Università degli Studi di Padova

Corso di Laurea in Informatica

Analisi Dei Requisiti

Azienda:
KIREY Srl

Soranzo Mendez Andrea Jesus
2075539

Indice

Elenco delle figure

1. Casi d'uso

1.1. UC1 - Visualizza applicazione

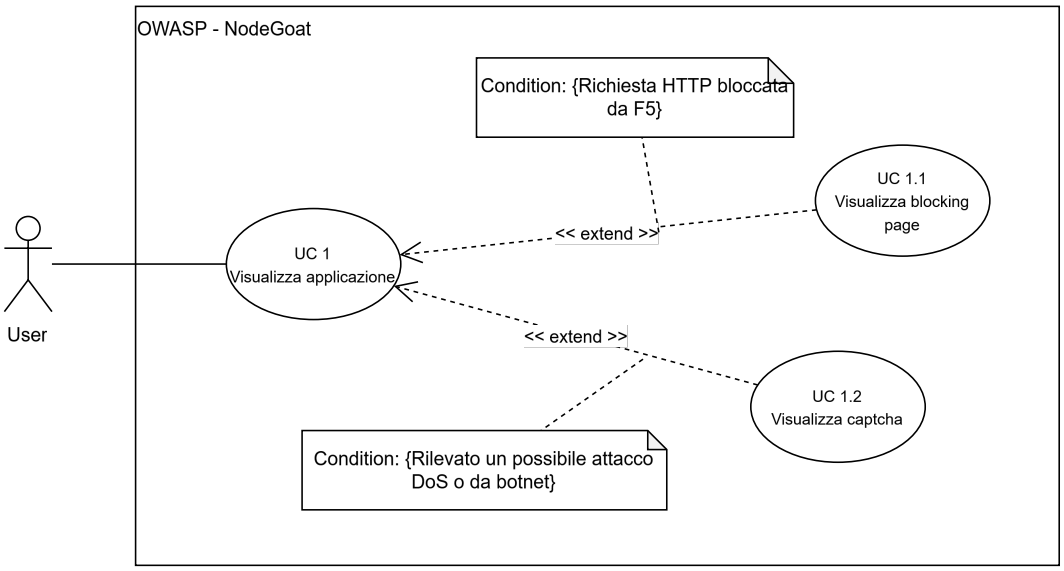

Figura 1: UC1 - Visualizza applicazione

- **Attore primario:**
  - Utente che ha accesso all'applicazione
- **Descrizione:**
  - L'utente può visualizzare e utilizzare l'applicazione normalmente
- **Precondizioni:**
  - L'utente ha accesso all'applicazione
  - Il server e il ***Web Application Firewall (WAF)***$_G$ sono operativi
- **Postcondizioni:**
  - L'utente è in grado di visualizzare e utilizzare l'applicazione
- **Estensioni:**
  - UC1.1 - Visualizza blocking page
  - UC1.2 - Visualizza ***CAPTCHA***$_G$

1.1.1. UC1.1 - Visualizza blocking page

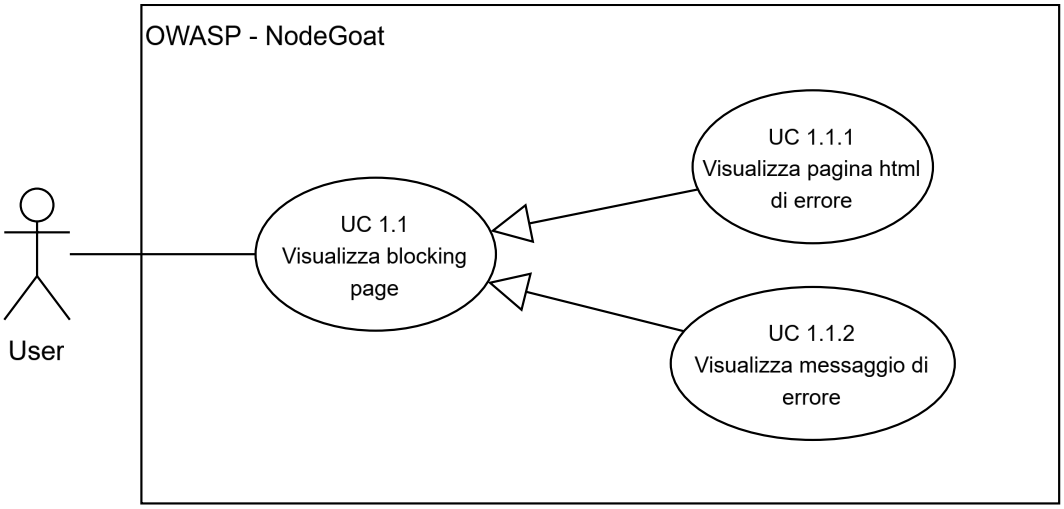

Figura 2: UC1.1 - Visualizza blocking page

- **Attore primario:**
  - Utente che ha accesso all'applicazione
- **Descrizione:**
  - Se un utente tenta di effettuare una richiesta ***Hypertext Transfer Protocol (HTTP)***$_G$ che risulta sospetta o illegale (es. accesso a risorse proibite o inserimento di attacchi web), verrà visualizzata la pagina di blocco impostata dall'admin del firewall.
- **Precondizioni:**
  - L'utente ha effettuato una richiesta ***HTTP***$_G$ al server
- **Postcondizioni:**
  - La richiesta non viene mandata al server
  - L'utente visualizza la pagina di blocco
- **Generalizzazioni:**
  - 1.1.1 - Visualizza pagina html di errore
  - 1.1.2 - Visualizza messaggio di errore

1.1.1.1. UC1.1.1 - Visualizza pagina html di errore

- **Attore primario:**
  - Utente che ha accesso all'applicazione
- **Descrizione:**

- L' utente dopo aver eseguito una richiesta ***HTTP***$_G$ sospetta o illegale viene reindirizzato ad una pagina HTML di errore

- **Precondizioni:**
  - L'utente ha effettuato una richiesta ***HTTP***$_G$ al server
- **Postcondizioni:**
  - L'utente reindirizzato ad una nuova pagina

1.1.1.2. UC1.1.2 - Visualizza messaggio di errore

- **Attore primario:**
  - Utente che ha accesso all'applicazione
- **Descrizione:**
  - L' utente dopo aver eseguito una richiesta ***HTTP***$_G$ sospetta o illegale visualizza sulla stessa pagina una finestra di errore
- **Precondizioni:**
  - L'utente ha effettuato una richiesta ***HTTP***$_G$ al server
- **Postcondizioni:**
  - L'utente visualizza il messaggio di errore

1.1.2. UC1.2 - Visualizza captcha

- **Attore primario:**
  - Utente che ha accesso all'applicazione
- **Descrizione:**
  - Se il sistema rileva un potenziale attacco di tipo ***Denial of Service (DoS)***$_G$ o un'attività sospetta riconducibile a una ***Botnet***$_G$, viene presentata la pagina di test ***CAPTCHA***$_G$ per bloccare le richieste malevole, poiché ***Bot***$_G$ automatizzati difficilmente riusciranno a completarlo.
- **Precondizioni:**
  - Vengono rilevate molte richieste in periodi di tempo brevi dallo stesso sorgente o da user agent sospetti
- **Postcondizioni:**
  - Viene presentata la pagina di test ***CAPTCHA***$_G$

