Security Testing Report

-

Cosimo Pio Gallo - cosimogll1@gmail.com

October 26, 2025

Contenuto

Informazioni all’interno del documento

Title: W13D2 Gallo Cosimo Pio Exploit file upload

Classificazione: Non Confidenziale

Autore: Gallo Cosimo Pio

e-mail: cosimogll1@gmail.com

legal: false

Informazioni del cliente e dell’attività

client: Prof Valerio Casalino activity: Valutazione Attività activity_type: Exploit file upload #data inizio: 01/10/2025

Sintesi

Sono Andato ad effettuare varie prove per eseguire un exploit file upload

Scope

I nostri target:

- 192.168.50.101
- http://192.168.50.101/DVWA

Sintesi delle vulnerabilità

Tabella delle vulnerabilità’ rilevate:

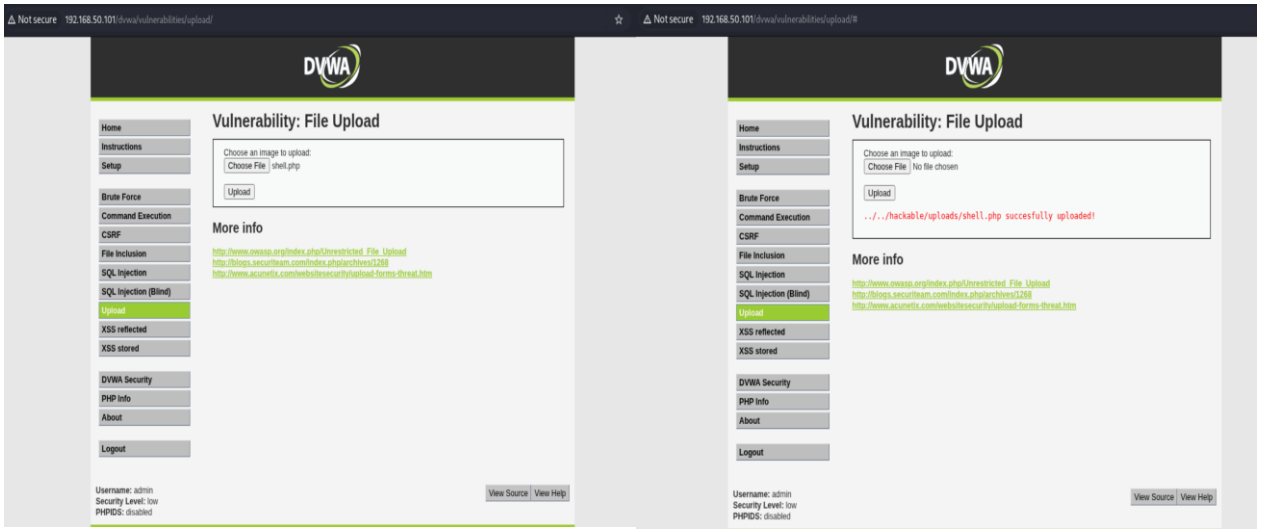
Nome vulnerabilità	Rischio	Σ
DVWA in low accetta tutte le estensioni	High	1
DVWA in medium accetta solo JPG/jpg	High	1
DVWA in medium accetta anche jpg	High	1

Vulnerabilità totali trovate	3

Vulnerabilità nel dettaglio

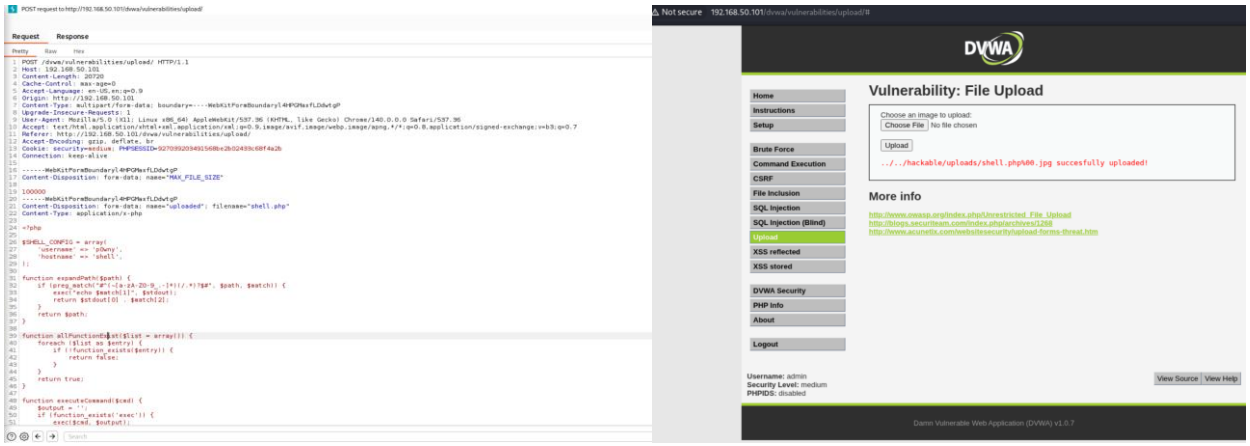
Vulnerabilità 1

Difficoltà LOW. La prima vulnerabilità trovata nella DVWA è quella della possibilità di uploadare tutti i tipi di file e quindi ogni tipo di estensione. Così facendo un attaccante potrebbe facilmente immettere una reverse shell nella nostra macchina.



