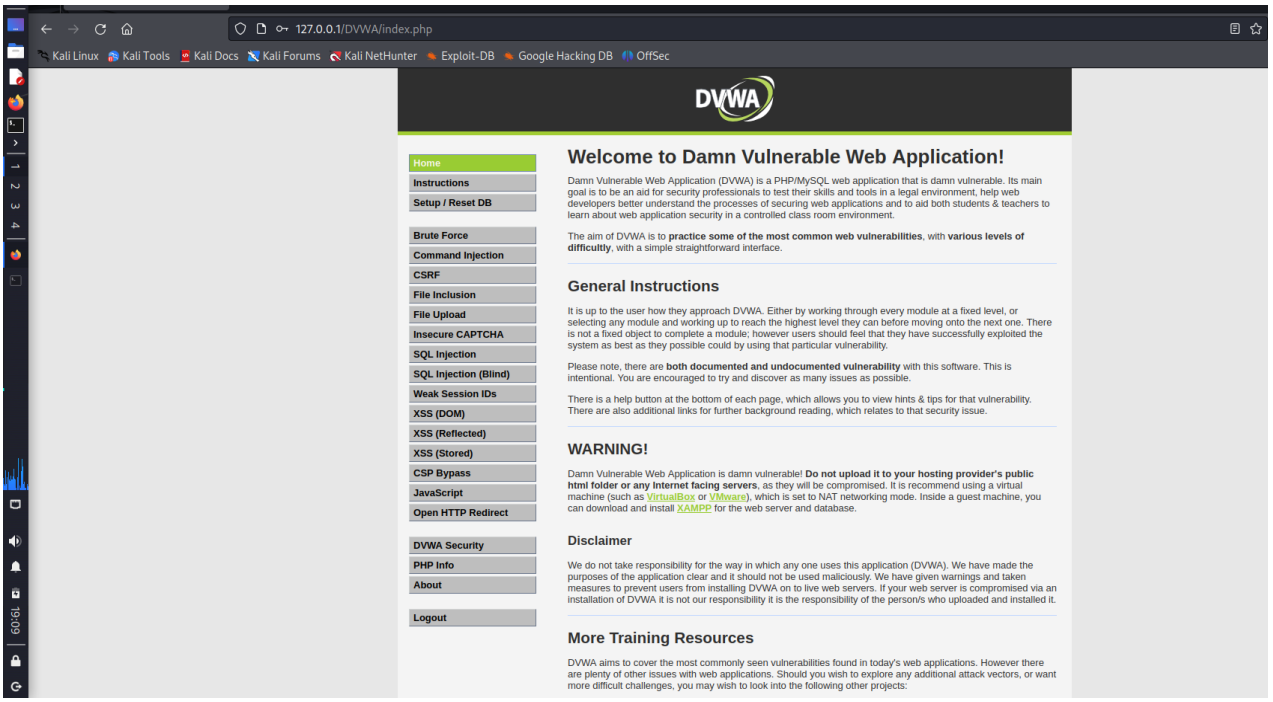
Traccia:
Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

La DVWA è un'applicazione web progettata appositamente per essere vulnerabile e utilizzata a scopo didattico o per fini di testing della sicurezza, questo permette agli sviluppatori, agli studenti e agli esperti di sicurezza di esercitarsi nel rilevamento, delle vulnerabilità comuni delle applicazioni web.

Una volta completato il procedimento di installazione e configurazione, dopo aver creato il database ed aver effettuato l'accesso possiamo trovare questa pagina:

