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: Abdelali Oudadas

Valutazione: 9/10

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. 1. Un hacker potrebbe usare queste tecniche per craccare un software e renderlo gratuito:

- Reverse Engeniring:
analizza il codice per comprendere la logica che sta dietro al programma.
-Debugging:
eseguendo il programma si osserva quando fallisce e quando fallisce il controllo della licenza
-Patching binario:
Modifica il file eseguibile per saltare i controlli di licenza
-Keyge:
crea uno script o un programma che genera chiavi di attivazione valide.
-Tampering della memoria:
modifica dei valori in memoria durante l'esecuzione per alterare lo stato di registrazione.
-Hooking:
quando avviene l'iniezione di codice personalizzato per intercettare e modificare la licenza.
-Emulazione di licenza:
intercettazione delle chiamate al server di licenza e risposta con un falso "attivato".
Molto buono. Elenco completo

2. XSS: è un attacco da utente a utente, in cui l'attaccante usa uno script malevolo in una pagina web vulnerabile che viene eseguito nel browser della vittima, l'obiettivo è rubare i cookie o alterare l'interfaccia per conto dell'utente.

CSRF: è un attacco da sito a utente in cui l'attaccante inganna il browser della vittima a inviare richieste non volute a quel sito. Il sito si fida della sessione attiva ma l'azione è scatenata da un contesto esterno.
Corretto.

3. L'escape è una necessario per prevenire attacchi dal esterno e file malevoli in caso contrario, c'è la possibilità di perdere il controllo della struttura o la query.
Corretto. Un po' sintetico

4. è un meccanismo di escaping in SQL che raddoppia i caratteri sensibili per prevenire attacchi Sql Injection.
Corretto. Un po' sintetico

5. Perchè un utente può bypassare la validazione lato client e quindi il server deve sempre effettuare un controllo lato server, visto che non ci si può fidare degli imput provenienti dal cliente.
Corretto. Un po' sintetico

6. Poichè il source code è alla portata di tutti, gli esperti nel capo possono verificare il codice e individuare possibili falle, vulnerabilità o bug e riportarlo ai porgrammatori per sistemarle.
Buono. Hai chiaro il vantaggio dell'open-source

7. Entrami usano firme difitali per garantire l'autenticità del software e distribuendo i pacchetti da fonti sicure, aumentando la sicurezza e riducendo il rischio di software malevolo
Buono. Concetto di firme e fonti sicure corretto,

8. Aiuta a difendersi da attacchi XSS bloccando l'esecuzione di script inline e i domini non autorizzati.
Corretto. CSP = anti-XSS

9. Si usa POst invece di GET quando si fanno acquisti online perchè i dati non compaiono nell'indirizzo del sito e non si rischia che qualcuno li attivi per sbaglio.
Sufficiente. CSRF token ?

10. Perchè la vulnerabilità permetteva a un attaccante di leggere porzioni di memoria del server, esponendo dati sensibili senza lasciare traccia, compromettendo l'integrità e la riservatezza delle connessioni HTTPS.
Buono. Hai capito la minaccia Heartbleed