Traccia: Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti. Esercizio Traccia e requisiti

1. Azioni preventive : 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 in modo da evidenziare le implementazioni. È richiesta sola modifica

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

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 .

4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica «più aggressiva» dell'infrastruttura: anche una soluzione al punto 2) integrando eventuali altri elementi di sicurezza (integrando Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

1.

Per difendere un'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è importante implementare diverse azioni preventive. Ecco alcune delle principali misure che potrebbero essere adottate:

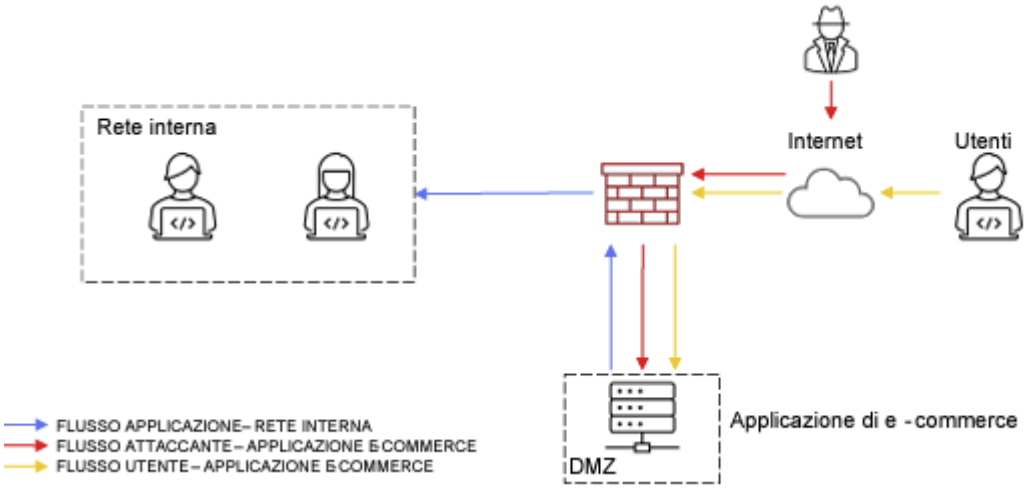
Per difendere contro SQL Injection (SQLi):

1. **Utilizzare Query Parametrizzate**:
   - Assicurati di utilizzare query parametrizzate o prepared statements per tutte le interazioni con il database. Questo approccio separa i dati dalle istruzioni SQL, impedendo che i dati dell'utente vengano interpretati come parte della query.
2. **Sanitizzazione e Validazione dei Dati**:
   - Implementa la validazione e la sanitizzazione rigorosa dei dati in ingresso. Verifica che i dati inseriti dagli utenti siano conformi ai formati previsti e rimuovi caratteri pericolosi.
3. **Utilizzare Stored Procedures**:
   - Preferisci l'uso di stored procedures al posto delle query SQL dinamiche quando possibile, riducendo la possibilità di SQL Injection.
4. **Implementare i Principi del Least Privilege**:
   - Configura le credenziali del database in modo che abbiano solo i permessi necessari per l'applicazione, minimizzando il danno possibile in caso di compromissione.

Per difendere contro Cross-Site Scripting (XSS):

1. **Sanitizzazione e Codifica dei Dati**:
   - Sanifica e codifica l'output HTML, JavaScript e CSS per evitare che il contenuto pericoloso venga eseguito nel browser. Usa librerie e framework che gestiscono automaticamente la codifica.
2. **Utilizzare Content Security Policy (CSP)**:

    - Implementa una Content Security Policy (CSP) per ridurre la possibilità di esecuzione di contenuti non autorizzati e script maligni. Definisci una politica CSP che consenta solo le risorse sicure.
3. **Evitare l'Inserimento di Dati Non Sanitizzati nelle Risposte**:
    - Non inserire direttamente dati non sanitizzati nelle risposte del server. Utilizza meccanismi di escape per evitare l'inclusione di contenuti malevoli.
4. **Impostare e Gestire Adeguatamente le Intestazioni di Sicurezza**:
    - Configura intestazioni di sicurezza come `X-XSS-Protection` e `X-Content-Type-Options` per proteggere ulteriormente l'applicazione.



