

Analisi dei Requisiti

v1.0.0

Registro delle Modifiche

Data	Versione	Descrizione	Redattore	Verificatore
2026/02/23	1.0.0	Revisione finale per RTB		Suar Alberto
2026/02/18	0.47.0	Refactoring generale di tutti casi d'uso con riscrittura di molti di essi	Basso Kevin	Suar Alberto
2026/02/16	0.46.0	Inserimento UC 47-53 e requisiti	Sandu Antonio	Suar Alberto
2026/02/15	0.45.1	Fix UC20-30, eliminazione UC23	Sgreva Andrea	Suar Alberto
2026/02/15	0.45.0	Modifica UC 16 e 19, aggiunta UC 41-46 e requisiti	Sandu Antonio	Suar Alberto
2026/02/13	0.44.7	Fix UC6, UC37-41	Sgreva Andrea	Suar Alberto
2026/02/13	0.44.6	Fix UC5, UC9-11	Sandu Antonio	Suar Alberto
2026/02/10	0.44.5	Fix vari degli UC + fix specifici UC13-15	Sgreva Andrea	Suar Alberto
2026/02/10	0.44.4	Fix della posizione del sistema in tutti i diagrammi UC	Sgreva Andrea	Suar Alberto
2026/02/10	0.44.3	Primo fix generale UC	Sgreva Andrea	Suar Alberto
2026/02/09	0.44.2	Sistemato formato dei link al glossario	Sandu Antonio	Suar Alberto
2026/02/09	0.44.1	Fix definizione attori	Sgreva Andrea	Suar Alberto
2026/02/08	0.44.0	Aggiunto UC12, inclusi diagrammi e requisiti associati. Fix alle precondizioni, attori e diagrammi di UC1, UC2, UC4	Sandu Antonio	Suar Alberto
2026/02/04	0.43.0	Classificazione Requisiti per priorità	Zago Alice	Suar Alberto
2026/02/04	0.42.1	Sistemata la sezione Attori + immagini separate per Front-end e Back-end	Sgreva Andrea	Suar Alberto

Data	Versione	Descrizione	Redattore	Verificatore
2026/02/03	0.42.0	Aggiunta diagrammi UC16-30	Sgreva Andrea	Suar Alberto
2026/02/02	0.41.0	Fix e aggiunta diagrammi mancanti UC6, UC9, UC10, UC12, UC13, UC14, UC15	Sgreva Andrea	Suar Alberto
2026/02/02	0.40.0	Fix e aggiunta diagrammi mancanti UC1-3	Sgreva Andrea	Suar Alberto
2026/02/01	0.39.0	Aggiunta Requisiti di Qualità e di Vincolo	Zago Alice	Suar Alberto
2026/01/27	0.38.0	Aggiunta dei requisiti funzionali UC36-UC29	Sgreva Andrea	Suar Alberto
2026/01/25	0.37.2	Fix alla struttura delle precondizioni, modifica a UC1-3 e relativi requisiti	Sandu Antonio	Suar Alberto
2026/01/24	0.37.1	Fix alla struttura di inclusioni ed estensioni	Sandu Antonio	Suar Alberto
2026/01/24	0.37.0	Inserimento diagrammi per UC36-41	Sgreva Andrea	Suar Alberto
2026/01/24	0.36.0	Modifica dei casi d'uso UC36, UC28 e UC28.1 e aggiunta di UC36.1, UC23, UC23.1, UC29 e UC29.1	Sgreva Andrea	Suar Alberto
2026/01/21	0.35.0	Inserimento diagrammi aggiornati per UC1-5 e UC26-37	Sandu Antonio	Suar Alberto
2026/01/21	0.34.0	Aggiunta di sottocasi di UC21 e 30 e altri fix	Berengan Riccardo	Suar Alberto
2026/01/19	0.33.1	Aggiunti requisiti funzionali UC12 e UC13, UC16-UC20 e UC20-UC20. Modifica requisiti UC5-UC15	Zago Alice	Suar Alberto

Data	Versione	Descrizione	Redattore	Verificatore
2026/01/18	0.32.1	Riorganizzazione requisiti funzionali relativi ai casi d'uso da UC1 a UC4	Zago Alice	Suar Alberto
2026/01/17	0.32.0	Modifica alla struttura dei requisiti	Sandu Antonio	Zago Alice
2026/01/17	0.31.0	Modifica UC18, 20 e da 24 a 29	Martinello Riccardo	Zago Alice
2026/01/17	0.30.2	Modificati requisiti funzionali. Eliminazione requisiti di performance	Zago Alice	Suar Alberto
2026/01/17	0.30.1	Modifica UC22. Aggiunta UC23, UC24	Berengan Riccardo	Suar Alberto
2026/01/16	0.29.0	Aggiunta UC36, UC28, UC28.1, UC29	Sgreva Andrea	Suar Alberto
2026/01/16	0.28.0	Aggiunta UC26, UC27, UC36 e UC37	Sandu Antonio	Suar Alberto
2026/01/16	0.27.0	Aggiunta UC21 e UC22	Berengan Riccardo	Suar Alberto
2026/01/15	0.26.0	Aggiunta UC18-UC20 con relativi sotto casi d'uso	Martinello Riccardo	Zago Alice
2026/01/15	0.25.1	Fix per UC17 e UC18	Sandu Antonio	Zago Alice
2026/01/15	0.25.0	UC17 e UC18	Berengan Riccardo	Zago Alice
2026/01/14	0.24.1	Fix minori al documento	Sandu Antonio	Zago Alice
2026/01/13	0.24.0	Requisiti funzionali relativi a UC9, UC10, UC11	Berengan Riccardo	Zago Alice
2026/01/12	0.23.0	Caso d'uso UC16 con relativi sottocasi e diagrammi	Zago Alice	Suar Alberto
2026/01/10	0.22.0	Requisiti funzionali relativi ad UC15	Berengan Riccardo	Zago Alice
2026/01/09	0.21.1	Fix minori label del documento	Martinello Riccardo	Zago Alice
2026/01/09	0.21.0	Caso d'uso UC15	Berengan Riccardo	Zago Alice

Data	Versione	Descrizione	Redattore	Verificatore
2026/01/09	0.20.0	Requisiti da UC6 a UC8	Zago Alice	Suar Alberto
2026/01/9	0.19.0	Aggiunti diagrammi per UC9 e UC10	Sandu Antonio	Zago Alice
2026/01/08	0.18.0	Modificati requisiti relativi a UC14. Aggiunti diagrammi UC14	Zago Alice	Suar Alberto
2026/01/06	0.17.0	Casi d'uso UC14, UC14.1, UC14.1.1 e UC14.2. Requisiti relativi a UC14	Zago Alice	Suar Alberto
2026/01/04	0.16.0	Aggiunta UC13 e relativi sottocasi	Berengan Riccardo	Zago Alice
2025/12/30	0.15.1	Piccoli fix e spell corrections	Basso Kevin	Zago Alice
2025/12/29	0.15.0	Classificazione dei requisiti. Requisiti relativi a UC1 - UC5, aggiunta sezione Classificazione Requisiti in Introduzione. Rielaborazione Introduzione per garantire maggiore formalità, diagrammi UC5	Suar Alberto	Basso Kevin
2025/12/29	0.14.0	Spunti su UC3, requisiti UC3, numerazione automatica requisiti	Basso Kevin	Suar Alberto
2025/12/28	0.13.0	Requisiti per UC1 e UC2	Suar Alberto	Basso Kevin
2025/12/28	0.12.0	Aggiunti diagrammi UC9 e UC12	Basso Kevin	Suar Alberto
2025/12/27	0.11.0	Diagrammi UC3. Modificato UC4 e aggiunti diagrammi.	Suar Alberto	Basso Kevin

Data	Versione	Descrizione	Redattore	Verificatore
		Rivalutare UC5 per maggiore chiarezza		
2025/12/27	0.10.0	Aggiunta UC da 7 a 12 con relativi sotto casi d'uso, aggiunta estensioni per UC4.3	Basso Kevin	Suar Alberto
2025/12/24	0.9.0	Aggiunto UC3	Suar Alberto	Basso Kevin
2025/12/24	0.8.0	Correzioni minori ai casi d'uso UC 5.1, aggiunto UC5.5, aggiornamento numerazione UC 5.X, Aggiunta UC6	Basso Kevin	Suar Alberto
2025/12/23	0.7.0	Correzione UML dei casi d'uso descritti, aggiunti UC2.1.2 e UC2.2.2. Esplicitate le postcondizioni e i trigger degli UC	Suar Alberto	Basso Kevin
2025/12/22	0.6.0	Correzione sezione Introduzione -> riferimenti. Fatti UC2, UC4, UC4.1.2, UC4.1.3 UC5. Inizio stesura Requisiti	Basso Kevin	Suar Alberto
2025/12/22	0.5.0	Aggiunti diagrammi dei casi d'uso UC1 e da UC1.1 a UC1.5. Modificate le postcondizioni delle estensioni	Suar Alberto	Basso Kevin
2025/12/22	0.4.0	Completato Introduzione e attori dei casi d'uso e correzione UC1.X	Basso Kevin	Suar Alberto
2025/12/22	0.3.1	Leggere correzioni lessicali	Basso Kevin	Suar Alberto
2025/12/21	0.3.0	Casi d'uso UC1 e da UC1.1 a UC1.5	Suar Alberto	Basso Kevin

Data	Versione	Descrizione	Redattore	Verificatore
		(compresi di estensioni)		
2025/12/20	0.2.0	Completamento sezione funzioni del prodotto e caratteristiche degli utenti	Basso Kevin	Suar Alberto
2025/12/18	0.1.0	Inizio stesura documento, introduzione, scopo e prospettiva del prodotto	Basso Kevin	Suar Alberto
2025/12/17	0.0.0	Creazione documento	Basso Kevin	Suar Alberto

Indice

Introduzione	15
Contesto del Progetto	15
Finalità del Documento	15
Scopo del Prodotto	15
Funzioni del Prodotto	15
Caratteristiche degli Utenti	16
Limitazioni	16
Glossario	16
Riferimenti	16
Riferimenti Normativi	16
Riferimenti Informativi	17
Casi d'Uso	18
Introduzione	18
Attori	18
Lista	20
UC1: Registrazione a CodeGuardian	20
UC1.0.1: Visualizzazione errore campi non inseriti	20
UC1.1: Inserimento username	21
UC1.1.1: Visualizzazione errore username non conforme	21
UC1.1.2: Visualizzazione errore username già in uso	22
UC1.2: Inserimento email	22
UC1.2.1: Visualizzazione errore email non valida	23
UC1.2.2: Visualizzazione errore email già in uso	23
UC1.3: Inserimento password	24
UC1.3.1: Visualizzazione errore password non conforme	24
UC2: Autenticazione a CodeGuardian	25
UC2.0.1: Visualizzazione errore campi non inseriti	25
UC2.1: Inserimento username	26
UC2.1.1: Visualizzazione errore username non conforme	26
UC2.1.2: Visualizzazione errore username non esistente	27
UC2.2: Inserimento password	27
UC2.2.1: Visualizzazione errore password non conforme	28
UC2.2.2: Visualizzazione errore password errata	28
UC3: Collegamento account GitHub	28
UC3.1: Interazione con avviso di reindirizzamento	29
UC3.1.1: Visualizzazione annullamento reindirizzamento	29
UC3.2: Visualizzazione esito associazione account	30
UC3.2.1: Visualizzazione errore sincronizzazione fallita	30
UC3.2.2: Visualizzazione errore account già associato	31
UC3.2.3: Visualizzazione rifiuto autorizzazione esterna	31
UC4: Richiesta analisi repository GitHub	32
UC4.0.1: Visualizzazione informativa report aggiornato	32
UC4.0.2: Visualizzazione informativa analisi in corso	33
UC4.1: Selezione aree di interesse	33
UC4.1.1: Visualizzazione errore nessuna area selezionata	34
UC5: Visualizzazione lista repository analizzati	34
UC5.0.1: Visualizzazione informativa lista repository vuota	35

UC5.0.2: Visualizzazione errore caricamento lista	35
UC5.1: Visualizzazione informazioni identificative repository	35
UC6: Visualizzazione report di analisi repository	36
UC6.1: Selezione sezioni del report	36
UC6.1.1: Visualizzazione informativa nessuna sezione selezionata	37
UC6.2: Visualizzazione metadati del report	37
UC6.2.1: Visualizzazione data report	38
UC6.2.2: Visualizzazione commit analizzato	38
UC6.2.3: Visualizzazione richiedente report	38
UC6.3: Visualizzazione sezioni analitiche e remediation	39
UC6.3.1: Visualizzazione lista remediation	40
UC6.3.1.1: Visualizzazione messaggio assenza criticità	40
UC7: Selezione intervallo temporale per confronto report	41
UC7.0.1: Visualizzazione errore intervallo non inserito	41
UC7.0.2: Visualizzazione informativa assenza report nel periodo	42
UC7.0.3: Visualizzazione errore intervallo incoerente	42
UC7.0.4: Visualizzazione errore intervallo troppo ampio	42
UC8: Visualizzazione metriche comparative tra report	43
UC9: Visualizzazione sezione analisi del codice	43
UC9.1: Visualizzazione sezione analisi statica del codice	44
UC9.2: Visualizzazione sezione test di unità	44
UC9.3: Visualizzazione remediation sezione codice	45
UC9.3.1: Visualizzazione informativa assenza remediation codice	45
UC10: Visualizzazione sezione analisi della sicurezza	46
UC10.1: Visualizzazione sezione analisi librerie e dipendenze	46
UC10.2: Visualizzazione sezione analisi sicurezza OWASP	47
UC10.3: Visualizzazione remediation sezione sicurezza	47
UC10.3.1: Visualizzazione informativa assenza remediation sicurezza	47
UC11: Visualizzazione sezione analisi della documentazione	48
UC11.1: Visualizzazione sezione errori di sintassi	49
UC11.2: Visualizzazione completezza della documentazione	49
UC11.3: Visualizzazione remediation sezione documentazione	49
UC11.3.1: Visualizzazione informativa assenza remediation documentazione	50
UC12: Visualizzazione ranking dei repository analizzati	50
UC12.1: Visualizzazione informativa assenza dati per ranking	51
UC13: Disconnessione account GitHub da CodeGuardian	51
UC14: Esportazione report di analisi	52
UC14.1: Selezione formato di esportazione	52
UC14.1.1: Visualizzazione errore formato mancante	53
UC14.2: Conferma esportazione	53
UC15: Modifica password profilo	54
UC15.1: Inserimento password corrente	54
UC15.1.1: Visualizzazione errore password corrente mancante	55
UC15.1.2: Visualizzazione errore password corrente errata	55
UC15.2: Inserimento nuova password	56
UC15.2.1: Visualizzazione errore nuova password mancante	56
UC15.2.2: Visualizzazione errore password non conforme	57
UC15.2.3: Visualizzazione errore password identica alla precedente	57
UC15.3: Conferma modifica password	57

UC15.4: Notifica avvenuta modifica password	58
UC16: Visualizzazione singola remediation di sezione generica	58
UC17: Verifica accessibilità repository GitHub	59
UC17.1: Comunicazione con GitHub	59
UC17.1.1: Errore di comunicazione con GitHub	60
UC17.2: Ricerca del repository	60
UC17.2.1: Accesso a repository privato	61
UC17.2.1.1: Repository inaccessibile	61
UC18: Accettazione di una singola remediation	62
UC19: Rifiuto di una singola remediation	63
UC20: Creazione raccolta report di analisi	64
UC20.0.1: Visualizzazione errore campi obbligatori mancanti	64
UC20.1: Inserimento nome raccolta	65
UC20.1.1: Visualizzazione errore nome non conforme	65
UC20.2: Inserimento URL repository GitHub	66
UC20.2.1: Visualizzazione errore URL non conforme	66
UC20.2.2: Visualizzazione errore repository non accessibile	67
UC20.2.3: Visualizzazione errore URL non inserito	67
UC20.3: Inserimento descrizione raccolta	67
UC21: Avvio analisi	68
UC21.1: Richiesta di clonazione del repository	69
UC21.1.1: Errore durante la clonazione del repository	69
UC21.2: Richiesta di analisi del codice	69
UC21.3: Richiesta di analisi della documentazione	70
UC21.4: Richiesta di analisi della sicurezza	70
UC22: Salvataggio stato analisi nel sistema di persistenza	71
UC22.0.1: Errore durante il salvataggio dello stato dell'analisi	71
UC23: Recupero dei risultati dagli strumenti di analisi	72
UC23.0.1: Gestione risultati incompleti	72
UC23.1: Controllo stato delle attività	73
UC23.2: Acquisizione dei dati analitici	73
UC24: Generazione del report finale	73
UC25: Salvataggio di un report	74
UC25.0.1: Errore durante il salvataggio del report	74
UC26: Invio notifica completamento dell'analisi del repository	75
UC26.0.1: Errore durante l'invio della notifica	75
UC27: Ricezione notifica completamento analisi	76
UC27.0.1: Notifica completamento analisi non ricevuta	76
UC28: Notifica errore critico durante l'analisi	77
UC28.0.1: Notifica errore critico non ricevuta	77
UC29: Gestione del codice OAuth GitHub	78
UC29.0.1: Fallimento della procedura di scambio OAuth	78
UC30: Visualizzazione singola remediation riguardante l'analisi del codice	78
UC31: Visualizzazione singola remediation riguardante l'analisi della sicurezza	79
UC32: Visualizzazione singola remediation riguardante l'analisi della documentazione	79
UC33: Accettazione singola remediation riguardante l'analisi del codice	80
UC33.0.1: Errore nell'applicazione della remediation codice	80
UC34: Rifiuto singola remediation riguardante l'analisi del codice	81
UC35: Accettazione singola remediation riguardante l'analisi della sicurezza	81

UC35.0.1: Errore nell'applicazione della remediation sicurezza	82
UC36: Rifiuto singola remediation riguardante l'analisi della sicurezza	82
UC37: Accettazione singola remediation riguardante l'analisi della documentazione	83
UC37.0.1: Errore nell'applicazione della remediation documentale	83
UC38: Rifiuto singola remediation riguardante l'analisi della documentazione	84
UC39: Richiesta analisi repository GitHub privato autorizzato	84
UC40: Inserimento di un proprio repository privato	85
UC40.0.1: Visualizzazione errore repository già presente	85
UC41: Visualizzazione catalogo repository privati inseriti	86
UC41.0.1: Visualizzazione informativa catalogo vuoto	86
UC42: Rimozione di un proprio repository privato	87
UC42.1: Conferma rimozione repository	87
UC42.1.1: Annullamento rimozione repository	88
UC43: Gestione permessi di accesso al repository privato	88
UC43.0.1: Visualizzazione informativa assenza utenti autorizzati	89
UC44: Aggiunta utente autorizzato	89
UC44.1: Inserimento credenziale utente da autorizzare	90
UC44.1.1: Visualizzazione errore formato identificativo non valido	90
UC44.1.2: Visualizzazione errore utente inesistente	91
UC44.1.3: Visualizzazione errore utente già autorizzato	91
UC44.1.4: Visualizzazione errore campo identificativo vuoto	91
UC45: Rimozione utente autorizzato	92
UC45.1: Conferma revoca autorizzazione	92
UC46: Rimozione di una raccolta di report	93
UC46.1: Conferma rimozione raccolta	93
UC46.1.1: Annullamento rimozione raccolta	94
UC47: Cancellazione profilo CodeGuardian	94
UC47.1: Conferma definitiva cancellazione profilo	95
Requisiti di Sistema	96
Requisiti Funzionali (FR)	96
Requisiti di Qualità (QR)	116
Requisiti di Vincolo (VR)	117

Indice immagini

Figure 1 UC1 - Registrazione	20
Figure 2 UC1.1 - Inserimento username	21
Figure 3 UC1.2 - Inserimento email	22
Figure 4 UC1.3 - Inserimento password	24
Figure 5 UC2 - Autenticazione	25
Figure 6 UC2.1 - Inserimento username	26
Figure 7 UC2.2 - Inserimento password	27
Figure 8 UC3 - Collegamento account GitHub	28
Figure 9 UC3.1 - Collegamento account GitHub	29
Figure 10 UC3.2 - Collegamento account GitHub	30
Figure 11 UC4 - Richiesta analisi repository GitHub	32
Figure 12 UC4.1 - Selezione aree di interesse	33
Figure 13 UC5 - Visualizzazione lista repository	34
Figure 14 UC6 - Visualizzazione report di analisi	36
Figure 15 UC6.1 - Selezione sezioni del report	36
Figure 16 UC6.2 - Visualizzazione metadati del report	37
Figure 17 UC6.3 - Visualizzazione sezioni analitiche e remediation	39
Figure 18 UC6.3.1 - Visualizzazione lista remediation	40
Figure 19 UC7 - Selezione intervallo temporale per confronto report	41
Figure 20 UC9 - Visualizzazione sezione analisi del codice	43
Figure 21 UC9.3 - Visualizzazione remediation sezione codice	45
Figure 22 UC10 - Visualizzazione sezione analisi della sicurezza	46
Figure 23 UC10.3 - Visualizzazione remediation sezione sicurezza	47
Figure 24 UC11 - Visualizzazione sezione analisi della documentazione	48
Figure 25 UC11.3 - Visualizzazione remediation sezione documentazione	49
Figure 26 UC12 - Visualizzazione ranking dei repository analizzati	50
Figure 27 UC14 - Esportazione report di analisi	52
Figure 28 UC14.1 - Selezione formato di esportazione	52
Figure 29 UC15 - Modifica password	54
Figure 30 UC15.1 - Inserimento password corrente	54
Figure 31 UC15.2 - Inserimento nuova password	56
Figure 32 UC16 - Visualizzazione singola remediation di sezione generica	58

Figure 33 UC17 - Verifica accessibilità repository GitHub	59
Figure 34 UC17.1 - Comunicazione con GitHub	59
Figure 35 UC17.2 - Ricerca del repository	60
Figure 36 UC17.2.1 - Accesso a repository privato	61
Figure 37 UC18 - Accettazione di una singola remediation	62
Figure 38 UC19 - Rifiuto singola remediation generica	63
Figure 39 UC20 - Creazione raccolta report di analisi	64
Figure 40 UC20.1 - Inserimento nome raccolta	65
Figure 41 UC20.2 - Inserimento URL repository GitHub	66
Figure 42 UC21 - Avvio analisi	68
Figure 43 UC21.1 - Richiesta di clonazione del repository	69
Figure 44 UC22 - Salvataggio stato analisi nel sistema di persistenza	71
Figure 45 UC23 - Recupero dei risultati dagli strumenti di analisi	72
Figure 46 UC25 - Salvataggio di un report	74
Figure 47 UC26 - Invio notifica completamento dell'analisi del repository	75
Figure 48 UC27 - Ricezione notifica completamento analisi	76
Figure 49 UC28 - Notifica errore critico durante l'analisi	77
Figure 50 UC29 - Gestione del codice OAuth GitHub	78
Figure 51 UC33 - Accettazione singola remediation riguardante l'analisi del codice	80
Figure 52 UC35 - Accettazione singola remediation riguardante l'analisi della sicurezza	81
Figure 53 UC37 - Accettazione singola remediation riguardante l'analisi della documentazione	83
Figure 54 UC39 - Richiesta analisi repository GitHub privato autorizzato	84
Figure 55 UC40 - Inserimento repository privato	85
Figure 56 UC41 - Visualizzazione catalogo repository privati inseriti	86
Figure 57 UC42 - Rimozione di un proprio repository privato	87
Figure 58 UC42.1 - Conferma rimozione repository	87
Figure 59 UC43 - Gestione permessi di accesso al repository privato	88
Figure 60 UC44 - Aggiunta utente autorizzato	89
Figure 61 UC44.1 - Inserimento credenziale utente da autorizzare	90
Figure 62 UC45 - Rimozione utente autorizzato	92
Figure 63 UC46 - Rimozione di una raccolta di report	93
Figure 64 UC46 - Conferma rimozione raccolta	93
Figure 65 UC47 - Cancellazione profilo CodeGuardian	94

Indice tabelle

Table 1 Definizione e gerarchia degli Attori	19
--	----

Introduzione

Contesto del Progetto

Il presente documento descrive l'Analisi dei Requisiti^G relativo al progetto Code Guardian^G, commissionato dall'azienda Var Group^G e realizzato dal gruppo di studenti Skarab Group^G nell'ambito del corso di Ingegneria del Software presso l'Università degli Studi di Padova.