1.2. UC2 - Gestione e creazione virtual server

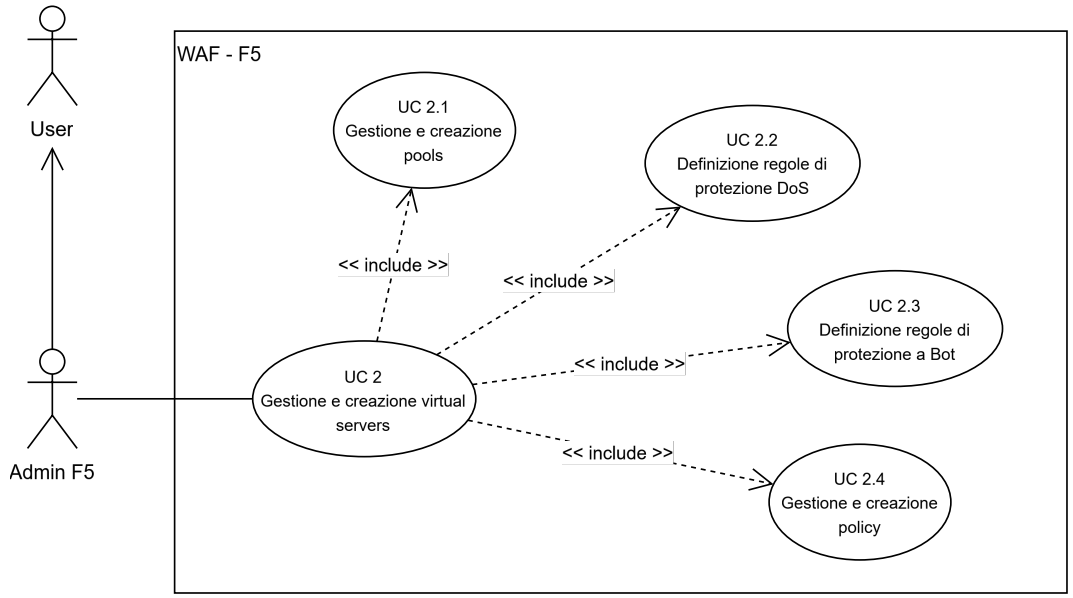

Figura 3: UC2 - Gestione e creazione virtual server

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può gestire e creare i ***Virtual server*** $_G$ ***F5*** $_G$, elementi fondamentali per analizzare e bilanciare tutto il traffico richiesto ai server interni che ospitano le applicazioni web
- **Precondizioni:**
  - Il servizio di BIG-IP ***Local Traffic Manager (LTM)*** $_G$ deve essere installato
- **Postcondizioni:**
  - Viene assegnato un nuovo ***Virtual server*** $_G$ al servizio BIG-IP ***LTM*** $_G$

1.2.1. UC2.1 - Gestione e creazione pools

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può gestire e creare ***Pool*** $_G$ di server. Questi raggruppamenti di server reali ricevono ed elaborano le richieste solo se non vengono bloccate dal ***WAF*** $_G$
- **Precondizioni:**

- Il servizio di BIG-IP ***LTM***$_G$ deve essere installato
- **Postcondizioni:**
  - Viene creata una nuova ***Pool***$_G$ di server

1.2.2. UC2.2 - Definizione regole di protezione DoS

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può definire regole di protezione contro gli attacchi ***DoS***$_G$. Questo permette al ***WAF***$_G$ di rilevarli e mitigarli utilizzando modalità anch'esse configurate dall'amministratore
- **Precondizioni:**
  - Il servizio di BIG-IP ***Application Security Manager (ASM)***$_G$ deve essere installato
- **Postcondizioni:**
  - Viene creata una nuova regola di protezione ***DoS***$_G$

1.2.3. UC2.3 - Definizione regole di protezione a Bot

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può definire regole di protezione contro gli attacchi provenienti da ***Bot***$_G$ o ***Botnet***$_G$. Questo permette al ***WAF***$_G$ di rilevarli e mitigarli utilizzando modalità anch'esse configurate dall'amministratore
- **Precondizioni:**
  - Il servizio di BIG-IP ***ASM***$_G$ deve essere installato
- **Postcondizioni:**
  - Viene creata una nuova regola di protezione per ***Bot***$_G$ e ***Botnet***$_G$

1.2.4. UC2.4 - Gestione e creazione policy

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**

- L'admin può gestire e creare ***Policy***$_G$ di sicurezza da associare a un ***Virtual server***$_G$. Queste ***Policy***$_G$ permettono di analizzare il traffico e definire regole specifiche per filtrare richieste sospette o illegali

- **Precondizioni:**
  - Il servizio di BIG-IP ***ASM***$_G$ deve essere installato
- **Postcondizioni:**
  - Viene creata una nuova ***Policy***$_G$

1.2.4.1. UC2.4.1 - Definizione di regole per data guard

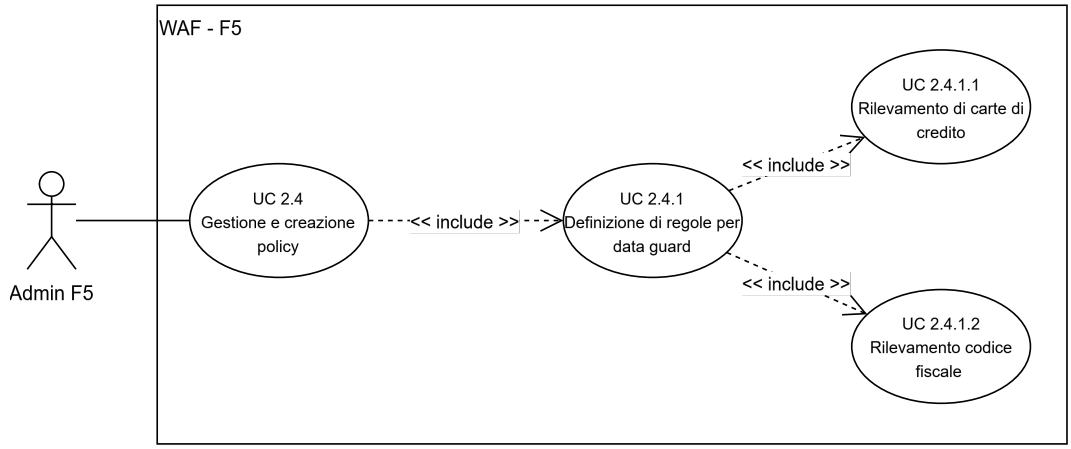

Figura 4: UC2.4.1 - Definizione di regole per data guard

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può definire regole di ***Data guard***$_G$ che permettono al ***WAF***$_G$ di identificare e censurare automaticamente informazioni sensibili degli utenti all'interno delle

  risposte ***HTTP***$_G$ da parte del server. Questo impedisce a potenziali attaccanti di visualizzare tali dati
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy***$_G$ possiede una regola per ***Data guard***$_G$

1.2.4.1.1. UC2.4.1.1 - Rilevamento di carte di credito

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può attivare la funzione per l'identificazione di numeri di carte di credito nelle risposte ***HTTP*** $_G$
- **Precondizioni:**
  - La funzione di rilevamento di carta di credito è disattivata
- **Postcondizioni:**
  - La funzione di rilevamento di carta di credito è attiva

1.2.4.1.2. UC2.4.1.2 - Rilevamento codice fiscale

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può attivare la funzione per l'identificazione di codici fiscali nelle risposte ***HTTP*** $_G$
- **Precondizioni:**
  - La funzione di rilevamento di codici fiscali è disattivata
- **Postcondizioni:**
  - La funzione di rilevamento di codici fiscali è attiva