- **Firewall per applicazioni web (WAF):** Aggiungi una sezione nella figura che mostra l'uso di un Web Application Firewall (WAF) sia nella DMZ che nella rete interna. Il WAF può filtrare e monitorare il traffico HTTP per prevenire SQLi e XSS.
- **Modifica della figura:** Inserisci un blocco che rappresenta il WAF, posizionato tra il server web e la rete interna, evidenziando la protezione contro le vulnerabilità dell'applicazione.

2.

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio durante un attacco DDoS (Distributed Denial of Service), possiamo seguire questi passaggi:

1. Calcolo dell'Impatto Economico

Dati forniti:

- Durata dell'interruzione: 10 minuti

- Spesa media per minuto degli utenti: 1.200 €

Calcolo dell'Impatto Totale:

1. **Calcolare la spesa totale degli utenti per l'intervallo di tempo non raggiungibile:**
   Spesa Totale=Spesa per Minuto×Durata dell’Interruzione\text{Spesa Totale} = \text{Spesa per Minuto} \times \text{Durata dell'Interruzione}Spesa Totale=Spesa per Minuto×Durata dell’Interruzione
   Spesa Totale=1.200 €×10 minuti\text{Spesa Totale} = 1.200 \, € \times 10 \, \text{minuti}Spesa Totale=1.200€×10minuti Spesa Totale=12.000 €\text{Spesa Totale} = 12.000 \, €Spesa Totale=12.000€

Quindi, l'impatto economico dovuto all'interruzione del servizio per 10 minuti è di **12.000 €**.

2. Valutazione di Azioni Preventive

Per mitigare l'impatto di attacchi DDoS e migliorare la resilienza dell'applicazione web, è possibile implementare diverse azioni preventive:

1. **Implementazione di Soluzioni Anti-DDoS:**
   - Utilizzare servizi anti-DDoS forniti da terze parti come Cloudflare, AWS Shield, o Akamai Kona Site Defender. Questi servizi possono rilevare e mitigare attacchi DDoS riducendo l'impatto sui server.
2. **Scalabilità e Bilanciamento del Carico:**
   - Implementare bilanciatori di carico per distribuire il traffico su più server. Questo aiuta a gestire meglio picchi di traffico, incluso il traffico proveniente da attacchi DDoS.
   - Usare soluzioni di scalabilità automatica che possono aumentare la capacità del sistema in risposta a picchi di traffico.
3. **Caching e CDN:**
   - Utilizzare reti di distribuzione dei contenuti (CDN) per ridurre il carico sui server originari e distribuire il traffico su più punti di presenza. Le CDN possono anche aiutare a mitigare gli attacchi DDoS.
4. **Filtraggio e Limitazione del Traffico:**
   - Configurare firewall e sistemi di filtraggio per bloccare il traffico sospetto o non richiesto. Limitare il numero di richieste da un singolo indirizzo IP per prevenire l'abuso.
5. **Monitoraggio e Allerta:**
   - Implementare sistemi di monitoraggio per rilevare attività anomale e lanciare allerte tempestive in caso di attacco. Questo consente una risposta rapida per mitigare l'impatto.
6. **Piani di Contingenza e Risposta agli Incidenti:**
   - Avere un piano di risposta agli incidenti ben definito e testato per gestire attacchi DDoS. Questo include procedure per il coordinamento tra i team e la comunicazione con i clienti.

3.