Il progetto ha come obiettivo la realizzazione di un sistema per l'automazione dei processi di audit^G e remediation^G delle vulnerabilità del software. L'architettura si basa sul paradigma degli agenti^G software intelligenti, operanti su repository di codice sorgente. La conformità del sistema è vincolata ai requisiti definiti nel Capitolato C2.

La piattaforma supporta attività di analisi statica del codice sorgente e di individuazione delle principali criticità di sicurezza, fornendo suggerimenti di correzione attraverso meccanismi automatizzati basati su modelli di linguaggio di grandi dimensioni (LLM^G).

Finalità del Documento

Il documento di **Analisi dei Requisiti** formalizza le specifiche del prodotto software, descrivendo in modo dettagliato le funzionalità, i vincoli e gli standard di qualità che il sistema Code Guardian deve soddisfare per rispondere alle esigenze del committente.

Il documento costituisce il riferimento primario per il gruppo di lavoro (Skarab Group^G) e per gli stakeholder^G, perseguendo i seguenti obiettivi:

- modellare le interazioni tra gli utenti e il sistema attraverso la definizione formale dei casi d'uso^G
- individuare e dettagliare i requisiti di sistema, distinguendo tra requisiti funzionali^G, di qualità^G e di vincolo^G
- classificare i requisiti in base alla priorità negoziale e strategica (obbligatori^G, opzionali^G, desiderabili^G), fornendo una guida per la pianificazione dello sviluppo;
- definire i criteri di accettazione del prodotto, stabilendo una base contrattuale oggettiva per le attività di verifica e validazione finale rispetto a quanto concordato con il proponente.

Scopo del Prodotto

Il prodotto che Skarab Group^G sviluppa è un sistema software^G multiagente^G per l'analisi di repository^G GitHub^G. Il sistema è progettato per essere modulare, scalabile e per operare in ambienti isolati, garantendo la sicurezza del sistema ospite durante l'esecuzione di codice non fidato.

L'obiettivo corrente è il rilascio di un MVP^G che dimostri l'efficacia dell'approccio a micro-agenti per la risoluzione automatica del debito tecnico.

Funzioni del Prodotto

Le funzionalità del sistema sono suddivise in quattro macro-aree operative, accessibili tramite un'interfaccia web (GUI^G):

- **Audit del Codice:** Esecuzione di analisi statica^G per l'identificazione di errori a tempo di compilazione e verifica della presenza/copertura dei test unitari.
- **Audit della Sicurezza:** Analisi delle dipendenze per l'individuazione di librerie obsolete o affette da vulnerabilità note e verifica della conformità agli standard OWASP^G.
- **Audit della Documentazione:** Controllo della completezza e della coerenza semantica della documentazione tecnica rispetto al codice sorgente, effettuato tramite LLM^G.
- **Remediation:** Generazione automatica di suggerimenti correttivi (snippet di codice o testo) per le criticità rilevate.

Caratteristiche degli Utenti

Il sistema è progettato per soddisfare le esigenze di diverse tipologie di utenti, con differenti livelli di competenza tecnica:

- **Sviluppatori Software:** Utenti tecnici che utilizzano il sistema per ottenere feedback immediato (“early feedback”) sul proprio codice e applicare le correzioni suggerite.
- **Manager IT:** Utenti con focus gestionale che utilizzano la dashboard per monitorare la qualità complessiva e la postura di sicurezza dei progetti aziendali.
- **Consulenti Informatici:** Utenti esterni che utilizzano il tool per eseguire audit di terze parti su repository legacy o in fase di acquisizione.

Limitazioni

Lo sviluppo e l'operatività del sistema sono soggetti ai seguenti vincoli e limitazioni:

- **Disponibilità dei Servizi Terzi:** La piena operatività dipende dalla raggiungibilità delle API^G di GitHub e dei provider LLM.
- **Vincoli di Esecuzione (Quota):** Le analisi semantiche sono soggette ai limiti di throughput e al modello di costo (token-based) dei fornitori LLM.
- **Trattamento Dati e Riservatezza:** Il sistema deve operare in modalità “stateless” per il codice sorgente; la persistenza dei dati analizzati è limitata alla durata della sessione di analisi, in conformità alle normative vigenti sul trattamento dei dati.
- **Perimetro Tecnologico (MVP):** Il supporto è circoscritto ai linguaggi di programmazione e ai framework definiti nel Piano di Progetto; l'estensibilità ad altri ecosistemi è prevista come requisito opzionale o futuro.

Glossario

Al fine di prevenire ambiguità interpretative, è stato redatto un glossario che definisce in modo univoco la terminologia tecnica, gli acronimi e i concetti di dominio utilizzati all'interno della documentazione.

Nel testo, **ogni termine evidenziato tramite una G come apice**, rimanda alla voce corrispondente del Glossario pubblicato sul sito ufficiale del gruppo, consentendo al lettore di accedere direttamente alla definizione associata.

La versione più recente del Glossario è disponibile al seguente link: [Link al Glossario](#).

Riferimenti

Riferimenti Normativi

I seguenti documenti hanno valore vincolante per la redazione dell'Analisi dei Requisiti:

- **Standard IEEE 830-1998** IEEE Recommended Practice for Software Requirements Specifications
<https://ieeexplore.ieee.org/document/720574>
(ultimo accesso: **12/02/2026**)
- **Standard IEEE 29148-2018** ISO/IEC/IEEE International Standard – Systems and software engineering – Life cycle processes – Requirements engineering
<https://ieeexplore.ieee.org/document/8559686>
(ultimo accesso: **12/02/2026**)
- **Capitolato C2:** Piattaforma ad agenti per l'audit e la remediation dei repository software.
<https://www.math.unipd.it/~tullio/IS-1/2025/Progetto/C2.pdf>
(ultimo accesso: **12/02/2026**)

- **Norme di Progetto:** regole, convenzioni e standard di qualità adottati dal gruppo.
<https://skarabgroup.github.io/DocumentazioneProgetto/RTB/NdP.pdf>
(versione: **v1.0.0**)

Riferimenti Informativi

- **Dispense del Corso di Ingegneria del Software sull'Analisi dei Requisiti**
<https://www.math.unipd.it/~tullio/IS-1/2025/Dispense/T05.pdf>
(ultimo accesso: **12/02/2026**)
- **Dispense del Corso di Ingegneria del Software sui Casi d'Uso**
<https://www.math.unipd.it/~rcardin/swea/2022/Diagrammi%20Use%20Case.pdf>
(ultimo accesso: **12/02/2026**)

Casi d'Uso

Introduzione

In questa sezione sono descritti i casi d'uso principali del sistema, che illustrano le interazioni funzionali tra gli utenti (umani e software) e l'applicazione.

La specifica dei casi d'uso adotta il formato e le convenzioni di modellazione definite alla sezione 2.1.6.3.1 del documento [Norme di Progetto](#). Si rimanda a tale documento per la descrizione dettagliata della struttura dei campi (precondizioni, postcondizioni, scenari) e della sintassi UML^G utilizzata.

Attori

Gli attori^G rappresentano le entità che interagiscono con il sistema Code Guardian^G. Essi sono classificati in base al ruolo svolto nell'interazione:

- **Attori Primari:** Entità che attivano una funzionalità del sistema per raggiungere uno scopo (User Goal). Possono essere utenti umani o processi di sistema autonomi.
- **Attori Secondari:** Sistemi, servizi o entità esterne con cui il sistema interagisce per completare un caso d'uso, ma che non ne scatenano l'esecuzione.

Di seguito vengono definiti i ruoli identificati nell'analisi.

Attore	Descrizione
Attori Primari (Utenti Umani)	
Utente non Registrato	Soggetto sprovvisto di un'identità digitale all'interno della piattaforma. Tale attore è autorizzato esclusivamente alla fruizione dei contenuti pubblici e all'esecuzione della procedura di creazione di un nuovo profilo utente.
Utente non Autenticato	Utente generico che accede alle funzionalità pubbliche della piattaforma (es. Home Page, Login, Registrazione) senza possedere o aver attivato una sessione valida.
Utente Autorizzato	Utente che ha completato con successo la procedura di autenticazione. Può configurare nuove analisi, consultare lo storico dei report e gestire il proprio profilo.
Utente Avanzato	Specializzazione dell'Utente Autorizzato che ha collegato il proprio account al provider GitHub ^G , abilitando l'accesso ai repository privati e funzionalità di integrazione avanzata.
Attori Primari (Sistemi Interni)	
OrCHEstratore	Componente software autonomo che agisce come attore sistemico. È responsabile dell'avvio e del coordinamento dei flussi di analisi automatizzati, della gestione degli ambienti di esecuzione e della centralizzazione delle comunicazioni tra gli agenti e il sistema di persistenza, senza richiedere intervento umano diretto durante l'elaborazione.
Attori Secondari (Sistemi Esterni)	
GitHub	Piattaforma di hosting esterna. Interagisce con il sistema per fornire l'accesso al codice sorgente (via API o clone) e ai metadati dei repository.
Servizi AWS	Infrastruttura cloud esterna di Amazon Web Service ^G utilizzata dal sistema come ambiente di calcolo e storage per l'esecuzione delle analisi intensive.
Strumenti di Analisi	Insieme degli strumenti terzi invocati dal sistema per l'esecuzione verticale delle scansioni di sicurezza e qualità del codice.

Table 1: Definizione e gerarchia degli Attori

Lista

UC1: Registrazione a CodeGuardian

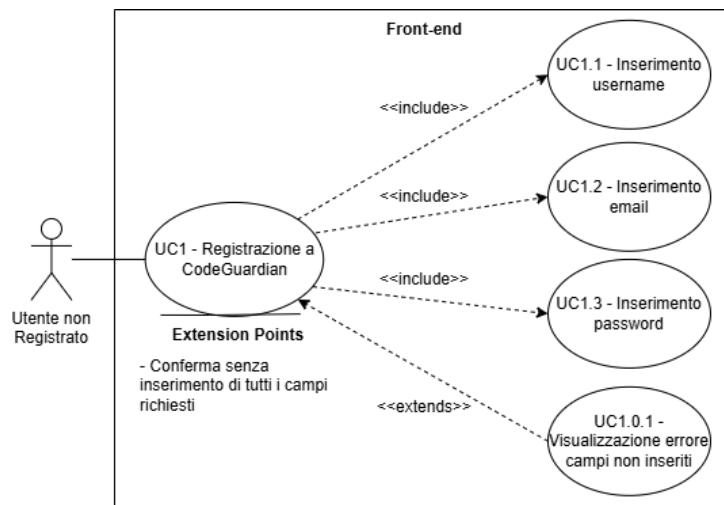


Figure 1: UC1 - Registrazione

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente non possiede le credenziali di un account CodeGuardian
 - L'utente ha visualizzato la sezione dedicata alla creazione di un nuovo profilo CodeGuardian
- **Post-condizioni:**
 - L'utente visualizza la conferma dell'avvenuta creazione dell'account CodeGuardian
 - L'utente dispone di credenziali valide di un account CodeGuardian per l'accesso alla piattaforma
- **Scenario principale:**
 - L'utente inserisce un username identificativo [UC1.1]
 - L'utente inserisce una email di contatto [UC1.2]
 - L'utente inserisce una password sicura [UC1.3]
 - L'utente impartisce il comando di conferma finale per completare la procedura
- **Inclusioni:**
 - [UC1.1]
 - [UC1.2]
 - [UC1.3]
- **Estensioni:**
 - [UC1.0.1]
- **Trigger:** L'utente seleziona la funzione di registrazione utente

UC1.0.1: Visualizzazione errore campi non inseriti

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di registrazione [UC1]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa il mancato inserimento dei dati obbligatori
 - L'utente ha la possibilità di completare i campi mancanti nel modulo
- **Scenario principale:**

- L'utente visualizza un avviso che segnala l'incompletezza delle informazioni fornite
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente impartisce il comando di conferma senza aver inserito tutti i dati richiesti

UC1.1: Inserimento username

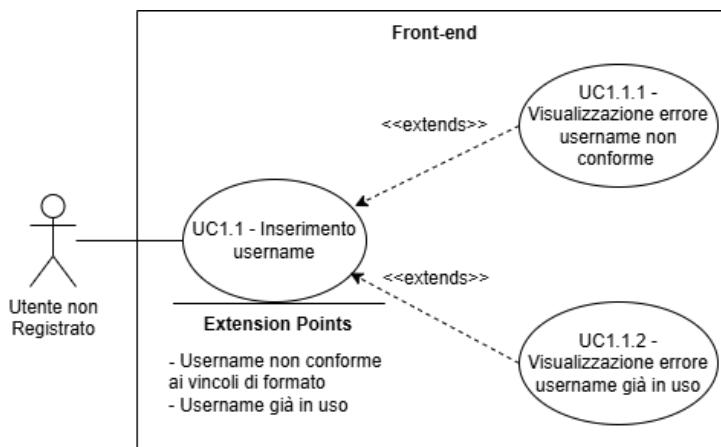


Figure 2: UC1.1 - Inserimento username

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di registrazione [UC1]
- **Post-condizioni:**
 - Il campo relativo all'username risulta popolato con un valore accettato
- **Scenario principale:**
 - L'utente fornisce l'identificativo scelto per la propria registrazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC1.1.1]
 - [UC1.1.2]
- **Trigger:** L'utente seleziona il campo di input dello username

UC1.1.1: Visualizzazione errore username non conforme

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente ha popolato il campo username [UC1.1]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa la non conformità dell'username inserito
 - L'utente ha la possibilità di fornire un nuovo valore per l'identificativo
- **Scenario principale:**

- L'utente visualizza un messaggio di errore in corrispondenza del campo username che specifica la non conformità del formato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di procedere con l'inserimento di un valore non conforme per l'username

UC1.1.2: Visualizzazione errore username già in uso

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente ha inserito lo username nella schermata di registrazione [UC1.1]
 - Lo username digitato risulta già associato a un account CodeGuardian esistente
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa la non disponibilità dell'username inserito
 - L'utente ha la possibilità di fornire un nuovo valore per l'identificativo
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala l'indisponibilità del nome utente scelto
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente inserisce un username che non risulta univoco

UC1.2: Inserimento email

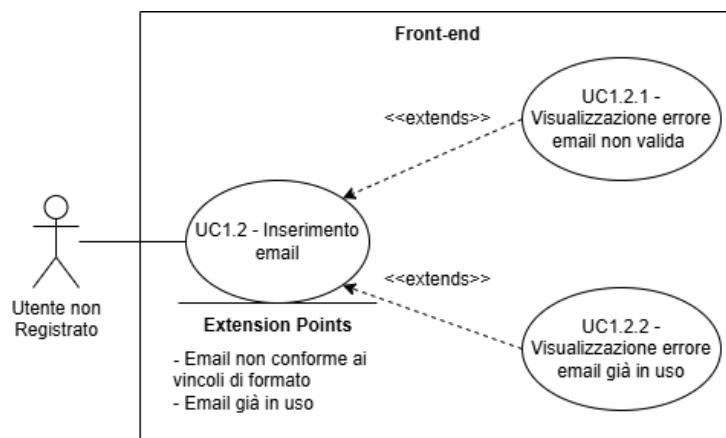


Figure 3: UC1.2 - Inserimento email

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di registrazione [UC1]
- **Post-condizioni:**
 - Il campo relativo all'email risulta popolato con un valore accettato
- **Scenario principale:**

- L'utente inserisce l'indirizzo email di contatto per il proprio profilo
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC1.2.1]
 - [UC1.2.2]
- **Trigger:** L'utente seleziona il campo di input dell'email

UC1.2.1: Visualizzazione errore email non valida

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente ha inserito un valore nel campo email [UC1.2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa la non validità dell'email inserita
 - L'utente ha la possibilità di fornire un nuovo valore per l'email
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore in corrispondenza del campo email che specifica la non conformità del formato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di procedere con l'inserimento di un valore non conforme per l'email

UC1.2.2: Visualizzazione errore email già in uso

- **Attore principale:** Utente non Registrato
- **Pre-condizioni:**
 - L'utente ha inserito un indirizzo email nel modulo di registrazione [UC1.2]
 - L'email inserita risulta già associata a un account esistente
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa l'indisponibilità dell'email inserita
 - L'utente ha la possibilità di fornire un nuovo valore per l'email
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala l'indisponibilità dell'email scelta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente inserisce un'email già presente nel sistema

UC1.3: Inserimento password

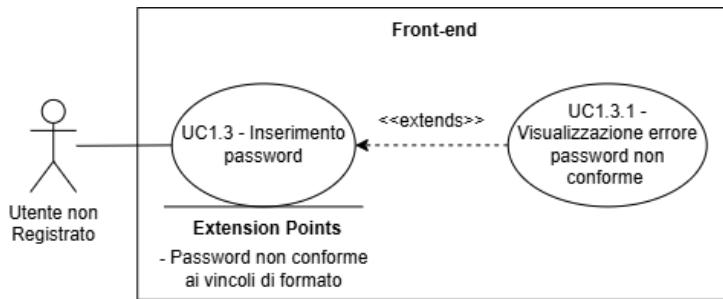


Figure 4: UC1.3 - Inserimento password

- **Attore principale:** Utente non Registrato
 - **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di registrazione [UC1]
 - **Post-condizioni:**
 - Il campo relativo alla password risulta popolato con un valore accettato
 - **Scenario principale:**
 - L'utente inserisce la chiave d'accesso per il proprio account
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - [UC1.3.1]
 - **Trigger:** L'utente seleziona il campo di input della password
- UC1.3.1: Visualizzazione errore password non conforme**
- **Attore principale:** Utente non Registrato
 - **Pre-condizioni:**
 - L'utente ha inserito una password nel modulo di registrazione [UC1.3]
 - **Post-condizioni:**
 - L'utente visualizza un messaggio circa la non conformità della password inserita
 - L'utente ha la possibilità di fornire un nuovo valore per la password
 - **Scenario principale:**
 - L'utente visualizza un messaggio di errore che specifica i requisiti di sicurezza non soddisfatti
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - Nessuna
 - **Trigger:** L'utente tenta di procedere con l'inserimento di una password non conforme ai criteri di sicurezza

