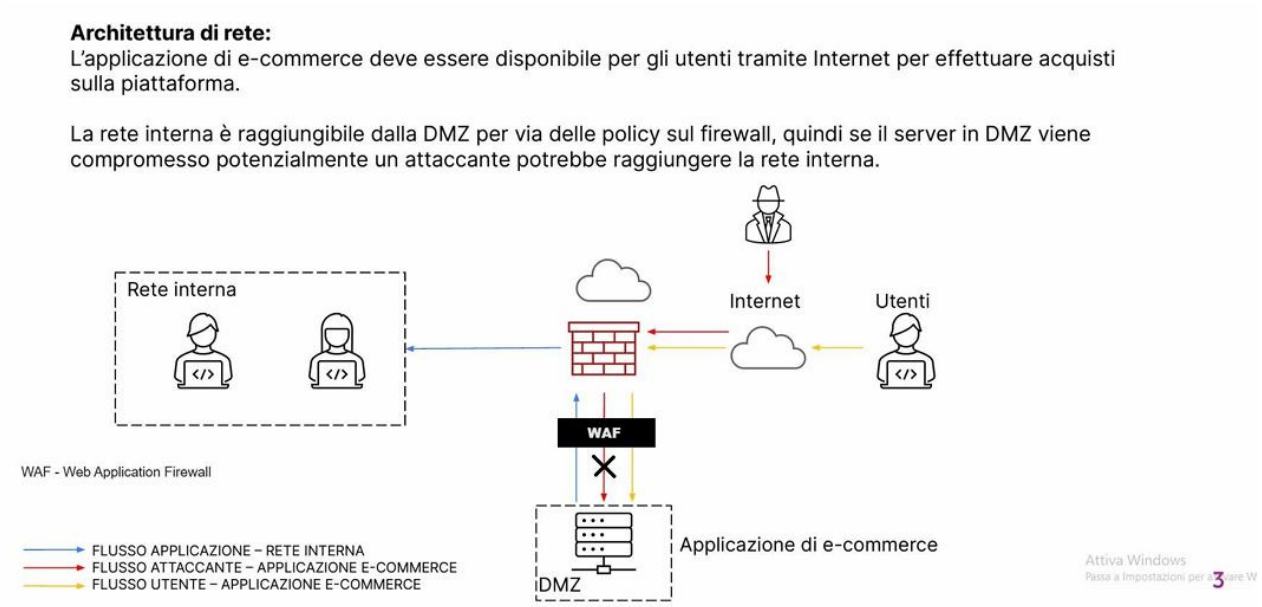
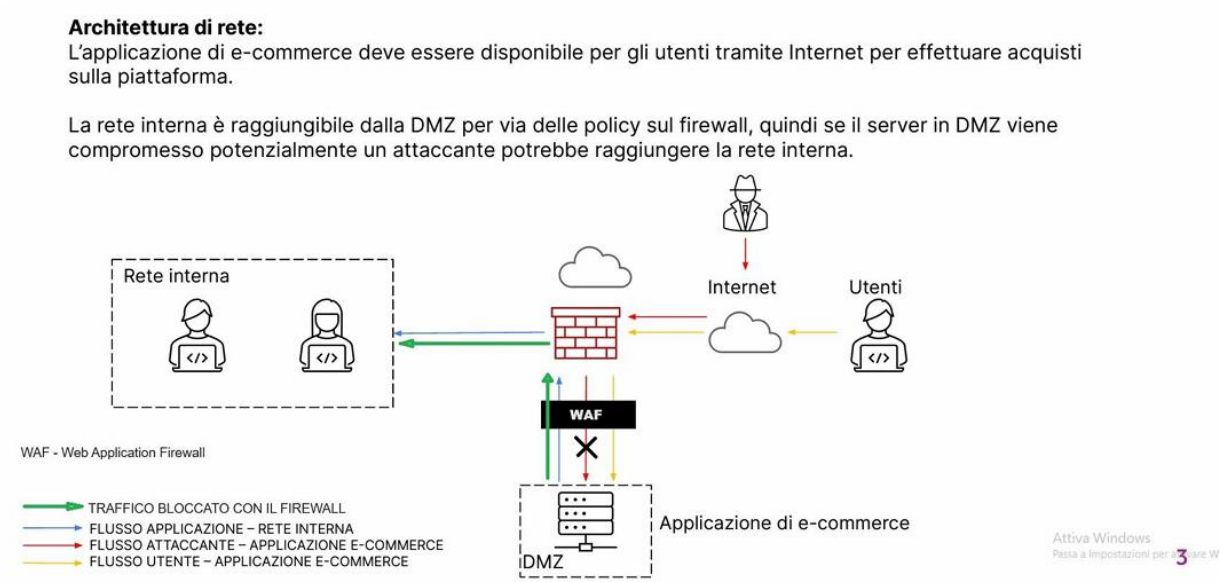
1- **Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura di sotto in modo da evidenziare le implementazioni.**

Le soluzioni per limitare attacchi SQLi e XSS sono varie, ma è sicuramente basilare, in fase implementativa, una programmazione che preveda un controllo di tutte le potenziali porte di accesso all'archivio di gestione dei dati. Dunque, la validazione degli input, le query parametrizzate tramite template ed una adeguata gestione del reporting degli errori possono rappresentare delle buone pratiche di programmazione utili allo scopo.
Un'altra soluzione è l'utilizzo di un WAF– Web application Firewall, il cui funzionamento è quello di monitorare, filtrare o bloccare il traffico dati proteggendo le Web App da possibili minacce.



2- **Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.**

Per fare un'analisi immediata calcoliamo il danno moltiplicando il guadagno di ogni minuto (1500 euro) per i 10 minuti in cui il sito sarà irraggiungibile; otterremo così 15 mila euro di danno. Per limitare le perdite e scongiurare attacchi futuri, è consigliata l'installazione di un Next Generation Firewall e la possibilità di un server separato per il full backup dell'intera applicazione e/o un cloud esterno (in alternativa, un sito di back up) da utilizzare nel caso il danno sia più grave dell'esempio in questione, tale da garantire ai clienti il continuo servizio.



3- Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

Blocchiamo con il firewall il traffico in uscita dalla web app alla rete interna, in modo da isolare la rete dai dati della web app, senza scollegarla da internet in modo che l'attaccante abbia ancora accesso alla stessa.

4- Modifica più aggressiva dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2