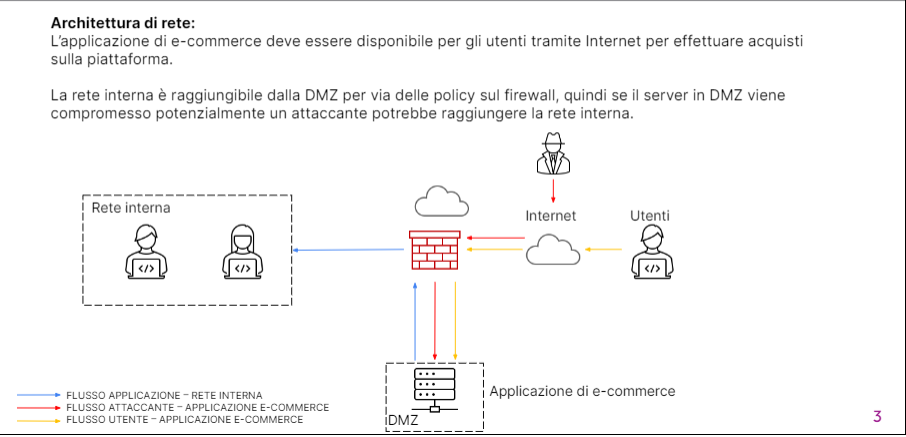
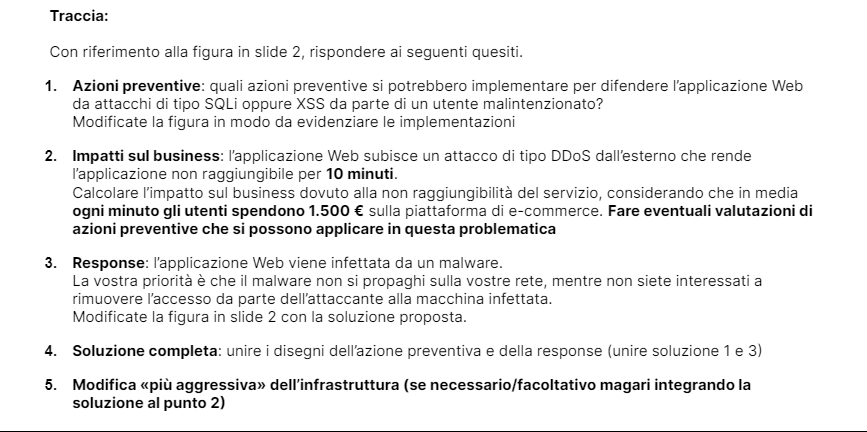
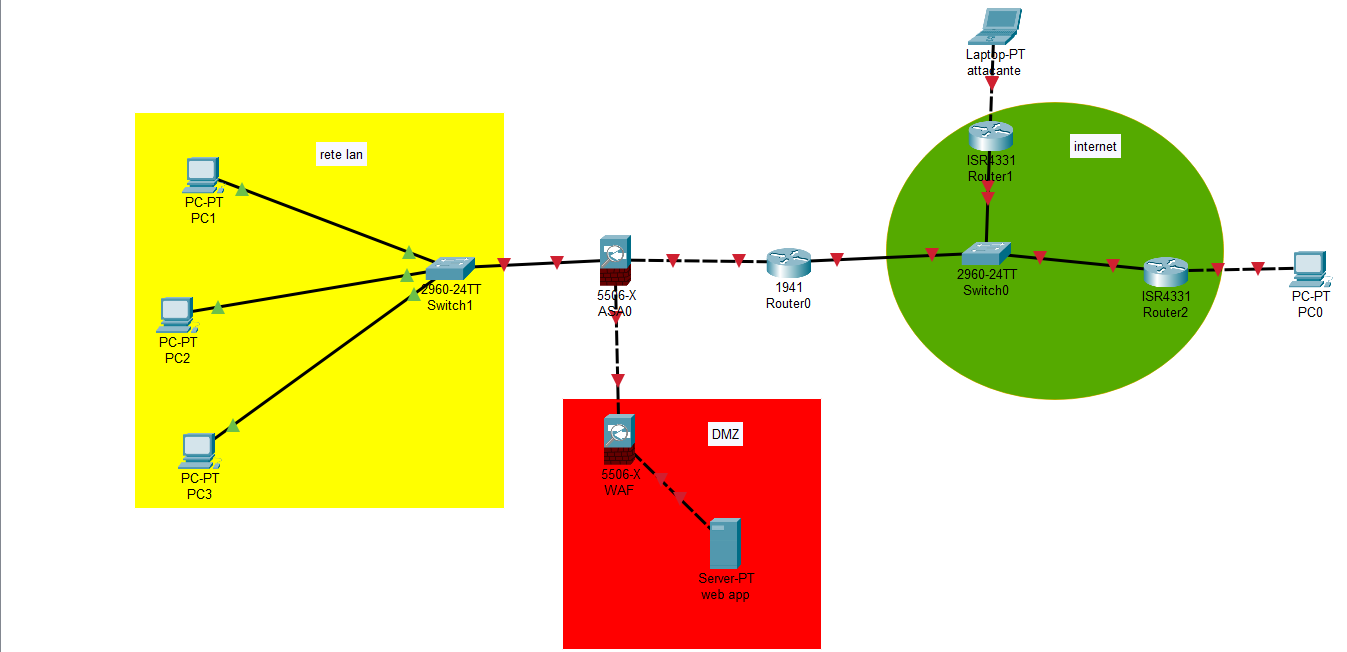
Azioni preventive



