ES S5 – L4

BONUS – Analisi delle vulnerabilità (CVE) tramite ChatGPT

Obiettivo dell’attività

L’obiettivo di questo esercizio bonus è utilizzare ChatGPT come strumento di supporto per l’individuazione e l’analisi di vulnerabilità note (CVE) relative a un software diffuso, comprendendone l’impatto, i possibili scenari di rischio e le principali strategie di mitigazione.

Software analizzato

Software scelto: WordPress

La scelta di WordPress è motivata dalla sua ampia diffusione e dall’elevato numero di installazioni presenti in contesti reali, rendendolo un target frequente di vulnerabilità e attacchi informatici.

Prompt utilizzato per l’individuazione delle CVE

Di seguito è riportato il prompt utilizzato per ottenere informazioni sulle vulnerabilità rilevanti (CVE) associate al software scelto:

Sto svolgendo un esercizio didattico di Cybersecurity.
Elenca le principali CVE rilevanti per WordPress.

Per ogni CVE indica:
- CVE ID
- breve descrizione della vulnerabilità
- impatto potenziale
- tipologia di vulnerabilità (es. XSS, SQL Injection, RCE, Privilege Escalation)
- modalità di sfruttamento (remoto/locale, autenticazione sì/no)
- gravità (bassa, media, alta, critica)
- possibili mitigazioni o soluzioni

Infine, suggerisci quali CVE risultano più critiche e meritevoli di approfondimento.

Individuazione delle CVE

Attraverso l’utilizzo di ChatGPT è stata ottenuta una lista di vulnerabilità note (CVE) relative a WordPress.
Le vulnerabilità individuate riguardano principalmente:

- Cross-Site Scripting (XSS)
- SQL Injection
- Privilege Escalation
- Remote Code Execution (RCE)

Sulla base delle informazioni fornite, sono state selezionate tre CVE considerate particolarmente rilevanti per gravità e potenziale impatto.

CVE selezionate per l’analisi

- **CVE-2022-21661**
- **CVE-2021-29447**
- **CVE-2020-36326**

La selezione è stata effettuata tenendo conto della gravità della vulnerabilità, della diffusione delle versioni colpite e della possibilità di sfruttamento in scenari realistici.

Analisi delle vulnerabilità

CVE-2022-21661

Questa vulnerabilità riguarda un problema di SQL Injection presente nel core di WordPress.
Un attaccante può sfruttarla per manipolare le query al database e ottenere accesso a informazioni sensibili.

Impatto:
Accesso non autorizzato al database e possibile compromissione dei dati.

Prerequisiti:
Attacco remoto, in alcuni casi con autenticazione di basso livello.

Mitigazioni:
Aggiornamento alla versione corretta di WordPress, sanitizzazione degli input e limitazione dei privilegi degli utenti.

Priorità: Alta.

CVE-2021-29447

Questa CVE è legata a una vulnerabilità di tipo XML External Entity (XXE).
Consente a un attaccante di leggere file locali o interagire con risorse interne al sistema.

Impatto:
Esposizione di file di configurazione e possibili accessi a sistemi interni.

Prerequisiti:
Attacco remoto tramite contenuti XML appositamente costruiti.

Mitigazioni:
Aggiornamento del software, disabilitazione delle entità XML esterne e controllo rigoroso degli input.

Priorità: Media-Alta.

CVE-2020-36326

Questa vulnerabilità consente una Privilege Escalation dovuta a una gestione non corretta dei permessi.

Impatto:
Un utente con privilegi limitati può ottenere diritti amministrativi, compromettendo completamente il sito.

Prerequisiti:
Utente autenticato con privilegi iniziali bassi.

Mitigazioni:
Aggiornamento del software, revisione dei ruoli utente e monitoraggio delle attività sospette.

Priorità: Alta.

Mitigazioni e piano di azione

Azioni immediate:

- Aggiornamento di WordPress all’ultima versione disponibile
- Applicazione delle patch di sicurezza
- Disabilitazione di plugin e temi non necessari

Azioni a breve termine:

- Revisione dei permessi degli utenti
- Scansioni di sicurezza periodiche
- Rafforzamento della configurazione del database

Azioni strutturali:

- Implementazione di un processo di patch management
- Monitoraggio continuo di log e accessi
- Backup regolari e test di ripristino

Conclusione

In questo esercizio bonus ho utilizzato ChatGPT per individuare e analizzare alcune vulnerabilità note (CVE) di WordPress.
L’attività mi ha permesso di comprendere l’importanza della gestione delle vulnerabilità, della priorità degli aggiornamenti e delle misure di mitigazione.
L’analisi delle CVE dimostra come l’utilizzo consapevole di strumenti di supporto possa facilitare la valutazione preliminare dei rischi, pur richiedendo sempre una verifica tramite fonti ufficiali.