# S9/L5 PEROJECT

EPICODE 2023/2024

4 FEBBRAIO 2024

## Sommario



**Traccia:**

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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

1. **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.

**1. Response:** l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

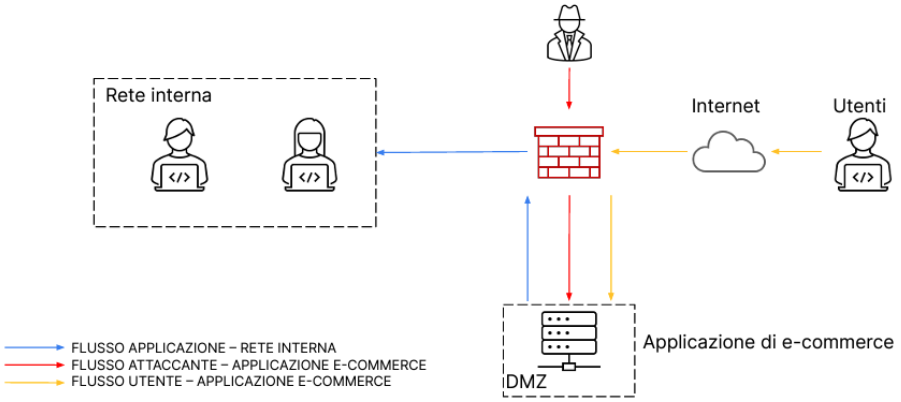
Modificate la figura in slide 2 con la soluzione proposta.

EPICODE

**Esercizio**
Traccia e requisiti

**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.




3

## 1. AZIONI PREVENTIVE

Prima di rispondere ai quesiti della traccia del progetto di oggi ricordiamo e definiamo cosa sono gli SQLi Injection e XSS attacks.
In questo modo possono essere comprese a pieno le azioni di rimedio nel caso in cui stiamo lavorando in un'azienda "x" ed essere pronti a risolvere gli attacchi in maniera adeguata e con prontezza.

**SQL Injection (SQLi):**
SQL Injection è una vulnerabilità di sicurezza che consente agli attaccanti di eseguire comandi SQL non autorizzati su un database.
Gli attaccanti sfruttano questa vulnerabilità inserendo del codice SQL dannoso nelle voci di input dell'applicazione web, il che può portare alla compromissione dei dati o all'esecuzione di azioni non autorizzate sul database.
**Cross-Site Scripting (XSS):**
Cross-Site Scripting è una vulnerabilità che consente agli attaccanti di inserire script dannosi all'interno di pagine web visualizzate da altri utenti.
Gli attaccanti sfruttano questa vulnerabilità inserendo script dannosi nei campi di input dell'applicazione web, che possono essere eseguiti sul browser degli utenti che visualizzano la pagina, compromettendo così la loro sessione o rubando informazioni sensibili.

La prima soluzione proposta per tali attacchi è sicuramente l'implementazione e l'utilizzo di un Web Application Firewall (WAF), è fondamentale per mitigare gli attacchi SQLi e XSS.

Ecco perché questa soluzione è essenziale:
**Protezione specializzata:** Un WAF è progettato specificamente per rilevare e bloccare attacchi alle applicazioni web, inclusi SQLi e XSS. A differenza dei firewall standard che operano a livello di rete, un WAF è in grado di analizzare il traffico HTTP/HTTPS in ingresso e in uscita per individuare e bloccare pattern sospetti o attacchi noti.

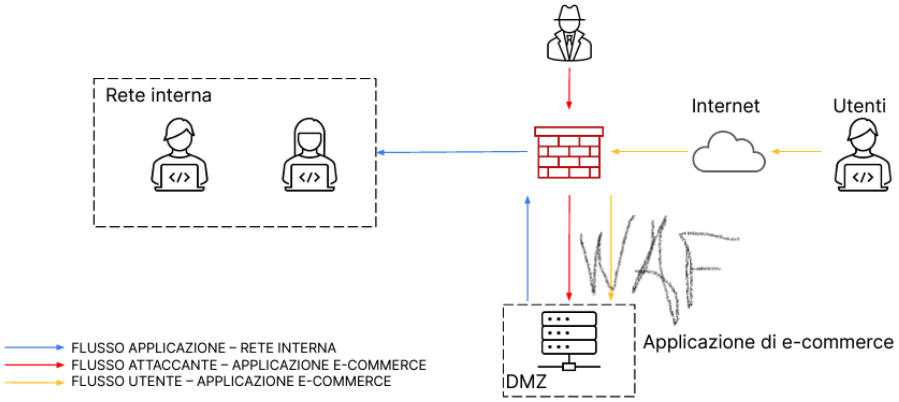
**Filtraggio dei dati in ingresso:** Un WAF può applicare filtri per validare e sanificare i dati in ingresso, proteggendo così l'applicazione da attacchi di tipo XSS. Questo impedisce agli attaccanti di inserire script dannosi all'interno dei campi di input dell'applicazione.