1) prima di andare ad analizzare metodi efficaci per difenderci da attacchi XSS e SQL , vediamo prima da vicino che cosa sono.

XSS🡪L'attacco XSS è una vulnerabilità che si verifica quando un'applicazione web permette l'inserimento di codice script non attendibile all'interno delle pagine visualizzate dagli utenti. Questo tipo di attacco sfrutta la mancanza di validazione o sanitizzazione dei dati inseriti dagli

utenti, consentendo a un malintenzionato di eseguire script malevoli all'interno del browser delle vittime

SQL 🡪 L'attacco di SQL Injection sfrutta le vulnerabilità nelle applicazioni web che non validano o sanificano correttamente i dati inseriti dagli utenti nelle query SQL. L'obiettivo principale di questo attacco è ottenere accesso non autorizzato al database sottostante o manipolare le query per ottenere informazioni riservate o compromettere l'integrità dei dati. Una volta analizzato ciò possiamo vedere come sfruttare, azioni preventive , vediamo nella foto 

Azioni preventive: Per difendere l'applicazione Web da attacchi di tipo SQLi e XSS, si possono implementare le seguenti azioni preventive:

XSS:

1)Validazione dei dati di input: Implementa una valida validazione dei dati di input lato server per assicurarti che solo dati validi e attesi vengano accettati. Filtra e controlla ogni dato inserito dagli utenti, assicurandoti che rispettino i criteri di input previsti (ad esempio, lunghezza, formato, caratteri consentiti, ecc.

2)Sanitizzazione dei dati di output: Prima di visualizzare qualsiasi dato fornito dagli utenti all'interno delle pagine web, assicurati di sanificarli correttamente. Ciò significa rimuovere o neutralizzare tutti i caratteri o tag potenzialmente dannosi, come script JavaScript, HTML o tag di evento. Utilizza librerie o strumenti che offrono funzioni di sanitizzazione dei dati, ad esempio l'encoding HTML o la rimozione di caratteri speciali.

3) L'utilizzo dei token CSRF aiuta a prevenire gli attacchi CSRF perché un attaccante esterno non sarà in grado di generare o ottenere il token corretto associato alla sessione utente. Anche se un attaccante riesce a convincere l'utente a inviare una richiesta manipolata, senza il token CSRF corretto, il server rifiuterà l'azione

4) Filtraggio delle richieste: Un WAF può esaminare le richieste HTTP in ingresso e bloccare quelle sospette o malevole che potrebbero contenere tentativi di attacco XSS. Può rilevare i modelli comuni utilizzati dagli attacchi XSS e impedire che le richieste dannose raggiungano le applicazioni web

SQL:

