Exploit File upload

Sommario

INTRODUZIONE ALL'ESERCIZIO 3

SUGGERIMENTO 3

SVOLGIMENTO ESERCIZIO 4

CONOSCENZE E CONFIGURAZIONI DI BASE 4

MEDIUM 4

Metodo estensione file 5

HIGH 6

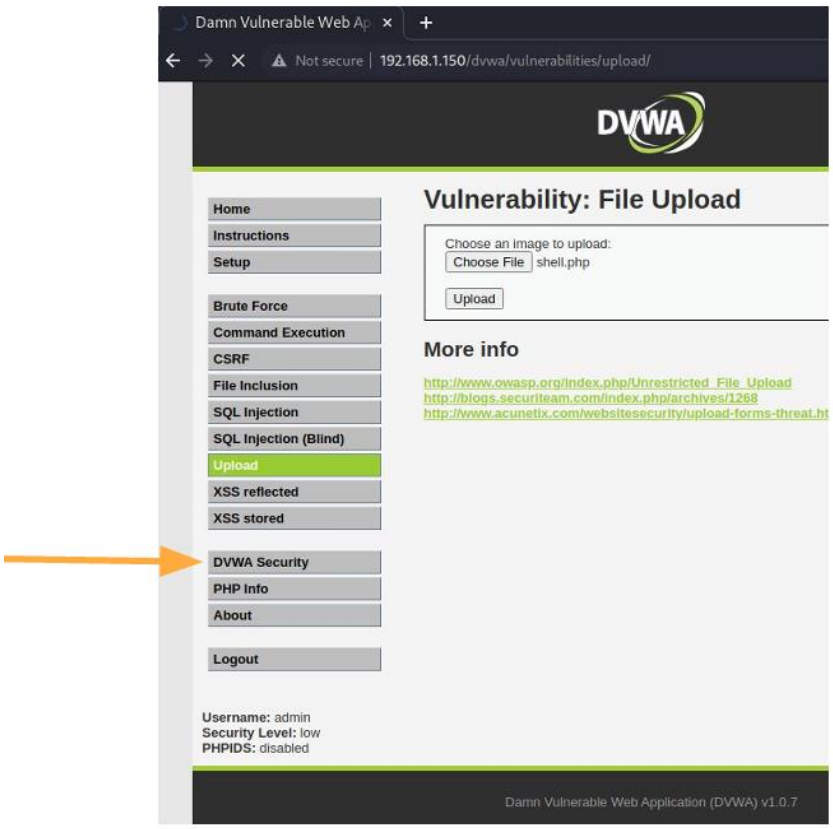
METODO ALTERNATIVO 6

Introduzione all'esercizio

Effettuare il File Upload di una shell ai livelli di sicurezza:

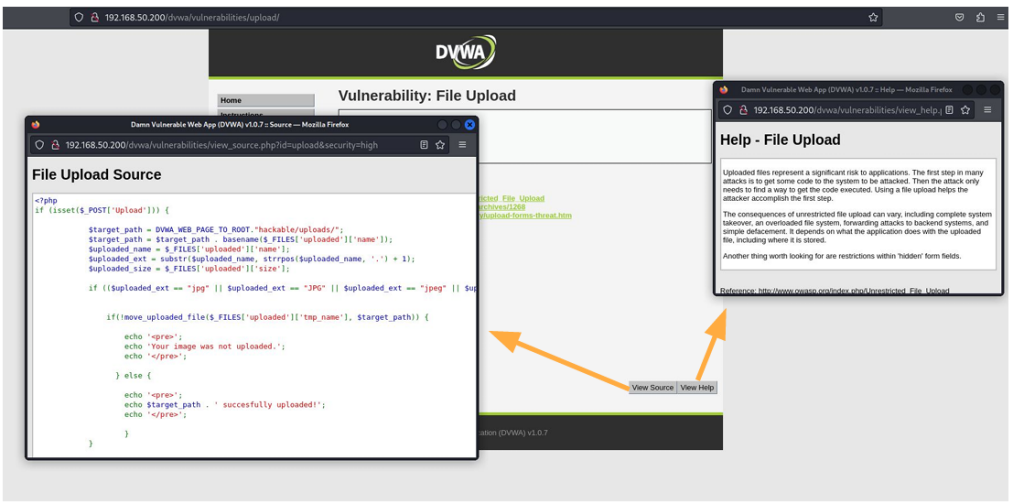
- Medium
- High

Utilizzare sempre BurpSuite per monitorare tutti gli step



Suggerimento

Le soluzioni sono pubbliche, prima di utilizzarle provate a studiare il codice php da "View Source" per capire come aggirare i controlli del server.