**Rilevamento delle query SQL dannose:** Un WAF può analizzare le richieste HTTP per individuare tentativi di SQL Injection e bloccarli prima che raggiungano il server dell'applicazione. Questo aiuta a proteggere il database da eventuali compromissioni dovute a SQLi.

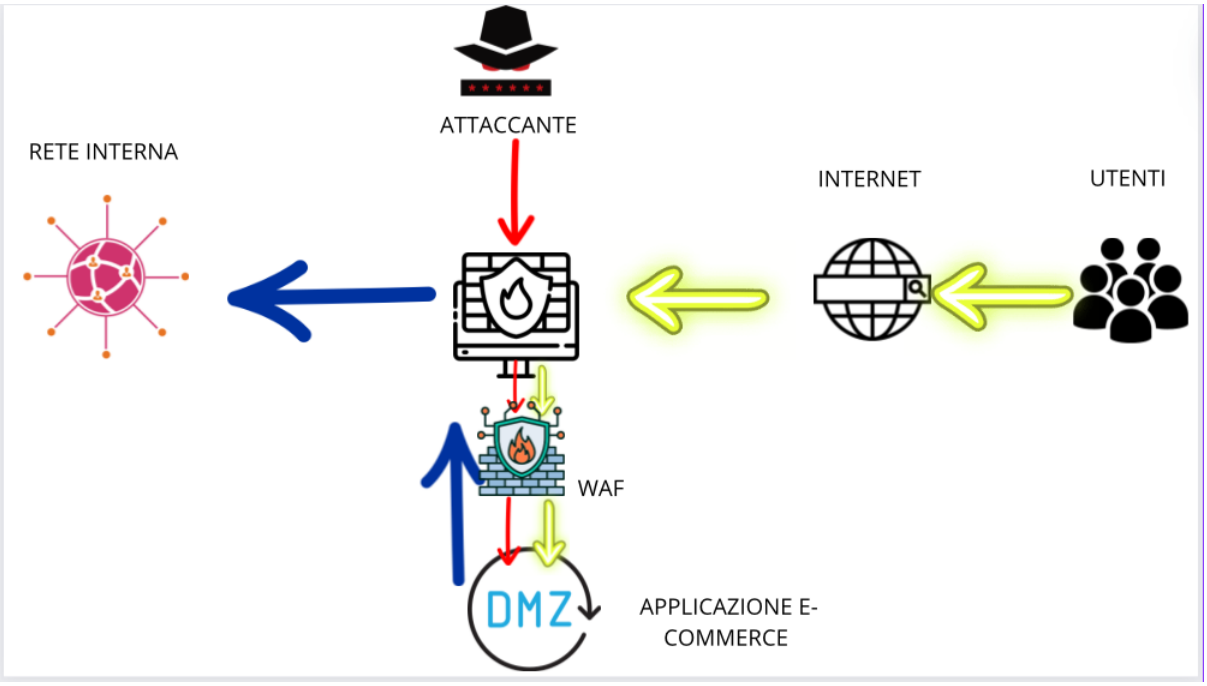
Nella figura modificata sulla slide 2, il WAF andrebbe posizionato tra Internet (utenti e potenziali attaccanti) e la Web App, agendo come una barriera protettiva che filtra e analizza il traffico in entrata per rilevare e bloccare eventuali attacchi SQLi e XSS.
Questa implementazione è cruciale per proteggere l'integrità e la sicurezza dell'applicazione web e dei dati sensibili che essa gestisce.

**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.



## SOLUZIONE ILLUSTRATA




## 2. BUSINESS IMPACT

Nella seconda soluzione invece è stato richiesto di calcolare l'impatto di un attacco Ddos.
Per definire l'impatto finanziario causato dalla non raggiungibilità della piattaforma di e-commerce per 10 minuti a causa di un attacco DDoS, possiamo utilizzare la seguente formula:

**Impatto sul business=Spesa media degli utenti al minuto×Durata dell'indisponibilità del servizio**

La "Spesa media degli utenti al minuto" rappresenta il guadagno potenziale per ogni minuto in cui la piattaforma è operativa e gli utenti possono effettuare acquisti.
La "Durata dell'indisponibilità del servizio" indica per quanto tempo la piattaforma è stata resa non raggiungibile a causa dell'attacco DDoS.
Applicando questa formula, possiamo calcolare l'impatto finanziario in termini di perdita di guadagno dovuta all'indisponibilità del servizio.

Dunque, considerando la formula precedentemente citata l'attacco di tipo DDoS ha causato la non raggiungibilità della piattaforma di e-commerce per 10 minuti.

Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10). Quindi, l'impatto sul business è:
**Impatto sul business = 1.500 € x 10 minuti = 15.000 €**
Ovvero, per 10 minuti di indisponibilità, l'azienda ha perso 15.000 € di acquisti potenziali.
Questo evidenzia l'importanza di avere misure di mitigazione e risposta agli attacchi DDoS per minimizzare l'impatto finanziario sul business.