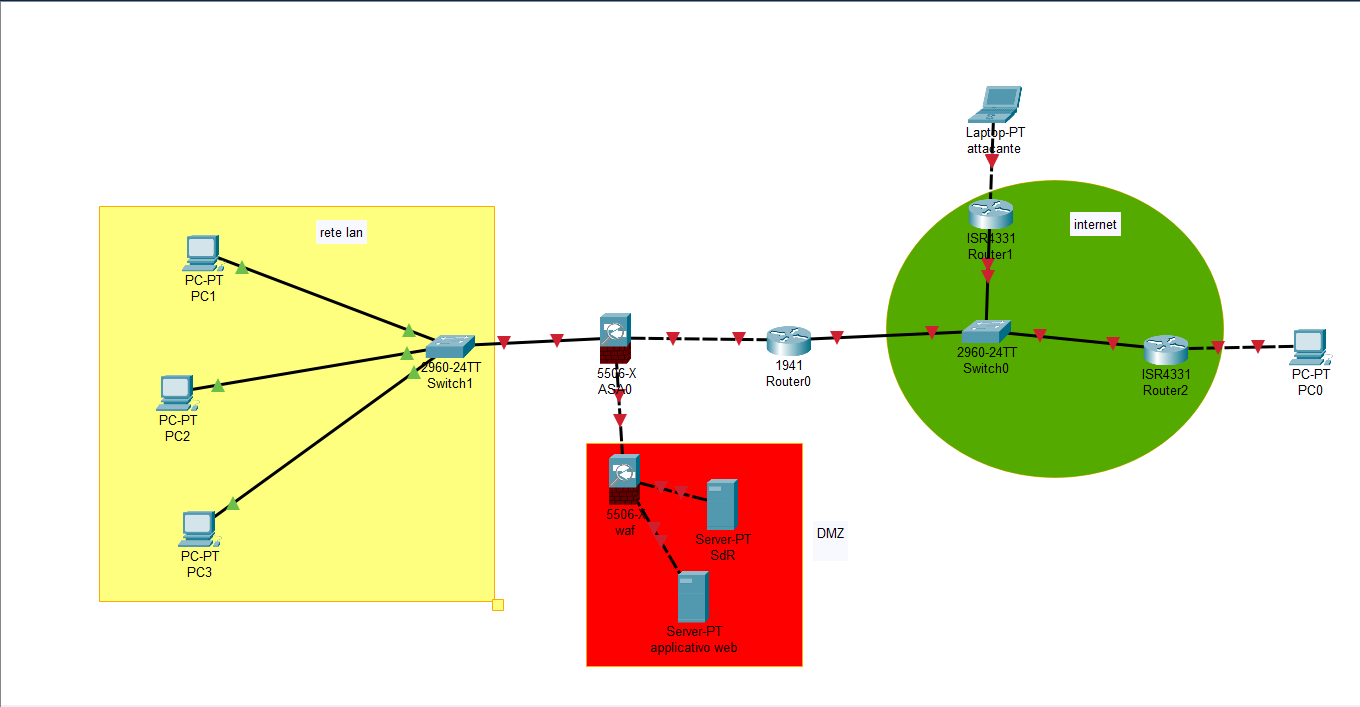
1) Validazione dei dati di input: Effettua una valida validazione dei dati di input lato server. Verifica che i dati rispettino i criteri di input previsti, come la lunghezza massima, il formato e i caratteri consentiti. Rifiuta o sanifica i dati di input che non rispettano tali criteri.

2) Aggiornamento regolare e patching: Mantieni sempre il tuo database e il software di gestione del database aggiornati con gli ultimi aggiornamenti di sicurezza e patch. Questo aiuta a correggere le vulnerabilità note che potrebbero essere sfruttate dagli attacchi di SQL Injection.

3) Utilizzo di parametri di query preparati (Prepared Statements): Utilizza parametri di query preparati nelle tue query SQL. Questa tecnica consente di separare i comandi SQL dai dati di input, evitando così l'iniezione di codice dannoso. I parametri vengono trattati come dati puri e non vengono interpretati come parte della query SQL

Impatti sul business:

ln caso di attacco Ddos, considerando in media una spesa media al minuto di 1.500 €, un downtime di 10 minuti causerebbe una perdita di circa 15.000€ , ma cos’è un attacco DDOS??

Attacco DDos 🡪 Un attacco DDoS è un tipo di attacco informatico in cui un grande numero di dispositivi o computer, vengono utilizzati per sovraccaricare un obiettivo specifico, come un sito web o un server, con un volume eccessivo di traffico. L'obiettivo principale di un attacco DDoS è rendere l'obiettivo inaccessibile agli utenti legittimi, impedendo loro di accedere ai servizi o alle risorse online, nella figura sottostante saranno mostrate le azioni preventive.

