$ linuxday --2026 --pontedera

Open source: trasparenza o vulnerabilità?

Link e risorse del seminario, nell'ordine in cui li abbiamo incontrati. Il codice aperto permette di controllare: tocca a noi guardarlo davvero.

Calisti Calisto · Linux Day · sabato 24 ottobre 2026 · I.T.I.S. G. Marconi, Pontedera

> i casi visti

xz Utils (2024)

La backdoor scoperta grazie a mezzo secondo di ritardo nei login SSH.

`CVE-2024-3094`
La scheda ufficiale della vulnerabilità.

Heartbleed (2014)

Una HeartbeatRequest con una lunghezza falsa: il server rimandava fino a 64 KB della sua memoria. Circa due anni prima della scoperta.

`heartbleed.com`
La spiegazione pubblicata dagli scopritori.

`CVE-2014-0160`
La scheda ufficiale della vulnerabilità.

`RFC 6520`
Lo standard dell'estensione Heartbeat di TLS: payload e length.

Log4Shell (2021)

Un difetto in una libreria Java di logging, spesso presente come dipendenza nascosta.

`CVE-2021-44228`
La scheda ufficiale della vulnerabilità.

> leggere le vulnerabilità

CVE, CVSS e KEV

Quale problema? Quanto è grave? È già stato sfruttato?

`cve.org`
Il catalogo degli identificativi CVE.

`nvd.nist.gov`
National Vulnerability Database: dettagli e punteggi CVSS.

`cisa.gov · catalogo KEV`
Le vulnerabilità sfruttate davvero negli attacchi.

Applicazioni web

I rischi più comuni, spiegati con esempi.

`owasp.org/Top10`
OWASP Top 10: i rischi più diffusi nelle applicazioni web.

> controllare le dipendenze e i progetti

Controllare le dipendenze

Strumenti SCA (Software Composition Analysis): scoprono se le librerie che usate hanno vulnerabilità note.

`github.com/pypa/pip-audit`
Controlla le dipendenze dei progetti Python.

`osv.dev`
Database aperto delle vulnerabilità nei pacchetti open source.

`github.com/google/osv-scanner`
Scanner che usa OSV per molti linguaggi.

Valutare un progetto

Capire come viene mantenuto un progetto open source e da dove arriva un pacchetto.

`scorecard.dev`
OpenSSF Scorecard: le pratiche di sicurezza di un repository.

`openssf.org`
Open Source Security Foundation.

`sigstore.dev`
Firma e verifica della provenienza dei pacchetti.

Chi è responsabile

La normativa europea sulla sicurezza dei prodotti con software.

`Regolamento (UE) 2024/2847`
Cyber Resilience Act, testo ufficiale su EUR-Lex.

> le demo, da rifare a casa

pip-audit su PyGoat

Analizziamo solo l'elenco delle dipendenze: non serve avviare l'applicazione.

```
# 1. scarica il progetto
git clone https://github.com/adeyosemanputra/pygoat.git
cd pygoat

# 2. installa lo strumento SCA in un ambiente virtuale
python3 -m venv demo
source demo/bin/activate
pip install pip-audit

# 3. controlla le dipendenze
pip-audit -r requirements.txt --no-deps --disable-pip
```

I risultati cambiano nel tempo: escono nuove vulnerabilità e nuove versioni corrette.

OpenSSF Scorecard

Il report pubblico si consulta dal browser, senza installare nulla.

`scorecard.dev/viewer/?uri=github.com/ossf/scorecard`

Il report usato nella demo. Sostituite l'indirizzo del repository per valutarne un altro.

```
# in alternativa, da terminale (serve un token GitHub)
export GITHUB_AUTH_TOKEN=...
scorecard --repo=github.com/ossf/scorecard --show-details
```

Non fermatevi al voto totale: leggete i singoli controlli e le motivazioni.

> tocca a voi

Allenarsi

Esercizi legali per imparare, dal terminale alla sicurezza web.

`overthewire.org/wargames/bandit`
Livelli progressivi per prendere confidenza con il terminale Linux.

`tryhackme.com`
Laboratori guidati di sicurezza, molti gratuiti.

`github.com/adeyosemanputra/pygoat`
PyGoat (OWASP): l'app volutamente vulnerabile della demo.

Gare per studenti

Competizioni di cybersecurity per mettersi alla prova.

`olicyber.it`
Olimpiadi Italiane di Cybersicurezza, per le scuole superiori.

`cyberchallenge.it`
Programma nazionale di formazione per ragazzi dai 16 ai 24 anni.

`ctftime.org`
Calendario mondiale delle gare Capture The Flag.

Community Linux

Persone con cui imparare e a cui dare una mano.

`lugmap.linux.it`
La mappa dei Linux User Group italiani: trovate quello più vicino.

`linuxday.it`
Il Linux Day in tutta Italia.

`ils.org`
Italian Linux Society.

Una regola per tutti: esercitatevi solo su sistemi vostri o in ambienti che vi autorizzano esplicitamente. L'accesso senza autorizzazione a un sistema informatico è un reato.
