Introduzione alle CTF

Lezione 1

Alessandro Righi   Cristiano Di Bari

Università degli Studi di Verona

3 Novembre 2023

Outline

1. Introduzione
2. Path traversal
    - Tool: Burp suite
3. SQL Injection
    - Tool: sqlmap
4. Cross site scripting
    - Tool: ngrok

Cosa sono le CTF?

Le *Capture The Flag* (CTF) sono delle sfide in cui i partecipanti devono trovare delle *flag*, ossia delle stringhe di testo, all'interno di sistemi informatici contenenti delle vulnerabilità di sicurezza.

Tipologie di CTF

Esistono due tipologie di CTF:

- *jeopardy*: il partecipante attacca una serie di servizi malevoli e sottomette le flag ad un sistema di verifica
- *Attack-Defence (AD)*: competizione a squadre dove ogni team deve attaccare i sistemi dell'avversario, e difendere i propri

Per queste lezioni di concentreremo sul primo tipo, di gran lunga le più diffuse, che è anche quello che organizza *Wurth*.

Tipologie di challenge

Tipicamente le challenge che si affrontano possono essere di 4 macro categorie:

- *Binary* è necessario ricercare vulnerabilità in un eseguibile, quali ad es. buffer overflow
- *Web* si tratta di trovare vulnerabilità in una web app, web API, o comunque applicativo esposto in rete
- *Crypto* è necessario decodificare un testo cifrato con un algoritmo (ovviamente vulnerabile)
- *Misc* sono challenge che non rientrano in nessuno dei tipi precedenti, e richiedono spesso creatività per essere affrontate

Per queste lezioni ci concentreremo sulla categoria *Web*.