CONSEGNA S9/L5

DOMANDE:

1. Azioni preventive: quali azioni preventive implementereste 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

Azioni preventive contro SQL Injection (SQLi):

Parameterized Statements/Prepared Statements:

- Utilizzare dichiarazioni parametriche o prepared statements per le query SQL.
- Evitare l'interpolazione diretta di input utente nelle query.

Validazione dell'Input:

- Validare e filtrare attentamente l'input utente.
- Accettare solo input che corrispondono ai formati attesi.

Least Privilege Principle:

- Assegnare i privilegi minimi necessari al database per l'utente con cui l'applicazione si connette al database.

Utilizzo di Stored Procedures:

- Utilizzare stored procedures quando possibile, riducendo la possibilità di iniezioni.

Azioni preventive contro Cross-Site Scripting (XSS):

Escaping Output:

- Effettuare l'escape delle variabili di output prima di renderle nella pagina HTML.

Content Security Policy (CSP):

- Implementare una CSP per limitare quali risorse possono essere caricate e da dove.

HTTPOnly e Secure Cookies:

- Impostare i cookie come HTTPOnly per impedire l'accesso via JavaScript.
- Utilizzare il flag "Secure" per garantire che i cookie vengano trasmessi solo su connessioni sicure (HTTPS).

Input Validation e Whitelisting:

- Validare e filtrare attentamente l'input utente, consentendo solo caratteri e formati necessari.
- Utilizzare whitelisting per accettare solo input noti e previsti.

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.

Per calcolare l'impatto finanziario dovuto a un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, possiamo utilizzare la seguente formula:

Impatto Finanziario = Durata della Disponibilità x Spesa Media per Minuto per Utente

Dato che l'applicazione è non raggiungibile per 10 minuti e gli utenti spendono in media 1.500 € al minuto, supponiamo che il numero medio di utenti al minuto sia N.

Quindi: **Impatto Finanziario = 10minuti × 1.500€**

Impatto Finanziario = 10minuti × 1.500€ / minuto

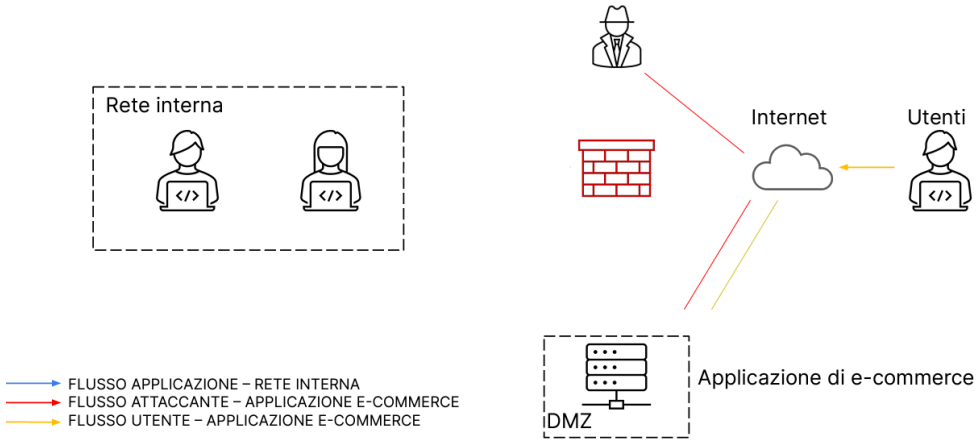
Impatto Finanziario = 15.000 €

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.

Si può adottare una strategia basata sull'isolamento della macchina infettata, e quindi la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non più connessa alla rete interna, ***come in figura sotto****.*

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Architettura di rete: L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.