Informazioni all'interno del documento

Title: W13D4 Gallo Cosimo Pio

Classificazione: Non Confidenziale

Autore: Gallo Cosimo Pio

email: cosimogll1@gmail.com

legal: false

Informazioni del cliente e dell'attivita'

client: Prof Valerio Casalino

activity: Valutazione Attivita'

activity_type: XSS REFLECTED, SQL INJECTION

data inizio: 03/10/2025

Sintesi

Tramite la DVWA andiamo ad effettuare gli esercizi di oggi che consistono nel: Scegliere una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection. Lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica. La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:- XSS reflected- SQL Injection (non blind)

Scope

I nostri target:

- 192.168.50.101
- http://192.168.50.101/DVWA

Sintesi delle vulnerabilita'

Tabella delle vulerabilita' rilevate:

Nome vulnerabilita'	**Rischio**	Σ
XSS Reflected	High	1
SQL Injection	High	1

Nome vulnerabilita'	Rischio	Σ
Vulnerabilita' totali trovate		2

Vulnerabilita' nel dettaglio

Vulnerabilita' 1 XSS Reflected

Difficolta' LOW. Possibilita' di inserire degli script malevoli per rubare cookie. script:

Window.location non fa altro che il redirect di una pagina verso un target che possiamo spcificare noi. Mettendoci in ascolto tramite NC su quella porta vedremo tutti i cookie di sessione

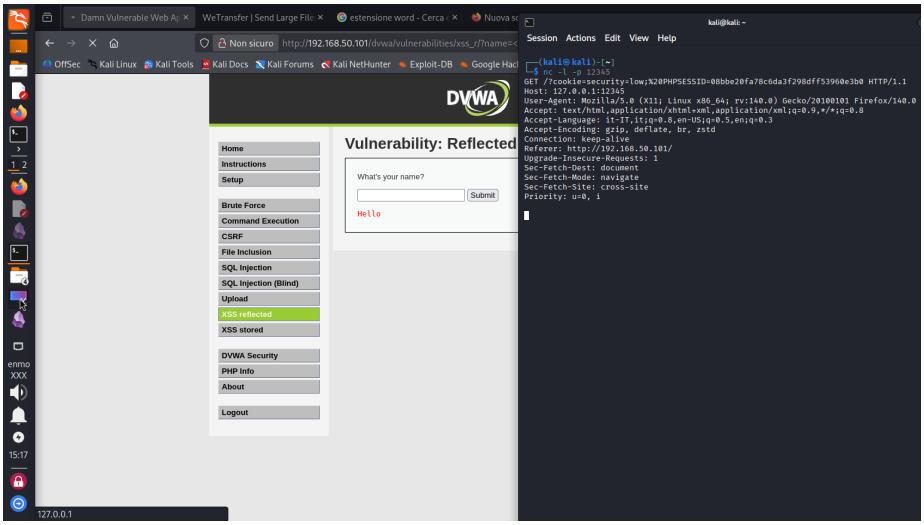
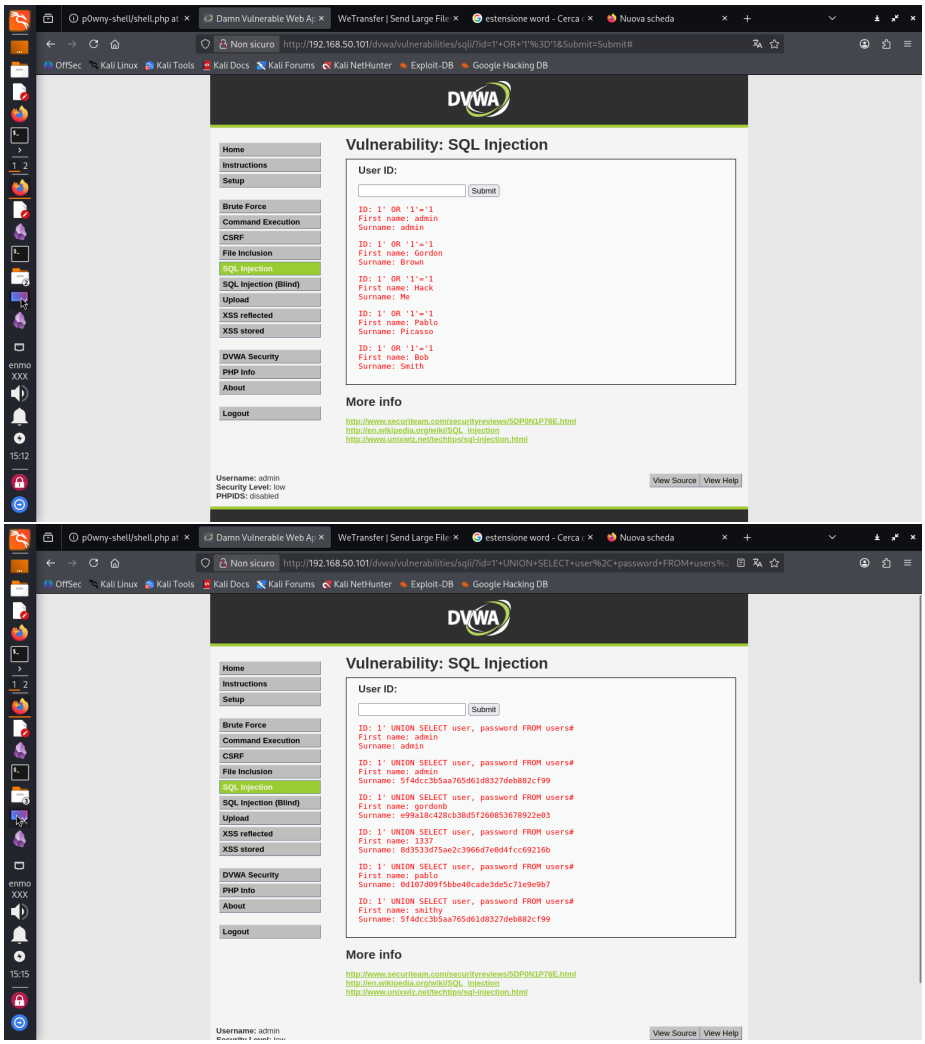


Figure 1: Screenshot

Vulnerabilita' 2 SQL Injection

Difficolta' LOW. Possibilita' di rubare le password degli utenti del sito. Tramite dei semplici codici quali: 1' OR '1'='1 (condizione sempre vera ci fara visualizzare tutti i nomi del database); 1' UNION SELECT user, passowrd FROM users# (tramite questa UNION l'app ci restituira' il nome utente con tutte le password)



Target vulnerabili

- Tutti gli utenti del database
- Cookie

Rimedi

Umentare la sicurezza.