

# ESERCIZIO S3L3

L'esercitazione di oggi si concentrava sulle web application.

Una volta impostati e avviati i programmi necessari quali:

- Database mysql
- Web server Apache

Avremo la possibilità di accedere ad un sito web contenuto nel web server 127.0.0.1. Il sito è raggiungibile con 127.0.0.1/DVWA. Configuriamo anche questo, per renderlo vulnerabile.

Una volta fatto facciamo partire Burpsuite, avviamo il proxy e controlliamo che “intercept” sia su “on”. Quindi avviamo il browser e andiamo su 127.0.0.1/DVWA.

Accediamo al sito con admin e password e torniamo su Burpsuite.

*A questo punto troveremo la richiesta di http di connessione al server, con in chiaro l'username e la password utilizzate.*

The screenshot displays two panels in Burp Suite. The top panel shows a 'Request' tab for a POST request to '127.0.0.1/DVWA/login.php'. The raw data shows a standard login attempt with 'username=admin&password=password&login=LoginUser\_token=2ef60e0b84f90ac60bbd0efdc27b261'. The bottom panel shows the 'Response' tab for the same request, displaying an HTML page with a 'Welcome :: Damn Vulnerable Web Application (DVWA)' message and a 'Login failed' error.

*Se proviamo ad accedere con delle credenziali errate, invece, troveremo questo:*

The screenshot displays two panels in Burp Suite. The top panel shows a 'Request' tab for a GET request to '127.0.0.1/DVWA/login.php'. The raw data shows a standard login attempt with 'username=admin&password=password&login=LoginUser\_token=2ef60e0b84f90ac60bbd0efdc27b261'. The bottom panel shows the 'Response' tab for the same request, displaying an HTML page with a 'Welcome :: Damn Vulnerable Web Application (DVWA)' message and a 'Login failed' error.