W20D4- FRANCESCO MONTALTO

1. AZIONI PREVENTIVE:

Query parametrizzate (Prepared Statements)

Le query parametrizzate sono query SQL in cui la struttura della query è separata dai dati forniti dall'utente.
In questo modo l'input dell'utente non viene interpretato come parte del codice SQL, ma solo come valore.

Applicazione pratica:
L'applicazione utilizza prepared statements o ORM sicuri per interagire con il database, evitando la concatenazione diretta di stringhe SQL. Questo impedisce a un attaccante di modificare la logica della query tramite input malevolo, prevenendo attacchi di SQL Injectio**n.**

Validazione degli input lato server

La validazione degli input consiste nel verificare che i dati inseriti dall'utente rispettino i formati, le lunghezze e i tipi previsti dall'applicazione**.**

Applicazione pratica:
Tutti i dati ricevuti dall'utente vengono controllati lato server utilizzando criteri di allow-list (ad esempio solo numeri, solo email valide, lunghezza massima). Input non conformi vengono rifiutati. Questo riduce sia il rischio di SQL Injection sia di XSS.

Output encoding

L'output encoding è il processo di codifica dei dati prima che vengano visualizzati nel browser dell'utente, in modo che eventuali caratteri speciali non vengano interpretati come codice eseguibile**.**

Applicazione pratica:
I dati provenienti dal database o dall'utente vengono codificati in base al contesto (HTML, attributi HTML, URL). In questo modo eventuali script inseriti da un attaccante vengono mostrati come testo e non eseguiti, prevenendo attacchi XSS.

Gestione sicura delle sessioni

La gestione sicura delle sessioni serve a proteggere i cookie di autenticazione da accessi non autorizzati, in particolare in caso di attacchi XSS.
Applicazione pratica:
I cookie di sessione sono configurati con i flag HttpOnly (non accessibili da JavaScript), Secure (inviati solo su HTTPS) e SameSite (limitano l'invio a contesti esterni). Questo riduce il rischio di furto di sessione tramite codice JavaScript malevolo.

Principio del minimo privilegio

Il principio del minimo privilegio prevede che ogni componente abbia solo i permessi strettamente necessari per svolgere la propria funzione.

Applicazione pratica:
L'account del database utilizzato dall'applicazione dispone solo dei permessi indispensabili (ad esempio SELECT, INSERT), evitando privilegi amministrativi. In questo modo, anche in caso di SQL Injection, l'impatto dell'attacco risulta limitato.

Contromisure infrastrutturali

Web Application Firewall (WAF) / Reverse Proxy

Un WAF è un componente che analizza il traffico HTTP diretto all'applicazione e blocca richieste malevole prima che raggiungano il server.

Applicazione pratica:

Il WAF è posizionato tra Internet e l'applicazione in DMZ e utilizza regole specifiche per identificare pattern di SQL Injection e XSS. Fornisce inoltre funzionalità di logging e rate limiting, riducendo il numero di richieste sospette.

Security headers

I security headers sono intestazioni HTTP che rafforzano la sicurezza del browser dell'utente.

Applicazione pratica:

L'applicazione utilizza header come Content-Security-Policy (CSP) per limitare l'esecuzione di script provenienti da fonti non autorizzate, riducendo la superficie di attacco XSS.

Logging e monitoraggio

Il logging e il monitoraggio permettono di rilevare tempestivamente tentativi di attacco e comportamenti anomali.

Applicazione pratica:

I log dell'applicazione e del WAF vengono centralizzati e analizzati per individuare tentativi ripetuti di SQL Injection o XSS, consentendo una risposta rapida agli incidenti.

