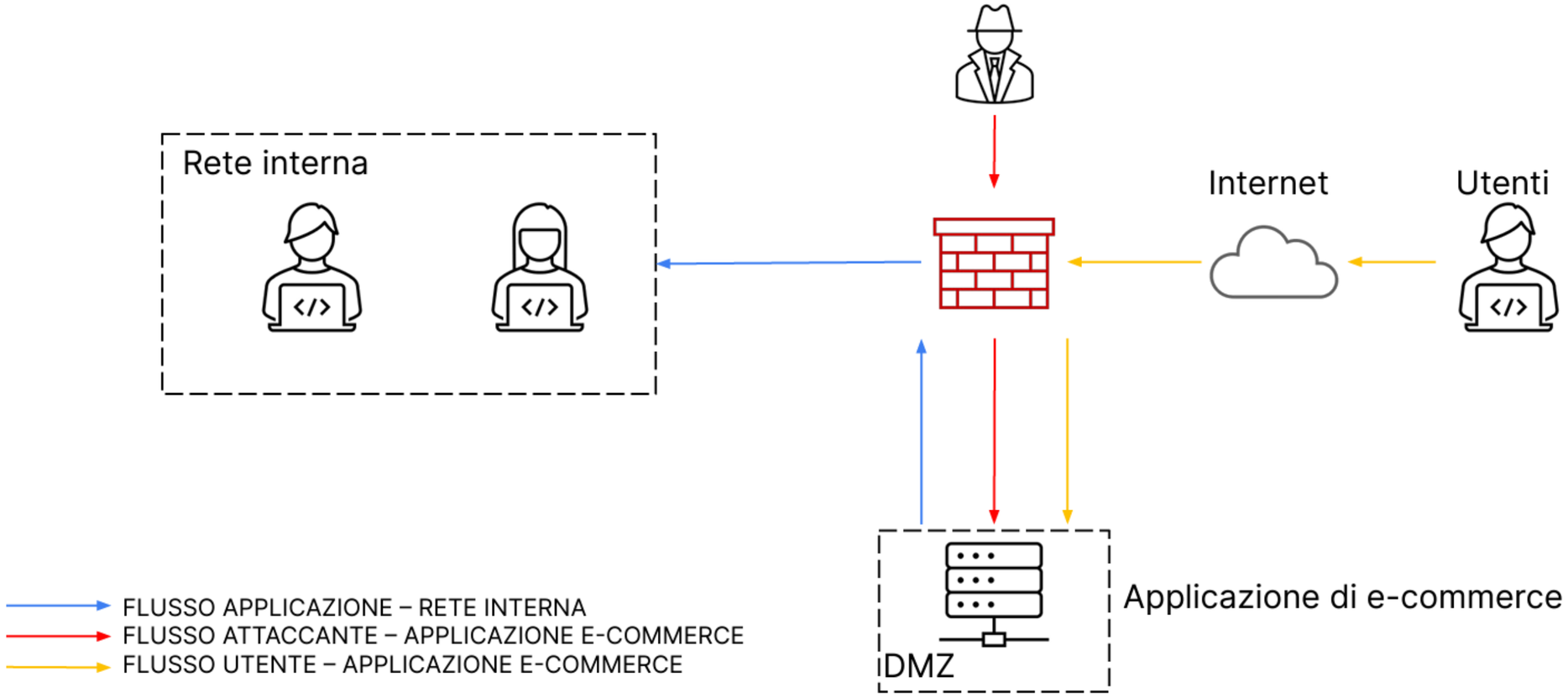
INCIDENT RESPONSE

BENEDETTA FORESTIERI

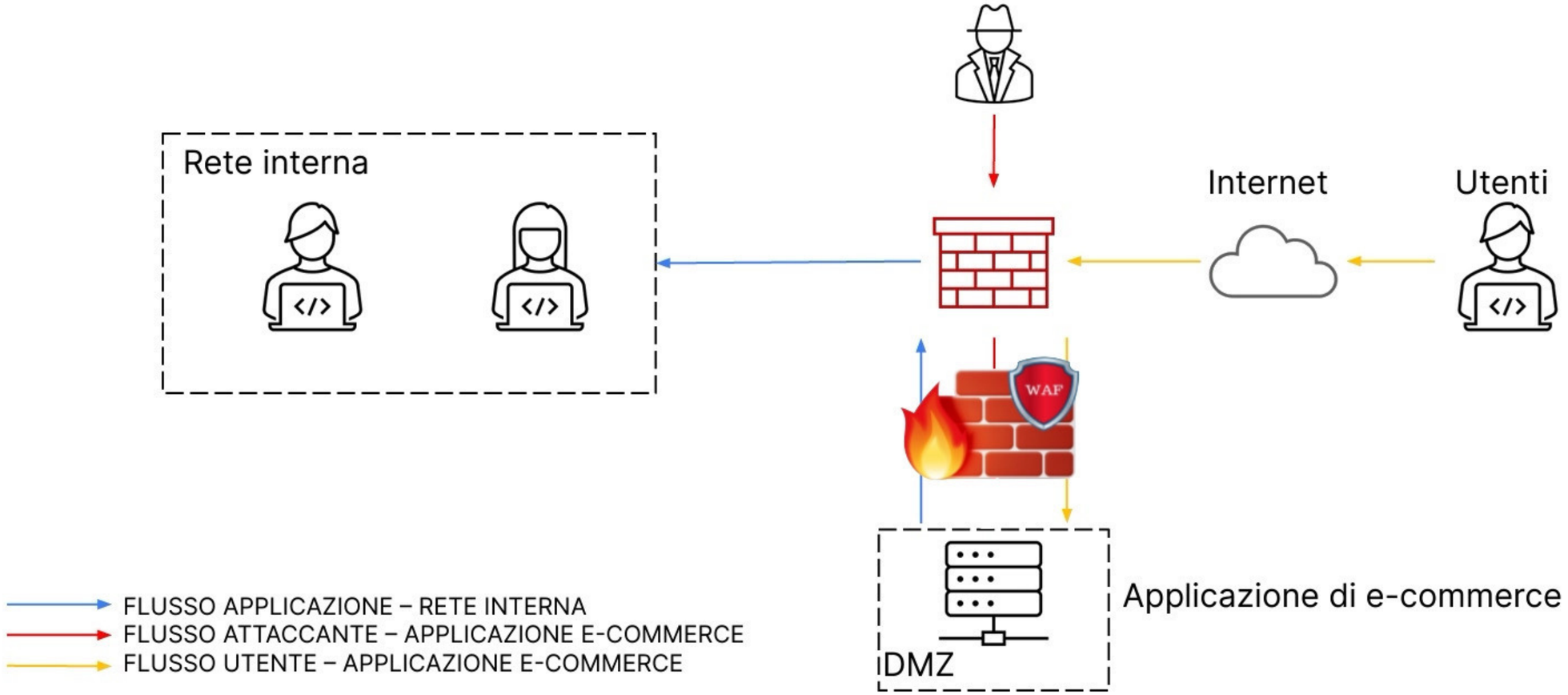
ARCHITETTURA DI RETE

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.



MISURE PREVENTIVE

L'integrazione di un Web Application Firewall (**WAF**) tra il firewall e la DMZ **rafforza la sicurezza del sistema,** focalizzandosi sulla protezione delle applicazioni web da minacce come SQL injection e cross-site scripting (XSS). Il WAF fornisce una difesa avanzata contro vulnerabilità specifiche delle applicazioni, identificando e bloccando attivamente tentativi di attacco, sia noti che sconosciuti. Questo strumento contribuisce ad una difesa completa del sistema, assicurando la **protezione delle applicazioni web da potenziali rischi a livello applicativo.**



MISURE PREVENTIVE

QUALI STRATEGIE PREVENTIVE POSSONO ESSERE ADOTTATE PER PROTEGGERE L'APPLICAZIONE WEB DA ATTACCHI DI TIPO SQLI O XSS DA PARTE DI UTENTI MALEVOLI?

- **Controlli anti-script in input:** Implementare un sistema di sicurezza che impedisca agli utenti di inserire la parola "script" come input, gestendo possibili rilevamenti di questa sequenza di caratteri e restituendo una stringa nulla o un parametro nullo.
- **Validazione dell'Input:** Implementare una rigorosa validazione dell'input dell'utente per accertarsi che siano conformi agli standard attesi. Questa pratica aiuta a bloccare input dannosi prima che raggiungano l'applicazione.