## 3. RESPONSE

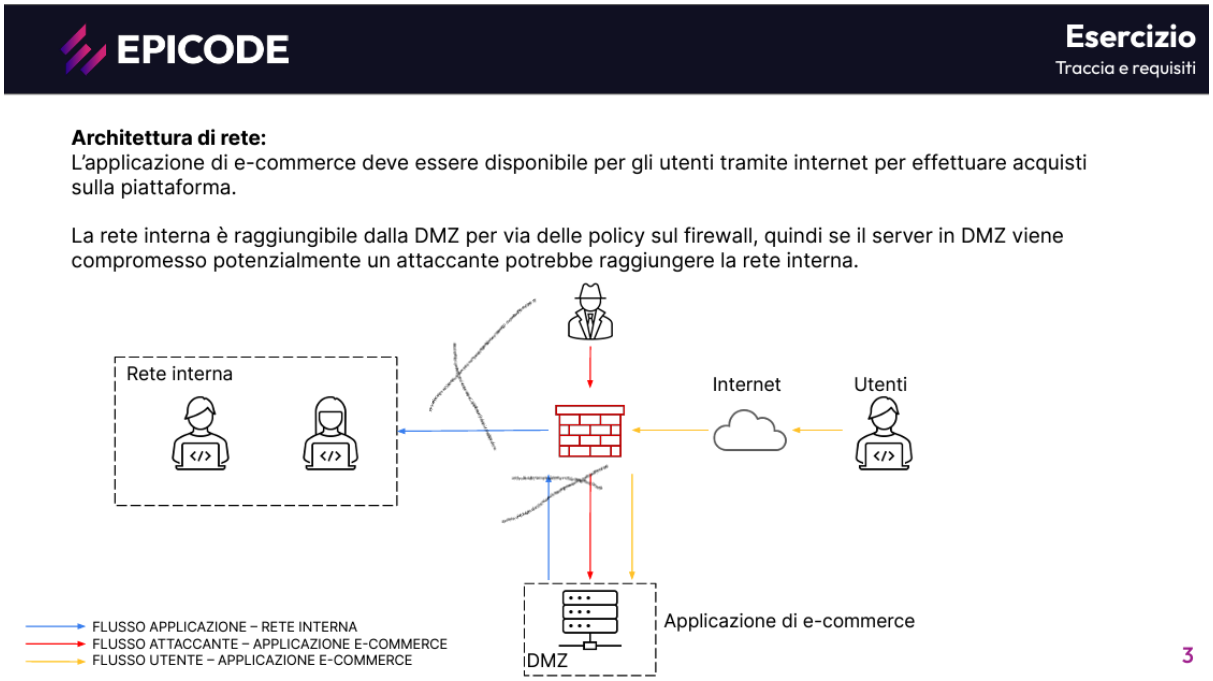
Per quanto riguarda il quesito dell'azione di risponde è fondamentale comprendere cos'è un malware e quali sono le sue implicazioni.

Il termine "malware" è una contrazione di "malicious software", e si riferisce a qualsiasi tipo di software progettato per infiltrarsi o danneggiare un sistema informatico senza il consenso dell'utente. I malware possono assumere varie forme, tra cui virus, worm, trojan, ransomware e spyware, o combinazioni di questi.
La strategia proposta per rispondere all'attacco del malware potrebbe prevedere le seguenti misure di sicurezza e azioni preventive:

**Isolamento della macchina infettata:**
Considerando la priorità di proteggere la rete interna, si adotta una strategia basata sull'isolamento della macchina infettata.
Questo significa che la macchina compromessa sarà direttamente collegata a Internet, rendendola accessibile all'attaccante ma non più connessa alla rete interna dell'azienda.
L'isolamento della macchina infetta impedisce al malware di propagarsi sulla rete interna e di compromettere ulteriormente altri dispositivi o server all'interno dell'ambiente aziendale.
Questa strategia permette di mantenere separata la macchina infetta dalla rete interna, minimizzando così il rischio di danni e proteggendo le risorse critiche dell'azienda.

**MOTIVI:**
**Priorità sulla sicurezza:** In una situazione di compromissione, la priorità principale è limitare i danni e prevenire la diffusione del malware. Isolando la macchina infettata, si riduce il rischio di ulteriori compromissioni e si proteggono le risorse aziendali critiche.

**Minimizzazione del rischio:** Mantenere la macchina infettata isolata dalla rete interna riduce significativamente il rischio di compromettere altri dispositivi o server. In questo modo, si proteggono i dati sensibili e l'integrità del sistema aziendale.
**Riduzione delle possibilità di controllo da parte dell'attaccante:** Collegando direttamente la macchina infetta a Internet, si concede all'attaccante accesso solo a quella macchina specifica, limitando la possibilità di ulteriori attacchi o manovre all'interno della rete interna.




In definitiva se guardiamo la figura e prendiamo in riferimento ciò che abbiamo appena spiegato, la soluzione implementata riguarda l'isolamento della macchina infetta e l'assenza di comunicazione diretta tra l'applicazione Web e la rete interna.
Questo garantisce un maggiore livello di sicurezza e protezione per l'ambiente aziendale.

## SOLUZIONE ILLUSTRATA