UC2: Autenticazione a CodeGuardian

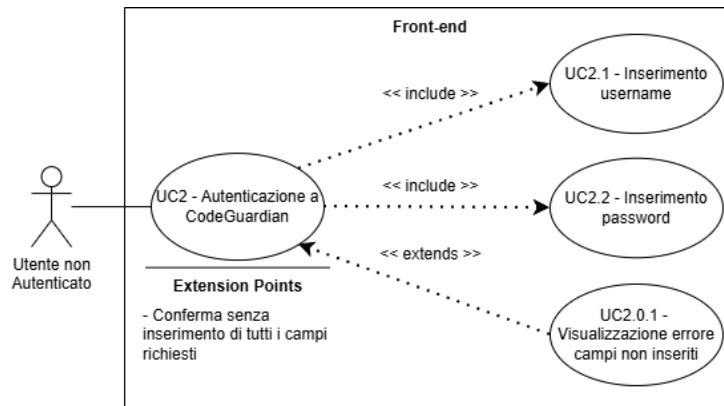


Figure 5: UC2 - Autenticazione

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente dispone di credenziali valide registrate nel sistema [UC1]
 - L'utente visualizza la sezione di accesso
- **Post-condizioni:**
 - L'utente visualizza la conferma di avvenuta autenticazione
 - L'utente ha accesso alle funzionalità riservate della piattaforma
- **Scenario principale:**
 - L'utente fornisce lo username identificativo [UC2.1]
 - L'utente fornisce la chiave d'accesso associata [UC2.2]
 - L'utente impartisce il comando di conferma per finalizzare l'accesso
- **Inclusioni:**
 - [UC2.1]
 - [UC2.2]
- **Estensioni:**
 - [UC2.0.1]
- **Trigger:** L'utente seleziona la funzione di login

UC2.0.1: Visualizzazione errore campi non inseriti

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di autenticazione [UC2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa il mancato inserimento dei dati obbligatori
 - L'utente ha la possibilità di completare i campi mancanti
- **Scenario principale:**
 - L'utente visualizza un avviso che segnala l'incompletezza delle informazioni fornite per l'accesso
- **Inclusioni:**
 - Nessuna
- **Estensioni:**

- ▶ Nessuna
- **Trigger:** L'utente impedisce il comando di conferma senza aver inserito tutte le credenziali

UC2.1: Inserimento username

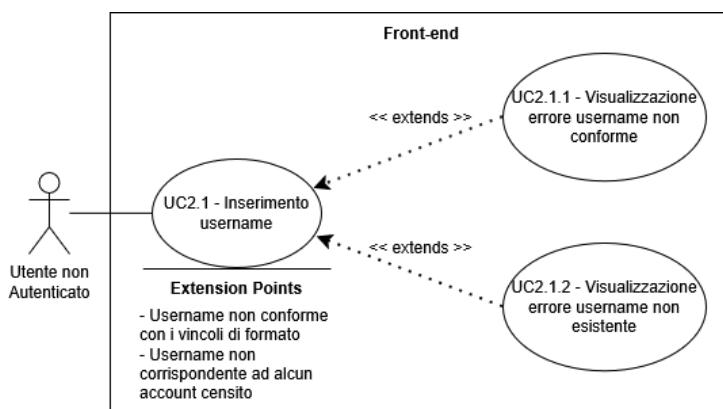


Figure 6: UC2.1 - Inserimento username

- **Attore principale:** Utente non Autenticato
 - **Pre-condizioni:**
 - ▶ L'utente sta visualizzando il modulo di autenticazione [UC2]
 - **Post-condizioni:**
 - ▶ Il campo relativo all'username risulta popolato con un valore accettato
 - **Scenario principale:**
 - ▶ L'utente digita lo username nel campo dedicato
 - **Inclusioni:**
 - ▶ Nessuna
 - **Estensioni:**
 - ▶ [\[UC2.1.1\]](#)
 - ▶ [\[UC2.1.2\]](#)
 - **Trigger:** L'utente seleziona il campo di input dello username
- UC2.1.1: Visualizzazione errore username non conforme**
- **Attore principale:** Utente non Autenticato
 - **Pre-condizioni:**
 - ▶ L'utente ha inserito un valore nel campo username [UC2.1]
 - **Post-condizioni:**
 - ▶ L'utente visualizza un messaggio circa la non conformità dell'username inserito
 - ▶ L'utente ha la possibilità di fornire un nuovo valore per l'identificativo
 - **Scenario principale:**
 - ▶ L'utente visualizza un messaggio di errore in corrispondenza del campo username che specifica la non conformità del formato
 - **Inclusioni:**
 - ▶ Nessuna
 - **Estensioni:**
 - ▶ Nessuna

- **Trigger:** L'utente tenta di procedere con un valore non conforme ai vincoli di formato

UC2.1.2: Visualizzazione errore username non esistente

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente ha inserito un username non presente nel sistema [UC2.1]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa l'invalidità delle credenziali fornite
 - L'utente ha la possibilità di fornire un nuovo valore per l'identificativo
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala l'inesistenza dell'identificativo inserito
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di autenticarsi con un username non censito

UC2.2: Inserimento password

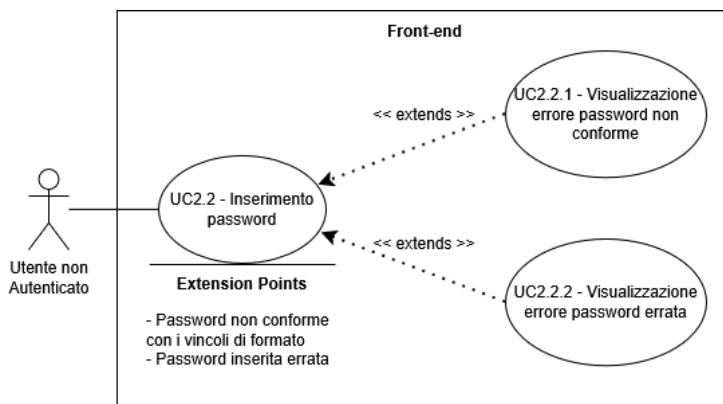


Figure 7: UC2.2 - Inserimento password

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di autenticazione [UC2]
 - L'utente ha inserito l'identificativo con il quale si è registrato [UC2.1]
- **Post-condizioni:**
 - Il campo relativo alla password risulta popolato con un valore accettato
- **Scenario principale:**
 - L'utente digita la chiave d'accesso nel campo dedicato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC2.2.1]
 - [UC2.2.2]
- **Trigger:** L'utente seleziona il campo di input della password

UC2.2.1: Visualizzazione errore password non conforme

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente ha inserito una password nel campo dedicato [UC2.2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa la non conformità della password
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che specifica il mancato rispetto dei criteri di sistema
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di procedere con una password formalmente non valida

UC2.2.2: Visualizzazione errore password errata

- **Attore principale:** Utente non Autenticato
- **Pre-condizioni:**
 - L'utente ha inserito una password non corrispondente a quella registrata [UC2.2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa l'errata combinazione delle credenziali
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala l'invalidità della chiave d'accesso
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di procedere con una password errata

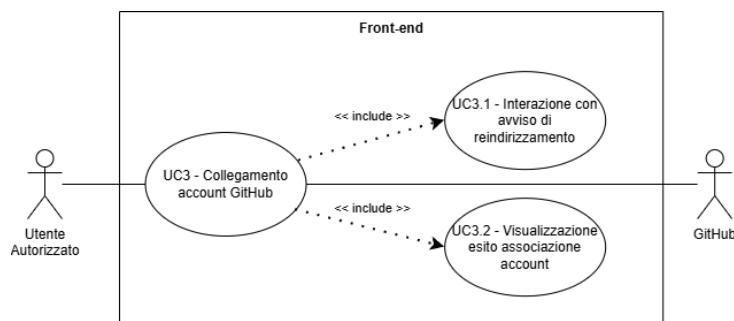
UC3: Collegamento account GitHub

Figure 8: UC3 - Collegamento account GitHub

- **Attore principale:** Utente Autorizzato
- **Attore secondario:** GitHub
- **Pre-condizioni:**
 - L'utente dispone di una sessione attiva nel sistema [UC2]

- L'utente non ha associato un profilo GitHub al proprio account
- L'utente visualizza la sezione relativa alle integrazioni esterne
- **Post-condizioni:**
 - L'utente visualizza la conferma dell'avvenuta associazione tra i profili
- **Scenario principale:**
 - L'utente interagisce con la notifica di reindirizzamento esterno [UC3.1]
 - L'utente effettua le operazioni di autorizzazione sulla piattaforma GitHub
 - L'utente visualizza l'esito della procedura di sincronizzazione [UC3.2]
- **Inclusioni:**
 - [UC3.1]
 - [UC3.2]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede l'integrazione del proprio profilo con GitHub

UC3.1: Interazione con avviso di reindirizzamento

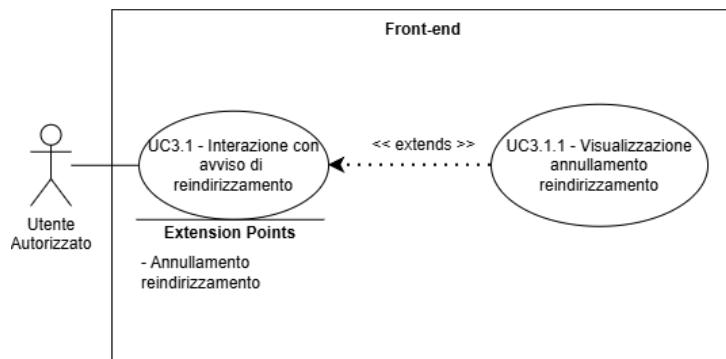


Figure 9: UC3.1 - Collegamento account GitHub

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha richiesto il collegamento del proprio profilo GitHub [UC3]
- **Post-condizioni:**
 - L'utente viene trasferito alla piattaforma esterna GitHub per le operazioni di autorizzazione
- **Scenario principale:**
 - L'utente visualizza l'avviso di trasferimento temporaneo su un dominio esterno
 - L'utente impartisce il comando di conferma per procedere con il reindirizzamento
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC3.1.1]
- **Trigger:** L'utente seleziona la funzione di integrazione con GitHub

UC3.1.1: Visualizzazione annullamento reindirizzamento

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**

- L'utente visualizza l'avviso di trasferimento a piattaforma esterna [UC3.1]
- **Post-condizioni:**
 - L'utente visualizza nuovamente la sezione dedicata alle integrazioni di CodeGuardian
 - La procedura di collegamento risulta annullata
- **Scenario principale:**
 - L'utente annulla l'operazione di collegamento
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente sceglie di non procedere verso la piattaforma esterna

UC3.2: Visualizzazione esito associazione account

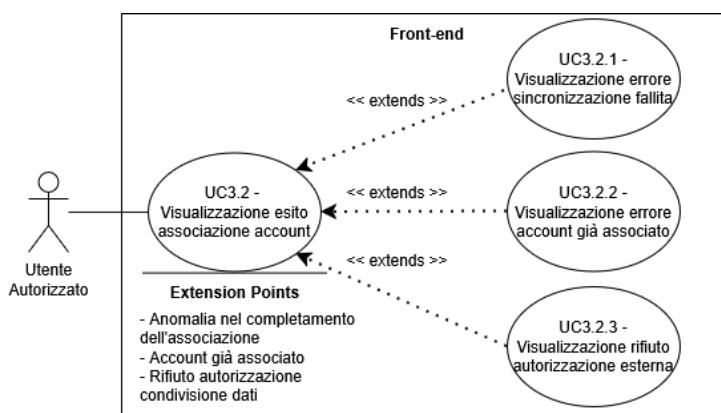


Figure 10: UC3.2 - Collegamento account GitHub

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha completato l'interazione con la piattaforma esterna GitHub [UC3.1]
 - L'utente è tornato alla piattaforma CodeGuardian
- **Post-condizioni:**
 - L'utente visualizza l'esito della procedura di associazione
- **Scenario principale:**
 - L'utente visualizza la conferma dell'avvenuta sincronizzazione tra l'account CodeGuardian e il profilo GitHub
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC3.2.1]
 - [UC3.2.2]
 - [UC3.2.3]
- **Trigger:** L'utente riaccede a CodeGuardian dopo l'interazione con GitHub

UC3.2.1: Visualizzazione errore sincronizzazione fallita

- **Attore principale:** Utente Autorizzato

- **Pre-condizioni:**
 - L'utente è tornato su CodeGuardian a seguito della procedura esterna [UC3.2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio di errore circa il fallimento della sincronizzazione
 - L'utente ha la possibilità di ripetere la procedura
- **Scenario principale:**
 - L'utente visualizza un avviso relativo all'impossibilità tecnica di completare l'operazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Il sistema rileva un'anomalia nel completamento della procedura di associazione

UC3.2.2: Visualizzazione errore account già associato

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente è tornato su CodeGuardian a seguito della procedura esterna [UC3.2]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa l'indisponibilità dell'account GitHub scelto
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che specifica l'impossibilità di procedere poiché il profilo GitHub risulta già collegato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di associare un account GitHub già in uso presso un altro profilo

UC3.2.3: Visualizzazione rifiuto autorizzazione esterna

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente è tornato su CodeGuardian a seguito della procedura esterna [UC3.2]
- **Post-condizioni:**
 - L'utente visualizza un avviso circa il mancato rilascio delle autorizzazioni
- **Scenario principale:**
 - L'utente visualizza un avviso che informa del mancato collegamento a causa del rifiuto espresso su GitHub
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente nega il consenso alla condivisione dei dati sulla piattaforma esterna

UC4: Richiesta analisi repository GitHub

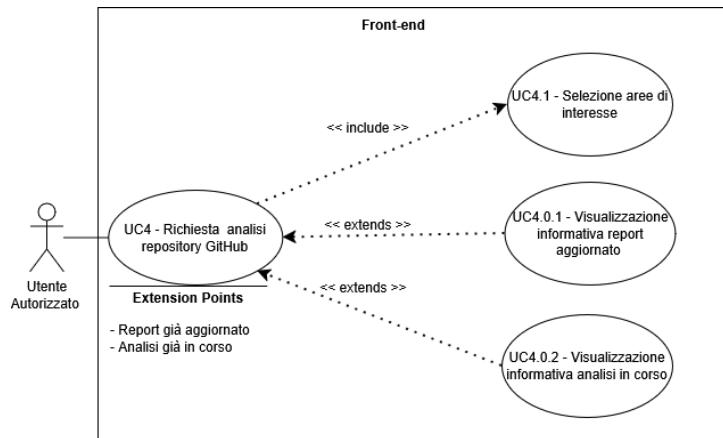


Figure 11: UC4 - Richiesta analisi repository GitHub

- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - L'utente accede alla collezione di report di un repository [UC20]
 - L'utente visualizza la sezione di configurazione dell'analisi
 - **Post-condizioni:**
 - L'utente visualizza la conferma di presa in carico della richiesta di analisi
 - **Scenario principale:**
 - L'utente seleziona le aree di interesse per l'audit [UC4.1]
 - L'utente impartisce il comando di conferma per l'invio della richiesta
 - **Inclusioni:**
 - [UC4.1]
 - **Estensioni:**
 - [UC4.0.1]
 - [UC4.0.2]
 - **Trigger:** L'utente seleziona la funzione di nuova analisi del repository
- UC4.0.1: Visualizzazione informativa report aggiornato**
- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - L'utente ha inviato una richiesta di analisi [UC4]
 - **Post-condizioni:**
 - L'utente visualizza l'informativa che indica la presenza di un report già aggiornato
 - **Scenario principale:**
 - L'utente visualizza un messaggio che segnala l'inutilità di una nuova analisi per coerenza dei dati
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - Nessuna

- **Trigger:** L'utente tenta di avviare un'analisi per un repository il cui stato coincide con l'ultimo report generato

UC4.0.2: Visualizzazione informativa analisi in corso

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha inviato una richiesta di analisi [UC4]
- **Post-condizioni:**
 - L'utente viene accodato ad una lista di attesa del report per il medesimo repository
- **Scenario principale:**
 - L'utente visualizza un messaggio di avvenuta presa a carico della analisi
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di avviare un'analisi mentre un'altra elaborazione è già attiva sul medesimo repository

UC4.1: Selezione aree di interesse

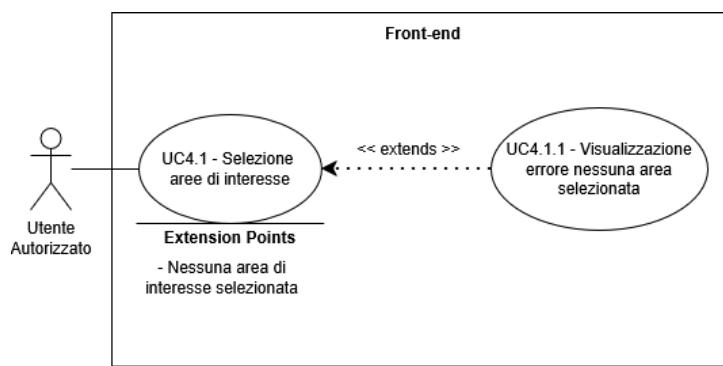


Figure 12: UC4.1 - Selezione aree di interesse

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta visualizzando il modulo di richiesta analisi [UC4]
- **Post-condizioni:**
 - Le preferenze sulle aree del repository da analizzare risultano impostate
- **Scenario principale:**
 - L'utente seleziona le informazioni del repository di suo interesse (test, sicurezza o documentazione)
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC4.1.1]
- **Trigger:** L'utente interagisce con le opzioni di configurazione dell'audit

UC4.1.1: Visualizzazione errore nessuna area selezionata

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta interagendo con la selezione delle aree [UC4.1]
- **Post-condizioni:**
 - L'utente visualizza un avviso circa la necessità di selezionare almeno un'area
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala la mancata scelta delle aree di interesse
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di confermare senza aver selezionato alcuna area di analisi

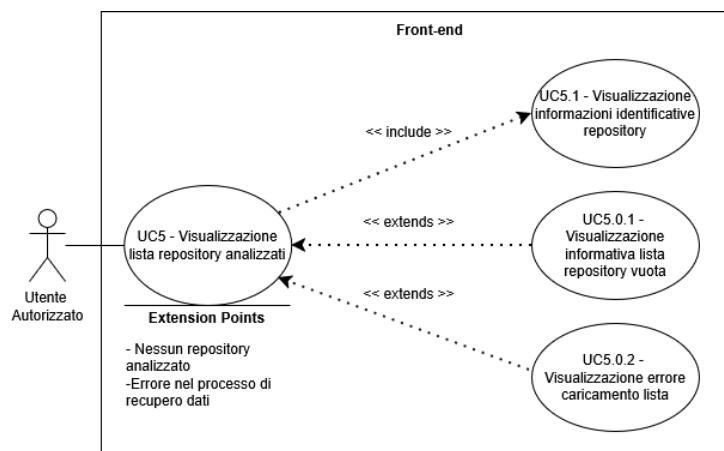
UC5: Visualizzazione lista repository analizzati

Figure 13: UC5 - Visualizzazione lista repository

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente dispone di una sessione attiva nel sistema [UC2]
 - L'utente accede alla sezione dedicata ai repository analizzati [UC20]
- **Post-condizioni:**
 - L'utente visualizza l'elenco dei repository per i quali è stato generato almeno un report
- **Scenario principale:**
 - L'utente visualizza la lista dei repository sottoposti a scansione
 - Ogni elemento della lista espone i dati identificativi del repository [UC5.1]
- **Inclusioni:**
 - [UC5.1]
- **Estensioni:**
 - [UC5.0.1]
 - [UC5.0.2]
- **Trigger:** L'utente seleziona la funzione di visualizzazione storico analisi

UC5.0.1: Visualizzazione informativa lista repository vuota

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha richiesto la visualizzazione della lista dei repository analizzati [UC5]
- **Post-condizioni:**
 - L'utente visualizza un messaggio informativo circa l'assenza di repository nella lista
- **Scenario principale:**
 - L'utente viene avvisato che non è stata ancora richiesta l'analisi di alcun repository
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accede alla sezione in assenza di repository censiti a sistema

UC5.0.2: Visualizzazione errore caricamento lista

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La visualizzazione della lista dei repository analizzati è stata richiesta [UC5]
- **Post-condizioni:**
 - Un avviso circa l'impossibilità tecnica di recuperare i dati dei repository risulta visibile a video
- **Scenario principale:**
 - L'utente visualizza una segnalazione di errore a seguito di un timeout o di un'anomalia di connessione con la persistenza
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Rilevamento di un'anomalia tecnica durante la fase di recupero dei dati

UC5.1: Visualizzazione informazioni identificative repository

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta visualizzando la lista dei repository analizzati [UC5]
- **Post-condizioni:**
 - L'utente dispone dei dati necessari per distinguere i diversi repository in elenco
- **Scenario principale:**
 - L'utente visualizza nome del repository, URL di riferimento e data dell'ultima analisi eseguita per ogni repository presente nella lista
- **Trigger:** L'utente accede alla schermata di riepilogo dei repository

UC6: Visualizzazione report di analisi repository

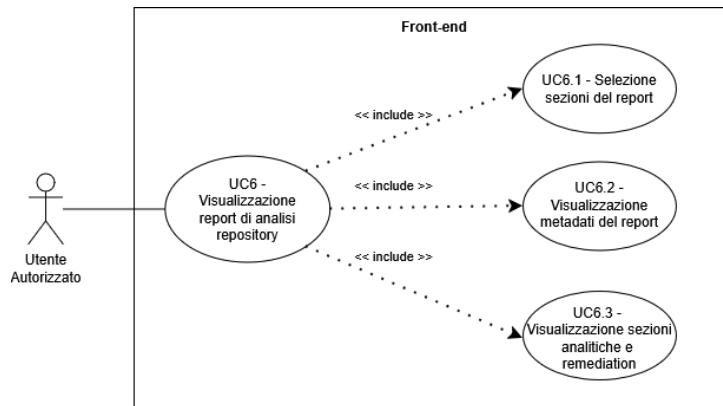


Figure 14: UC6 - Visualizzazione report di analisi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente seleziona un repository dalla lista dei repository analizzati [UC5]
- **Post-condizioni:**
 - L'utente visualizza il contenuto dettagliato del report di analisi selezionato
- **Scenario principale:**
 - L'utente seleziona le sezioni specifiche dell'audit da consultare [UC6.1]
 - L'utente visualizza i metadati generali del report [UC6.2]
 - L'utente visualizza le informazioni analitiche delle sezioni scelte [UC6.3]
- **Inclusioni:**
 - [UC6.1]
 - [UC6.2]
 - [UC6.3]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la consultazione dei dettagli di un repository analizzato

