Task 10/12/24: Exploit DVWA - XSS e SQL injection

Traccia

Argomento:

Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application DVWA.

Istruzioni:

Configurazione del Laboratorio:

- Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante).
- Verificate la comunicazione tra le due macchine utilizzando il comando ping.

Impostazione della DVWA

- Accedete alla DVWA dalla macchina Kali Linux tramite il browser.
- Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.

Sfruttamento delle Vulnerabilità:

- Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).
- Utilizzate le tecniche viste nella lezione teorica per sfruttare con successo entrambe le vulnerabilità.

Task 10/12/24: Exploit DVWA - XSS e SQL injection

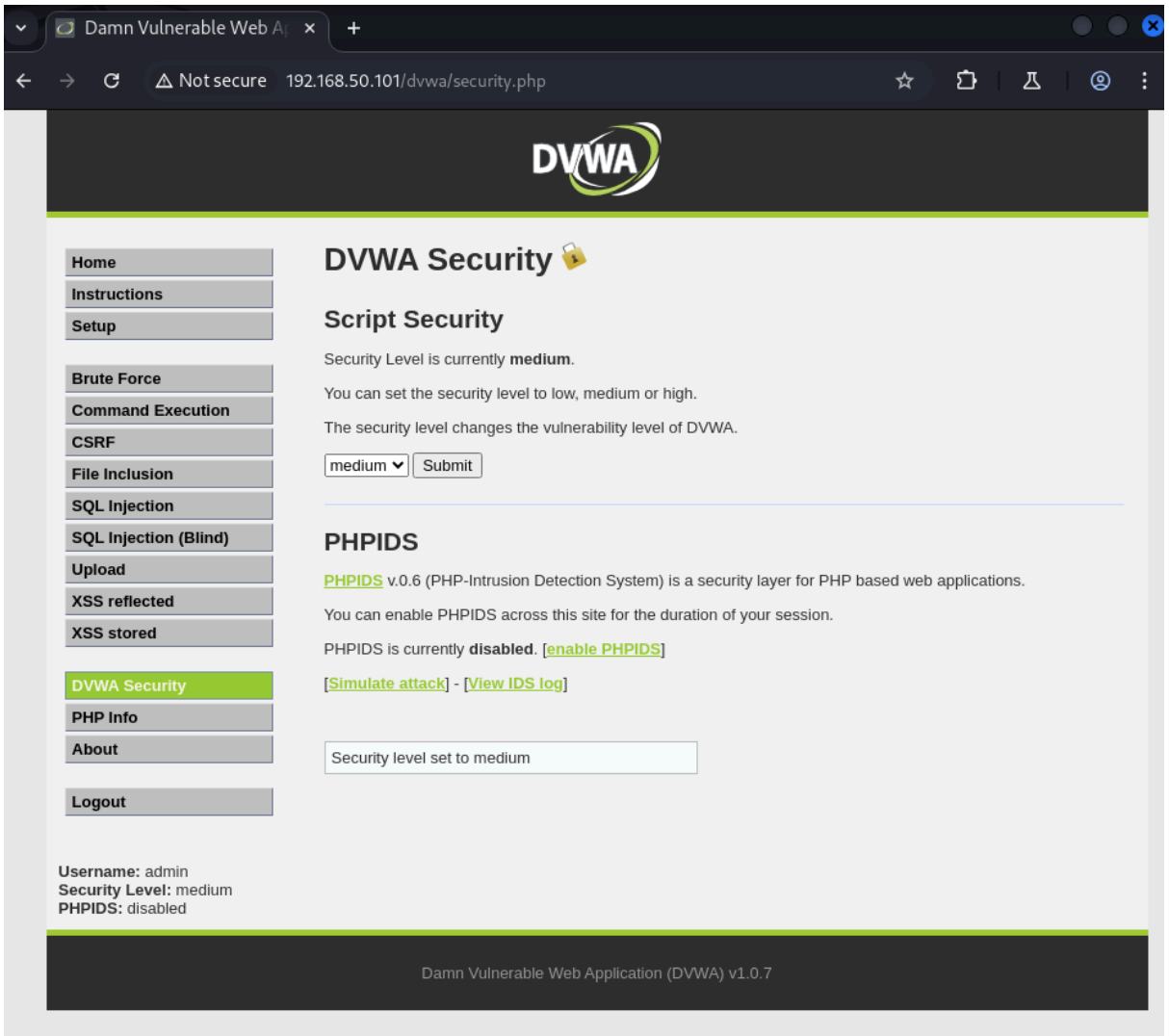
Report

Test di Vulnerabilità su DVWA

Questa relazione documenta i test effettuati per identificare vulnerabilità in Damn Vulnerable Web Application (DVWA). I test sono stati eseguiti con il livello di sicurezza impostato su MEDIUM, utilizzando strumenti come Burp Suite e SQLmap.