1.2.4.2. UC2.4.2 - Gestione dei parametri URL

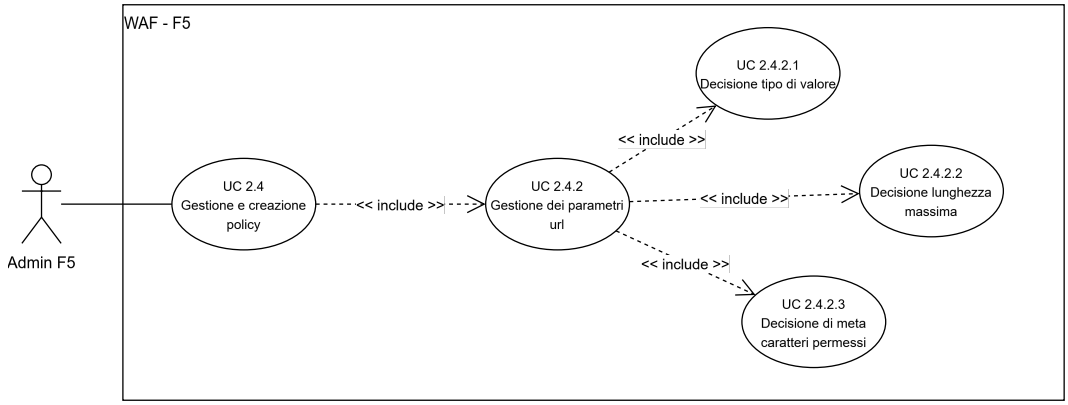

Figura 5: UC2.4.2 - Gestione dei parametri URL

- **Attore primario:**
  - Admin del ***WAF*$_G$ *F5*$_G$**
- **Descrizione:**
  - L'admin può gestire e definire come i parametri URL devono essere strutturati in qualsiasi richiesta ***HTTP*$_G$**
- **Precondizioni:**
  - La ***Policy*$_G$** alla quale si vuole assegnare queste regole deve essere presente
  - Tutti i parametri URL sono permessi indipendentemente dalla loro struttura
- **Postcondizioni:**
  - La ***Policy*$_G$** possiede le regole riguardanti la struttura dei parametri URL

1.2.4.2.1. UC2.4.2.1 - Decisione tipo di valore

- **Attore primario:**
  - Admin del ***WAF*$_G$ *F5*$_G$**
- **Descrizione:**
  - L'admin può decidere che tipo di valore deve essere il parametro URL nella richiesta ***HTTP*$_G$**
- **Precondizioni:**
  - Il tipo di valore è impostato su «qualsiasi»
- **Postcondizioni:**
  - Il tipo di valore è impostato su quello deciso dall'admin

1.2.4.2.2. UC2.4.2.2 - Decisione lunghezza massima

- **Attore primario:**
  - Admin del ***WAF*$_G$ *F5*$_G$**
- **Descrizione:**
  - L'admin può decidere la lunghezza massima del parametro URL nella richiesta ***HTTP*$_G$**, per evitare attacchi di ***Buffer overflow*$_G$**
- **Precondizioni:**
  - La lunghezza massima è impostata su «qualsiasi»
- **Postcondizioni:**
  - La lunghezza massima è impostata al valore deciso dall'admin

1.2.4.2.3. UC2.4.2.3 - Decisione di metacaratteri permessi

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può decidere quali ***Metacaratteri*** $_G$ sono permessi e quali no all'interno del valore di un input in una richiesta ***HTTP*** $_G$
- **Precondizioni:**
  - Tutti i ***Metacaratteri*** $_G$ non sono permessi
- **Postcondizioni:**
  - La configurazione decisa dall'admin viene applicata

1.2.4.3. UC2.4.3 - Gestione URL

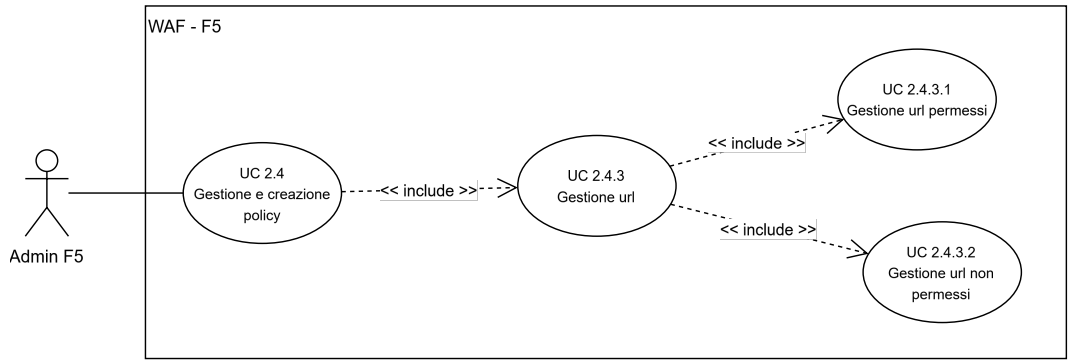

Figura 6: UC2.4.3 - Gestione URL

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può gestire e definire quali URL sono permessi e quali no, limitando così l'utente a un set ristretto di URL navigabili
- **Precondizioni:**
  - La ***Policy*** $_G$ alla quale si vuole assegnare queste regole deve essere presente
  - Tutti gli URL sono navigabili
- **Postcondizioni:**
  - La ***Policy*** $_G$ possiede le regole riguardanti quali URL sono permessi e quali no

1.2.4.3.1. UC2.4.3.1 - Gestione URL permessi

- **Attore primario:**
  - Admin del WAF_G $F5_G$
- **Descrizione:**
  - L'admin può definire quali URL sono permessi
- **Precondizioni:**
  - Tutti gli URL sono permessi
- **Postcondizioni:**
  - Solo gli URL elencati dall'admin sono permessi

1.2.4.3.2. UC2.4.3.2 - Gestione URL non permessi

- **Attore primario:**
  - Admin del WAF_G $F5_G$
- **Descrizione:**
  - L'admin può definire quali URL non sono permessi
- **Precondizioni:**
  - Tutti gli URL sono permessi
- **Postcondizioni:**
  - Gli URL elencati dall'admin non sono permessi

1.2.4.4. UC2.4.4 - Gestione delle sessioni utente

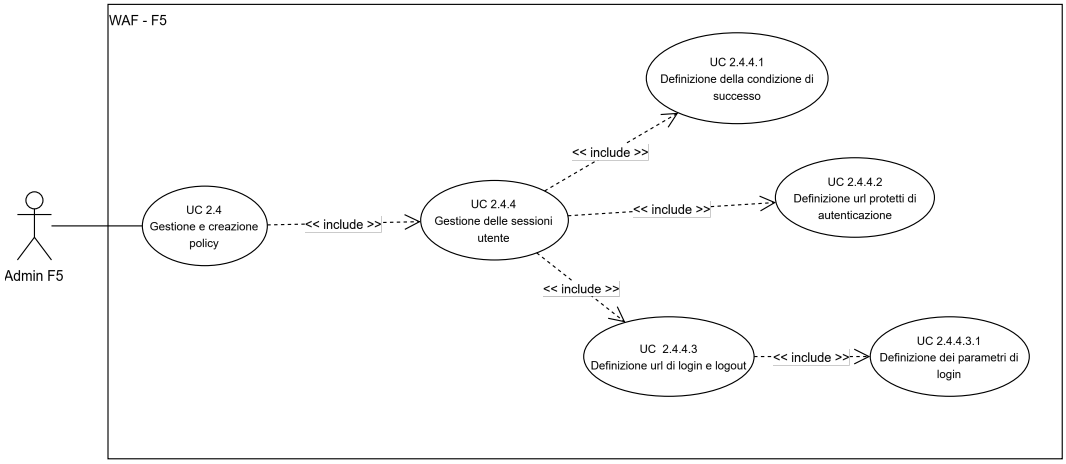

Figura 7: UC2.4.4 - Gestione delle sessioni utente

- **Attore primario:**

  - Admin del ***WAF$_G$ F5$_G$***
- **Descrizione:**
  - L'admin può definire e gestire regole e condizioni per impedire agli utenti di accedere a pagine che richiedono autenticazione, se non sono autenticati.
- **Precondizioni:**
  - La ***Policy$_G$*** alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy$_G$*** possiede le regole e condizioni per identificare se un utente risulta non autenticato