UC6.1: Selezione sezioni del report

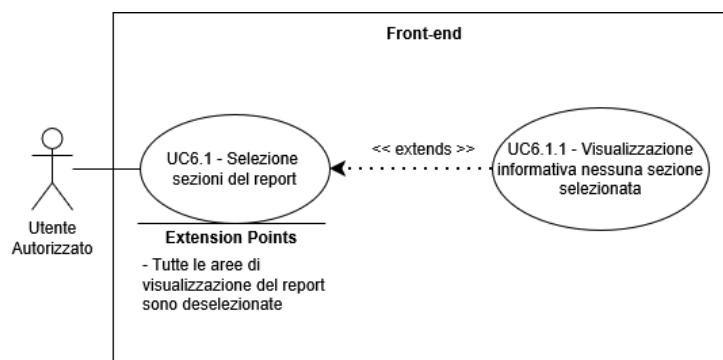


Figure 15: UC6.1 - Selezione sezioni del report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente si trova nella schermata di dettaglio del report [UC6]

- **Post-condizioni:**
 - Le preferenze di visualizzazione per il report corrente risultano impostate
- **Scenario principale:**
 - L'utente seleziona o deselectiona le aree dell'analisi (Codice, Sicurezza, Documentazione) da mostrare a video
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC6.1.1]
- **Trigger:** L'utente interagisce con i filtri di visualizzazione del report

UC6.1.1: Visualizzazione informativa nessuna sezione selezionata

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente interagisce con la selezione delle sezioni [UC6.1]
- **Post-condizioni:**
 - L'utente visualizza un avviso circa la necessità di selezionare almeno un'area per popolare il report
- **Scenario principale:**
 - L'utente visualizza un messaggio che inibisce il rendering dei dati analitici fino alla selezione di un'area
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente deselectiona tutte le aree di visualizzazione del report

UC6.2: Visualizzazione metadati del report

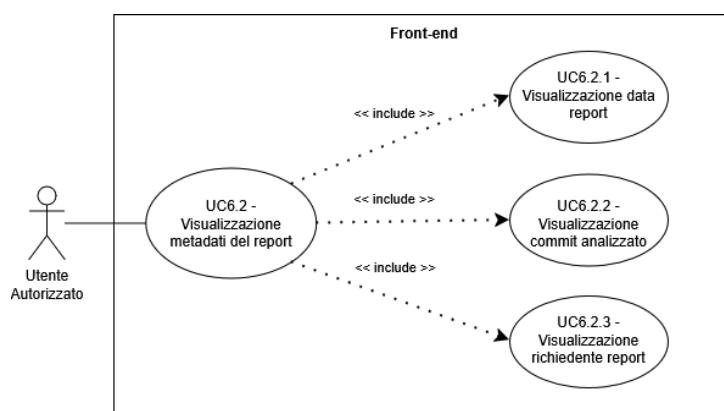


Figure 16: UC6.2 - Visualizzazione metadati del report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio di un report di analisi [UC6]
- **Post-condizioni:**

- L'utente visualizza le informazioni di contesto dell'analisi
- **Scenario principale:**
 - L'utente visualizza la data di esecuzione del report [UC6.2.1]
 - L'utente visualizza l'identificativo del commit analizzato [UC6.2.2]
 - L'utente visualizza il profilo del richiedente dell'analisi [UC6.2.3]
- **Inclusioni:**
 - [UC6.2.1]
 - [UC6.2.2]
 - [UC6.2.3]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accede alla testata del report di analisi

UC6.2.1: Visualizzazione data report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza l'area metadati del report [UC6.2]
- **Post-condizioni:**
 - L'utente ha preso visione della data e dell'ora di generazione del report
- **Scenario principale:**
 - L'utente visualizza il timestamp relativo al completamento dell'analisi
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente consulta le informazioni cronologiche del report

UC6.2.2: Visualizzazione commit analizzato

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza l'area metadati del report [UC6.2]
- **Post-condizioni:**
 - L'utente identifica univocamente la versione del codice sorgente analizzata
- **Scenario principale:**
 - L'utente visualizza l'hash o il riferimento abbreviato del commit GitHub analizzato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente consulta il riferimento alla versione del repository

UC6.2.3: Visualizzazione richiedente report

- **Attore principale:** Utente Autorizzato
-

- **Pre-condizioni:**
 - L'utente visualizza l'area metadati del report [UC6.2]
- **Post-condizioni:**
 - L'utente visualizza l'identità del profilo che ha originato la richiesta di analisi
- **Scenario principale:**
 - L'utente visualizza lo username dell'Utente Autorizzato che ha avviato il processo di audit
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente consulta la paternità della richiesta di analisi

UC6.3: Visualizzazione sezioni analitiche e remediation

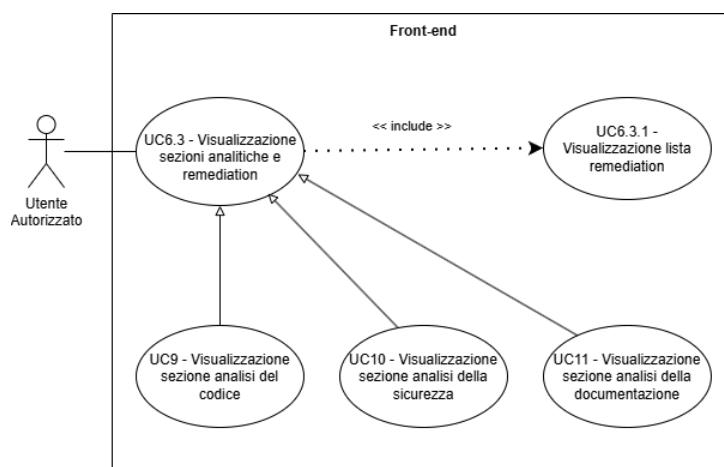


Figure 17: UC6.3 - Visualizzazione sezioni analitiche e remediation

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha selezionato almeno una sezione da visualizzare [UC6.1]
- **Post-condizioni:**
 - L'utente visualizza i risultati tecnici dell'analisi per le aree scelte
- **Scenario principale:**
 - L'utente visualizza le metriche e le criticità relative alla sezione consultata
 - L'utente visualizza l'elenco dei suggerimenti di risoluzione (remediation) [6.3.1]
- **Inclusioni:**
 - [6.3.1]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente scorre i risultati dell'analisi
- **Generalizzazione:**
 - [UC9]
 - [UC10]
 - [UC11]

UC6.3.1: Visualizzazione lista remediation

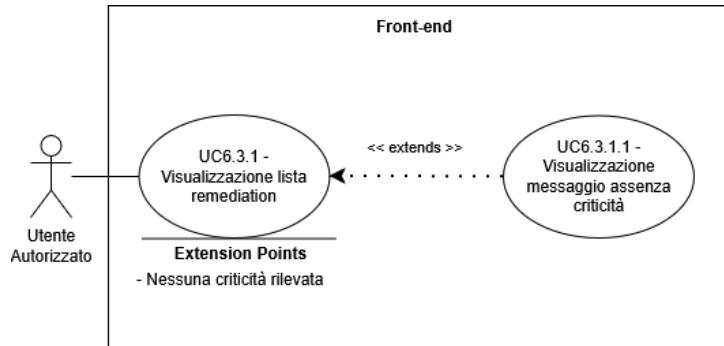


Figure 18: UC6.3.1 - Visualizzazione lista remediation

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza una sezione analitica del report [UC6.3]
- **Post-condizioni:**
 - L'utente visualizza l'elenco delle azioni correttive proposte
- **Scenario principale:**
 - L'utente visualizza la lista delle remediation suggerite
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [6.3.1.1]
- **Trigger:** L'utente consulta l'area dedicata ai miglioramenti per una sezione

UC6.3.1.1: Visualizzazione messaggio assenza criticità

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta visualizzando la sezione delle remediation [UC6.3.1]
- **Post-condizioni:**
 - L'utente visualizza un messaggio informativo circa l'assenza di miglioramenti necessari
- **Scenario principale:**
 - L'utente viene informato che la sezione analizzata rispetta tutti gli standard e non richiede interventi
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Il sistema non individua criticità o suggerimenti per la sezione selezionata

UC7: Selezione intervallo temporale per confronto report

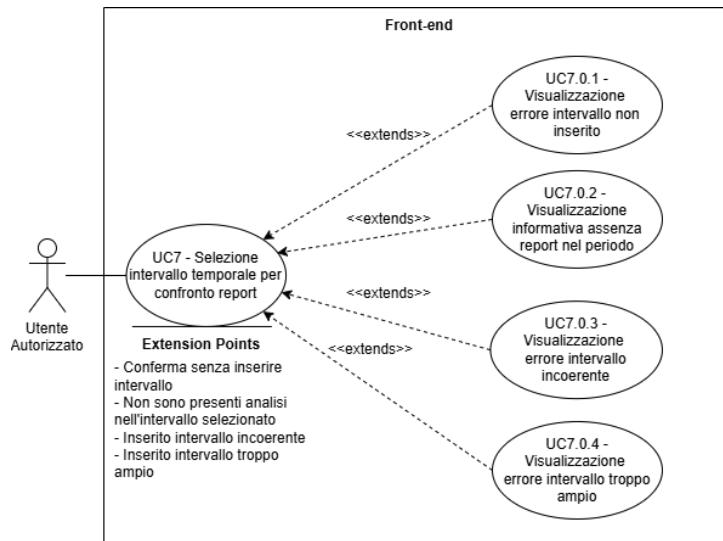


Figure 19: UC7 - Selezione intervallo temporale per confronto report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio di un report di analisi [UC6]
 - L'utente accede alla funzione di confronto storico
- **Post-condizioni:**
 - L'utente imposta l'intervallo temporale per il recupero dei dati di confronto
 - L'utente visualizza la comparazione tra il report attuale e quelli del periodo scelto
- **Scenario principale:**
 - L'utente definisce i limiti temporali (data inizio e data fine) per la generazione del confronto
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC7.0.1]
 - [UC7.0.2]
 - [UC7.0.3]
 - [UC7.0.4]
- **Trigger:** L'utente richiede la modifica del periodo temporale per l'analisi comparativa

UC7.0.1: Visualizzazione errore intervallo non inserito

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente interagisce con i selettori di data [UC7]
- **Post-condizioni:**
 - L'utente visualizza un avviso circa la necessità di popolare i campi data
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala la mancanza dei parametri temporali obbligatori
- **Inclusioni:**

- Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di confermare il confronto senza aver definito l'intervallo

UC7.0.2: Visualizzazione informativa assenza report nel periodo

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha definito un intervallo temporale [UC7]
- **Post-condizioni:**
 - L'utente visualizza un messaggio circa l'assenza di analisi storiche nel periodo indicato
- **Scenario principale:**
 - L'utente viene informato che non esistono report archiviati coerenti con le date selezionate
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona un periodo in cui non sono state effettuate analisi

UC7.0.3: Visualizzazione errore intervallo incoerente

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha impostato le date di inizio e fine [UC7]
- **Post-condizioni:**
 - L'utente visualizza un avviso relativo all'ordine cronologico errato delle date
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore che segnala come la data di inizio sia successiva a quella di fine
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente inserisce limiti temporali logicamente invertiti

UC7.0.4: Visualizzazione errore intervallo troppo ampio

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha definito un intervallo temporale [UC7]
- **Post-condizioni:**
 - L'utente visualizza un avviso circa il superamento del limite massimo di interrogazione
- **Scenario principale:**

- L'utente visualizza un messaggio che segnala l'impossibilità di elaborare confronti su periodi eccessivamente estesi
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona un intervallo che eccede i vincoli di sistema

UC8: Visualizzazione metriche comparative tra report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha definito l'intervallo temporale per il confronto storico [UC7]
- **Post-condizioni:**
 - L'utente visualizza la comparazione analitica tra i report del periodo selezionato
- **Scenario principale:**
 - L'utente visualizza l'andamento delle metriche tramite rappresentazioni grafiche
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la generazione della vista comparativa

UC9: Visualizzazione sezione analisi del codice

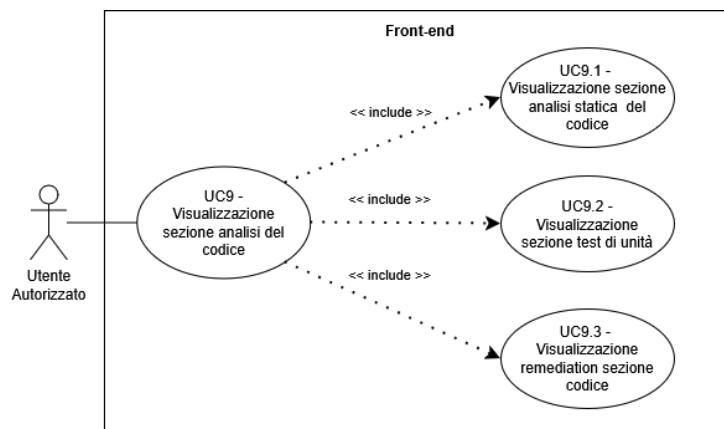


Figure 20: UC9 - Visualizzazione sezione analisi del codice

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha incluso l'area "Codice" nei filtri di visualizzazione del report [UC6.1]
- **Post-condizioni:**
 - L'utente visualizza i dettagli tecnici relativi all'analisi statica e alla copertura del codice
- **Scenario principale:**
 - L'utente visualizza i risultati dell'analisi statica del codice [UC9.1]
 - L'utente visualizza le metriche sulla copertura dei test di unità [UC9.2]

- L'utente visualizza il riepilogo delle remediation per l'area codice [UC9.3]
 - **Inclusioni:**
 - [UC9.1]
 - [UC9.2]
 - [UC9.3]
 - **Estensioni:**
 - Nessuna
 - **Trigger:** L'utente accede all'area dedicata all'analisi del codice nel report di analisi
 - **Specializzazione:**
 - [UC6.3]
- UC9.1: Visualizzazione sezione analisi statica del codice**
- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - L'utente visualizza la sezione analisi del codice [UC9]
 - **Post-condizioni:**
 - L'utente ha preso visione dei bug, vulnerabilità e code smell rilevati tramite analisi statica
 - **Scenario principale:**
 - L'utente visualizza il dettaglio tecnico dei rilievi emersi dall'analisi del codice
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - Nessuna
 - **Trigger:** L'utente consulta i dati di analisi statica
- UC9.2: Visualizzazione sezione test di unità**
- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - L'utente visualizza la sezione analisi del codice [UC9]
 - **Post-condizioni:**
 - L'utente ha preso visione delle percentuali di copertura e l'esito dei test di unità
 - **Scenario principale:**
 - L'utente visualizza le metriche relative alla qualità e quantità dei test eseguiti sul repository
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - Nessuna
 - **Trigger:** L'utente consulta i dati di copertura test

UC9.3: Visualizzazione remediation sezione codice

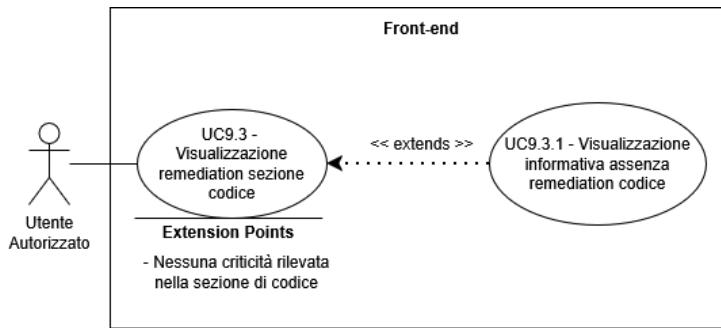


Figure 21: UC9.3 - Visualizzazione remediation sezione codice

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la sezione analisi del codice [UC9]
- **Post-condizioni:**
 - L'utente ha preso visione delle proposte di miglioramento specifiche per il codice analizzato
- **Scenario principale:**
 - L'utente visualizza l'elenco dei suggerimenti correttivi per i difetti del codice
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC9.3.1]
- **Trigger:** L'utente accede alla lista delle azioni correttive per il codice

UC9.3.1: Visualizzazione informativa assenza remediation codice

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta consultando le remediation del codice [UC9.3]
- **Post-condizioni:**
 - L'utente visualizza l'esito positivo sulla qualità del codice
- **Scenario principale:**
 - L'utente viene informato del fatto che non sono stati individuati difetti che richiedano remediation nell'area codice
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Il processo di analisi non rileva criticità nell'area del codice sorgente

UC10: Visualizzazione sezione analisi della sicurezza

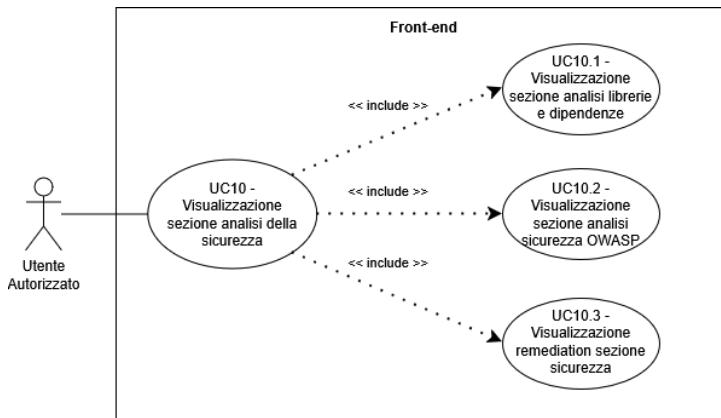


Figure 22: UC10 - Visualizzazione sezione analisi della sicurezza

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha incluso l'area "Sicurezza" nei filtri di visualizzazione del report [UC6.1]
- **Post-condizioni:**
 - L'utente visualizza i dettagli relativi alla sicurezza delle dipendenze e alla conformità OWASP
- **Scenario principale:**
 - L'utente visualizza l'audit sulle librerie e dipendenze del codice [UC10.1]
 - L'utente visualizza i rilievi sulla conformità agli standard OWASP [UC10.2]
 - L'utente visualizza il riepilogo delle remediation per l'area sicurezza [UC10.3]
- **Inclusioni:**
 - [UC10.1]
 - [UC10.2]
 - [UC10.3]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accede all'area dedicata all'analisi della sicurezza nel report di analisi
- **Specializzazione:**
 - [UC6.3]

UC10.1: Visualizzazione sezione analisi librerie e dipendenze

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la sezione analisi della sicurezza [UC10]
- **Post-condizioni:**
 - L'utente ha visualizzato le vulnerabilità note (CVE) rilevate nelle dipendenze del repository
- **Scenario principale:**
 - L'utente visualizza l'elenco delle librerie obsolete o affette da criticità di sicurezza
- **Inclusioni:**
 - Nessuna
- **Estensioni:**

- ▶ Nessuna
- **Trigger:** L'utente consulta i dati relativi alle dipendenze del codice

UC10.2: Visualizzazione sezione analisi sicurezza OWASP

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - ▶ L'utente visualizza la sezione analisi della sicurezza [\[UC10\]](#)
- **Post-condizioni:**
 - ▶ L'utente ha visualizzato i rilievi di conformità basati sulla Top 10 OWASP
- **Scenario principale:**
 - ▶ L'utente visualizza le potenziali minacce identificate secondo gli standard di sicurezza internazionali
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ Nessuna
- **Trigger:** L'utente consulta i dati di conformità OWASP

UC10.3: Visualizzazione remediation sezione sicurezza

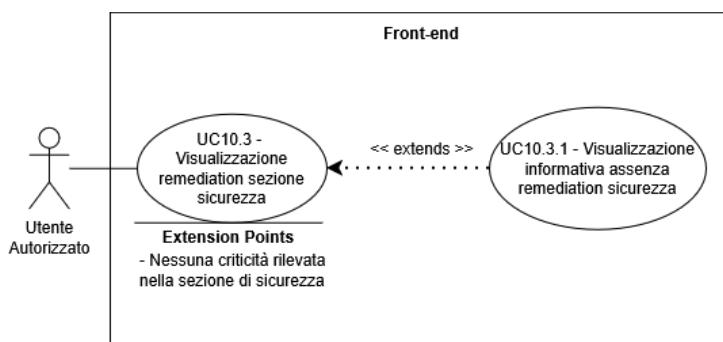


Figure 23: UC10.3 - Visualizzazione remediation sezione sicurezza

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - ▶ L'utente visualizza la sezione analisi della sicurezza [\[UC10\]](#)
- **Post-condizioni:**
 - ▶ L'utente ha visualizzato le proposte di risoluzione per le vulnerabilità identificate
- **Scenario principale:**
 - ▶ L'utente visualizza l'elenco delle azioni correttive per la sicurezza
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ [\[UC10.3.1\]](#)
- **Trigger:** L'utente accede alla lista delle azioni correttive per la sicurezza

UC10.3.1: Visualizzazione informativa assenza remediation sicurezza

- **Attore principale:** Utente Autorizzato

- **Pre-condizioni:**
 - L'utente sta consultando le remediation della sicurezza [UC10.3]
- **Post-condizioni:**
 - L'utente visualizza l'esito positivo sulla robustezza del repository
- **Scenario principale:**
 - L'utente viene informato del fatto che non sono stati individuati difetti che richiedano remediation nell'area sicurezza
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Il processo di analisi non rileva vulnerabilità nell'area sicurezza