Impostazione della DVWA

Impostato il livello di sicurezza su MEDIUM.



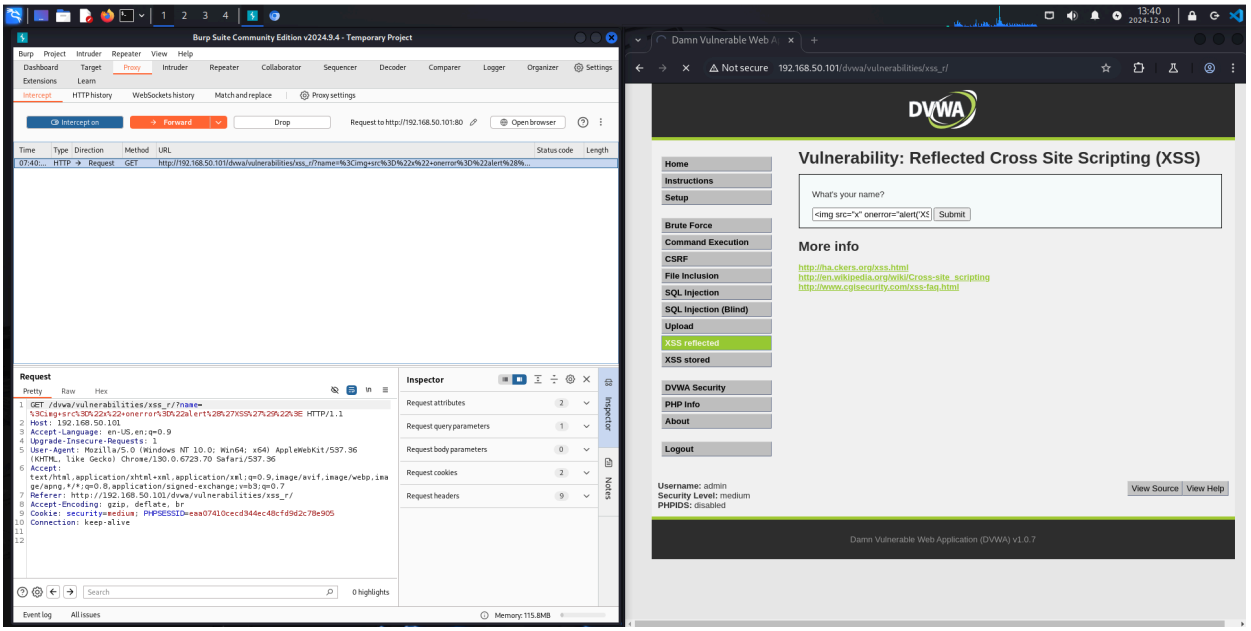
Sfruttamento delle vulnerabilità

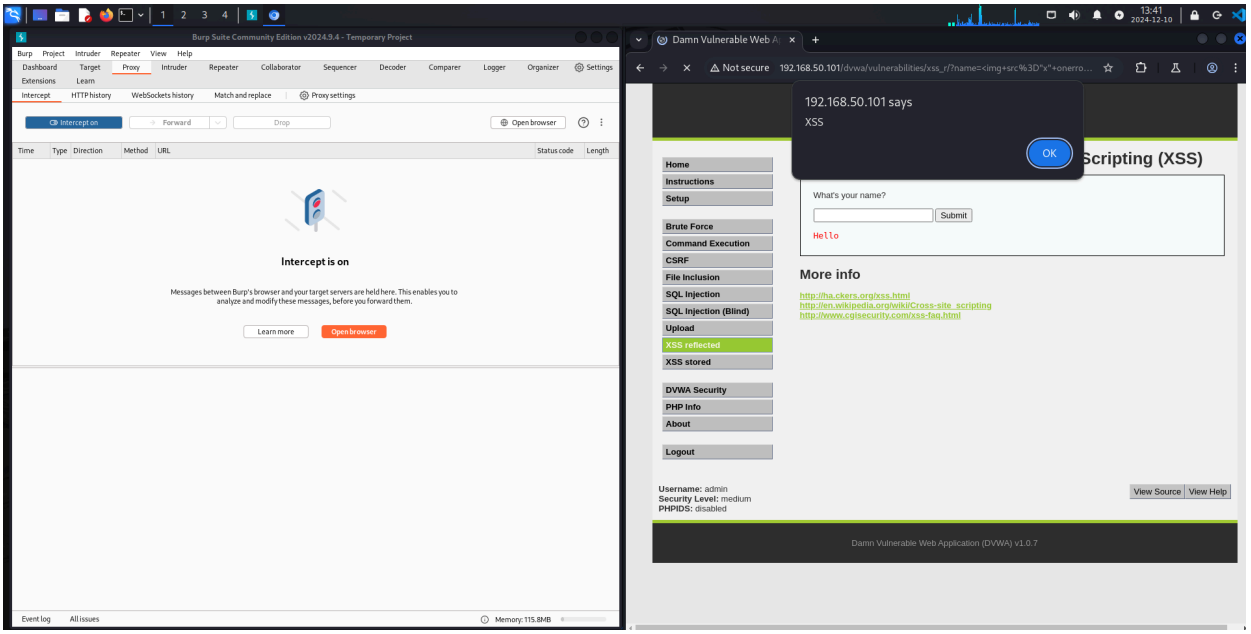
1. Vulnerabilità XSS Reflected

Tipo di XSS: Reflected XSS (Non-persistent)
Questo tipo di vulnerabilità consente di inserire del codice JavaScript malevolo che viene riflesso immediatamente nella risposta del server e viene eseguito nel browser dell'utente.

Payload scelto: <img src="x" onerror="alert('XSS')">
Questo payload sfrutta un'immagine inesistente per innescare l'evento onerror, che esegue uno script arbitrario.

Motivo della scelta: Al livello MEDIUM, DVWA utilizza funzioni come htmlspecialchars() per impedire l'esecuzione di codice HTML semplice come <script>. Tuttavia, i parametri negli attributi HTML (es. src) potrebbero non essere correttamente sanificati, consentendo bypass tramite eventi come onerror.