1.2.4.4.1. UC2.4.4.1 - Definizione della condizione di successo

- **Attore primario:**
  - Admin del ***WAF$_G$ F5$_G$***
- **Descrizione:**
  - L'admin deve definire la condizione di successo del login affinché il ***WAF$_G$*** possa riconoscere che l'accesso sia avvenuto correttamente.
- **Precondizioni:**
  - Nessuna condizione definita, quindi tutti i tentativi di accesso falliscono
- **Postcondizioni:**
  - Vengono applicate le condizioni di successo definite dall'admin

1.2.4.4.2. UC2.4.4.2 - Definizione URL protetti da autenticazione

- **Attore primario:**
  - Admin del ***WAF$_G$ F5$_G$***
- **Descrizione:**
  - L'admin deve definire gli URL che richiedono l'autenticazione dell'utente per essere accessibili.
- **Precondizioni:**
  - Nessun URL è definito
- **Postcondizioni:**
  - Vengono applicati dei controlli di sessione agli URL definiti

1.2.4.4.3. UC2.4.4.3 - Definizione URL di login e logout

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin deve definire quali URL corrispondono alle pagine di login e logout
- **Precondizioni:**
  - Nessuna pagina è definita
- **Postcondizioni:**
  - Vengono definiti gli URL di login e logout

1.2.4.4.3.1. UC2.4.4.3.1 - Definizione dei parametri di login

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può definire i parametri necessari per l'autenticazione dell'utente su un determinato URL
- **Precondizioni:**
  - Non esistono parametri di login definiti per l'URL
- **Postcondizioni:**
  - Vengono definiti i parametri di login per l'URL

1.2.4.5. UC2.4.5 - Gestione richieste HTTP

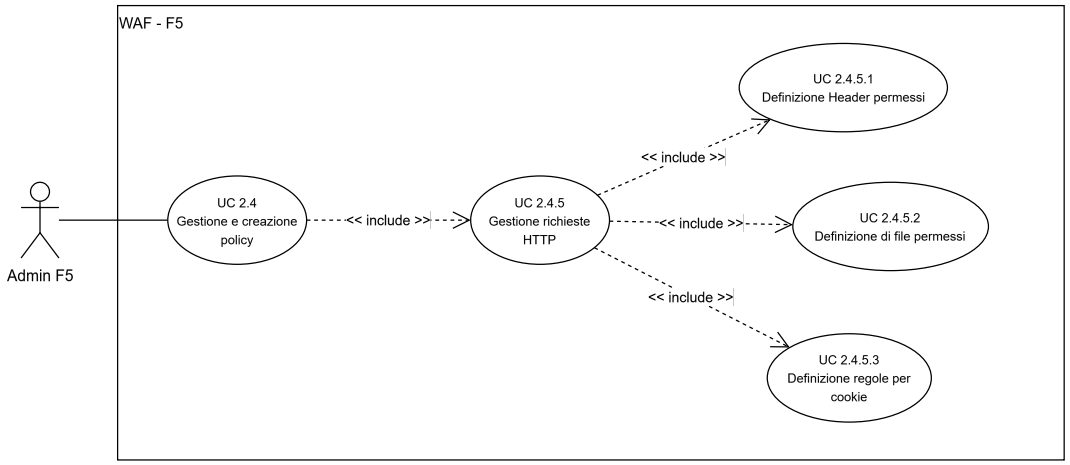

Figura 8: UC2.4.5 - Gestione richieste HTTP

- **Attore primario:**
  - Admin del ***WAF*$_G$** ***F5*$_G$**
- **Descrizione:**
  - L'admin può gestire e definire una serie di regole per individuare e filtrare le richieste ***HTTP*$_G$** sospette che potrebbero compromettere l'intero sistema o i dati degli utenti registrati
- **Precondizioni:**
  - La ***Policy*$_G$** alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy*$_G$** possiede le regole per individuare richieste ***HTTP*$_G$** sospette

1.2.4.5.1. UC2.4.5.1 - Definizione Header permessi

- **Attore primario:**
  - Admin del ***WAF*$_G$** ***F5*$_G$**
- **Descrizione:**
  - L'admin può definire gli header ***HTTP*$_G$** permessi in una richiesta
- **Precondizioni:**
  - La lista degli header permessi contiene solo «PUT», «GET», «POST»
- **Postcondizioni:**
  - Viene applicata la lista definita dall'admin

1.2.4.5.2. UC2.4.5.2 - Definizione di file permessi

- **Attore primario:**
  - Admin del ***WAF*$_G$** ***F5*$_G$**
- **Descrizione:**
  - L'admin può definire i file permessi nelle richieste e risposte ***HTTP*$_G$**
- **Precondizioni:**
  - La lista è vuota
- **Postcondizioni:**
  - Viene applicata la lista definita dall'admin

1.2.4.5.3. UC2.4.5.3 - Definizione regole per cookie

- **Attore primario:**

- Admin del *WAF*$_G$ *F5*$_G$

- **Descrizione:**
  - L'admin può definire regole da applicare ai cookie per prevenirne la manomissione e contrastare attacchi basati sulla loro alterazione.
- **Precondizioni:**
  - Non sono presenti regole
- **Postcondizioni:**
  - Vengono applicate le regole definite dall'admin

1.2.4.6. UC2.4.6 - Gestione attacchi brute force

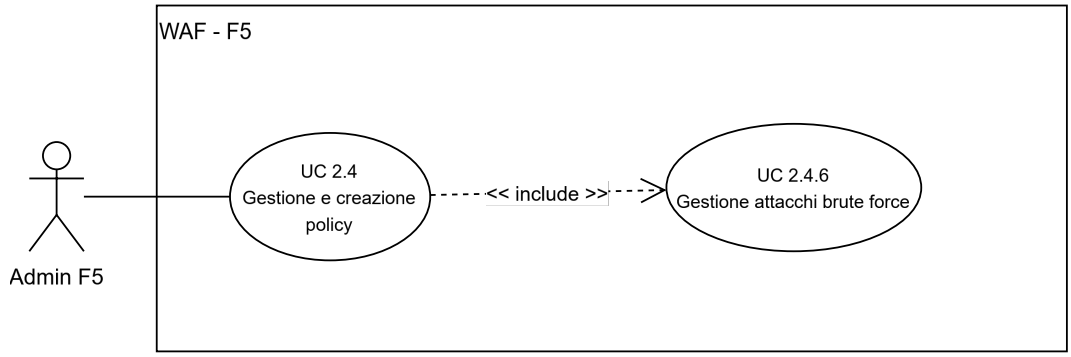

Figura 9: UC2.4.6 - Gestione regole per protezioni avanzate

- **Attore primario:**
  - Admin del *WAF*$_G$ *F5*$_G$

- **Descrizione:**
  - L'admin può gestire e creare regole per individuare e mitigare attacchi di tipo ***Brute force***$_G$
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy***$_G$ possiede regole per individuare e mitigare attacchi di tipo ***Brute force***$_G$