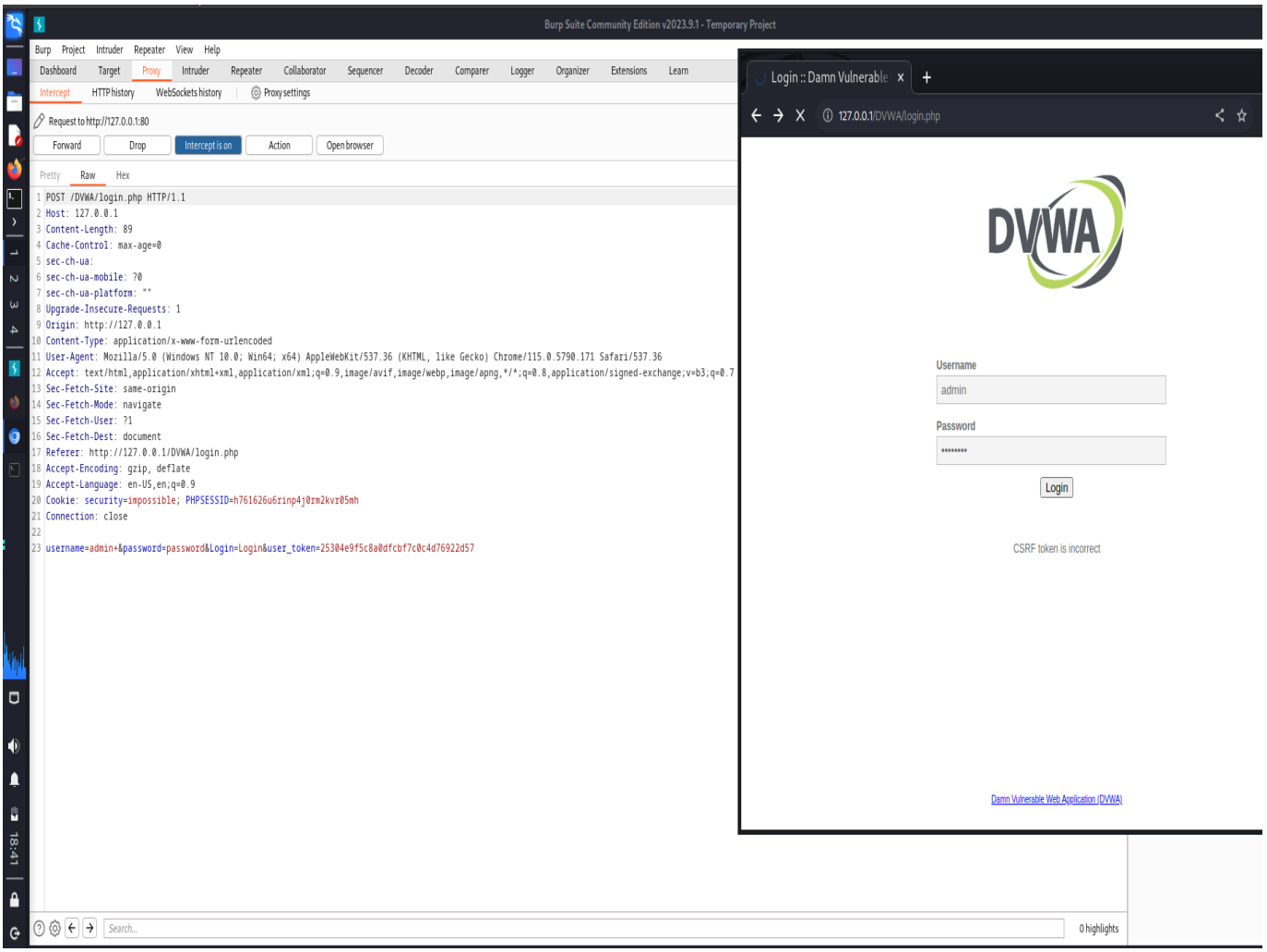


Una volta che DVWA sarà attiva effettueremo un pò di pratica con Burpsuite.

Burp Suite, è un intercepting proxy, uno strumento che permette di intercettare e filtrare, il traffico tra client e server di destinazione, utile nella sicurezza informatica, tramite le sue molteplici funzionalità, il programma ci permette di analizzare e modificare le richieste inserendo come esempio dati falsi, permettendo quindi, di trovare e scovare