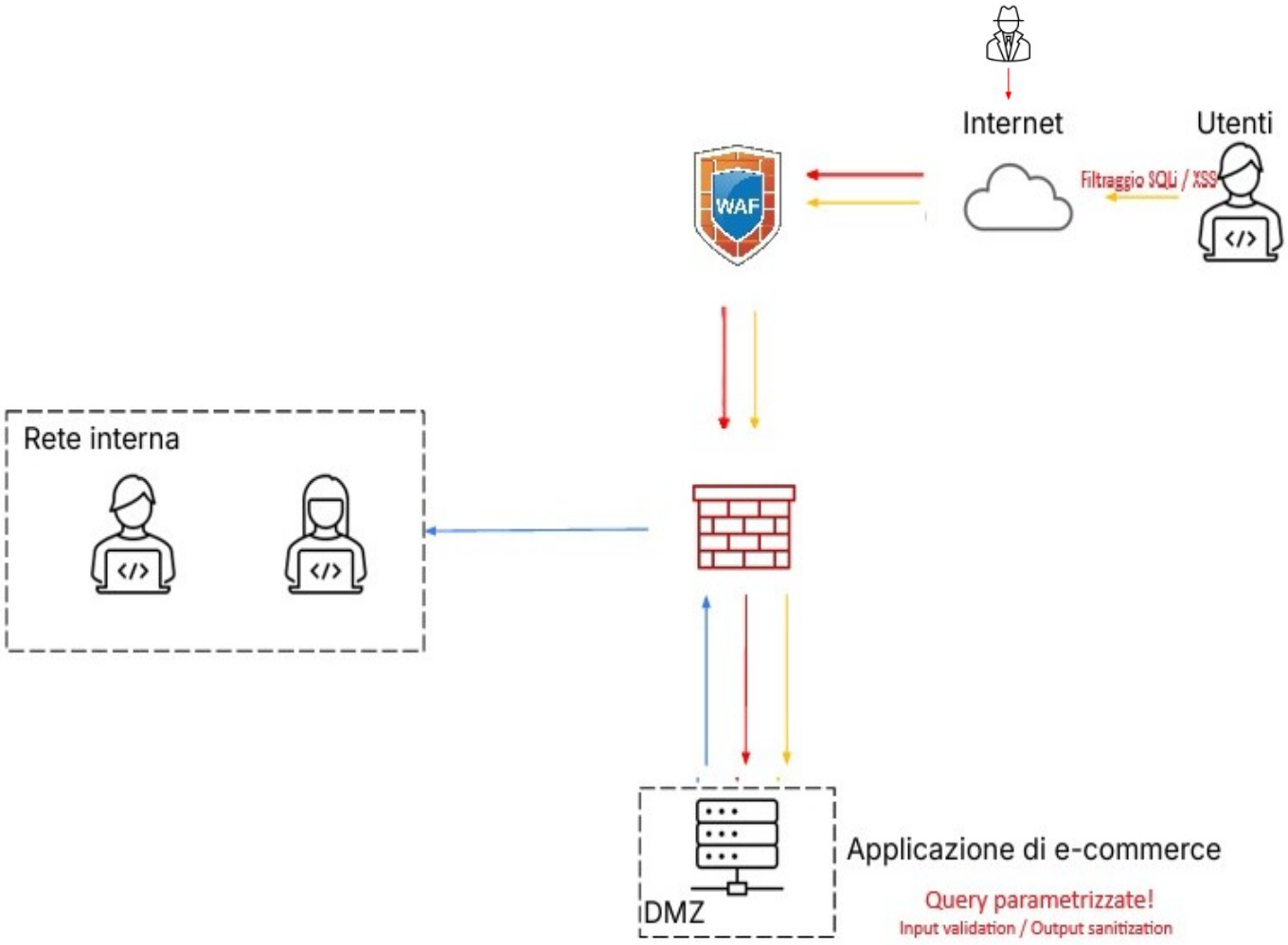
Protezione della rete interna

Regole firewall restrittive tra DMZ e rete interna

Poiché la rete interna è raggiungibile dalla DMZ, è necessario limitare rigorosamente i flussi consentit**i.**

Applicazione pratica:

Il firewall applica una policy "deny by default" tra DMZ e rete interna, consentendo solo i servizi strettamente necessari (ad esempio l'accesso al database su porte specifiche). Questo riduce il rischio di propagazione di un attacco verso la rete interna.


Internet
Utenti
WAF
Filtraggio SQLi / XSS
Rete interna
DMZ
Applicazione di e-commerce
Query parametrizzate!
Input validation / Output sanitization

2- IMPATTI SUL BUSINESS:

In condizioni normali, il valore medio degli acquisti effettuati dagli utenti sulla piattaforma è (come scritto) pari a 1.500 € al minuto.

Calcolo dell'impatto economico:

L'impatto economico dovuto alla non disponibilità del servizio è calcolato come segue:
-Spesa media per minuto: 1.500 €
-Durata dell'indisponibilità: 10 minuti

Impatto economico totale = 1.500 € × 10 = 15.000 €

Pertanto, un attacco DDoS che renda l'applicazione non raggiungibile per 10 minuti comporta una perdita diretta stimata di 15.000 € in mancati ricavi.

Azioni preventive:

-Servizi di protezione DDoS e CDN: l'utilizzo di una Content Delivery Network con funzionalità anti-DDoS consente di assorbire e distribuire il traffico malevolo, mantenendo disponibile il servizio.

-Rate limiting e filtraggio del traffico: limitare il numero di richieste per singolo indirizzo IP o sessione riduce l'efficacia di attacchi volumetrici di base.

-Scalabilità dell'infrastruttura: l'adozione di sistemi scalabili permette di gestire picchi di traffico improvvisi, legittimi o malevoli.

-Monitoraggio e alerting: il monitoraggio continuo del traffico consente di rilevare tempestivamente anomalie e attivare rapidamente le contromisure.