UC11: Visualizzazione sezione analisi della documentazione

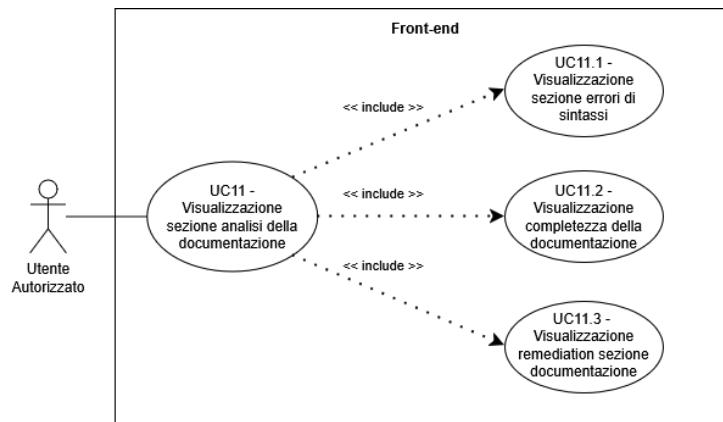


Figure 24: UC11 - Visualizzazione sezione analisi della documentazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'area "Documentazione" è stata selezionata per la visualizzazione [UC6.1]
- **Post-condizioni:**
 - L'utente visualizza i dettagli analitici relativi alla qualità della documentazione
- **Scenario principale:**
 - L'utente visualizza i rilievi sugli errori sintattici rilevati [UC11.1]
 - L'utente visualizza le metriche di completezza documentale [UC11.2]
 - L'utente visualizza l'elenco delle remediation per la documentazione [UC11.3]
- **Inclusioni:**
 - [UC11.1]
 - [UC11.2]
 - [UC11.3]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accede all'area dedicata all'analisi della documentazione nel report di analisi
- **Specializzazione:**

- [UC6.3]

UC11.1: Visualizzazione sezione errori di sintassi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la sezione analisi della documentazione [UC11]
- **Post-condizioni:**
 - L'utente ha preso visione delle incongruenze sintattiche
- **Scenario principale:**
 - L'utente visualizza il dettaglio degli errori formali individuati nei file di testo
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente consulta i risultati dell'analisi sintattica dei file

UC11.2: Visualizzazione completezza della documentazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la sezione analisi della documentazione [UC11]
- **Post-condizioni:**
 - L'utente ha visualizzato il rapporto tra codice sorgente e documentazione esistente
- **Scenario principale:**
 - L'utente visualizza le percentuali di copertura descrittiva degli elementi del repository
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente consulta il grado di esaustività della documentazione

UC11.3: Visualizzazione remediation sezione documentazione

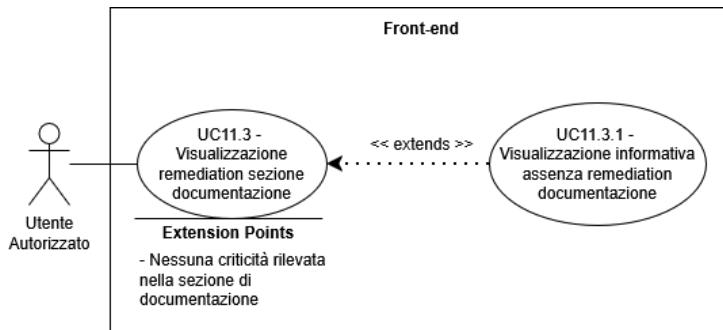


Figure 25: UC11.3 - Visualizzazione remediation sezione documentazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la sezione analisi della documentazione [UC11]

- **Post-condizioni:**
 - L'utente ha visualizzato le proposte correttive per la documentazione
- **Scenario principale:**
 - L'utente visualizza l'elenco dei suggerimenti di miglioramento riguardanti la documentazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC11.3.1]
- **Trigger:** L'utente accede ai suggerimenti correttivi per l'area documentale

UC11.3.1: Visualizzazione informativa assenza remediation documentazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente consulta l'area delle remediation per la documentazione [UC11.3]
- **Post-condizioni:**
 - L'utente visualizza un riscontro positivo sull'integrità documentale
- **Scenario principale:**
 - L'utente viene informato del fatto che non sono stati individuati difetti che richiedano remediation nell'area documentazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'analisi non rileva criticità documentali nel repository

UC12: Visualizzazione ranking dei repository analizzati

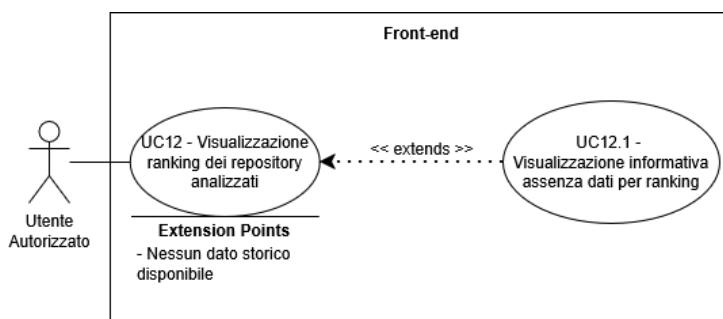


Figure 26: UC12 - Visualizzazione ranking dei repository analizzati

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha eseguito l'autenticazione al sistema [UC2]
- **Post-condizioni:**
 - L'utente ha visualizzato la graduatoria dei repository ordinata per punteggio di qualità
- **Scenario principale:**
 - L'utente visualizza la lista dei repository analizzati ordinati in base al punteggio globale calcolato

- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC12.1]
- **Trigger:** L'utente richiede la consultazione della classifica globale dei propri repository

UC12.1: Visualizzazione informativa assenza dati per ranking

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente accede alla sezione di ranking [UC12]
 - Non esistono repository analizzati associati all'account
- **Post-condizioni:**
 - L'utente ha ricevuto un messaggio di errore che segnala l'assenza di dati per popolare la classifica
- **Scenario principale:**
 - L'utente visualizza un messaggio che gli suggerisce l'avvio di una prima analisi
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accede alla sezione ranking senza dati storici disponibili

UC13: Disconnessione account GitHub da CodeGuardian

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha precedentemente collegato un account GitHub [UC3]
- **Post-condizioni:**
 - L'utente visualizza un messaggio di conferma della disconnessione dell'account GitHub
- **Scenario principale:**
 - L'utente conferma la volontà di rimuovere l'integrazione con GitHub tramite comando dedicato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la rimozione del collegamento con il provider esterno GitHub

UC14: Esportazione report di analisi

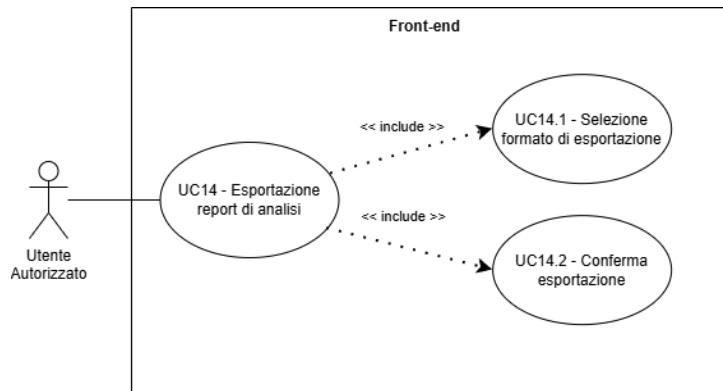


Figure 27: UC14 - Esportazione report di analisi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza un report di analisi [UC6]
- **Post-condizioni:**
 - L'utente visualizza il file nel formato richiesto disponibile al download
- **Scenario principale:**
 - L'utente seleziona il formato desiderato per l'esportazione [UC14.1]
 - L'utente conferma la richiesta di generazione del file [UC14.2]
- **Inclusioni:**
 - [UC14.1]
 - [UC14.2]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la versione scaricabile del report di analisi

UC14.1: Selezione formato di esportazione

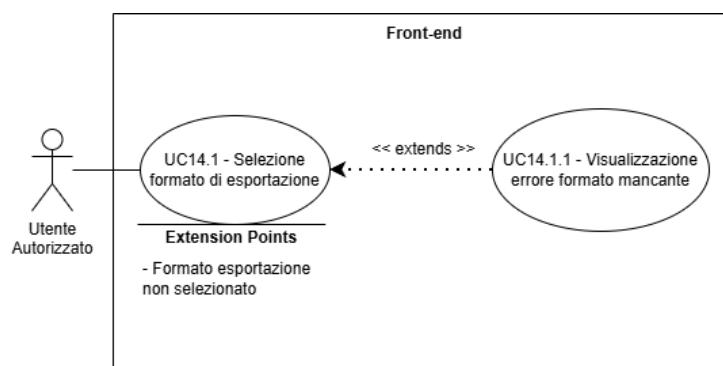


Figure 28: UC14.1 - Selezione formato di esportazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha avviato la procedura di esportazione [UC14]
- **Post-condizioni:**
 - Il formato di output risulta correttamente impostato

- **Scenario principale:**
 - L'utente seleziona un formato tra le opzioni disponibili
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC14.1.1]
- **Trigger:** L'utente interagisce con il selettore dei formati di esportazione

UC14.1.1: Visualizzazione errore formato mancante

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente tenta di confermare l'esportazione senza aver selezionato un formato
- **Post-condizioni:**
 - L'utente ha ricevuto il messaggio d'errore di mancato inserimento del formato
 - L'utente ha nuovamente la possibilità di selezionare un formato
- **Scenario principale:**
 - L'utente visualizza un messaggio di avviso circa l'obbligatorietà della scelta del formato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Mancata selezione del formato durante la conferma di esportazione

UC14.2: Conferma esportazione

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - Un formato valido è stato selezionato [UC14.1]
- **Post-condizioni:**
 - L'utente viene notificato dell'avvio del processo di parsing dei dati e creazione del file
- **Scenario principale:**
 - L'utente attiva il comando di finalizzazione dell'esportazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente conferma l'operazione di download del report

UC15: Modifica password profilo

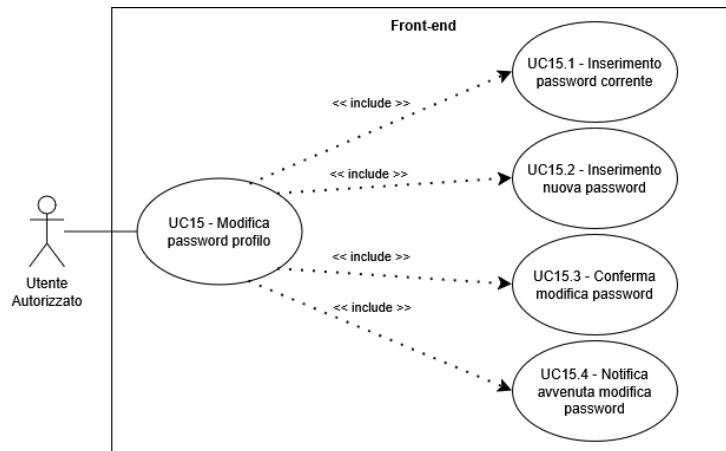


Figure 29: UC15 - Modifica password

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente è autenticato e visualizza l'area gestione profilo [UC2]
- **Post-condizioni:**
 - Le credenziali di accesso risultano aggiornate con il nuovo valore cifrato
- **Scenario principale:**
 - L'utente inserisce la chiave di accesso attuale [UC15.1]
 - L'utente definisce la nuova chiave di accesso [UC15.2]
 - L'utente impartisce il comando di conferma della modifica [UC15.3]
 - L'utente visualizza la notifica di avvenuto aggiornamento [UC15.4]
- **Inclusioni:**
 - [UC15.1]
 - [UC15.2]
 - [UC15.3]
 - [UC15.4]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la variazione delle proprie credenziali di accesso

UC15.1: Inserimento password corrente

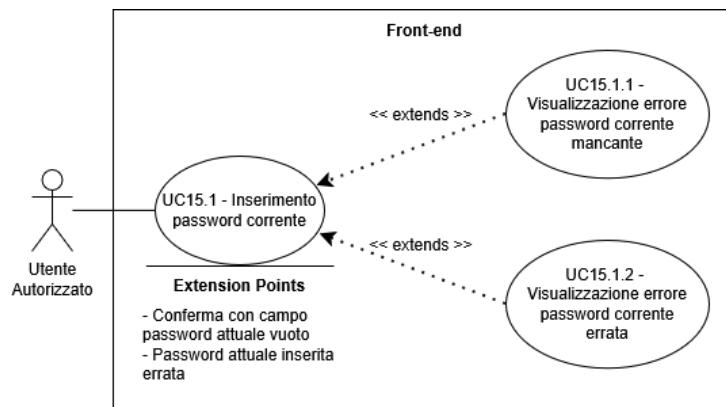


Figure 30: UC15.1 - Inserimento password corrente

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza il modulo di modifica password [UC15]
- **Post-condizioni:**
 - La validità della chiave di accesso attuale risulta verificata
- **Scenario principale:**
 - L'utente digita la password attualmente associata al profilo
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC15.1.1]
 - [UC15.1.2]
- **Trigger:** L'utente seleziona il campo relativo alla password attuale

UC15.1.1: Visualizzazione errore password corrente mancante

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - Il campo relativo alla password attuale non risulta popolato
- **Post-condizioni:**
 - L'utente visualizza un avviso circa l'obbligatorietà del dato
- **Scenario principale:**
 - L'utente riceve una segnalazione di errore per il mancato inserimento della password attuale
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di confermare la modifica con il campo password attuale vuoto

UC15.1.2: Visualizzazione errore password corrente errata

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La password attuale inserita non corrisponde a quella memorizzata
- **Post-condizioni:**
 - La procedura di modifica viene interrotta per incongruenza dei dati
- **Scenario principale:**
 - L'utente visualizza un messaggio di errore relativo all'invalidità della password attuale fornita
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente fornisce una chiave di accesso attuale non corretta

UC15.2: Inserimento nuova password

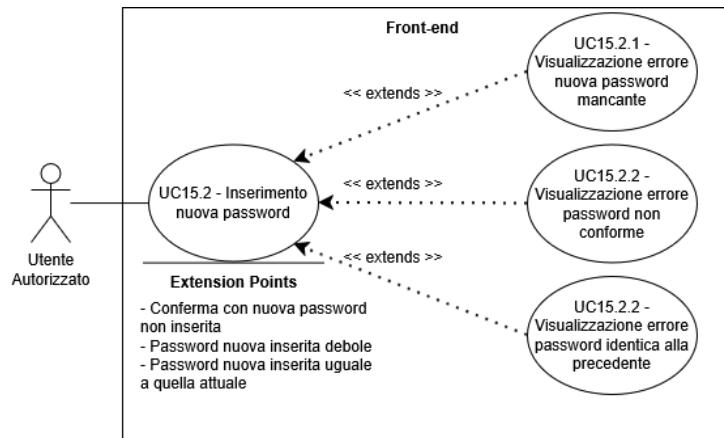


Figure 31: UC15.2 - Inserimento nuova password

- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - L'utente visualizza il modulo di modifica password [UC15]
 - **Post-condizioni:**
 - La nuova chiave di accesso risulta conforme ai criteri di sicurezza stabiliti
 - **Scenario principale:**
 - L'utente definisce il nuovo valore per l'autenticazione
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - [UC15.2.1]
 - [UC15.2.2]
 - [UC15.2.3]
 - **Trigger:** L'utente seleziona il campo relativo alla nuova password
- UC15.2.1: Visualizzazione errore nuova password mancante**
- **Attore principale:** Utente Autorizzato
 - **Pre-condizioni:**
 - Il campo relativo alla nuova password non risulta popolato
 - **Post-condizioni:**
 - L'utente visualizza un avviso circa la necessità di definire un nuovo valore
 - **Scenario principale:**
 - L'utente riceve una segnalazione di errore per il mancato inserimento della nuova password
 - **Inclusioni:**
 - Nessuna
 - **Estensioni:**
 - Nessuna
 - **Trigger:** L'utente tenta di confermare la modifica senza aver definito una nuova password

UC15.2.2: Visualizzazione errore password non conforme

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La nuova password inserita non rispetta i requisiti di complessità previsti
- **Post-condizioni:**
 - L'utente visualizza il dettaglio dei requisiti di sicurezza non soddisfatti
- **Scenario principale:**
 - L'utente riceve una segnalazione circa la scarsa robustezza della nuova chiave scelta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente inserisce una nuova password formalmente non valida

UC15.2.3: Visualizzazione errore password identica alla precedente

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La nuova password inserita coincide con quella attualmente in uso
- **Post-condizioni:**
 - La procedura viene inibita per mancata variazione del valore
- **Scenario principale:**
 - L'utente riceve un avviso che segnala l'impossibilità di utilizzare la password attuale come nuova password
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente tenta di utilizzare la medesima chiave di accesso già attiva

UC15.3: Conferma modifica password

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - I campi del modulo risultano popolati con dati validi e verificati [UC15.1], [UC15.2]
- **Post-condizioni:**
 - L'aggiornamento delle credenziali viene trasmesso per la persistenza
- **Scenario principale:**
 - L'utente aziona il comando di conferma definitiva per l'aggiornamento del profilo
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente conferma la volontà di procedere con il cambio password

UC15.4: Notifica avvenuta modifica password

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La persistenza dei nuovi dati è stata completata con successo [UC15.3]
- **Post-condizioni:**
 - L'utente visualizza l'esito positivo dell'operazione di modifica
- **Scenario principale:**
 - L'utente riceve conferma visiva dell'avvenuto aggiornamento delle credenziali
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Il completamento con successo della procedura di aggiornamento

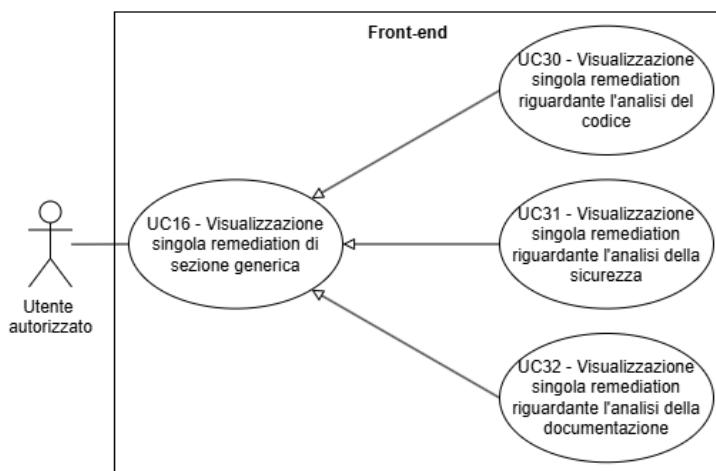
UC16: Visualizzazione singola remediation di sezione generica

Figure 32: UC16 - Visualizzazione singola remediation di sezione generica

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta visualizzando la lista delle remediations [UC6.3.1]
 - L'utente seleziona una remediation specifica
- **Post-condizioni:**
 - L'utente ha visualizzato i dettagli della remediation
- **Scenario principale:**
 - L'utente visualizza i dettagli della remediation proposta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona una remediation dalla lista proposta

- **Generalizzazione:**
 - [\[UC30\]](#)
 - [\[UC31\]](#)
 - [\[UC32\]](#)

UC17: Verifica accessibilità repository GitHub

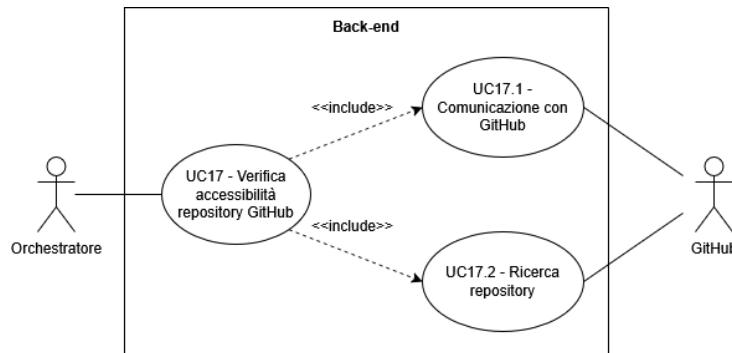


Figure 33: UC17 - Verifica accessibilità repository GitHub

- **Attore principale:** Orchestratore
- **Attore secondario:** GitHub
- **Pre-condizioni:**
 - L'orchestratore recupera l'URL di riferimento dai metadati della collezione di report di analisi [\[UC20\]](#)
- **Post-condizioni:**
 - L'accessibilità del repository è stata accertata e l'orchestratore dispone dei permessi di lettura per avviare la analisi
- **Scenario principale:**
 - L'orchestratore stabilisce una connessione con la piattaforma GitHub [\[UC17.1\]](#)
 - L'orchestratore esegue la ricerca del repository per determinarne la disponibilità [\[UC17.2\]](#)
- **Inclusioni:**
 - [\[UC17.1\]](#)
 - [\[UC17.2\]](#)
- **Estensioni:**
 - Nessuna
- **Trigger:** L'Orchestratore riceve una richiesta di analisi di un repository esterno