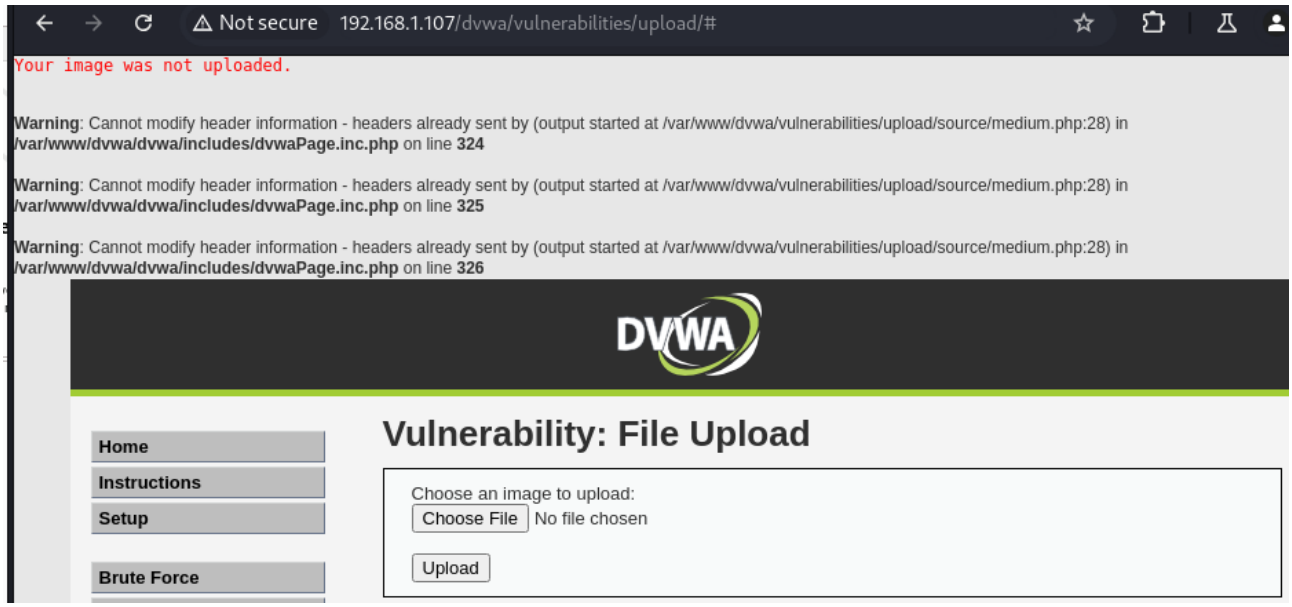
Soluzione pubblica https://medium.com/@eudorina67/dvwa-file-upload-vulnerabilities-40104b54d488