1.2.4.7. UC2.4.7 - Gestione attacchi CSRF

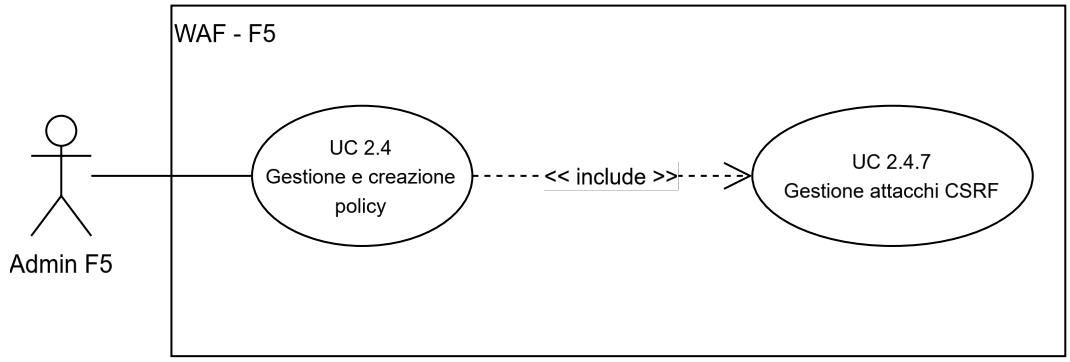

Figura 10: UC2.4.7 - Gestione attacchi CSRF

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può gestire e creare regole per individuare e mitigare attacchi di tipo ***Cross-Site Request Forgery (CSRF)***$_G$
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy***$_G$ possiede regole per individuare e mitigare attacchi di tipo ***CSRF***$_G$

1.2.4.8. UC2.4.8 - Gestione attacchi SSRF

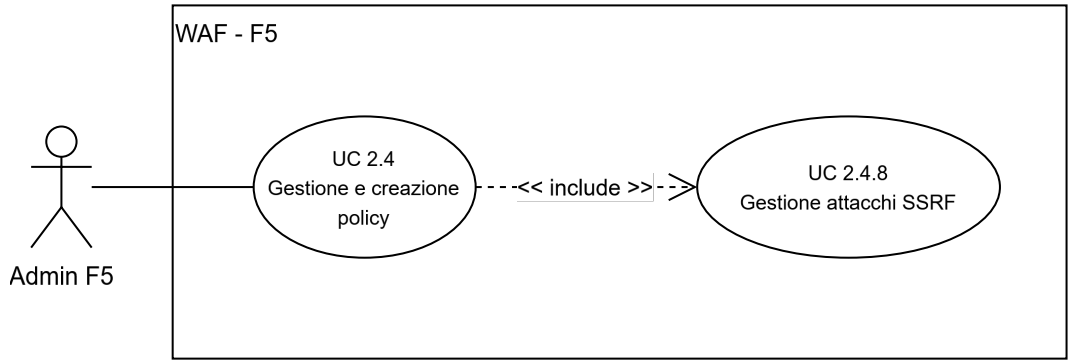

Figura 11: UC2.4.8 - Gestione attacchi SSRF

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può gestire e creare regole per individuare e mitigare attacchi di tipo ***Server-Side Request Forgery (SSRF)*** $_G$
- **Precondizioni:**
  - La ***Policy*** $_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy*** $_G$ possiede regole per individuare e mitigare attacchi di tipo ***SSRF*** $_G$

1.2.4.9. UC2.4.9 - Definizione di attack signatures

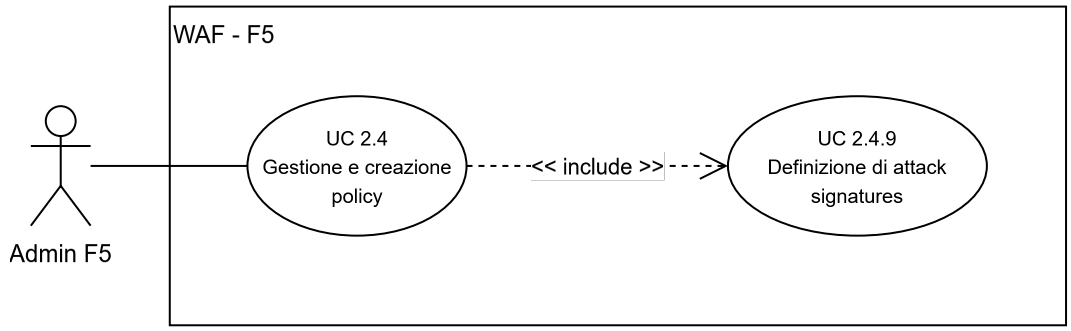

Figura 12: UC2.4.9 - Definizione di attack signatures

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**

- L'admin può definire ulteriori ***Attack signatures***$_G$ oltre a quelle già proposte dal modulo BIG-IP ***ASM***$_G$

- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - La ***Policy***$_G$ possiede le attack signature definite dall'admin oltre a quelle già presenti di default

1.2.4.10. UC2.4.10 - Configurazione IP Intelligence

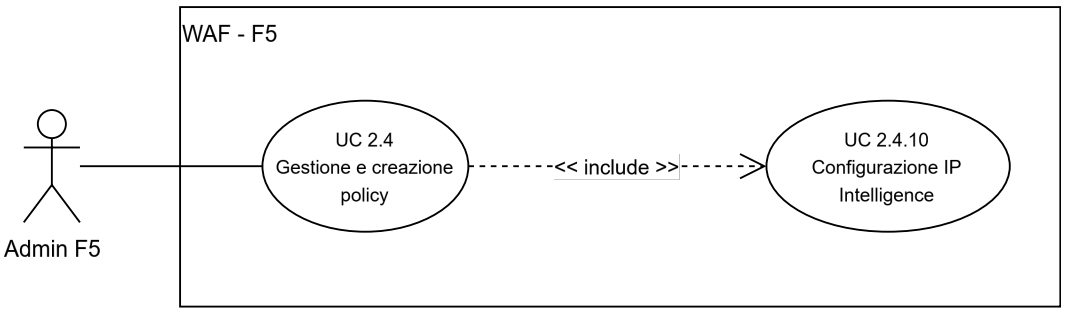

Figura 13: UC2.4.10 - Configurazione IP Intelligence

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può abilitare e configurare il modulo IP Intelligence. Questo modulo utilizza un database remoto per determinare la reputazione di un indirizzo IP che effettua una richiesta ***HTTP***$_G$, bloccando quelle provenienti da IP con reputazione negativa
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - Il modulo di IP Intelligence viene attivato sulla ***Policy***$_G$ selezionata

1.2.4.11. UC2.4.11 - Configurazione learning modes

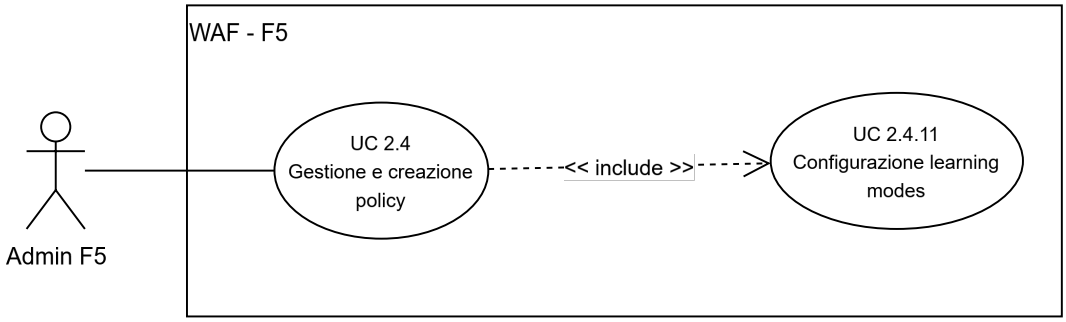

Figura 14: UC2.4.11 - Configurazione learning modes

- **Attore primario:**
  - Admin del WAF_G $F5_G$
- **Descrizione:**
  - L'admin può configurare quali tipi di violazioni generano suggerimenti per ottimizzare le regole del WAF_G. Questo permette di ridurre i falsi positivi o aumentare il livello di protezione per specifiche richieste
- **Precondizioni:**
  - La $Policy_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - Viene applicata la configurazione scelta dall'admin

