Esercitazione WEEK 16 D1 (2)

Exploit TWiki

Ettore Farris

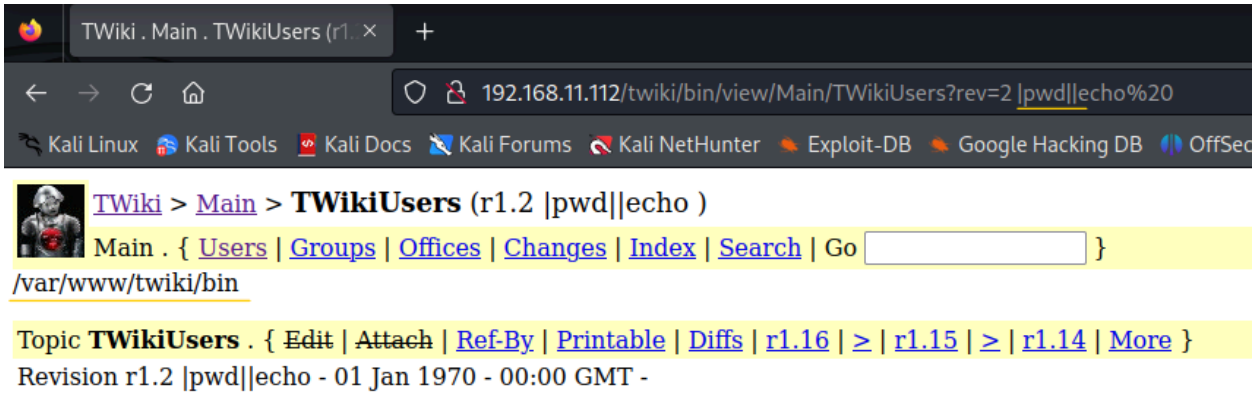
Descrizione sintetica

Sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Svolgimento

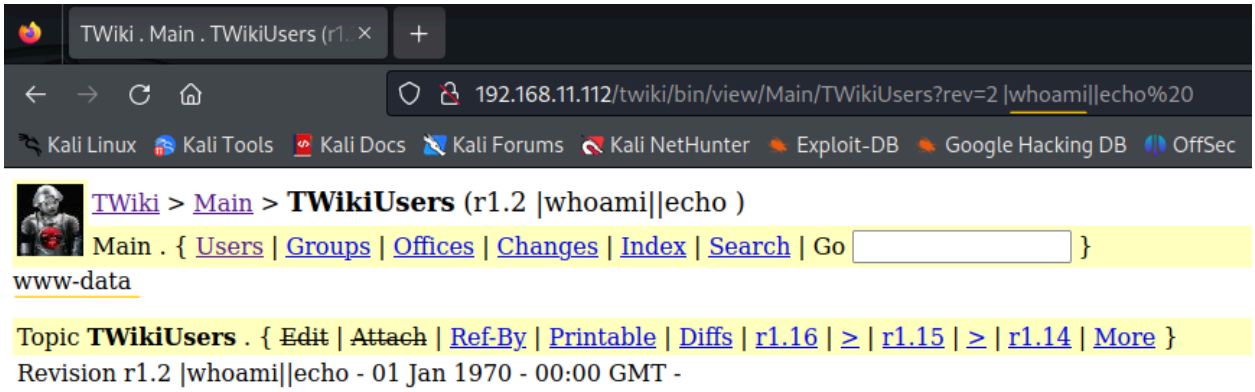
L'applicazione TWiki è vulnerabile in quanto il parametro *"rev"* consente l'inserimento di codice arbitrario. Infatti, se all'URL si inserisce il parametro in questo modo *?rev=2|**comando**||echo%20* è possibile ottenere delle informazioni sul target. Esempi:

- Directory corrente con il comando *pwd*



-

- Utente corrente con il comando *whoami*



- Processi attivi con il comando *ps aux*