Svolgimento esercizio

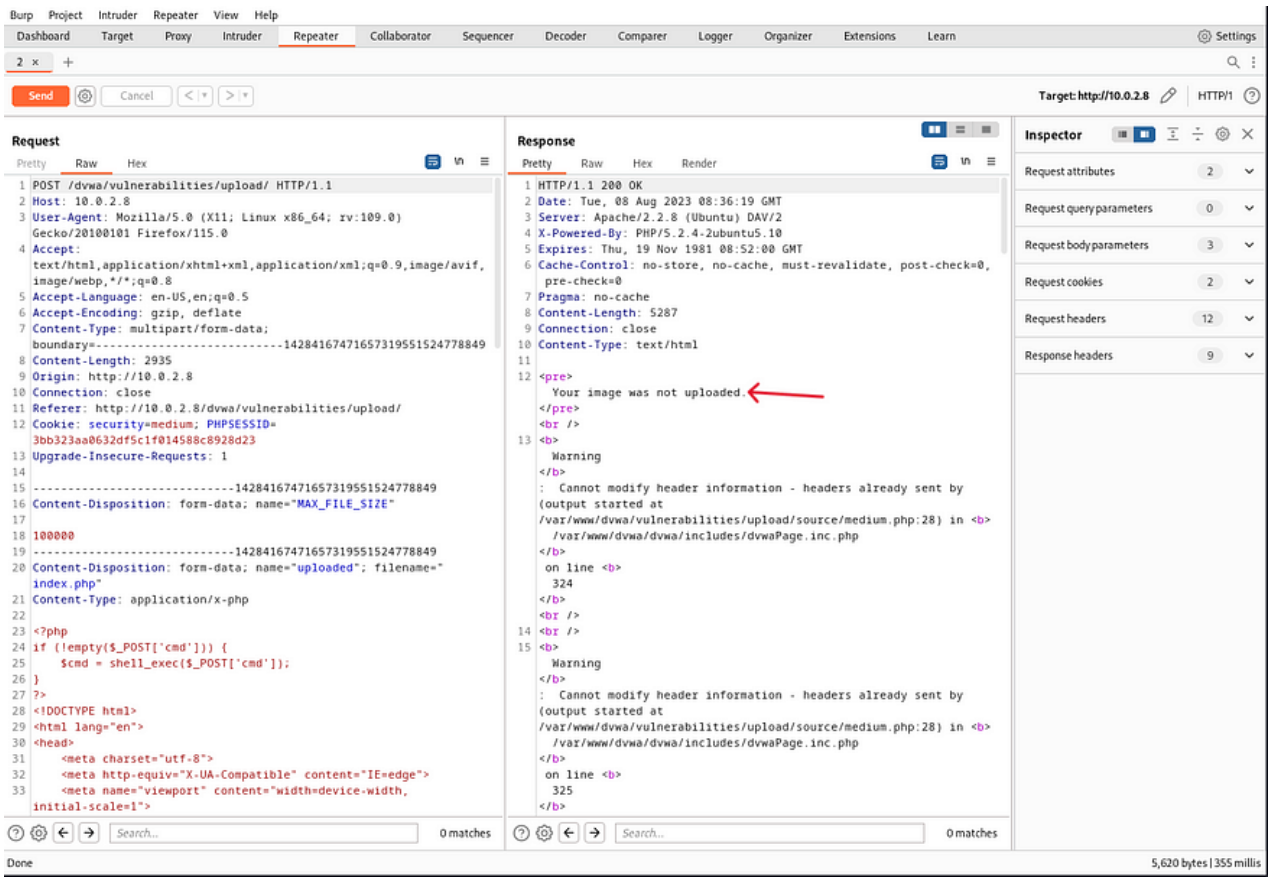
Conoscenze e configurazioni di base

Questo esercizio è una continuazione del report M4\W13\D2 tuttavia il livello di sicurezza è stato incrementato a “medium” e “high”.

Medium



Come da immagine se si carica un file PHP non lo fa caricare.

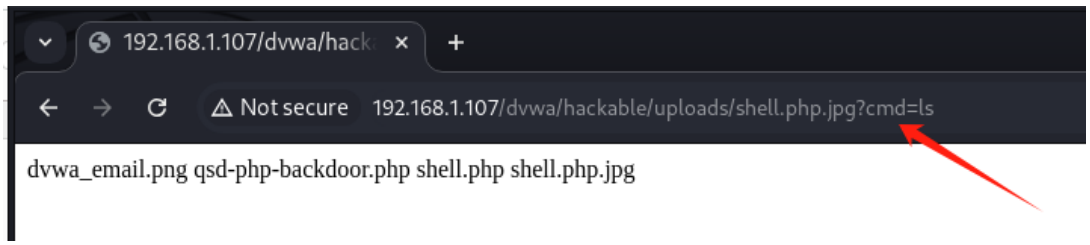


Dall’intercettazione si capisce che le tipologie di file accettate sono solo immagini.

Metodo estensione file

Per superare questa protezione si potrebbe cambiare l'estensione del file.

Infatti confondendo il filtro come file immagine, si può caricarlo con successo.



Questo metodo funziona come da ultima immagine.

High

Eseguendo lo stesso Upload come effettuato al livello Medium, risulta ugualmente possibile il caricamento e l'utilizzo del link http://192.168.1.105/dvwa//hackable/uploads/shell.php.jpeg?cmd=ls in questo caso per inviare un semplice comando **ls**

Metodo Alternativo

Durante il Upload del file php, cambiare il pacchetto intercettato, facendolo credere al server come fosse un immagine jpeg, sostituire la dicitura con quella in immagine.