- **Firewall:** Attivare un firewall per monitorare e regolare il flusso del traffico in entrata e in uscita, al fine di attenuare possibili attacchi.
- **Autenticazione per ogni utente:** Richiedere l'autenticazione per ogni utente, garantendo così un ulteriore strato di sicurezza e verificando l'identità degli accessi.
- **Test periodici sulla sicurezza:** Effettuare regolarmente test di sicurezza per valutare la resistenza dell'applicazione contro possibili vulnerabilità, assicurando il mantenimento di standard elevati in materia di sicurezza.
- **Limitazione dei privilegi degli utenti**: Ridurre i livelli di autorizzazione di ciascun utente per prevenire l'esecuzione di query o script da parte di utenti non autorizzati.
- **Aggiornamenti Regolari e Patching:** Mantenere l'applicazione e tutte le librerie utilizzate aggiornate con le ultime patch di sicurezza. Gli attaccanti spesso cercano di sfruttare vulnerabilità note che possono essere corrette con gli aggiornamenti.
- **Limitare i Punti di Accesso:** Ridurre al minimo i punti di accesso all'applicazione esponendo solo le funzionalità essenziali. Ciò riduce la superficie di attacco e facilita la gestione della sicurezza.
- **Formazione degli Sviluppatori:** Fornire formazione continua agli sviluppatori sull'importanza delle pratiche di sicurezza del codice. Gli sviluppatori informati sono essenziali per mantenere un'applicazione sicura.