UC17.1: Comunicazione con GitHub

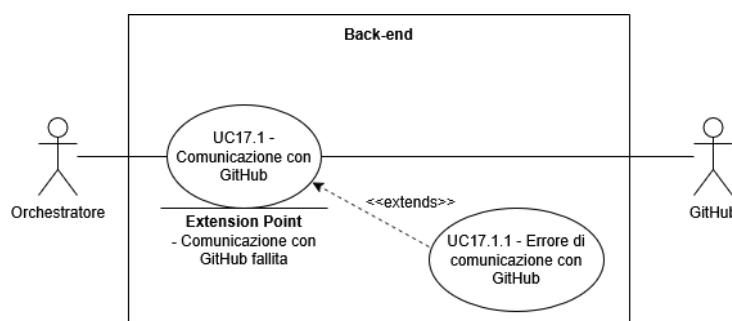


Figure 34: UC17.1 - Comunicazione con GitHub

- **Attore principale:** Orchestratore
- **Attore secondario:** GitHub
- **Pre-condizioni:**
 - La procedura di verifica è stata inizializzata [UC17]
- **Post-condizioni:**
 - Il canale di comunicazione con la piattaforma esterna risulta operativo
- **Scenario principale:**
 - L'orchestratore interroga i servizi remoti per verificarne l'operatività
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC17.1.1]
- **Trigger:** Tentativo di contatto con i servizi API di GitHub

UC17.1.1: Errore di comunicazione con GitHub

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - Il contatto con la piattaforma esterna non produce risposta o restituisce un errore di rete [UC17.1]
- **Post-condizioni:**
 - La procedura viene interrotta per impossibilità tecnica di collegamento
- **Scenario principale:**
 - L'orchestratore rileva l'irreperibilità dei servizi esterni necessari
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Mancata risposta o timeout della connessione remota

UC17.2: Ricerca del repository

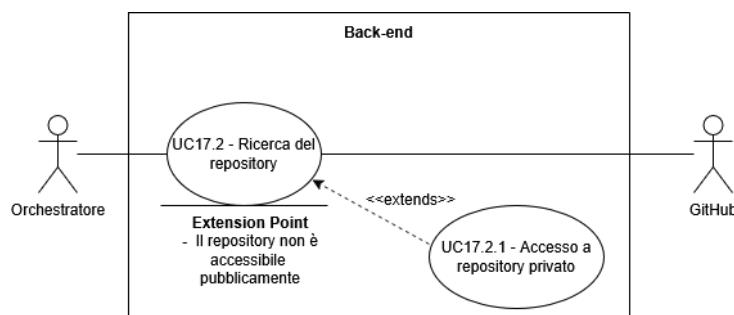


Figure 35: UC17.2 - Ricerca del repository

- **Attore principale:** Orchestratore
- **Attore secondario:** GitHub
- **Pre-condizioni:**

- ▶ La comunicazione con i servizi remoti è stata stabilita con successo [UC17.1]
- **Post-condizioni:**
 - ▶ L'individuazione del repository e la convalida dell'accesso sono completate
- **Scenario principale:**
 - ▶ L'orchestratore ricerca il repository come risorsa pubblica
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ [UC17.2.1]
- **Trigger:** Interrogazione dei metadati della risorsa remota

UC17.2.1: Accesso a repository privato

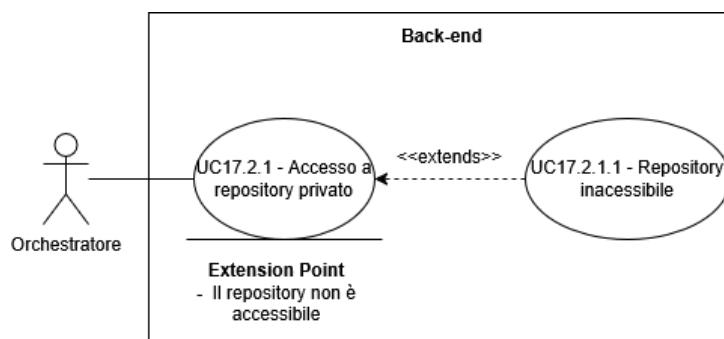


Figure 36: UC17.2.1 - Accesso a repository privato

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - ▶ La risorsa non risulta accessibile pubblicamente [UC17.2]
- **Post-condizioni:**
 - ▶ L'autorizzazione all'accesso è ottenuta tramite l'uso di credenziali o token validi
- **Scenario principale:**
 - ▶ L'orchestratore recupera le credenziali associate all'utente richiedente
 - ▶ L'orchestratore utilizza il token di sessione per convalidare l'accesso privato
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ [UC17.2.1.1]
- **Trigger:** Esito negativo della ricerca pubblica del repository

UC17.2.1.1: Repository inaccessibile

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - ▶ Ogni tentativo di accesso (pubblico e privato via credenziali/token) ha dato esito negativo [UC17.2.1]
- **Post-condizioni:**
 - ▶ L'audit viene annullato per mancanza definitiva dei permessi di lettura

- **Scenario principale:**
 - L'orchestratore rileva il diniego di accesso persistente per la risorsa specificata
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Fallimento di tutti i metodi di autorizzazione disponibili

UC18: Accettazione di una singola remediation

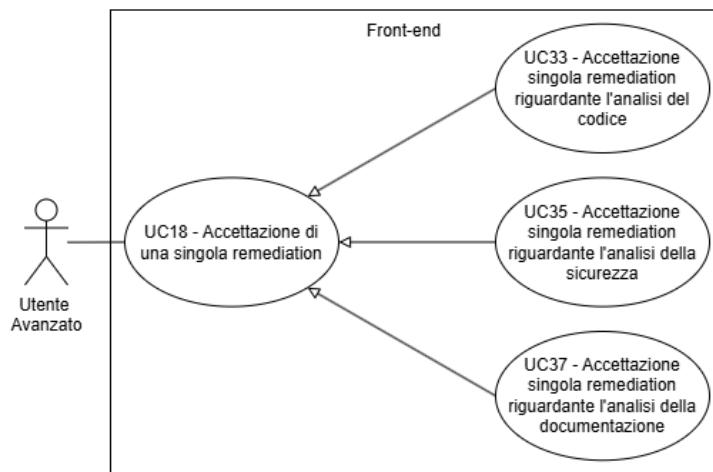


Figure 37: UC18 - Accettazione di una singola remediation

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente sta visualizzando il dettaglio di una singola remediation [UC16]
- **Post-condizioni:**
 - La proposta correttiva viene applicata alla sezione specifica del repository di riferimento
 - Lo stato della remediation risulta aggiornato nella dashboard di CodeGuardian
- **Scenario principale:**
 - L'utente esprime la volontà di applicare la modifica suggerita tramite l'apposito comando di conferma
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente accetta la proposta di remediation visualizzata
- **Generalizzazione:**
 - [UC33]
 - [UC35]
 - [UC37]

UC19: Rifiuto di una singola remediation

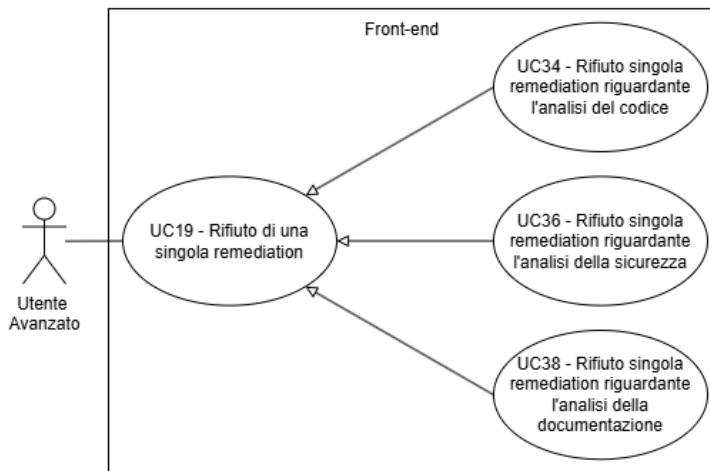


Figure 38: UC19 - Rifiuto singola remediation generica

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio di una singola remediation [UC16]
- **Post-condizioni:**
 - La proposta correttiva viene scartata e rimossa dall'elenco delle azioni pendenti
- **Scenario principale:**
 - L'utente esprime il dissenso rispetto all'applicazione della remediation proposta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente rifiuta esplicitamente la proposta di remediation
- **Generalizzazioni:**
 - [UC34]
 - [UC36]
 - [UC38]

UC20: Creazione raccolta report di analisi

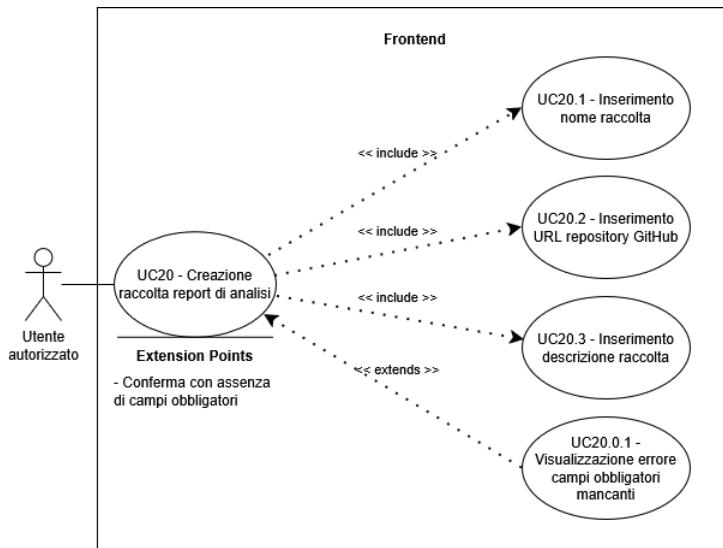


Figure 39: UC20 - Creazione raccolta report di analisi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente dispone di una sessione attiva nel sistema [UC2]
- **Post-condizioni:**
 - Una nuova collezione di report risulta creata e disponibile per l'archiviazione delle analisi del repository
 - L'utente visualizza un messaggio di successo della procedura di creazione della raccolta
- **Scenario principale:**
 - L'utente definisce il nome identificativo della raccolta [UC20.1]
 - L'utente specifica l'URL del repository di riferimento [UC20.2]
 - L'utente fornisce una descrizione facoltativa della raccolta [UC20.3]
 - L'utente impartisce il comando di conferma per la creazione della raccolta
- **Inclusioni:**
 - [UC20.1]
 - [UC20.2]
 - [UC20.3]
- **Estensioni:**
 - [UC20.0.1]
- **Trigger:** L'utente richiede la creazione di un nuovo contenitore per i report di analisi

UC20.0.1: Visualizzazione errore campi obbligatori mancanti

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente sta compilando il modulo di creazione nuova raccolta [UC20]
- **Post-condizioni:**
 - La procedura di creazione viene inibita fino al completamento dei dati necessari
 - L'utente ha ricevuto il messaggio di errore riguardante il mancato popolamento dei campi obbligatori
 - L'utente ha nuovamente accesso all'inserimento dei campi per la procedura

- **Scenario principale:**
 - L'utente riceve una segnalazione circa l'incompletezza dei dati obbligatori forniti
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Tentativo di conferma della creazione con campi obbligatori non popolati

UC20.1: Inserimento nome raccolta

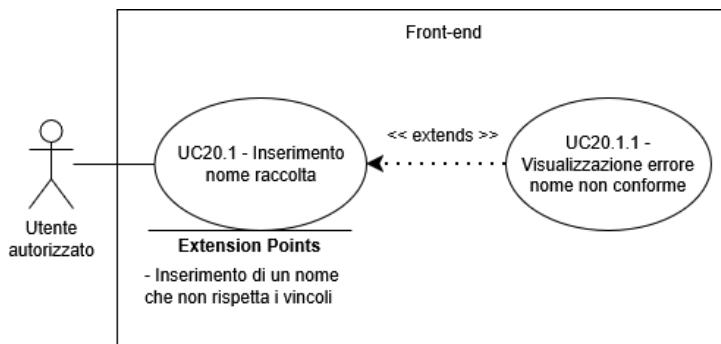


Figure 40: UC20.1 - Inserimento nome raccolta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza il modulo di creazione raccolta [UC20]
- **Post-condizioni:**
 - Il nome identificativo risulta acquisito e conforme ai vincoli di formato
- **Scenario principale:**
 - L'utente digita il nome scelto per la nuova raccolta di report
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC20.1.1]
- **Trigger:** L'utente seleziona il campo dedicato all'identificativo della raccolta

UC20.1.1: Visualizzazione errore nome non conforme

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha inserito un valore nel campo nome [UC20.1]
- **Post-condizioni:**
 - L'utente visualizza il dettaglio dei criteri di nomenclatura non rispettati
- **Scenario principale:**
 - L'utente riceve un avviso circa la non validità formale del nome inserito
- **Inclusioni:**
 - Nessuna
- **Estensioni:**

- ▶ Nessuna
- **Trigger:** Inserimento di un nome che non rispetta i vincoli alfanumerici o di lunghezza

UC20.2: Inserimento URL repository GitHub

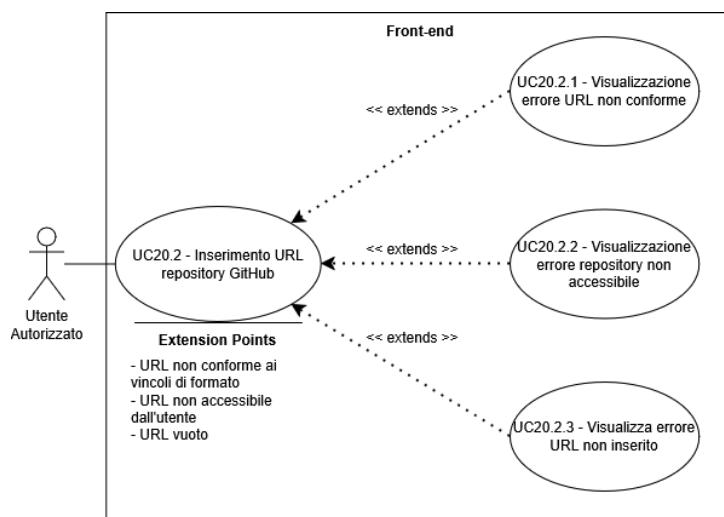


Figure 41: UC20.2 - Inserimento URL repository GitHub

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - ▶ L'utente visualizza il modulo di creazione raccolta [\[UC20\]](#)
- **Post-condizioni:**
 - ▶ L'indirizzo remoto del repository risulta acquisito e verificato
- **Scenario principale:**
 - ▶ L'utente digita l'URL del repository GitHub associato alla raccolta
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ [\[UC20.2.1\]](#)
 - ▶ [\[UC20.2.2\]](#)
 - ▶ [\[UC20.2.3\]](#)
- **Trigger:** L'utente seleziona il campo dedicato all'indirizzo del repository

UC20.2.1: Visualizzazione errore URL non conforme

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - ▶ L'utente ha inserito un valore nel campo URL [\[UC20.2\]](#)
- **Post-condizioni:**
 - ▶ L'utente visualizza una segnalazione circa l'invalidità sintattica dell'indirizzo
- **Scenario principale:**
 - ▶ L'utente riceve un messaggio di errore relativo al mancato rispetto del protocollo o del dominio richiesto
- **Inclusioni:**
 - ▶ Nessuna

- **Estensioni:**
 - Nessuna
- **Trigger:** Inserimento di un URL formalmente non valido

UC20.2.2: Visualizzazione errore repository non accessibile

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha fornito un URL sintatticamente corretto [UC20.2]
- **Post-condizioni:**
 - La procedura viene interrotta a causa dell'irreperibilità della risorsa remota
- **Scenario principale:**
 - L'utente visualizza un avviso circa l'inesistenza o l'inaccessibilità del repository specificato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Mancato riscontro positivo dai servizi remoti per l'URL indicato

UC20.2.3: Visualizzazione errore URL non inserito

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - Il campo relativo all'URL del repository risulta vuoto durante la fase di convalida
- **Post-condizioni:**
 - L'utente visualizza l'avviso di obbligatorietà per il campo URL
- **Scenario principale:**
 - L'utente riceve una segnalazione circa la necessità di fornire l'indirizzo del repository
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Tentativo di procedere senza aver popolato il campo URL

UC20.3: Inserimento descrizione raccolta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza il modulo di creazione raccolta [UC20]
- **Post-condizioni:**
 - La nota descrittiva risulta acquisita
- **Scenario principale:**
 - L'utente fornisce informazioni testuali aggiuntive per contestualizzare la raccolta
- **Inclusioni:**
 - Nessuna

- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona il campo destinato alla descrizione

UC21: Avvio analisi

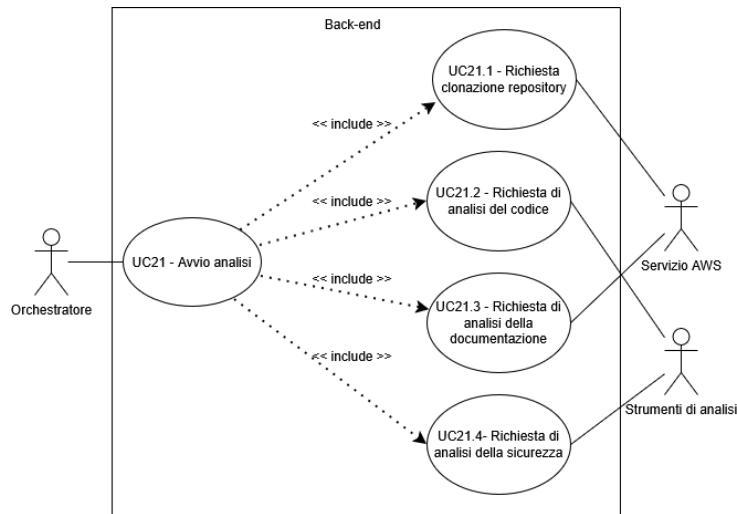


Figure 42: UC21 - Avvio analisi

- **Attore principale:** OrCHEstratore
- **Attore secondario:** Servizio AWS, Strumenti di Analisi
- **Pre-condizioni:**
 - L'accessibilità del repository è stata verificata con successo [UC17]
- **Post-condizioni:**
 - Le procedure di analisi automatica risultano inizializzate presso i rispettivi strumenti esterni
- **Scenario principale:**
 - L'orchestratore richiede la clonazione del repository da analizzare [UC21.1]
 - L'orchestratore inoltra la richiesta di analisi allo strumento per il codice [UC21.2]
 - L'orchestratore inoltra la richiesta di analisi allo strumento per la documentazione [UC21.3]
 - L'orchestratore inoltra la richiesta di analisi allo strumento per la sicurezza [UC21.4]
- **Inclusioni:**
 - [UC21.1]
 - [UC21.2]
 - [UC21.3]
 - [UC21.4]
- **Estensioni:**
 - Nessuna
- **Trigger:** Convalida positiva delle autorizzazioni di accesso al repository remoto

UC21.1: Richiesta di clonazione del repository

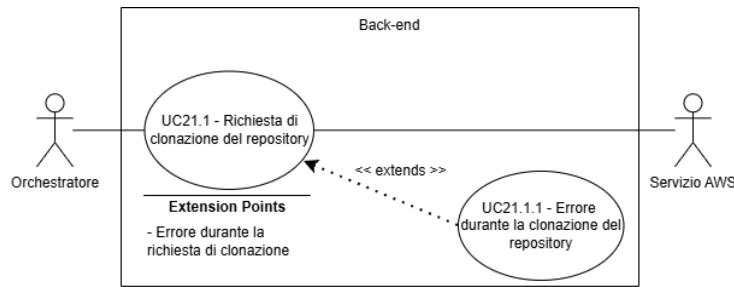


Figure 43: UC21.1 - Richiesta di clonazione del repository

- **Attore principale:** OrCHEstratore
- **Attore secondario:** Servizio AWS
- **Pre-condizioni:**
 - L'orchestratore dispone dell'URL e delle credenziali/token di accesso verificati [UC17]
- **Post-condizioni:**
 - La codebase del repository risulta disponibile in un ambiente di esecuzione locale per l'elaborazione
- **Scenario principale:**
 - L'orchestratore trasmette le coordinate della risorsa e i parametri di autenticazione al servizio di clonazione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC21.1.1]
- **Trigger:** Avvio della fase di preparazione del codice sorgente

UC21.1.1: Errore durante la clonazione del repository

- **Attore principale:** OrCHEstratore
- **Attore secondario:** Servizio AWS
- **Pre-condizioni:**
 - La procedura di clonazione del repository è stata avviata [UC21.1]
- **Post-condizioni:**
 - La procedura di analisi viene interrotta e lo stato di errore viene registrato
- **Scenario principale:**
 - L'orchestratore riceve una notifica di fallimento o timeout dal servizio di clonazione remota
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Incapacità tecnica di replicare la codebase nell'ambiente locale

UC21.2: Richiesta di analisi del codice

- **Attore principale:** OrCHEstratore

- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - La codebase del repository è stata clonata con successo [UC21.1]
- **Post-condizioni:**
 - Lo strumento di analisi statica del codice ha preso in carico i file sorgente per l'elaborazione
- **Scenario principale:**
 - L'orchestratore inoltra i file della codebase allo strumento specializzato nella rilevazione di bug e code smell
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Disponibilità locale dei sorgenti per l'audit del codice

UC21.3: Richiesta di analisi della documentazione

- **Attore principale:** Orchestratore
- **Attore secondario:** Servizio AWS
- **Pre-condizioni:**
 - La codebase del repository è stata clonata con successo [UC21.1]
- **Post-condizioni:**
 - Lo strumento di analisi documentale ha preso in carico la codebase per la verifica della sintassi e completezza
- **Scenario principale:**
 - L'orchestratore inoltra i file di documentazione e i sorgenti al servizio incaricato dell'analisi qualitativa
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Disponibilità locale dei sorgenti per l'audit documentale

UC21.4: Richiesta di analisi della sicurezza

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - La codebase del repository è stata clonata con successo [UC21.1]
- **Post-condizioni:**
 - Lo strumento di scansione di sicurezza ha iniziato la verifica delle vulnerabilità secondo gli standard OWASP
- **Scenario principale:**
 - L'orchestratore inoltra la codebase allo strumento incaricato del controllo dei rischi di sicurezza
- **Inclusioni:**

- Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Disponibilità locale dei sorgenti per l'audit di sicurezza

UC22: Salvataggio stato analisi nel sistema di persistenza

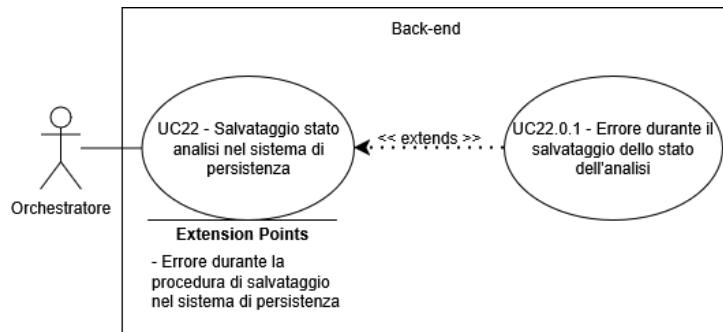


Figure 44: UC22 - Salvataggio stato analisi nel sistema di persistenza

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - Gli strumenti esterni di analisi risultano correttamente inizializzati [UC21]
- **Post-condizioni:**
 - Lo stato dell'analisi risulta registrato come "pending" e associato univocamente al repository e all'utente richiedente
- **Scenario principale:**
 - L'orchestratore effettua la persistenza dei dati di tracciamento dell'analisi, impostando il flag di avanzamento allo stato di attesa
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC22.0.1]
- **Trigger:** Conferma di avvenuto avvio degli strumenti di analisi esterni

UC22.0.1: Errore durante il salvataggio dello stato dell'analisi

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - L'orchestratore ha avviato la procedura di registrazione dello stato [UC22]
- **Post-condizioni:**
 - L'orchestratore inoltra una segnalazione relativa all'impossibilità tecnica di tracciare l'avanzamento dell'audit
- **Scenario principale:**
 - L'orchestratore rileva un'anomalia nel collegamento con il servizio di persistenza
 - L'orchestratore genera una notifica di errore per informare l'utente del problema riscontrato nel tracciamento
- **Inclusioni:**
 - Nessuna

- **Estensioni:**
 - Nessuna
- **Trigger:** Rilevamento di un errore critico durante la scrittura dei dati di stato nel database

UC23: Recupero dei risultati dagli strumenti di analisi

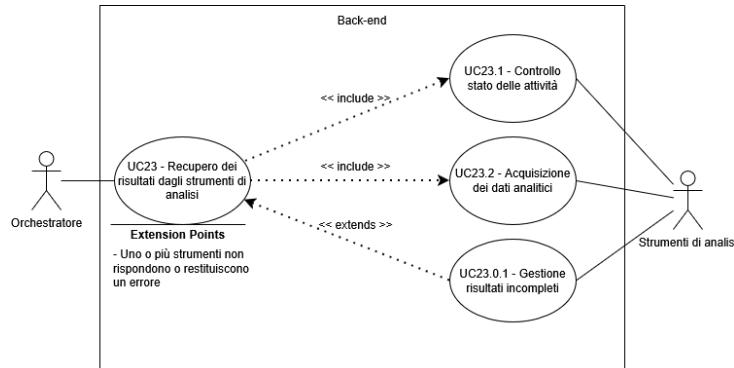


Figure 45: UC23 - Recupero dei risultati dagli strumenti di analisi

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - Gli strumenti di analisi hanno iniziato a lavorare sul codice [UC21]
- **Post-condizioni:**
 - L'orchestratore ha ottenuto tutte le informazioni prodotte dagli strumenti per comporre il report
- **Scenario principale:**
 - L'orchestratore controlla se gli strumenti hanno finito il lavoro [UC23.1]
 - L'orchestratore raccoglie i dati e i risultati dell'analisi [UC23.2]
- **Inclusioni:**
 - [UC23.1]
 - [UC23.2]
- **Estensioni:**
 - [UC23.0.1]
- **Trigger:** Uno o più strumenti terminano l'elaborazione del codice

UC23.0.1: Gestione risultati incompleti

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - L'orchestratore sta aspettando i dati dagli strumenti [UC23]
- **Post-condizioni:**
 - L'analisi procede solo con i dati che è stato possibile recuperare
- **Scenario principale:**
 - Uno strumento impiega troppo tempo o segnala un errore interno
 - L'orchestratore decide di proseguire con i soli dati disponibili per non bloccare l'intero processo
- **Trigger:** Tempo di attesa massimo superato o errore di uno strumento esterno

UC23.1: Controllo stato delle attività

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - Le analisi sono in corso presso gli strumenti esterni
- **Post-condizioni:**
 - Si conosce quali strumenti hanno finito e quali sono ancora al lavoro
- **Scenario principale:**
 - L'orchestratore verifica periodicamente se le analisi esterne sono pronte o riceve un segnale di fine lavori
- **Trigger:** Intervallo di tempo programmato per il controllo dello stato

UC23.2: Acquisizione dei dati analitici

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
 - Uno o più strumenti hanno completato l'analisi [\[UC23.1\]](#)
- **Post-condizioni:**
 - I dati dell'analisi sono stati trasferiti correttamente all'orchestratore
- **Scenario principale:**
 - L'orchestratore preleva i file dei risultati e le informazioni di riepilogo generate dagli strumenti
- **Trigger:** Disponibilità dei dati confermata dagli strumenti

UC24: Generazione del report finale

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - Gli output grezzi sono stati acquisiti correttamente dagli strumenti di analisi [\[UC23\]](#)
- **Post-condizioni:**
 - Il report di analisi finale risulta aggregato, validato e pronto per la persistenza
- **Scenario principale:**
 - L'orchestratore esegue la sintesi dei dati provenienti dai diversi moduli analitici (codice, sicurezza, documentazione)
 - L'orchestratore normalizza le metriche e le remediation in un formato strutturato coerente
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Disponibilità della totalità (o della quota parziale valida) dei risultati degli strumenti di analisi

UC25: Salvataggio di un report

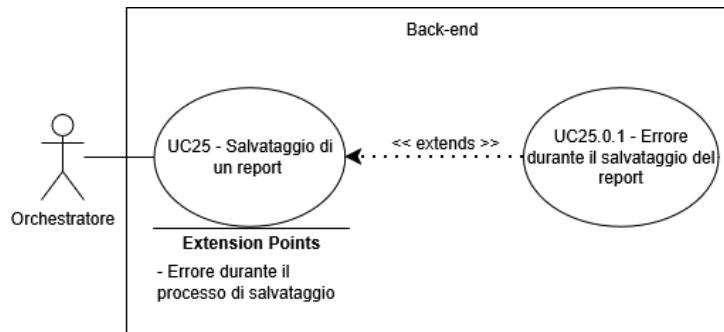


Figure 46: UC25 - Salvataggio di un report

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - Il report di analisi finale risulta generato e validato [UC24]
- **Post-condizioni:**
 - Il report di analisi risulta archiviato in modo permanente e lo stato dell'attività risulta aggiornato a “completed”
- **Scenario principale:**
 - L'orchestratore provvede alla scrittura del report nel sistema di persistenza, associandolo al repository e al profilo dell'utente richiedente
 - L'orchestratore aggiorna i metadati dell'analisi per riflettere il completamento della procedura
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC25.0.1]
- **Trigger:** Completamento delle operazioni di sintesi e aggregazione del report finale

UC25.0.1: Errore durante il salvataggio del report

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - L'orchestratore ha avviato la procedura di persistenza del report [UC25]
 - L'orchestratore rileva un errore di connessione o un'anomalia interna durante la fase di scrittura dei dati
- **Post-condizioni:**
 - L'utente visualizza una segnalazione circa il mancato salvataggio dei risultati dell'analisi
- **Scenario principale:**
 - L'orchestratore genera una notifica di errore per informare l'utente circa l'irreperibilità del report generato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Rilevamento di un'eccezione critica durante la fase di archiviazione dei dati

UC26: Invio notifica completamento dell'analisi del repository

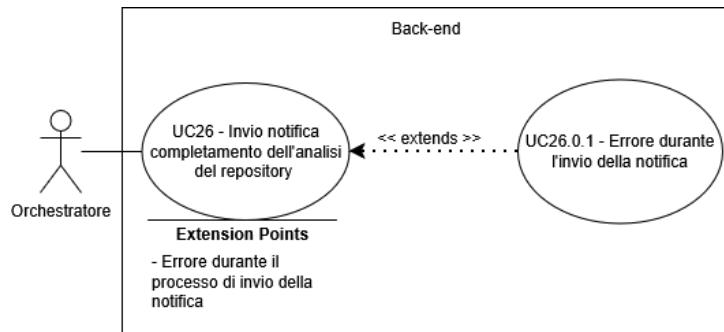


Figure 47: UC26 - Invio notifica completamento dell'analisi del repository

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - Il report di analisi risulta correttamente archiviato e lo stato è aggiornato a "completed" [UC25]
- **Post-condizioni:**
 - Il messaggio informativo relativo alla disponibilità del nuovo report risulta inoltrato ai canali di comunicazione dell'utente
- **Scenario principale:**
 - L'orchestratore provvede all'inoltro di una notifica (push o email) contenente il riferimento al report appena generato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC26.0.1]
- **Trigger:** Avvenuto aggiornamento dello stato dell'analisi a 'completed' nel sistema di persistenza

UC26.0.1: Errore durante l'invio della notifica

- **Attore principale:** Orchestratore
- **Pre-condizioni:**
 - La procedura di invio notifica è stata inizializzata [UC26]
- **Post-condizioni:**
 - La mancata consegna del messaggio viene registrata nei log di errore per finalità di audit interno
- **Scenario principale:**
 - L'orchestratore rileva un'anomalia tecnica o un'interruzione di servizio nel canale di comunicazione esterno
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Rilevamento di un errore di connessione o rifiuto da parte del fornitore del servizio di messaggistica

UC27: Ricezione notifica completamento analisi

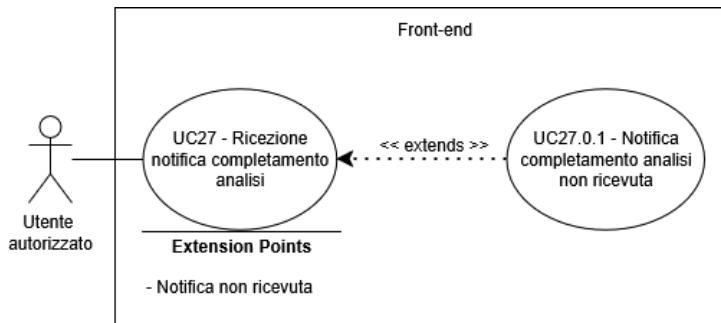


Figure 48: UC27 - Ricezione notifica completamento analisi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La procedura di inoltro della notifica è stata eseguita dall'orchestratore [UC26]
- **Post-condizioni:**
 - L'utente dispone dell'informazione relativa alla conclusione dell'audit tramite i propri canali di comunicazione
- **Scenario principale:**
 - L'utente riceve il messaggio informativo di completamento
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC27.0.1]
- **Trigger:** Disponibilità del messaggio di notifica sui canali di comunicazione dell'utente

UC27.0.1: Notifica completamento analisi non ricevuta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La procedura di inoltro della notifica è stata eseguita [UC26]
- **Post-condizioni:**
 - L'utente non riceve l'avviso proattivo a causa di impedimenti tecnici esterni o di connettività
- **Scenario principale:**
 - L'utente non riceve il messaggio a causa di anomalie nei servizi di terze parti o problemi di rete locale
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Mancata consegna o ricezione del messaggio informativo a seguito dell'invio

UC28: Notifica errore critico durante l'analisi

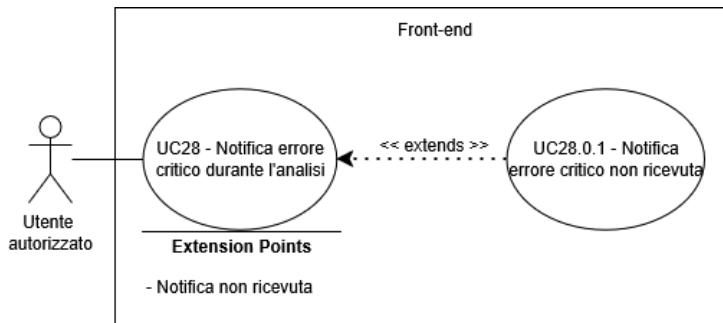


Figure 49: UC28 - Notifica errore critico durante l'analisi

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha una procedura di analisi pendente nel sistema [UC22]
 - L'orchestratore ha rilevato un'anomalia bloccante in una delle fasi di audit
- **Post-condizioni:**
 - L'utente dispone dell'informazione relativa al fallimento dell'analisi e alle cause riscontrate
- **Scenario principale:**
 - L'utente riceve il messaggio informativo di errore critico
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC28.0.1]
- **Trigger:** L'orchestratore rileva l'impossibilità di proseguire con l'analisi e invia la notifica di errore

UC28.0.1: Notifica errore critico non ricevuta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'orchestratore ha tentato l'invio della notifica di fallimento
- **Post-condizioni:**
 - L'utente non riceve l'avviso di errore ma lo stato di fallimento risulta consultabile nella dashboard
- **Scenario principale:**
 - Il messaggio di errore non viene recapitato per problemi di rete o dei servizi di messaggistica esterni
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Mancata ricezione della comunicazione di errore

UC29: Gestione del codice OAuth GitHub

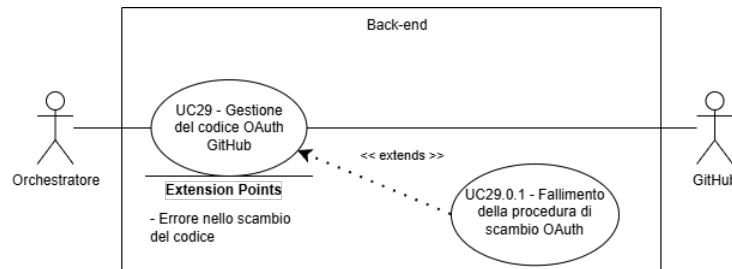


Figure 50: UC29 - Gestione del codice OAuth GitHub

- **Attore principale:** Orchestratore
- **Attore secondario:** GitHub
- **Pre-condizioni:**
 - L'orchestratore ha acquisito un codice di autorizzazione temporaneo (OAuth Code)
- **Post-condizioni:**
 - Il token di accesso risulta ottenuto, crittografato e associato all'account utente
- **Scenario principale:**
 - L'orchestratore richiede a GitHub lo scambio del codice temporaneo con un token di accesso
 - L'orchestratore provvede alla crittografia e alla persistenza del token nel database
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC29.0.1]
- **Trigger:** Ricezione di un codice di autorizzazione valido dal fornitore esterno

UC29.0.1: Fallimento della procedura di scambio OAuth

- **Attore principale:** Orchestratore
- **Attore secondario:** GitHub
- **Pre-condizioni:**
 - Il codice temporaneo risulta scaduto o non valido ai fini dello scambio
- **Post-condizioni:**
 - L'integrazione viene annullata e l'utente viene informato della necessità di ripetere l'autenticazione
- **Scenario principale:**
 - GitHub restituisce un errore di protocollo durante la richiesta di scambio del token
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Rilevamento di un errore di validazione del codice da parte del fornitore esterno

UC30: Visualizzazione singola remediation riguardante l'analisi del codice

- **Attore principale:** Utente Autorizzato

- **Pre-condizioni:**
 - L'utente visualizza l'elenco delle remediation nella sezione di analisi del codice [[UC9.3](#)]
 - L'utente seleziona una singola remediation dall'elenco
- **Post-condizioni:**
 - L'utente visualizza i dettagli tecnici e la proposta di risoluzione della remediation selezionata
- **Scenario principale:**
 - L'utente seleziona una remediation dalla lista dell'area "Codice"
 - L'utente visualizza le informazioni di dettaglio della remediation proposta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona una specifica remediation dalla lista dell'area codice
- **Specializzazione:**
 - [[UC16](#)]

UC31: Visualizzazione singola remediation riguardante l'analisi della sicurezza

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza l'elenco delle remediation nella sezione di analisi della sicurezza [[UC10.3](#)]
 - L'utente seleziona una singola remediation dall'elenco
- **Post-condizioni:**
 - L'utente visualizza le specifiche della vulnerabilità e le azioni correttive di sicurezza proposte
- **Scenario principale:**
 - L'utente seleziona una remediation dalla lista dell'area "Sicurezza"
 - L'utente visualizza le informazioni di dettaglio della remediation proposta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona una specifica remediation dalla lista dell'area sicurezza
- **Specializzazione:**
 - [[UC16](#)]

UC32: Visualizzazione singola remediation riguardante l'analisi della documentazione

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza l'elenco delle remediation nella sezione di analisi della documentazione [[UC11.3](#)]
 - L'utente seleziona una singola remediation dall'elenco
- **Post-condizioni:**
 - L'utente visualizza i rilievi sintattici e le proposte di integrazione documentale associati alla remediation selezionata

- **Scenario principale:**
 - L'utente seleziona una remediation dalla lista dell'area "Documentazione"
 - L'utente visualizza le informazioni di dettaglio della remediation proposta
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente seleziona una specifica remediation dalla lista dell'area documentazione
- **Specializzazione:**
 - [UC16]

UC33: Accettazione singola remediation riguardante l'analisi del codice

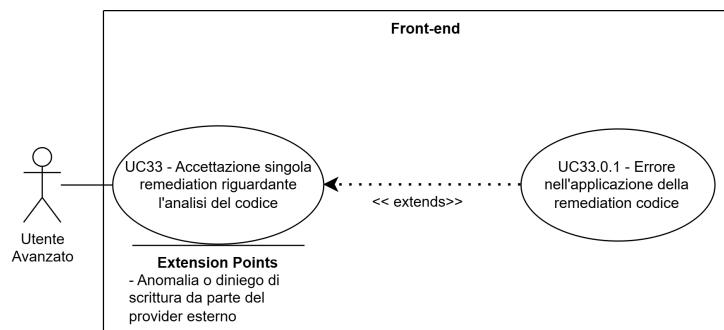


Figure 51: UC33 - Accettazione singola remediation riguardante l'analisi del codice

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation per il codice [UC30]
- **Post-condizioni:**
 - L'utente riscontra l'applicazione delle modifiche suggerite alla codebase del repository di riferimento
 - L'utente visualizza lo stato della remediation aggiornato come eseguita nella dashboard
- **Scenario principale:**
 - L'utente impartisce il comando di accettazione della remediation del codice
 - Il sistema applica la correzione automatica sul repository e aggiorna lo stato della remediation
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC33.0.1]
- **Trigger:** L'utente impartisce il comando di accettazione della remediation per il codice
- **Specializzazione:**
 - [UC18]

UC33.0.1: Errore nell'applicazione della remediation codice

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha confermato l'accettazione della remediation [UC33]

- **Post-condizioni:**
 - L'utente visualizza un avviso di fallimento dell'operazione e la codebase risulta invariata
- **Scenario principale:**
 - Il sistema rileva un errore durante la fase di commit o di scrittura sul repository remoto
 - L'utente visualizza un messaggio che descrive l'impossibilità di applicare la remediation
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Anomalia tecnica o diniego di scrittura da parte del provider esterno

UC34: Rifiuto singola remediation riguardante l'analisi del codice

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation per il codice [UC30]
- **Post-condizioni:**
 - L'utente visualizza la remediation marcata come rifiutata o rimossa dalla lista delle azioni pendenti
 - La codebase del repository rimane invariata
- **Scenario principale:**
 - L'utente impedisce il comando di rifiuto della remediation del codice
 - Il sistema scarta la proposta correttiva e aggiorna lo stato nella dashboard
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente impedisce il comando di rifiuto della remediation del codice
- **Specializzazione:**
 - [UC19]

UC35: Accettazione singola remediation riguardante l'analisi della sicurezza

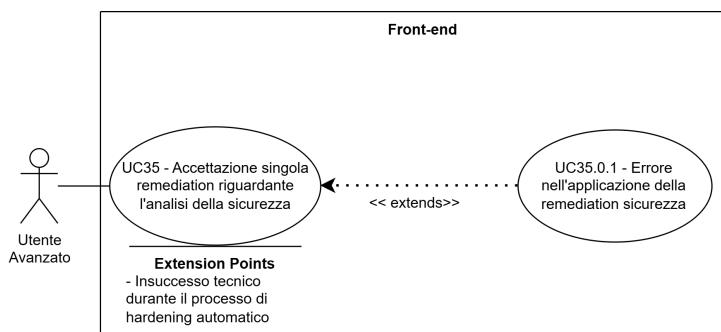


Figure 52: UC35 - Accettazione singola remediation riguardante l'analisi della sicurezza

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation di sicurezza [UC31]

- **Post-condizioni:**
 - L'utente riscontra l'applicazione delle patch/configurazioni suggerite nel repository di riferimento
 - L'utente visualizza lo stato della remediation aggiornato come eseguita nella dashboard
- **Scenario principale:**
 - L'utente impartisce il comando di accettazione della remediation di sicurezza
 - Il sistema applica le azioni correttive e aggiorna lo stato della remediation
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [\[UC35.0.1\]](#)
- **Trigger:** L'utente impartisce il comando di accettazione della remediation di sicurezza
- **Specializzazione:**
 - [\[UC18\]](#)

