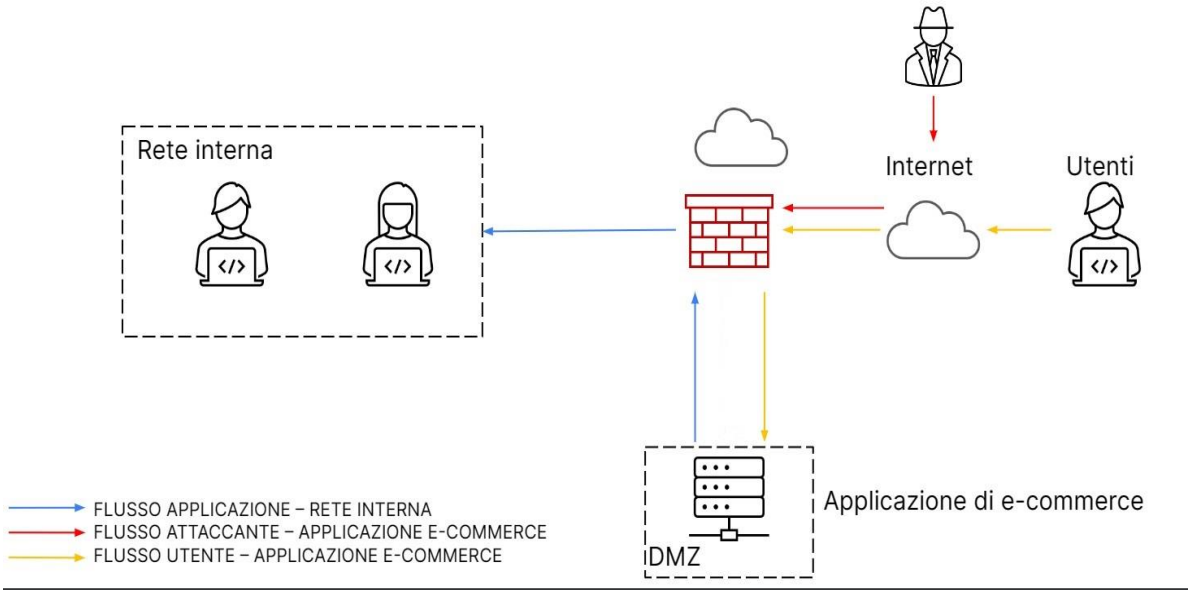
Risposta 1 e 3 esercizio

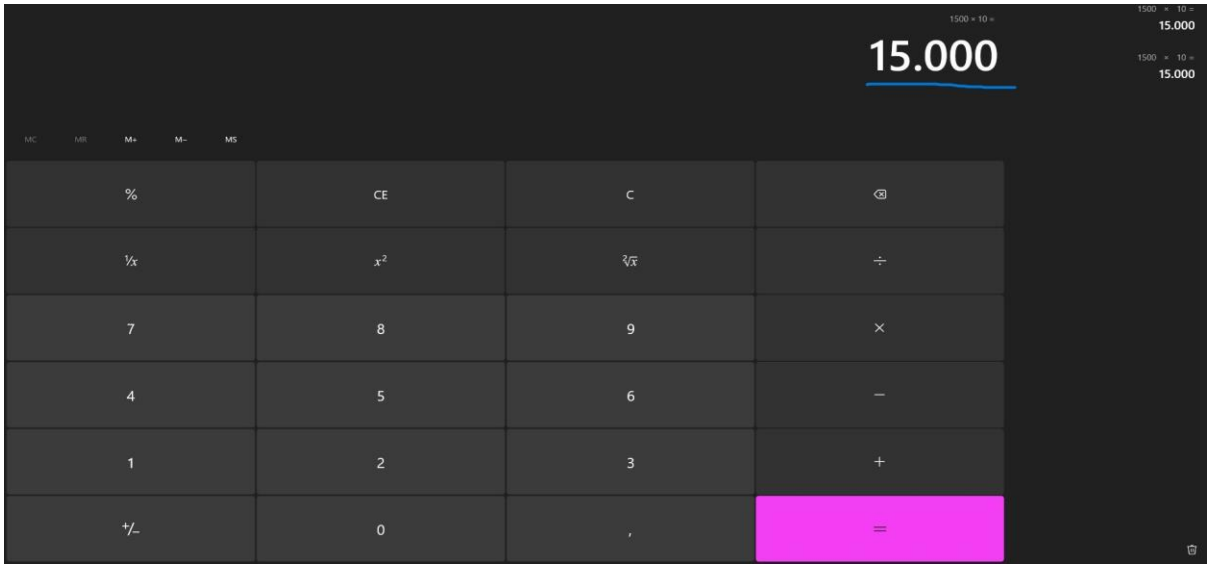


*Per quanto riguarda l'attacco "**Xss**", la cosa più giusta da fare è togliere tutti i caratteri non convenzionali di input dalla web app tipo **(<> script etc.)** cambiando tutto con **le espressioni regolari** perché il codice maligno può entrare attraverso gli URL, ragion per cui se non abbiamo questa difesa alzata l'attaccante entra tranquillamente.*

*Invece per "**Sqli**" è simile ma non uguale, bisogna sanare gli **input** degli utenti, aggiornare sempre tutto plugins etc. Gestire bene i privilegi di **SQL**, ed implementare le proprie logiche in modo da renderlo più sicuro, tenendo costantemente aggiornati, il rischio si riduce di molto.*

Nella foto, è stato solo cancellato il flusso malevolo, il malintenzionato ancora può accedere via Internet al sito.

Risposta 2-5



Secondo il calcolo delle perdite "*sle = av * ef ovvero 1500 * 10 = 15.000*", la perdita ammonta ogni 10 minuti a 15.000 euro, un dato significativo per il business della Web App

*Per difendersi dal "**Ddos**" conviene mettersi in modalità amministratore, un utente normale non può avere permessi e quindi avendo i permessi una volta fatto ciò, usare una "**VPN**" per nascondere l'indirizzo "**IP**".*

*Se vogliamo una modifica più aggressiva della struttura, possiamo cambiare il router se non è performante e usare un **VPN**, e bisogna anche usare un **firewall software*** per mitigare *l'attacco, ad esempio Norton360 un firewall multistrato, ma ce ne sono tanti.*