1.2.4.12. UC2.4.12 - Definizione tecnologie applicazione

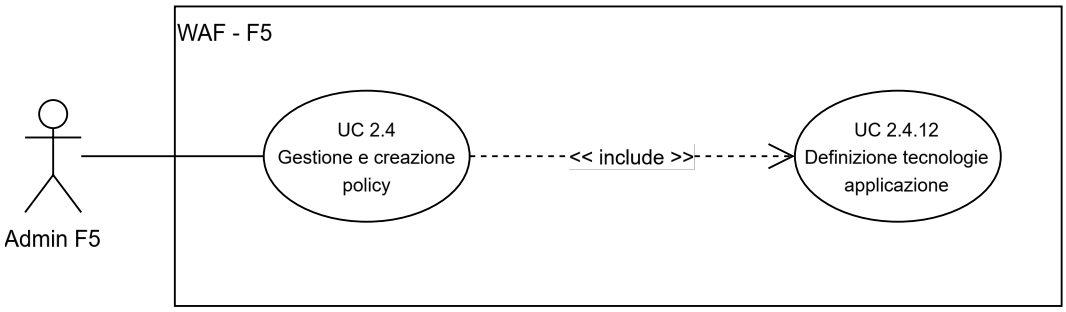

Figura 15: UC2.4.12 - Definizione tecnologie applicazione

- **Attore primario:**
  - Admin del WAF_G $F5_G$

- **Descrizione:**
  - L'admin può definire le tecnologie utilizzate dall'applicazione web. In questo modo, il ***WAF***$_G$ può comprendere gli attacchi più comuni specifici per quella tecnologia e proporre un set iniziale di regole sufficienti per mitigarli.
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - Vengono create delle attack signature inerenti alle tecnologie elencate
  - Viene aggiornato l'elenco delle tecnologie della ***Policy***$_G$

1.2.4.13. UC2.4.13 - Importazione threat campaign

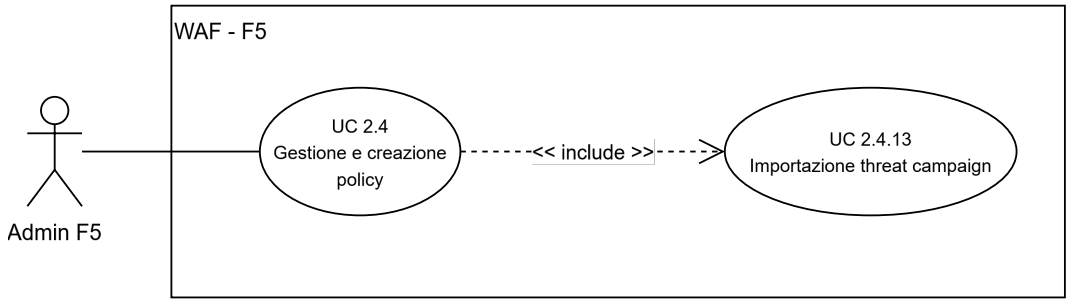

Figura 16: UC2.4.13 - Importazione threat campaign

- **Attore primario:**
  - Admin del ***WAF***$_G$ ***F5***$_G$
- **Descrizione:**
  - L'admin può importare uno o più file di ***Threat campaign***$_G$ per fornire al ***WAF***$_G$ informazioni sugli attacchi più comuni o attualmente in uso.
- **Precondizioni:**
  - La ***Policy***$_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - Vengono generate delle ***Attack signatures***$_G$ per mitigare gli attacchi elencati nei file di ***Threat campaign***$_G$

1.2.4.14. UC2.4.14 - Configurazione pagine di blocco

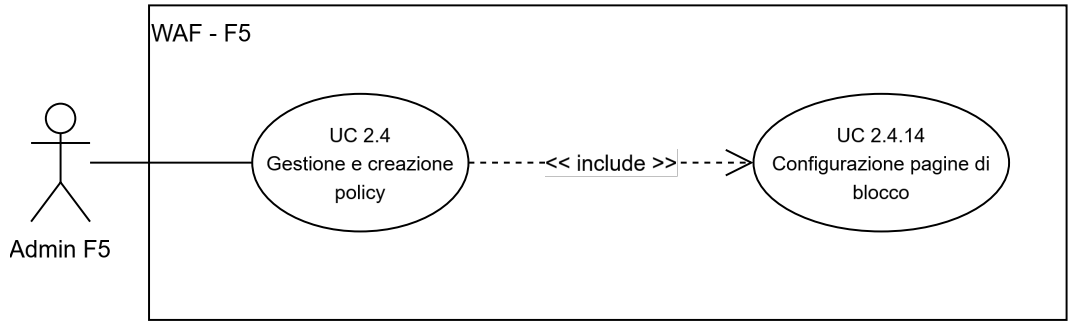

Figura 17: UC2.4.14 - Configurazione pagine di blocco

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**
  - L'admin può personalizzare le pagine di blocco visualizzate dagli utenti quando una loro richiesta viene classificata come illegale dal ***WAF*** $_G$
- **Precondizioni:**
  - La ***Policy*** $_G$ alla quale si vuole assegnare queste regole deve essere presente
- **Postcondizioni:**
  - Viene aggiornato lo stile delle pagine di blocco

1.3. UC3 - Definizione profili di logging

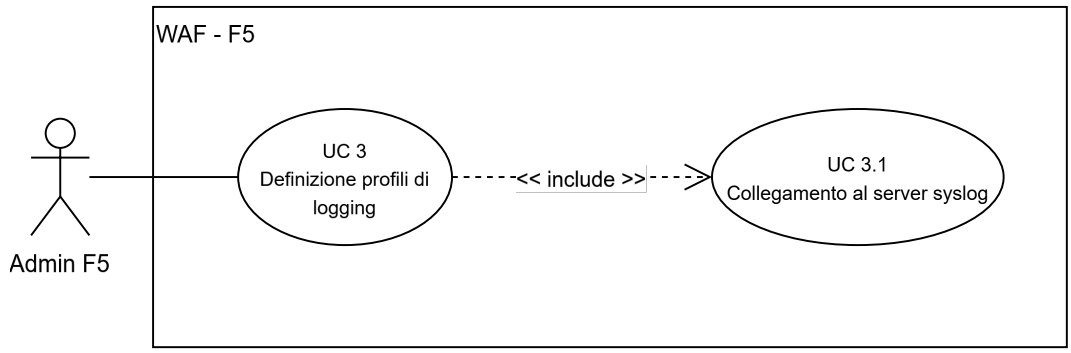

Figura 18: UC3 - Definizione profili di logging

- **Attore primario:**
  - Admin del ***WAF*** $_G$ ***F5*** $_G$
- **Descrizione:**

- L'admin ha la possibilità di creare profili e configurazioni personalizzate per la gestione e l'archiviazione di tutti i log generati dal firewall

