# Consegna S6-L1

## Consegna: Sfruttamento di una Vulnerabilità di File Upload su DVWA

⚜️ **Tag:** #pentesting #dvwa #fileupload #php #burpsuite

**Argomento:**
Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

---

### Obiettivi

1. **Configurazione del Laboratorio:**
   - Configurare il proprio ambiente virtuale in modo che la macchina **Metasploitable** sia raggiungibile dalla macchina **Kali Linux**.
   - Assicurarsi che ci sia comunicazione bidirezionale tra le due macchine (es. test con ping).
2. **Esercizio Pratico:**
   - Sfruttare la vulnerabilità di file upload presente sulla DVWA per ottenere il controllo remoto della macchina bersaglio.
   - Caricare una semplice shell in PHP (es. `shell.php`) tramite l'interfaccia di upload della DVWA.
   - Utilizzare la shell per eseguire comandi da remoto sulla macchina **Metasploitable**.
3. **Monitoraggio con BurpSuite:**
   - Intercettare e analizzare richieste HTTP/HTTPS verso la DVWA utilizzando **BurpSuite**.
   - Familiarizzarsi con gli strumenti e le tecniche utilizzate dagli

hacker etici per monitorare e analizzare il traffico web.

---

## Traccia dell’Esercizio

1. **Preparazione dell’Ambiente:**
   - Configurare la macchina virtuale **Metasploitable**.
   - Configurare la macchina virtuale **Kali Linux**.
   - Verificare la connessione tra le due macchine con un semplice ping.
2. **Caricamento della Shell PHP:**
   - Accedere alla DVWA sulla macchina **Metasploitable** tramite il browser della macchina **Kali Linux**.
   - Navigare alla sezione **File Upload** della DVWA.
   - Creare una semplice shell PHP (es. `shell.php`) e caricarla tramite il modulo di upload.
   - Verificare che il file sia stato caricato con successo.
3. **Esecuzione della Shell PHP:**
   - Accedere alla shell caricata tramite il browser.
   - Utilizzare la shell per eseguire comandi da remoto sulla macchina **Metasploitable**.
4. **Intercettazione e Analisi con BurpSuite:**
   - Avviare **BurpSuite** e configurare il browser per utilizzarlo come proxy.
   - Intercettare le richieste HTTP/HTTPS relative al processo di upload e di esecuzione della shell.
   - Analizzare le richieste e le risposte per comprendere il funzionamento e individuare eventuali vulnerabilità.

---

## Suggerimenti

- Configurare il livello di sicurezza della **DVWA** su **LOW** tramite la scheda **DVWA Security**.
- Mantenere aperta una sessione di **BurpSuite** per monitorare e analizzare le richieste.
- Utilizzare il seguente esempio di codice per la shell PHP minimale:

```php
<?php system($_REQUEST['cmd']); ?>
```

- Intercettare e analizzare le richieste GET con **BurpSuite**.

---

## Consegna

1. Codice PHP utilizzato.
2. Screenshot del caricamento del file (browser).
3. Intercettazioni delle richieste (screenshot di **BurpSuite**).
4. Risultati delle richieste effettuate.
5. Eventuali informazioni scoperte sulla macchina interna.
6. **Bonus:** Utilizzare una shell PHP più sofisticata.

---

# 🔑 Chiavi:

[pentesting, dvwa, fileupload, shellphp, burpsuite]