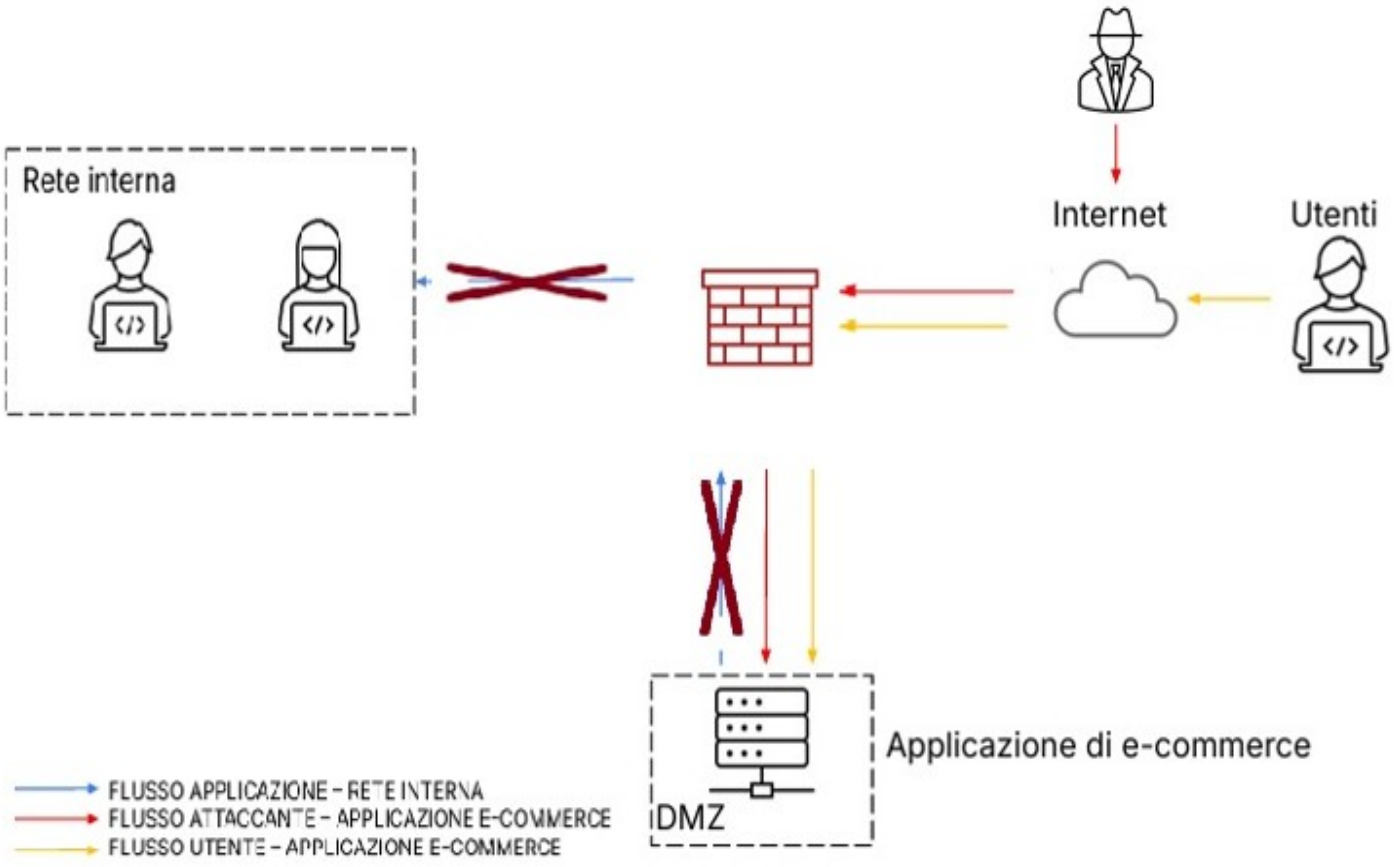
3- RESPONSE:

In seguito all’infezione malware dell’applicazione Web collocata in DMZ, la priorità è impedire la propagazione dell’infezione verso la rete interna.
Poiché non è richiesto rimuovere l’accesso dell’attaccante alla macchina compromessa, la strategia adottata è il contenimento dell’incidente tramite isolamento di rete.

La soluzione prevede l’applicazione di regole restrittive sul firewall per bloccare completamente il traffico tra la DMZ e la rete interna, impedendo qualsiasi comunicazione in uscita dalla macchina infetta verso i sistemi interni. In questo modo, anche in presenza di malware attivo, non è possibile estendere l’infezione alla rete aziendale.

L’accesso Internet all’applicazione Web rimane invece attivo, consentendo sia il traffico legittimo degli utenti sia l’eventuale accesso dell’attaccante alla macchina compromessa, come richiesto dalla consegna.

Questa configurazione consente di contenere l’incidente, mantenendo isolata la DMZ e preservando l’integrità della rete interna, senza intervenire sulla macchina infetta o sull’accesso esterno.



4- SOLUZIONE COMPLETA