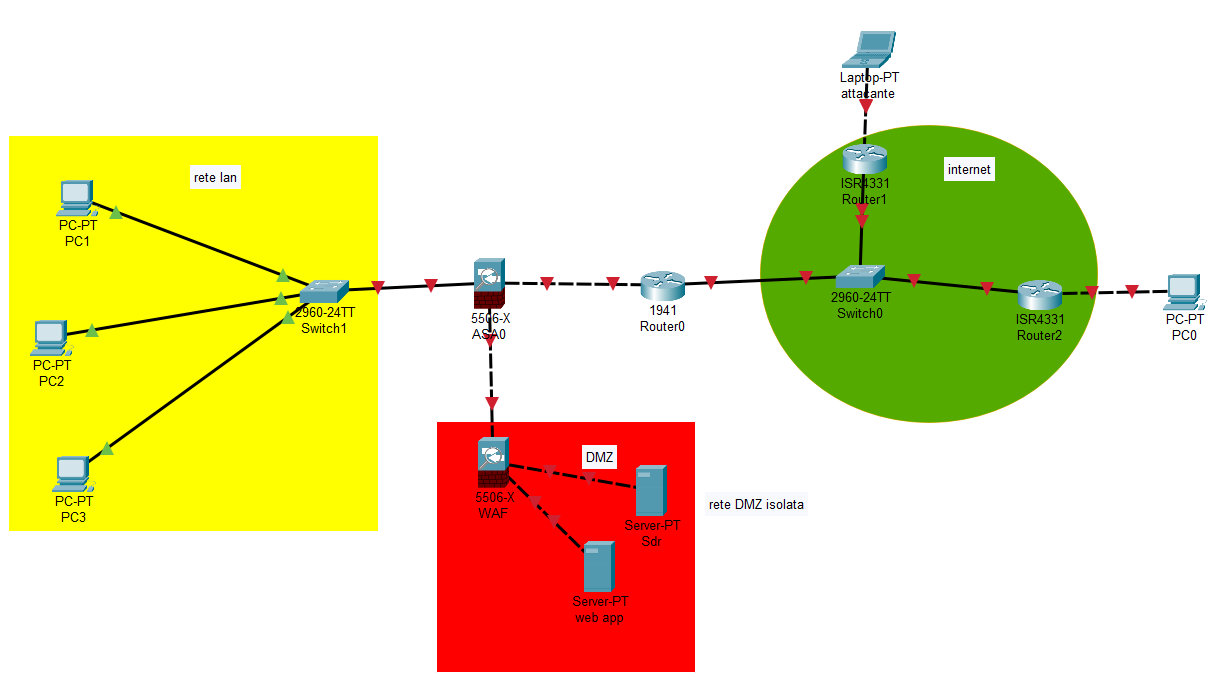
Azioni preventive :

1) Configurazione adeguata del server di ridondanza: Assicurati di configurare correttamente il server di ridondanza in modo che sia pronto a intervenire e fornire il servizio in caso di interruzione del server principale. Verifica che le impostazioni di sincronizzazione dei dati, le regole di bilanciamento del carico e altre configurazioni siano corrette e funzionanti

2) configura un firewall per filtrare il traffico indesiderato verso il tuo server. Imposta regole che permettano solo il traffico necessario per il corretto funzionamento delle tue applicazioni e blocca o limita il traffico non autorizzato

3) aggiornamenti regolari del software: Mantieni il software del server e tutte le applicazioni installate aggiornate con gli ultimi aggiornamenti di sicurezza. Questi aggiornamenti spesso correggono vulnerabilità note che potrebbero essere sfruttate dagli attaccanti

Response: impedire la propagazione del malware, priorità assoluta.



