**ESERCITAZIONE FINALE**
(21 gennaio 2026)

Corso: **3770/10840604-011/606/DEC/25**
Titolo: **ESPERTO IN SICUREZZA INFORMATICA – ED. ROVIGO**
Sede: **ROVIGO (RO), Via N. Badaloni 2**

Modulo 3: **MONITORAGGIO DELLA SICUREZZA DEL SISTEMA INFORMATIVO**

Docente: Davide Gessi

Corsista: Vadym Vykhvaten

Valutazione: 8/10

# Securing Software Esercitazione

1. **Attraverso quali tecniche un attore malevolo potrebbe “craccare” un software, cioè bypassare la registrazione o il pagamento per poterlo usare gratuitamente?**
2. **Distingui la natura dei due tipi di attacchi “cross-site” discussi:**
   **- Cross-Site Scripting (XSS)**
   **- Cross-Site Request Forgery (CSRF)**
3. **Perché è necessario “fare l'escape” (cioè neutralizzare) alcuni caratteri nei dati di input?**
4. **Nel contesto di SQL, che cos’è una prepared statement (istruzione preparata)?**
5. **Perché la validazione lato client (client-side validation) è considerata meno sicura rispetto a quella lato server (server-side validation)?**
6. **Riferimento alla vignetta GeekHero**
   **Dal punto di vista pratico, la vignetta sopra ha probabilmente ragione nel rappresentare il comportamento della maggior parte degli utenti verso il software open-source.**
   **Tuttavia, anche se questo fosse la tua opinione, perché potrebbe comunque essere una buona idea usare (o sviluppare) più software open-source, dal punto di vista della sicurezza informatica?**
7. **In che modo i package manager (come apt, yum, npm, ecc.) sono simili agli app store (Apple App Store, Google Play Store, Microsoft Store, ecc.) dal punto di vista della cybersecurity?**
8. **Contro quale tipo di minaccia aiuta a difendersi l’uso del campo Content-Security-Policy (CSP) nel nostro codice sorgente?**
9. **Fornisci un esempio concreto di una situazione in cui potresti voler usare il metodo HTTP POST invece del metodo GET.**
10. **Heartbleed (CVE-2014-0160)**
    **Il bug noto come Heartbleed, scoperto nel 2014, generò un’enorme preoccupazione su Internet: fu uno dei primi casi in cui una vulnerabilità informatica venne diffusa anche dai media generalisti, mentre i ricercatori di sicurezza cercavano di avvisare il pubblico e incoraggiare un aggiornamento urgente dei sistemi.**
    **Leggi informazioni su Heartbleed, ad esempio dalla pagina Wikipedia o da altre fonti affidabili (come un video divulgativo).**
    **Perché Heartbleed rappresentava una minaccia così grave per la sicurezza degli utenti?**
    **Qua la vignetta obbligatoria xkcd**

# Risposte:

1. PHISHING ,CODE INJECTION **Parziale**
2. CSRF ti fa fare una cosa che non voi tipo cambiare password o emeil o fare pagare invece XSS e rubare tuoi dati e vedere cosa fai **Concettualmente corretto**
3. perche posono esere interpretati come come comandi e non come carateri **Corretto.**
4. serve per prevenire inject sql **Molto sintetico ma giusto**
5. perche lato server vene controlata invece lato cliente po esere ragirata **Corretto. Distinzione client/server chiara**
6. perche sarebe visibile a tutti e migliorato da persone e tutto open surs **Corretto.** Open source = visibile, migliorabile, comunità
7. perche sono uficiali semplice di utilizo e instalare agiornate pero non garantiscuno sicurezza a 100% anche se hano protacoli **Buono. centralizzazione, aggiornamenti**
8. serve x protegirsi da javascript se vene emesso in un sito x rubare dati **Corretto**
9. get clicando il linc e ti fa acedere subito invece POST lo usi x cose molto inportanti e con conferma di eseguimento operazione **Corretto concettualmente**
10. ti permete tramite server chiedere dati e server sensa controlare ti ristituisce tutto che nella sua memoria e po avere pasword e chiavi di protezione **Buono.** Hai capito il cuore di Heartbleed