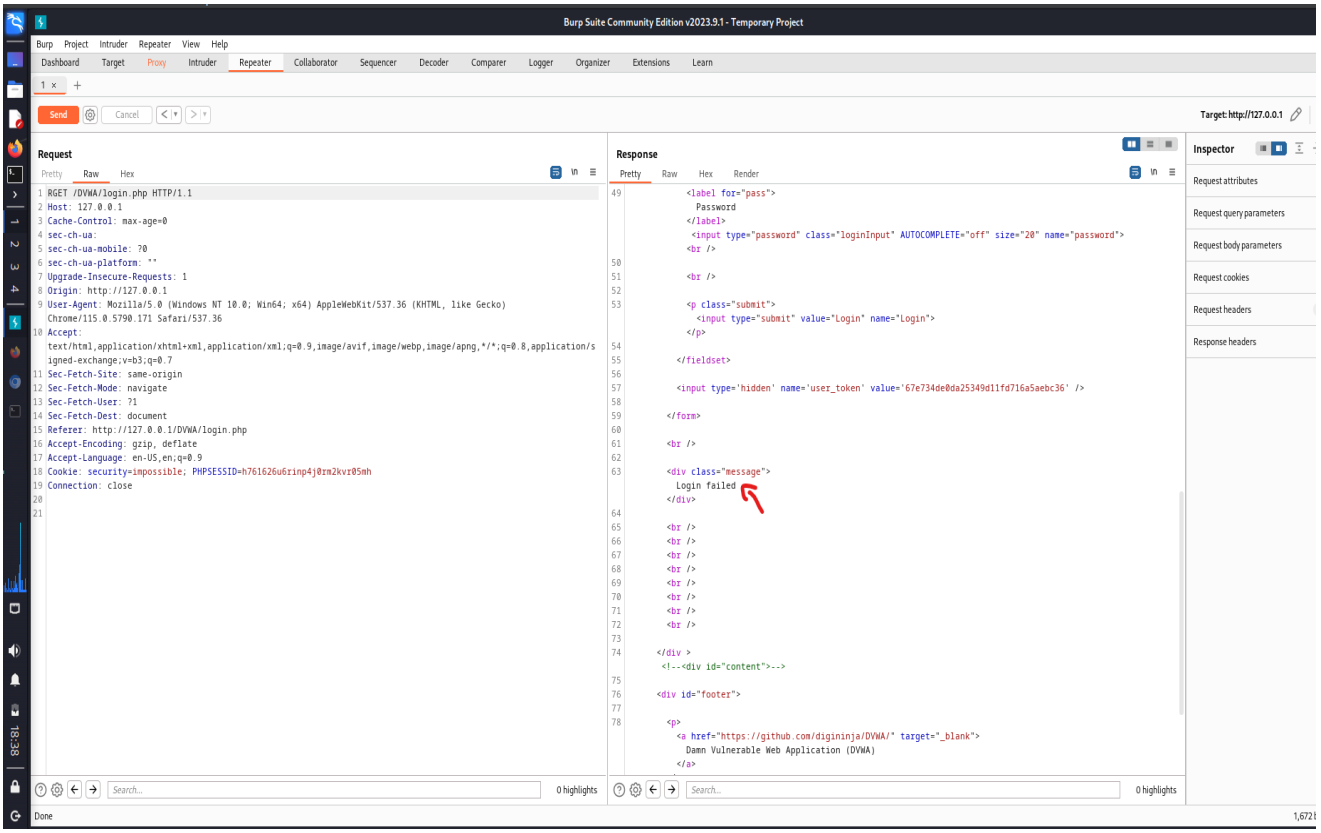
eventuali vulnerabilità. Ha altre funzionalità ma questa è la più essenziale, comunque nelle successive foto allegate, vedremo vari esempi.

Adesso avviamo, Burpsuite e facciamo un pò di pratica, utilizzeremo Chromium come browser ma se ne possono impostare anche altri, prima di questo clicchiamo su proxy e subito dopo su intercept is off per cambiarlo in on e avviarlo, una volta fatto questo apriamo Chromium che è il browser di Burpsuite e scriveremo sulla barra degl indirizzi, <<127.0.0.1/DVWA/login.php>>, proveremo successivamente a inserire username e password, che saranno “admin” e “password” e cliccheremo su login, il risultato sarà questo:



Lo step successivo sarà quello di provare a inserire username e password errati e mandare la richiesta, (si modificheranno direttamente da Burpsuite), con il tasto destro del mouse, clicchiamo su “send to

repeater", poi andremo sulla sezione repeater e clicchiamo su “send”, sulla destra ci comparirà il comando follow redirection, premendo su quello, ci darà la risposta dal server, ovvero login failed:



Spiegherò adesso cosa succede quando clicchiamo sui vari comandi utilizzati durante i test pratici:

Forward: Quando Burpsuite, intercetta una richiesta premendo su questo comando, questo permetterà di inoltrare la richiesta al server di destinazione;
Drop: Questo comando permette di eliminare la richiesta corrente evitando che arrivi al server di destinazione;
Send to repeater: manderà la richiesta al modulo repeater, questo permetterà di semplificare il processo di analisi del traffico apportando modifiche ed eseguendo test sulla stessa richiesta;
send: invierà la richiesta al server e riceverà una risposta dal server come nel caso di sopra;
follow redirection: seguirà eventuali reindirizzamenti senza richiedere l’intervento manuale dell’utente, quindi se una richiesta riceve automaticamente un codice di stato di reindirizzamento, Burp Suite

seguirà automaticamente la nuova URL indicata nella risposta senza richiedere conferma.

Adesso spiegherò i metodi del protocollo di rete HTTP, che possiamo vedere sopra come GET e POST ma ce ne sono altri:
GET: viene utilizzato per richiedere una risorsa web, dati dal server, ad esempio è utilizzato per per richiedere pagine web, immagini o altri contenuti;
POST: viene utilizzato per inviare parametri all'interno della richiesta, quando si desidera inviare dati al server per essere elaborati, come ad esempio l'invio di un modulo o l'invio di dati di una richiesta complessa.