Vulnerabilità 2

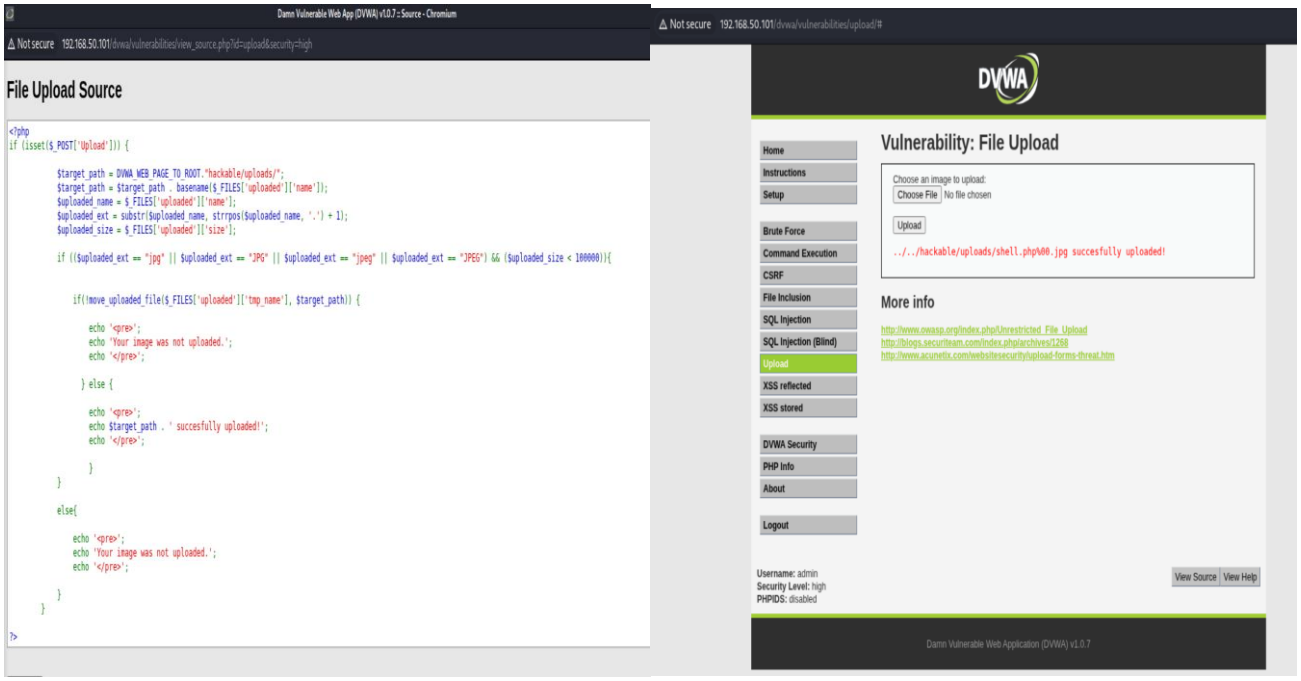
Difficoltà MEDIUM. La seconda vulnerabilità trovata nella DVWA è quella della possibilità di uploadare tramite file jpg un reverse shell. Questo lo vediamo inserendo prima una reverse shell normale e di conseguenza andando a leggere l'errore prodotto tramite burpsuite. Quindi andiamo a modificare il nome del file in modo tale però da farlo rimanere un php tramite il sito https://jorgectf.gitbook.io/awae-oswe-preparation-resources.



Vulnerabilità 3

Difficoltà HIGH. La terza vulnerabilità trovata nella DVWA è nel mio caso simile alla seconda. Confrontandomi con i miei colleghi di corso io non ho dovuto effettuare nessun passaggio in

più rispetto alla seconda vulnerabilità nella modalità MEDIUM. Quindi ho semplicemente ricaricato il file in php della mia reversa shell ed è filato tutto liscio e da qui deduco che la macchina in difficoltà HIGH sia anch'essa vulnerabile ai file JPG/jpg.



Target vulnerabili

- Upload di file con estensione JPG/jpg

Descrizione

Per rendere efficaci le nostre reverse shell in tutte le difficoltà basta semplicemente cambiare l'estensione tramite il sito citato sopra.

Rimedi

Aumentare la sicurezza e far sì che i file accettati non siano file normali ma che vengano prima controllati da un software apposito.

Risorse utilizzate

- https://jorgectf.gitbook.io/awae-oswe-preparation-resources