Response:

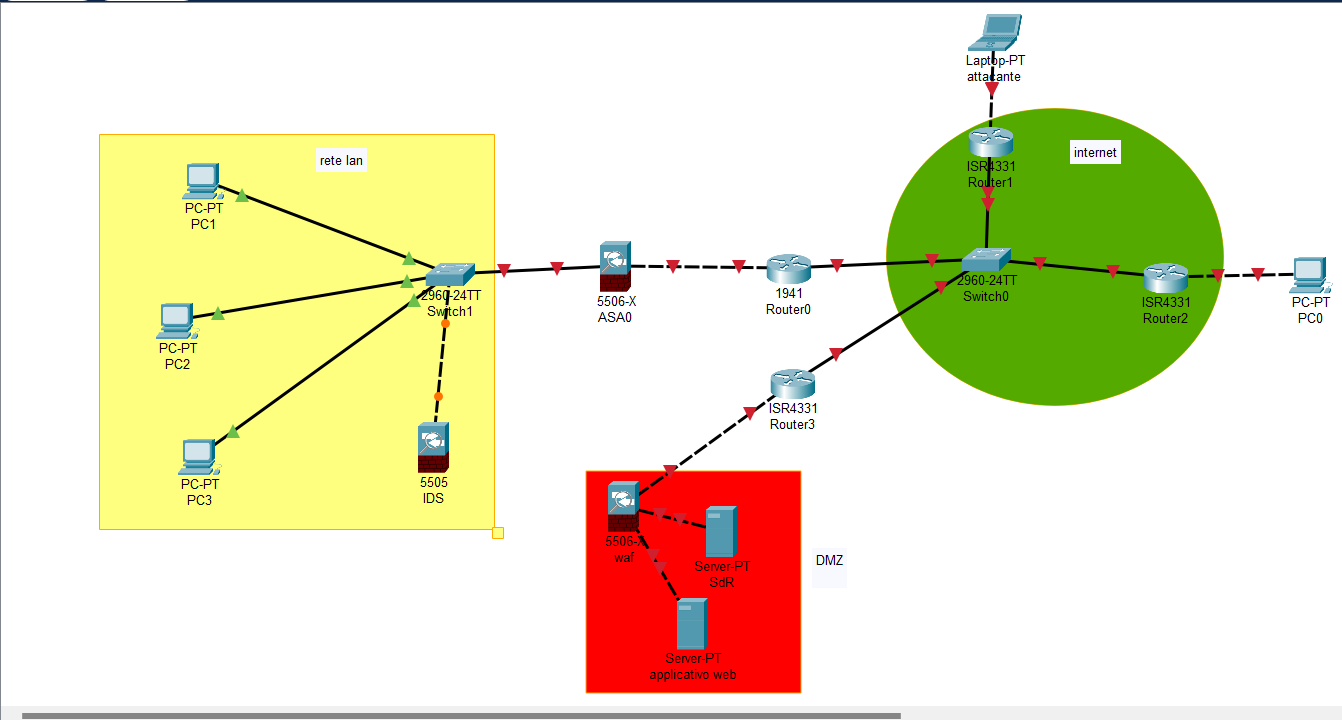
1) Isolamento della macchina infettata: Isola immediatamente la macchina infettata dalla tua rete principale. Questo può essere fatto disconnettendo fisicamente la macchina dalla rete o attraverso la segmentazione di rete tramite VLAN o subnet dedicate

2) Isolamento controllato: Anziché interrompere completamente l'accesso dell'attaccante, puoi considerare l'isolamento controllato della macchina infettata. Ciò implica l'impostazione di restrizioni di rete, come limitare il traffico in ingresso e in uscita o creare un'area di quarantena separata. In questo modo, puoi ridurre il rischio di propagazione del malware senza interrompere completamente l'accesso dell'attaccante

3) Analisi approfondita: Esegui un'analisi completa della macchina infettata per identificare il tipo e la natura del malware presente. Utilizza strumenti antivirus e antimalware aggiornati per individuare e rimuovere il malware, senza tuttavia terminare l'accesso dell'attaccante

4) Analisi forense: Coinvolgi esperti di sicurezza informatica o consulenti forensi digitali per condurre un'analisi forense completa della macchina infettata. Questo ti consentirà di ottenere una comprensione approfondita delle tecniche utilizzate dall'attaccante e delle potenziali vulnerabilità sfruttate

Rete alternativa:



L'architettura in questo caso proposta, isolerebbe la rete del applicativo web da quella interna in modo da non comprometterla in caso di attacco, si usa poi un altro provider per la rete del Server web.

Viene aggiunto poi un IDS alla rete interna per aumentarne la sicurezza.

Inoltre integra le soluzioni precedentemente proposte