- **Precondizioni:**
  - L'amministratore desidera creare profili personalizzati per ottimizzarne l'organizzazione
- **Postcondizioni:**
  - Il profilo di logging viene applicato al firewall

1.3.1. UC3.1 - Collegamento al server syslog

- **Attore primario:**
  - Admin del ***WAF*$_G$** ***F5*$_G$**
- **Descrizione:**
  - L'admin ha la possibilità di archiviare tutti i log generati in un server ***Syslog*$_G$** esterno per diminuire il carico e l'utilizzo della memoria utilizzata dal ***WAF*$_G$**
- **Precondizioni:**
  - L'amministratore intende minimizzare il carico del firewall spostando l'archiviazione dei dati su un server esterno
- **Postcondizioni:**
  - Il server esterno riceve i log impostati dall'admin tramite il profilo di logging

2. Requisiti

I requisiti del progetto sono stati definiti dopo il periodo di formazione, durante una breve riunione tra noi stagisti e i due tutor aziendali. Di seguito sono presentate le tabelle che illustrano i diversi tipi di requisiti (funzionali, di qualità e di vincolo), dove ciascun requisito è identificato da una nomenclatura che ne indica la classificazione:

- **M**: Obbligatorio
- **D**: Desiderabile
- **O**: Opzionale

2.1. Requisiti funzionali

Requisito	Descrizione	Classificazione	Fonte
RF0	L'utente deve visualizzare la applicazione web normalmente	M	UC1
RF1	L'utente deve visualizzare il *CAPTCHA*$_G$ nel caso il *WAF*$_G$ rilevi troppe richieste in brevi periodi di tempo	M	UC1.2
RF2	L'utente deve visualizzare una pagina di blocco nel caso in cui una richiesta venga rilevata sospetta e venga bloccata dal *WAF*$_G$	M	UC1.1
RF3	L'admin *F5*$_G$ deve gestire e creare dei *Virtual server*$_G$ in modo da permettere gli utenti di collegarsi all'applicazione web	M	UC2
RF4	L'admin *F5*$_G$ deve gestire e creare i server pools	M	UC2.1
RF5	L'admin *F5*$_G$ deve definire le regole per la protezione da attacchi *DoS*$_G$	M	UC2.2
RF6	L'admin *F5*$_G$ deve definire le regole di protezione da attacchi da parte di *Bot*$_G$ e *Botnet*$_G$	M	UC2.3

RF7	L'admin *F5*$_G$ deve gestire e creare le *Policy*$_G$ da assegnare al *WAF*$_G$ in modo che riesca a filtrare le richieste sospette	M	UC2.4
RF8	L'admin *F5*$_G$ deve definire le regole per la protezione dei dati personali contenute nelle risposte del server	M	UC2.4.1
RF9	L'admin *F5*$_G$ deve definire le regole per il rilevamento di numeri di carte di credito	M	UC2.4.1.1
RF10	L'admin *F5*$_G$ deve definire le regole per il rilevamento di codici fiscali	M	UC2.4.1.2
RF11	L'admin *F5*$_G$ deve definire regole da applicare ai parametri che vengono passati al server tramite URL	M	UC2.4.2
RF12	L'admin *F5*$_G$ deve definire il tipo di valore consentito per parametro	M	UC2.4.2.1
RF13	L'admin *F5*$_G$ deve definire la massima lunghezza del valore per parametro	M	UC2.4.2.2
RF14	L'admin *F5*$_G$ deve definire quali metacaratteri sono consentiti per parametro	M	UC2.4.2.3
RF15	L'admin *F5*$_G$ deve definire quali URL sono permessi e visibili all'utente	M	UC2.4.3.1
RF16	L'admin *F5*$_G$ deve definire quali URL non sono permessi e non visibili all'utente	M	UC2.4.3.2
RF17	L'admin *F5*$_G$ deve definire come vengono gestite le sessioni utente	M	UC2.4.4
RF18	L'admin *F5*$_G$ deve definire la condizione di successo per il login	M	UC2.4.4.1
RF19	L'admin *F5*$_G$ deve definire gli URL accessibili solo dopo l'autenticazione dell'utente	M	UC2.4.4.2
RF20	L'admin *F5*$_G$ deve definire gli URL di login e logout	M	UC2.4.4.3

RF21	L'admin *F5*$_G$ deve definire i parametri di login e logout	M	UC2.4.4.3.1
RF22	L'admin *F5*$_G$ deve creare regole per filtrare determinati tipi di richieste *HTTP*$_G$	M	UC2.4.5
RF23	L'admin *F5*$_G$ deve definire quali header sono permessi	M	UC2.4.5.1
RF24	L'admin *F5*$_G$ deve definire quali file sono consentiti	M	UC2.4.5.2
RF25	L'admin *F5*$_G$ deve definire regole per garantire l'autenticazione dei cookie	M	UC2.4.5.3
RF26	L'admin *F5*$_G$ deve gestire come vengono mitigati gli attacchi di tipo *Brute force*$_G$	M	UC2.4.6
RF27	L'admin *F5*$_G$ deve gestire come vengono mitigati gli attacchi *CSRF*$_G$	M	UC2.4.7
RF28	L'admin *F5*$_G$ deve gestire come vengono mitigati gli attacchi *SSRF*$_G$	M	UC2.4.8
RF29	L'admin *F5*$_G$ deve definire le *Attack signatures*$_G$	M	UC2.4.9
RF30	L'admin *F5*$_G$ deve configurare il modulo di IP Intelligence	M	UC2.4.10
RF31	L'admin *F5*$_G$ deve configurare le modalità di apprendimento del *WAF*$_G$	M	UC2.4.11
RF32	L'admin *F5*$_G$ deve definire le tecnologie utilizzate dall'applicazione web	M	UC2.4.12
RF33	L'admin *F5*$_G$ deve importare le *Threat campaign*$_G$	M	UC2.4.13
RF34	L'admin *F5*$_G$ deve creare e definire le pagine di blocco	M	UC2.4.14
RF35	L'admin *F5*$_G$ deve creare dei profili di logging	M	UC3
RF36	L'admin *F5*$_G$ deve instaurare il collegamento con il server *Syslog*$_G$ per memorizzare tutti i log creati dal *WAF*$_G$	D	UC3.1

2.2. Requisiti qualitativi

Requisito	Descrizione	Classificazione	Fonte
RQ0	La *Policy*$_G$ assegnata al *WAF*$_G$ deve essere conforme alla top 10 di *Open Worldwide Application Security Project (OWASP)*$_G$	M	Progetto
RQ1	Il *WAF*$_G$ deve essere testato tramite il tool *F5*$_G$-*WAF*$_G$-tester per verificarne la sua efficacia	M	Progetto
RQ2	Il *WAF*$_G$ deve essere in grado di bloccare gli attacchi di tipo *Javascript (JS)*$_G$ e *SQL injection*$_G$	M	Progetto
RQ3	Il *WAF*$_G$ deve essere in grado di bloccare gli attacchi di manomissione dei cookie e delle sessioni utente	M	Progetto
RQ4	Il *WAF*$_G$ deve essere in grado di bloccare gli attacchi *Cross-Site Scripting (XSS)*$_G$	M	Progetto
RQ5	Il *WAF*$_G$ deve essere in grado di bloccare gli attacchi *Insecure Direct Object Reference (IDOR)*$_G$	O	Decisione personale
RQ6	Il *WAF*$_G$ deve essere in grado di mascherare le informazioni sensibili degli utenti	M	Progetto
RQ7	Il *WAF*$_G$ deve essere in grado di rilevare e bloccare attacchi *DoS*$_G$	M	Progetto
RQ8	Il *WAF*$_G$ deve essere in grado di rilevare e bloccare attacchi di *Brute force*$_G$	M	Progetto

2.3. Requisiti di vincolo

Requisito	Descrizione	Classificazione	Fonte

RV0	Utilizzo del modulo ***LTM*$_G$** di BIG-IP per abilitare funzioni di bilanciamento delle risorse e monitoraggio dello stato	M	Progetto
RV1	Utilizzo del modulo ***ASM*$_G$** di BIG-IP per analizzare i pacchetti ***HTTP*$_G$** e HTTPS in modo tale da proteggere l'applicazione da attacchi	M	Progetto
RV2	Utilizzo di ***Rsyslog*$_G$** per il server dedicato al tracciamento di tutti i log del ***WAF*$_G$**	D	Decisione personale

Glossario

WAF : Firewall specializzato che protegge le applicazioni web da attacchi e traffico internet indesiderato (es. botnet, attacchi DoS), analizzando il traffico HTTP e HTTPS.. 5, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31.