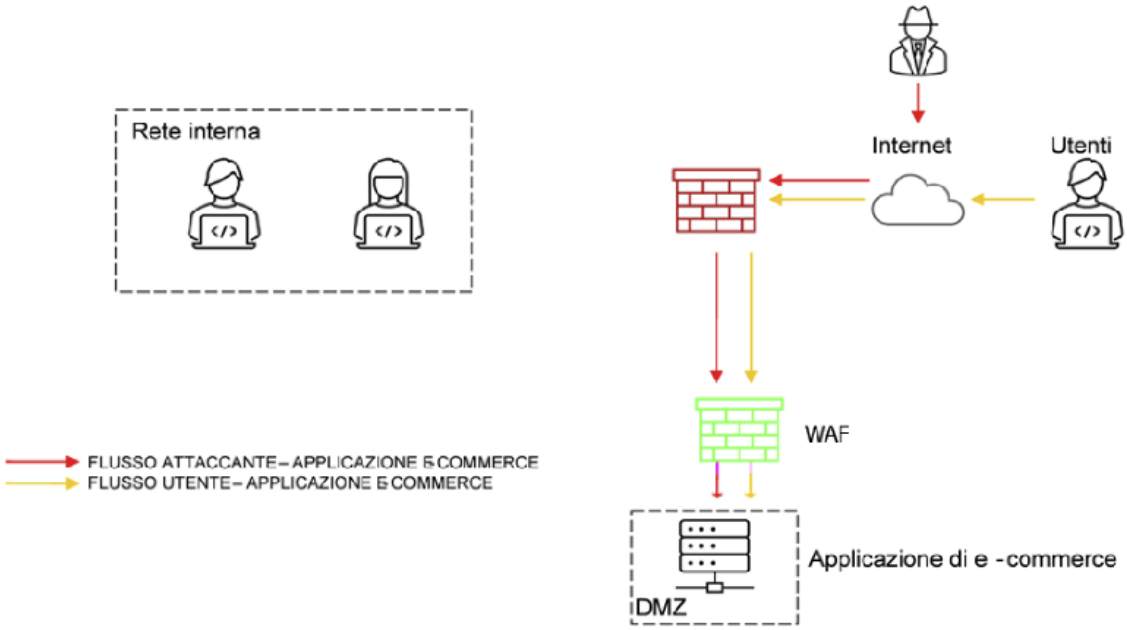
- **Segmentazione della Rete**: Modifica la figura per mostrare la macchina infettata isolata in una sottorete separata. Questo segmento della rete dovrebbe essere completamente disconnesso dalla rete principale per prevenire la diffusione del malware.

- **Firewall e Regole di Accesso**: Aggiungi un firewall tra la macchina infettata e la rete principale. Configura il firewall per bloccare tutto il traffico in entrata e in uscita verso la rete principale, permettendo solo comunicazioni limitate o monitorate.

Ecco come potresti visualizzare queste modifiche:

- **Rete Principale**: Una rete centrale, con dispositivi e server normali.
- **Segmento Isolato**: Un segmento della rete isolato da firewall e regole di accesso, con la macchina infettata all'interno.
- **Firewall**: Un firewall tra il segmento isolato e la rete principale, con regole di accesso definite.
- **Monitoraggio**: Icone di strumenti di monitoraggio su entrambi i lati del firewall.
- **Dati Bloccati**: Linee o simboli che mostrano il blocco del traffico tra la macchina infettata e la rete principale.

Questa configurazione visualizzerà chiaramente che la macchina compromessa è isolata per evitare la propagazione del malware, mentre l'accesso all'attaccante non viene immediatamente rimosso.



5.

Proposta 1: Potenziamento della Sicurezza Fisica e Digitale

- **Firewall Avanzato e UTM (Unified Threat Management):** Implementazione di un firewall di ultima generazione con funzionalità UTM. (2000 - 3000 euro)

- **Sistema di Monitoraggio e Rilevamento delle Minacce (SIEM):** Implementazione di una soluzione SIEM per il monitoraggio in tempo reale e l'analisi delle minacce. (2000 - 3000 euro)

Totale Stimato: 6000 euro

Proposta 2: Integrazione di Sicurezza per le Reti e la Protezione dei Dati

- **Sicurezza di Rete:**
  - **Firewall e VPN:** Aggiornamento o sostituzione del firewall con un modello avanzato e implementazione di una VPN per il traffico remoto. (2500 - 4000 euro)
  - **Sistema di Prevenzione delle Intrusioni (IPS):** Implementazione di un IPS per rilevare e prevenire attività sospette. (1500 - 2000 euro)

- **Backup e Recupero Dati:**
  - **Sistema di Backup e Ripristino:** Implementazione di un sistema di backup automatico e ripristino dei dati su cloud o su hardware dedicato. (2000 - 3000 euro)
  - **Crittografia dei Dati:** Implementazione di soluzioni di crittografia per proteggere i dati sensibili. (1000 - 1500 euro)

Totale Stimato: 7000 - 10500 euro