IMPATTI SUL BUSINESS

L'APPLICAZIONE WEB SUBISCE UN ATTACCO DI TIPO DDOS DALL'ESTERNO CHE RENDE L'APPLICAZIONE NON RAGGIUNGIBILE PER 10 MINUTI -> IMPATTO FINANZIARIO TOTALE: 10 MINUTI * 1.500 €/MINUTO = 15.000€

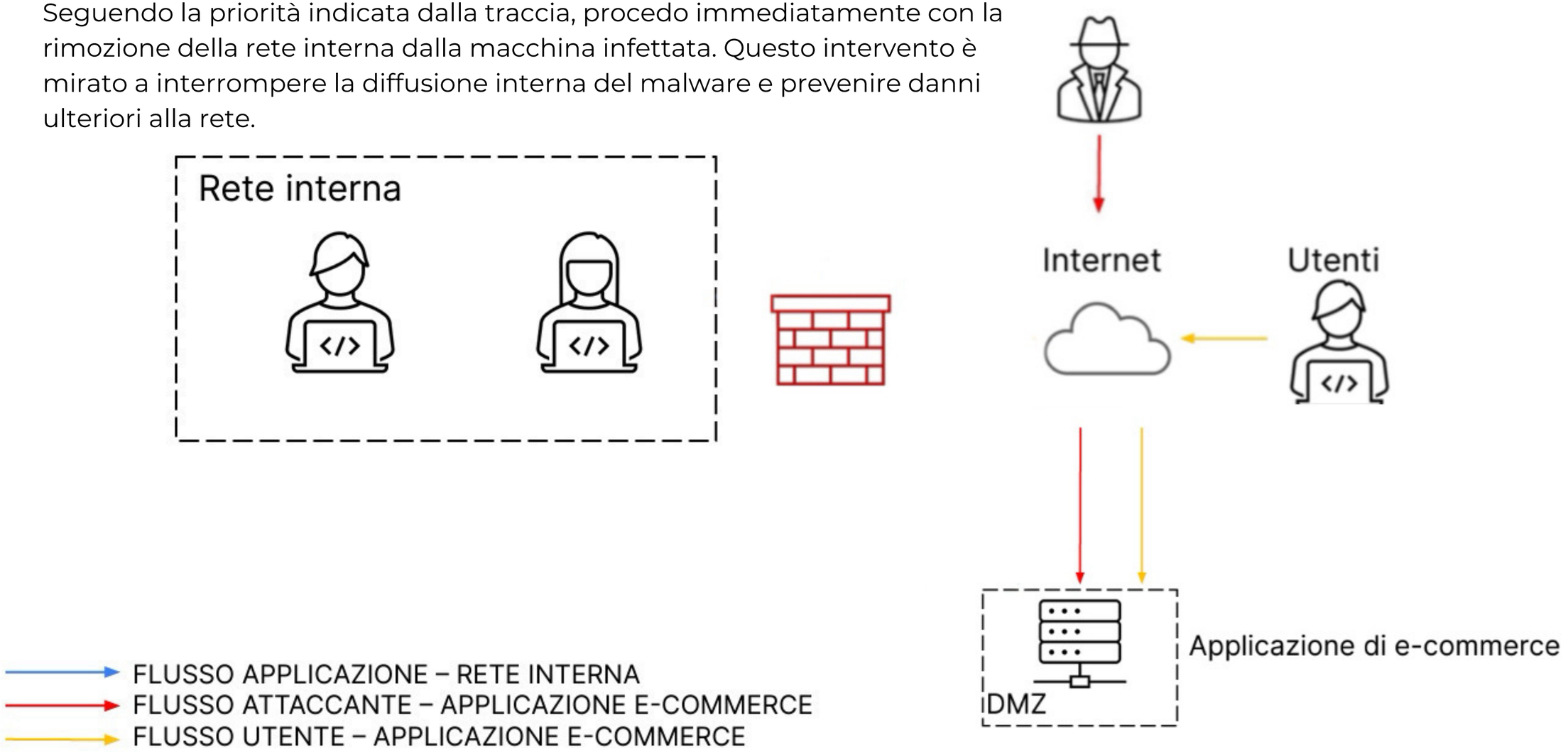
Azioni preventive:

- **Ridondanza e Failover:** Configurare sistemi ridondanti e meccanismi di failover per garantire la continuità del servizio durante un attacco, coinvolgendo la distribuzione su più data center o server di backup.
  - Vantaggi: Assicura la disponibilità continua del servizio in situazioni di attacco o interruzione.
  - Svantaggi: Potenzialmente costoso e richiede risorse costanti.
- **Pianificazione di Backup e Ripristino:** Implementare un piano dettagliato di backup e ripristino con strategie regolari per recuperare rapidamente i dati dopo un attacco.
  - Vantaggi: Permette un recupero rapido e affidabile dei dati in caso di interruzione.
  - Svantaggi: Necessità di una pianificazione accurata delle copie di sicurezza.
- **Server Standby Sempre Pronto:** Mantenere un server di backup sempre attivo per garantire una sostituzione immediata del server principale in caso di interruzione.
  - Vantaggi: Assicura una risposta istantanea e continua del servizio.
  - Svantaggi: Può comportare costi elevati e richiede risorse costanti.
- **Noleggio di un Server Temporaneo:** Noleggiare un server temporaneo come alternativa meno onerosa al server standby sempre pronto.
  - Vantaggi: Riduce i costi rispetto a un server standby sempre attivo.
  - Svantaggi: Implica una perdita di alcuni minuti durante il riavvio dei servizi, non offre una risposta immediata come un server standby.
- **Accesso Immediato ai Dati di Backup:** Garantire l'accesso immediato ai dati di backup per abbreviare il periodo di inattività del servizio.
  - Vantaggi: Cruciale per un recupero rapido e minimizzazione del downtime.
  - Svantaggi: Richiede una pianificazione accurata delle copie di sicurezza, ma spesso si dimostra una soluzione efficace.
- **Formazione del Personale:** Assicurarsi che il personale sia ben addestrato per rispondere a un attacco DDoS, fornendo documentazione chiara sui passaggi da seguire durante il recupero.

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.

Seguendo la priorità indicata dalla traccia, procedo immediatamente con la rimozione della rete interna dalla macchina infettata. Questo intervento è mirato a interrompere la diffusione interna del malware e prevenire danni ulteriori alla rete.



RESPONSE

Successivamente a questo passo, o in scenari simili, è opportuno prendere in considerazione le seguenti azioni:

- **Isolamento della macchina infettata:** Eseguire un isolamento fisico/logico della macchina infettata dalla rete. Ciò può essere realizzato attraverso la disconnessione fisica del dispositivo o mediante la configurazione di politiche di rete che limitano la comunicazione della macchina.
- **Analisi approfondita del malware:** Condurre una scansione dettagliata per individuare e analizzare il malware. Utilizzare strumenti antivirus, e altre soluzioni avanzate per la sicurezza al fine di identificare e comprendere la natura del malware.
- **Implementazione di misure di contenimento:** Applicare misure di contenimento per prevenire la diffusione del malware. Queste possono includere la disabilitazione di servizi di rete, la modifica delle regole del firewall e l'aggiornamento delle politiche di sicurezza per limitare le interazioni della macchina infetta.
- **Notifica alle autorità competenti:** Nel caso appropriato, notificare le autorità competenti, come il CSIRT (Computer Security Incident Response Team) o le forze dell'ordine, per avviare indagini e ricevere assistenza nelle fasi successive.
- **Identificazione della fonte dell'infezione:** Effettuare una ricerca per identificare la fonte dell'infezione al fine di prevenire attacchi simili in futuro. Analizzare i log di sicurezza, monitorare il traffico di rete e condurre indagini approfondite per comprendere come il malware abbia ottenuto accesso all'applicazione web.
- **Monitoraggio costante:** Implementare un monitoraggio costante per rilevare eventuali attività sospette e garantire che le misure di sicurezza siano efficaci nel prevenire la propagazione del malware nel tempo.