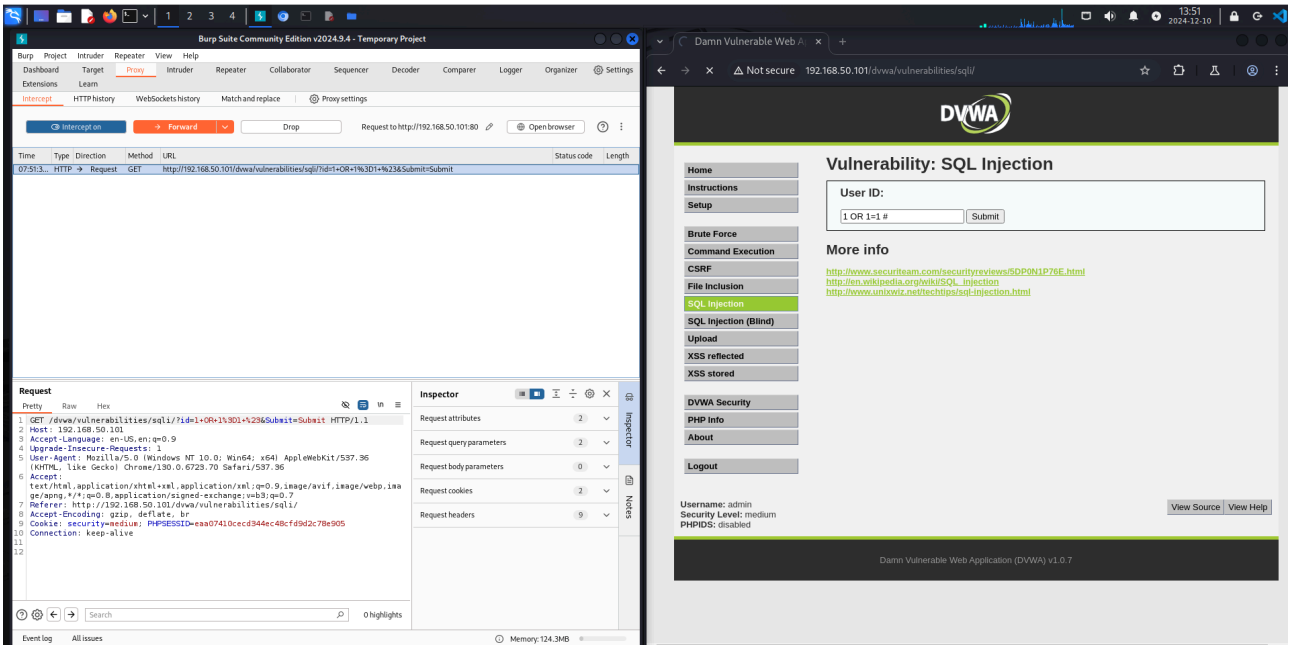


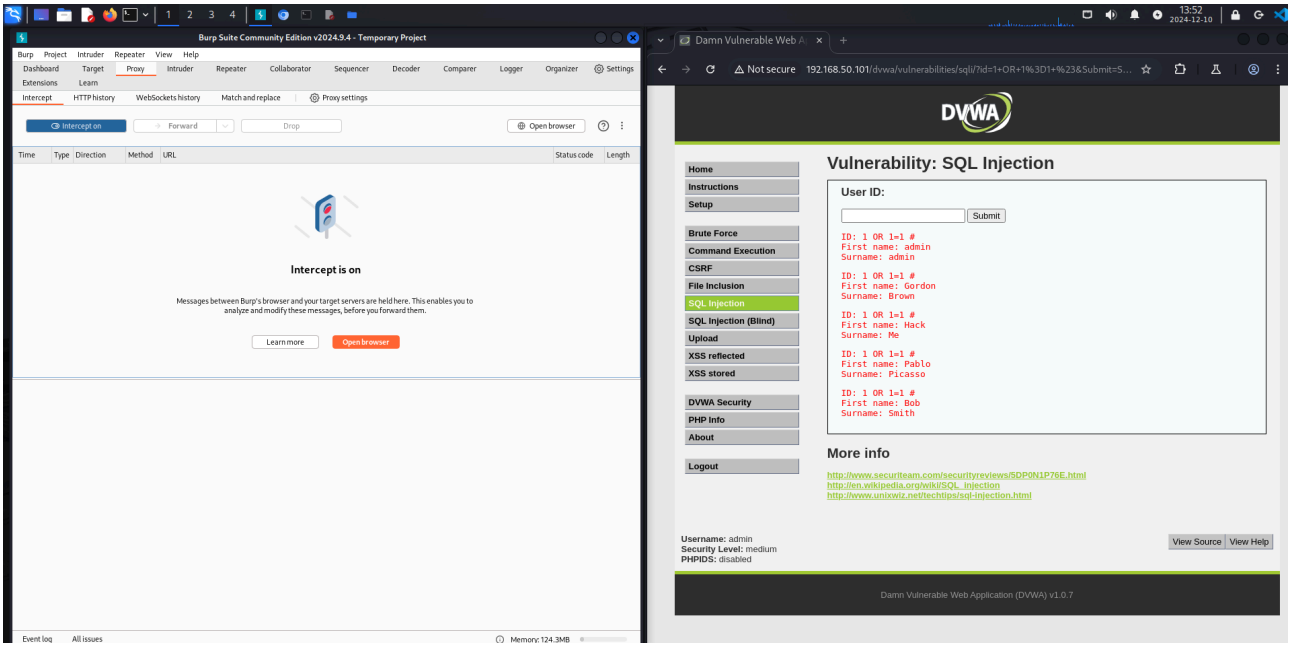
2. Vulnerabilità SQL Injection

Tipo di SQL Injection: Classic SQL Injection (Non-blind)
Questo tipo di vulnerabilità permette di manipolare una query SQL attraverso input non correttamente sanitizzati.

Payload scelto: 1 OR 1=1 #
1 OR 1=1: Aggiunge una condizione sempre vera alla query SQL, facendo sì che il database restituisca tutti i risultati o bypassi controlli specifici.
#: Commenta tutto ciò che segue nella query, annullando eventuali ulteriori controlli o condizioni che avrebbero potuto invalidare l'iniezione.

Motivo della scelta: Al livello MEDIUM, DVWA potrebbe utilizzare una protezione base come mysql_real_escape_string() per eseguire l'escaping di caratteri speciali. Tuttavia, queste protezioni non impediscono attacchi che sfruttano logiche condizionali come l'uso di OR o il commento della query.





Scansione database con sicurezza MEDIUM tramite SQLmap

1. Identificazione del Target ed Esecuzione di SQLmap con Dump completo del database

Tipo di comando: sudo sqlmap --cookie="${cookie}" -u "${url}" --random-agent --level=5 --risk=3 --tamper=space2comment --dump-all
Questo comando ha estratto tutti i dati disponibili nel database, dimostrando che la vulnerabilità era sfruttabile in modo completo.

2. Elenco delle tabelle nel database dvwa

Tipo di comando: sudo sqlmap --cookie="${cookie}" -u "${url}" --random-agent --level=5 --risk=3 --tamper=space2comment -D dvwa --tables
Questo passaggio ha mostrato tutte le tabelle disponibili nel database dvwa, consentendo di scegliere quelle più interessanti per il test.

3. Estrazione di dati specifici dalla tabella `users`

Tipo di comando: sudo sqlmap --cookie="${cookie}" -u "${url}" --random-agent --level=5 --risk=3 --tamper=space2comment -D dvwa -T users --columns -C user,password --dump
Questo comando ha estratto i valori delle colonne user e password dalla tabella users, rivelando e poi convertendo gli hash delle password.