F5 : Azienda leader nella fornitura di soluzioni per la sicurezza delle applicazioni, l'ottimizzazione della rete e la gestione del traffico. I suoi prodotti principali, come i Big-IP, sono spesso utilizzati per il bilanciamento del carico, creazione di Web Application Firewall (WAF) e la gestione delle API.. 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 28, 29, 30.

OWASP : Organizzazione no-profit che si dedica a migliorare la sicurezza del software.. 30.

HTTP : Protocollo fondamentale su cui si basa la comunicazione dati sul World Wide Web. Definisce le regole e il formato con cui browser web e server scambiano messaggi.. 6, 7, 10, 11, 12, 13, 17, 22, 29, 31.

DoS : Categoria di attacchi informatici il cui obiettivo principale è rendere inaccessibile un servizio, una risorsa di rete o un server ai suoi utenti legittimi. Questo tipo di attacco non mira solitamente a rubare informazioni, ma a impedirne il corretto funzionamento o l'accessibilità.. 7, 9, 27, 30.

Virtual server : Componente logica fondamentale sui sistemi F5 BIG-IP. Funziona come un punto di ascolto virtuale (un indirizzo IP virtuale e una porta) sul dispositivo F5, attraverso il quale il traffico di rete viene intercettato, ispezionato e bilanciato prima di essere inoltrato ai server reali.. 8, 10, 27.

Pool : Una Pool F5 è una componente logica essenziale all'interno di un dispositivo F5 BIG-IP che rappresenta una collezione di server reali che ospitano la stessa applicazione o servizio.. **8, 9.**

Bot : Programma software automatizzato progettato per eseguire compiti specifici su Internet o altre reti, spesso con una frequenza molto più elevata di quanto sarebbe possibile per un essere umano.. **7, 9, 27.**

Botnet : Rete di computer (o altri dispositivi connessi a internet, come smartphone, dispositivi IoT, ecc.) infettati da software dannoso e controllati da un singolo attaccante, noto come bot-herder. Ogni dispositivo compromesso nella botnet esegue comandi inviati dal bot-herder senza che il proprietario ne sia consapevole per eseguire attività illecite.. **7, 9, 27.**

Data guard : Funzionalità specifica del WAF di F5 BIG-IP, progettata per la protezione delle informazioni sensibili che transitano nelle richieste e risposte HTTP/HTTPS. Il suo scopo principale è prevenire la fuoriuscita accidentale o intenzionale di dati confidenziali, mascherandoli o bloccandoli prima che raggiungano destinatari non autorizzati.. **10.**

Policy : Potente strumento configurabile sui dispositivi F5 BIG-IP che consente agli admin di controllare e manipolare il traffico di rete in ingresso e in uscita. Offrono un modo più strutturato e intuitivo per definire regole e condizioni che il traffico deve soddisfare, e le azioni da intraprendere quando tali condizioni sono soddisfatte.. **10, 12, 13, 15, 17, 19, 20, 22, 23, 24, 25, 28, 30.**

Buffer overflow : vulnerabilità software che si verifica quando un programma tenta di scrivere più dati in un'area di memoria temporanea (buffer) di quanti essa possa contenerne. Di conseguenza, i dati in eccesso e sovrascrivono la memoria adiacente, che potrebbe contenere altre istruzioni del programma o dati critici.. **12.**

Metacaratteri : Caratteri speciali che hanno un significato particolare e predefinito all'interno di un linguaggio o di un sistema, piuttosto che rappresentare se stessi. Non vengono interpretati letteralmente, ma agiscono come istruzioni o indicatori che influenzano il modo in cui altri caratteri o stringhe vengono elaborati o abbinati.. 13.

Brute force : Attacco informatico che consiste nel tentare sistematicamente ogni possibile combinazione di caratteri, numeri e simboli per indovinare una password, una chiave crittografica o una chiave di accesso.. 19, 29, 30.

CSRF : Vulnerabilità di sicurezza che inganna un utente autenticato a eseguire azioni indesiderate su un'applicazione web.. 19, 29.

SSRF : Vulnerabilità di sicurezza che permette a un attaccante di indurre il server di un'applicazione web a effettuare richieste HTTP arbitrarie a un dominio a scelta dell'attaccante.. 20, 29.

Attack signatures : Regole o pattern predefinite utilizzate dal WAF di F5 per identificare e bloccare attacchi noti o classi di attacchi contro un'applicazione web e i suoi componenti.. 21, 24, 29.

Syslog : Protocollo standard per l'invio e la raccolta di messaggi di log da diversi dispositivi di rete e sistemi operativi in un sistema di gestione centralizzato.. 26, 29.

CAPTCHA : Misura di sicurezza utilizzata per determinare se l'utente che interagisce con un sistema informatico è un essere umano o un programma automatico.. 5, 7, 27.

Threat campaign : Insieme di attacchi informatici che condividono uno scopo comune, strumenti simili, infrastrutture o tecniche.. 24, 29.

IDOR : Vulnerabilità di controllo degli accessi che si verifica quando un'applicazione web espone un riferimento diretto a un oggetto interno (come un file, un database

entry, una chiave, una directory) e non verifica adeguatamente se l'utente è autorizzato ad accedervi.. 30.

SQL injection : Vulnerabilità di iniezione nelle applicazioni web. Permette a un attaccante di manipolare le query SQL che un'applicazione esegue sul suo database, iniettando codice malevolo tramite l'input dell'utente.. 30.

XSS : Vulnerabilità che permette a un attaccante di iniettare codice malevolo (solitamente JavaScript, ma anche HTML o CSS) nelle pagine web visualizzate da altri utenti.. 30.

Rsyslog : Software open-source leader per la raccolta, l'elaborazione e l'inoltro di messaggi di log in sistemi Unix/Linux. È un'implementazione avanzata del protocollo Syslog standard, progettata per essere veloce, sicura e altamente configurabile.. 31.

Acronimi e abbreviazioni

WAF : Web Application Firewall.5, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31.

OWASP : Open Worldwide Application Security Project. 30.

HTTP : Hypertext Transfer Protocol. 6, 7, 10, 11, 12, 13, 17, 22, 29, 31.

DoS : Denial of Service. 7, 9, 27, 30.

LTM : Local Traffic Manager. 8, 9, 31.

ASM : Application Security Manager. 9, 10, 21, 31.

CSRF : Cross-Site Request Forgery. 19, 29.

SSRF : Server-Side Request Forgery. 20, 29.

IDOR : Insecure Direct Object Reference. 30.

JS : Javascript. 30.

XSS : Cross-Site Scripting. 30.