RELAZIONE INTERCETTAZIONE BURPSUITE COMANDO LS

Richiesta GET (nella parte sinistra)

1. **URL**: Il client ha inviato una richiesta HTTP GET a http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls.
    - Questo URL include un parametro cmd=ls, il che significa che il client sta cercando di eseguire il comando UNIX ls (list) tramite la web shell shell.php.
    - La web shell shell.php è stata caricata nella directory uploads di DVWA.
2. **Header**:
    - **User-Agent**: Un normale browser (in questo caso Chrome) viene utilizzato per inviare la richiesta, simulando un accesso legittimo.
    - **Connection**: keep-alive indica che la connessione rimane aperta per successive richieste.
    - **Host**: 192.168.50.101 è l'IP locale del server vulnerabile.

Risposta HTTP (nella parte destra)

1. **Codice di stato**: Il server risponde con **200 OK**, il che indica che la richiesta è stata processata correttamente.
2. **Server**: Il server web è **Apache/2.2.8** con PHP versione **5.2.4-2ubuntu5.10**, che è piuttosto vecchia e potenzialmente vulnerabile.
3. **X-Powered-By**: Conferma che il server è alimentato da PHP.
4. **Risultato del comando**:
    - La web shell ha eseguito il comando ls, e la risposta HTML contiene l'elenco dei file presenti nella directory:
        - dvwa_email.png
        - shell.php

    Questo indica che la web shell è operativa e che l'attaccante può eseguire comandi arbitrari nel contesto del server.

Conclusione

Questo scenario evidenzia una **vulnerabilità di file upload** e la possibilità di eseguire comandi arbitrari tramite una **web shell**. L'attaccante è riuscito a caricare uno script PHP (shell.php) su un server vulnerabile e a eseguire comandi di sistema (ls) per vedere i file presenti nella directory di upload.