UC35.0.1: Errore nell'applicazione della remediation sicurezza

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha confermato l'accettazione della remediation di sicurezza [\[UC35\]](#)
- **Post-condizioni:**
 - L'utente visualizza un avviso di fallimento dell'operazione e la vulnerabilità risulta non mitigata
- **Scenario principale:**
 - Il sistema rileva il fallimento della procedura di aggiornamento dipendenze o hardening
 - L'utente visualizza un messaggio che descrive l'impossibilità di applicare la remediation
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Insuccesso tecnico durante il processo di hardening automatico

UC36: Rifiuto singola remediation riguardante l'analisi della sicurezza

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation di sicurezza [\[UC31\]](#)
- **Post-condizioni:**
 - L'utente visualizza la remediation marcata come rifiutata o rimossa dalla lista delle azioni pendenti
 - Il repository rimane invariato rispetto alla vulnerabilità segnalata
- **Scenario principale:**
 - L'utente impartisce il comando di rifiuto della remediation di sicurezza
 - Il sistema scarta la proposta di mitigazione e aggiorna lo stato nella dashboard
- **Inclusioni:**
 - Nessuna

- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente impedisce il comando di rifiuto della remediation di sicurezza
- **Specializzazione:**
 - [UC19]

UC37: Accettazione singola remediation riguardante l'analisi della documentazione

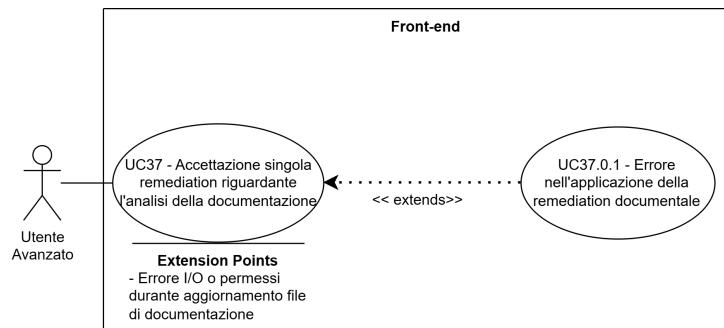


Figure 53: UC37 - Accettazione singola remediation riguardante l'analisi della documentazione

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation documentale [UC32]
- **Post-condizioni:**
 - L'utente riscontra l'aggiornamento dei file di documentazione nel repository secondo la proposta
 - L'utente visualizza lo stato della remediation aggiornato come eseguita nella dashboard
- **Scenario principale:**
 - L'utente impedisce il comando di accettazione della remediation documentale
 - Il sistema applica le correzioni ai file documentali e aggiorna lo stato della remediation
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC37.0.1]
- **Trigger:** L'utente impedisce il comando di accettazione della remediation documentale
- **Specializzazione:**
 - [UC18]

UC37.0.1: Errore nell'applicazione della remediation documentale

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha confermato l'accettazione della remediation documentale [UC37]
- **Post-condizioni:**
 - L'utente visualizza un errore di sincronizzazione e la documentazione remota risulta invariata
- **Scenario principale:**
 - Il sistema rileva un errore di I/O o permessi durante l'aggiornamento dei file testuali
 - L'utente visualizza un messaggio che descrive l'impossibilità di applicare la remediation

- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Errore di I/O o di permessi durante l'aggiornamento dei file di documentazione

UC38: Rifiuto singola remediation riguardante l'analisi della documentazione

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza il dettaglio della remediation documentale [UC32]
- **Post-condizioni:**
 - L'utente visualizza la remediation marcata come rifiutata o rimossa dalla lista delle azioni pendenti
 - La documentazione del repository rimane invariata
- **Scenario principale:**
 - L'utente impedisce il comando di rifiuto della remediation documentale
 - Il sistema scarta la proposta di miglioramento e aggiorna lo stato nella dashboard
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente impedisce il comando di rifiuto della remediation documentale
- **Specializzazione:**
 - [UC19]

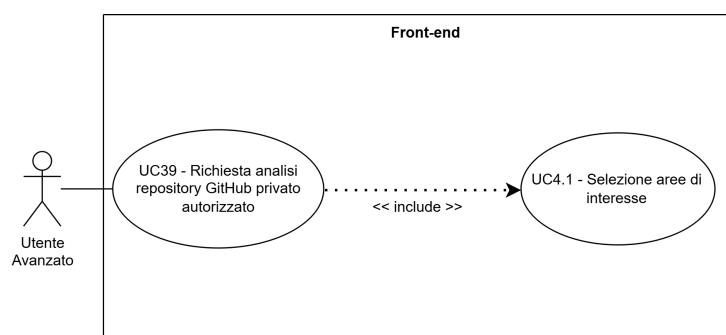
UC39: Richiesta analisi repository GitHub privato autorizzato

Figure 54: UC39 - Richiesta analisi repository GitHub privato autorizzato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha collegato GitHub e dispone dell'integrazione abilitata [UC3]
 - L'utente visualizza la sezione di configurazione dell'analisi
- **Post-condizioni:**
 - L'utente visualizza la conferma di presa in carico della richiesta di analisi del repository privato
- **Scenario principale:**
 - L'utente inserisce l'URL del repository privato da analizzare [UC20.2]

- L'utente seleziona le aree di interesse per l'audit [\[UC4.1\]](#)
- L'utente conferma l'invio della richiesta di analisi
- **Inclusioni:**
 - [\[UC4.1\]](#)
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede una nuova analisi per un repository privato

UC40: Inserimento di un proprio repository privato

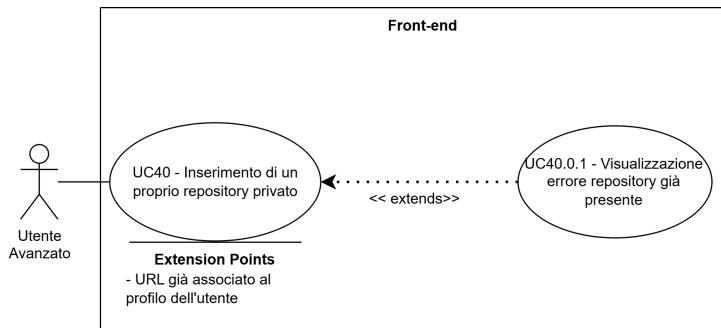


Figure 55: UC40 - Inserimento repository privato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha collegato il proprio profilo GitHub [\[UC3\]](#)
 - L'utente visualizza l'area di gestione dei propri repository privati
- **Post-condizioni:**
 - L'utente visualizza l'esito di registrazione del repository privato e la risorsa risulta disponibile nel catalogo personale
 - La repository inserita può essere analizzata anche da utenti non proprietari qualora i token dimostrassero l'accessibilità alla repository in quanto collaboratori
- **Scenario principale:**
 - L'utente inserisce l'URL del repository privato di sua proprietà [\[UC20.2\]](#)
 - L'utente conferma l'aggiunta del repository al catalogo personale
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [\[UC40.0.1\]](#)
- **Trigger:** L'utente richiede l'inserimento di un repository privato personale nel sistema

UC40.0.1: Visualizzazione errore repository già presente

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente ha inserito un URL già associato al proprio profilo [\[UC40\]](#)
- **Post-condizioni:**
 - L'utente visualizza un avviso di duplicazione e il catalogo rimane invariato
- **Scenario principale:**

- L'utente visualizza un messaggio che segnala la presenza del repository nel catalogo personale
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Convalida di un URL già associato al profilo dell'utente

UC41: Visualizzazione catalogo repository privati inseriti

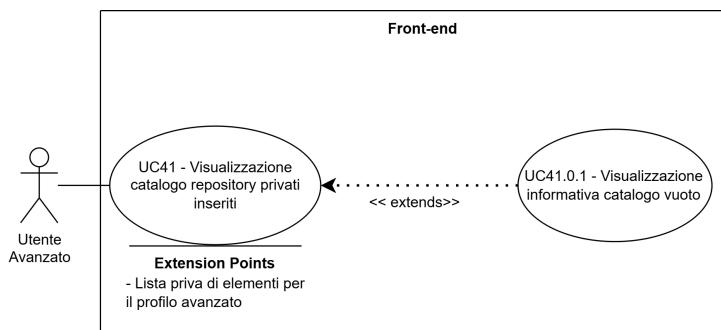


Figure 56: UC41 - Visualizzazione catalogo repository privati inseriti

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente dispone di una sessione attiva e ha collegato GitHub [[UC3](#)]
- **Post-condizioni:**
 - L'utente visualizza l'elenco dei repository privati registrati nel proprio catalogo personale
- **Scenario principale:**
 - L'utente accede alla sezione di gestione repository privati
 - L'utente visualizza la lista dei repository privati registrati
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [[UC41.0.1](#)]
- **Trigger:** L'utente accede alla sezione dedicata alla gestione dei propri repository

UC41.0.1: Visualizzazione informativa catalogo vuoto

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente accede alla sezione e non ha registrato alcun repository privato [[UC41](#)]
- **Post-condizioni:**
 - L'utente visualizza un'informativa circa l'assenza di repository nel catalogo personale
- **Scenario principale:**
 - L'utente visualizza un messaggio che suggerisce l'inserimento del primo repository privato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**

- ▶ Nessuna
- **Trigger:** Recupero di una lista priva di elementi per il profilo avanzato

UC42: Rimozione di un proprio repository privato

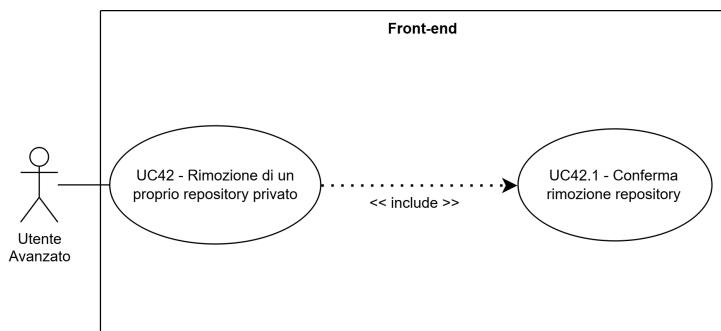


Figure 57: UC42 - Rimozione di un proprio repository privato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - ▶ L'utente visualizza il catalogo dei propri repository privati [UC41]
- **Post-condizioni:**
 - ▶ L'utente visualizza l'esito di rimozione e il repository non risulta più presente nel catalogo personale
- **Scenario principale:**
 - ▶ L'utente seleziona la funzione di rimozione per un repository specifico
 - ▶ L'utente conferma o annulla l'operazione di rimozione [UC42.1]
- **Inclusioni:**
 - ▶ [UC42.1]
- **Estensioni:**
 - ▶ Nessuna
- **Trigger:** L'utente richiede l'eliminazione di un repository dal catalogo personale

UC42.1: Conferma rimozione repository

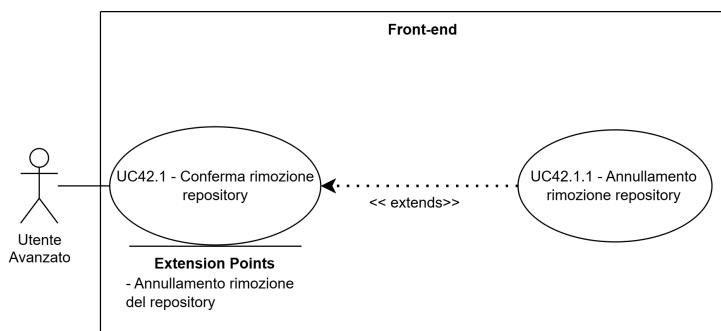


Figure 58: UC42.1 - Conferma rimozione repository

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - ▶ L'utente ha avviato la procedura di rimozione [UC42]
- **Post-condizioni:**
 - ▶ L'utente conferma o annulla la rimozione del repository dal catalogo personale

- **Scenario principale:**
 - L'utente conferma la rimozione definitiva del repository
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC42.1.1]
- **Trigger:** Visualizzazione dell'avviso di conferma eliminazione risorsa

UC42.1.1: Annullamento rimozione repository

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza la richiesta di conferma [UC42.1]
- **Post-condizioni:**
 - L'utente annulla l'operazione e il repository rimane presente nel catalogo personale
- **Scenario principale:**
 - L'utente seleziona il comando di annullamento della rimozione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente aziona il comando di annullamento dell'operazione di eliminazione

UC43: Gestione permessi di accesso al repository privato

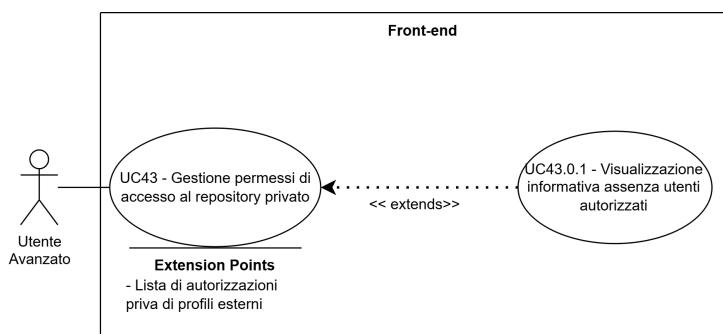


Figure 59: UC43 - Gestione permessi di accesso al repository privato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente seleziona un repository dal proprio catalogo [UC41]
- **Post-condizioni:**
 - L'utente visualizza l'elenco dei profili autorizzati alla consultazione dei report per la risorsa selezionata
- **Scenario principale:**
 - L'utente accede alla sezione di gestione permessi per il repository scelto
 - L'utente visualizza la lista degli utenti autorizzati
- **Inclusioni:**

- Nessuna
- **Estensioni:**
 - [\[UC43.0.1\]](#)
- **Trigger:** L'utente richiede il dettaglio delle autorizzazioni per una risorsa specifica

UC43.0.1: Visualizzazione informativa assenza utenti autorizzati

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente consulta la sezione permessi e la lista risulta vuota [\[UC43\]](#)
- **Post-condizioni:**
 - L'utente visualizza un messaggio che indica l'assenza di profili terzi autorizzati
- **Scenario principale:**
 - L'utente visualizza un'informativa che segnala che l'accesso è limitato al proprietario
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Recupero di una lista di autorizzazioni priva di profili esterni

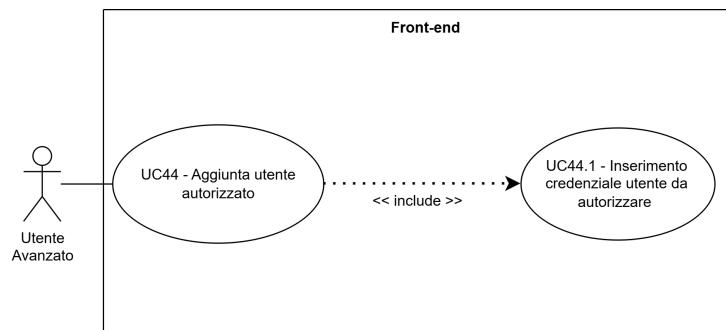
UC44: Aggiunta utente autorizzato

Figure 60: UC44 - Aggiunta utente autorizzato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'utente visualizza la gestione permessi di un repository [\[UC43\]](#)
- **Post-condizioni:**
 - L'utente visualizza il profilo inserito tra gli utenti autorizzati per la risorsa selezionata
- **Scenario principale:**
 - L'utente inserisce lo username o l'email del profilo da autorizzare [\[UC44.1\]](#)
 - L'utente conferma l'aggiunta dell'autorizzazione
- **Inclusioni:**
 - [\[UC44.1\]](#)
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede l'estensione dei permessi di accesso a un altro utente della piattaforma

UC44.1: Inserimento credenziale utente da autorizzare

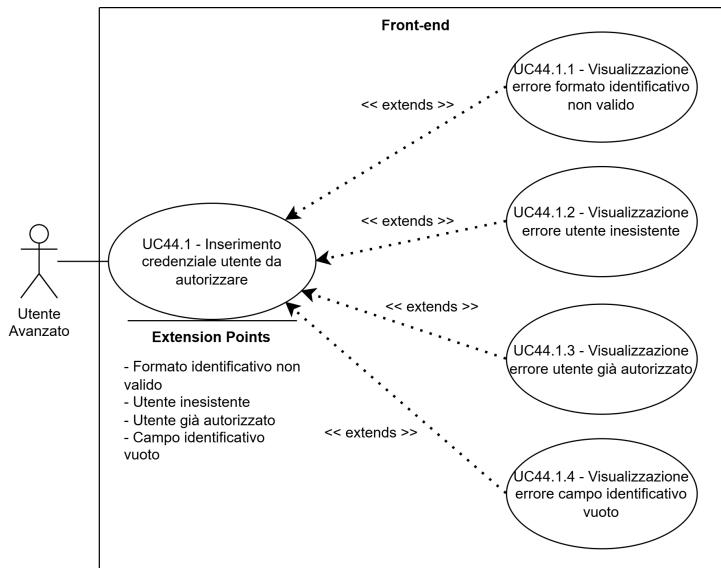


Figure 61: UC44.1 - Inserimento credenziale utente da autorizzare

- Attore principale:** Utente Avanzato
- Pre-condizioni:**
 - L'utente visualizza il campo di input per l'autorizzazione [UC44]
- Post-condizioni:**
 - L'utente ha inserito un identificativo valido riferibile a un profilo esistente e autorizzabile
- Scenario principale:**
 - L'utente digita lo username o l'email del destinatario dell'autorizzazione
 - Il sistema valida l'identificativo e mostra l'esito della verifica
- Inclusioni:**
 - Nessuna
- Estensioni:**
 - [UC44.1.1]
 - [UC44.1.2]
 - [UC44.1.3]
 - [UC44.1.4]
- Trigger:** L'utente interagisce con il campo di ricerca profili per l'assegnazione dei permessi

UC44.1.1: Visualizzazione errore formato identificativo non valido

- Attore principale:** Utente Avanzato
- Pre-condizioni:**
 - L'utente ha inserito uno username/email in formato non valido [UC44.1]
- Post-condizioni:**
 - L'utente visualizza un errore di formato e può correggere l'identificativo
- Scenario principale:**
 - L'utente visualizza un messaggio che indica il formato richiesto
- Inclusioni:**
 - Nessuna

- **Estensioni:**
 - Nessuna
- **Trigger:** Validazione formale negativa dell'identificativo inserito

UC44.1.2: Visualizzazione errore utente inesistente

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - L'identificativo inserito non corrisponde a nessun profilo esistente [UC44.1]
- **Post-condizioni:**
 - L'utente visualizza un avviso che segnala l'inesistenza del profilo
- **Scenario principale:**
 - L'utente visualizza un messaggio che indica che il destinatario non è registrato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Ricerca profilo senza risultati

UC44.1.3: Visualizzazione errore utente già autorizzato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - Il profilo inserito è già presente tra gli autorizzati [UC43]
- **Post-condizioni:**
 - L'utente visualizza un avviso di duplicazione e la lista permessi rimane invariata
- **Scenario principale:**
 - L'utente visualizza un messaggio che segnala che l'utente è già autorizzato
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Tentativo di aggiungere un profilo già autorizzato

UC44.1.4: Visualizzazione errore campo identificativo vuoto

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - Il campo identificativo risulta vuoto durante la conferma [UC44.1]
- **Post-condizioni:**
 - L'utente visualizza un avviso di obbligatorietà del campo identificativo
- **Scenario principale:**
 - L'utente visualizza un messaggio che richiede l'inserimento dello username o dell'email
- **Inclusioni:**
 - Nessuna

- **Estensioni:**
 - ▶ Nessuna
- **Trigger:** Conferma con campo identificativo non popolato

UC45: Rimozione utente autorizzato

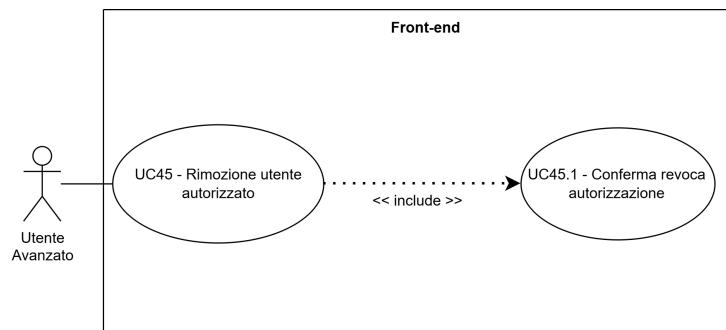


Figure 62: UC45 - Rimozione utente autorizzato

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - ▶ L'utente visualizza la lista dei profili autorizzati per un repository [UC43]
- **Post-condizioni:**
 - ▶ L'utente visualizza l'esito della revoca e il profilo selezionato non risulta più autorizzato
- **Scenario principale:**
 - ▶ L'utente seleziona un profilo dalla lista degli autorizzati
 - ▶ L'utente conferma o annulla la revoca dell'autorizzazione [UC45.1]
- **Inclusioni:**
 - ▶ [UC45.1]
- **Estensioni:**
 - ▶ Nessuna
- **Trigger:** L'utente richiede l'eliminazione di un profilo dalla lista degli autorizzati

UC45.1: Conferma revoca autorizzazione

- **Attore principale:** Utente Avanzato
- **Pre-condizioni:**
 - ▶ La procedura di revoca è stata inizializzata [UC45]
- **Post-condizioni:**
 - ▶ L'utente conferma o annulla la revoca dei permessi di accesso
- **Scenario principale:**
 - ▶ L'utente conferma la revoca dell'autorizzazione per il profilo selezionato
- **Inclusioni:**
 - ▶ Nessuna
- **Estensioni:**
 - ▶ Nessuna
- **Trigger:** Visualizzazione dell'avviso di conferma per la revoca dei permessi

UC46: Rimozione di una raccolta di report

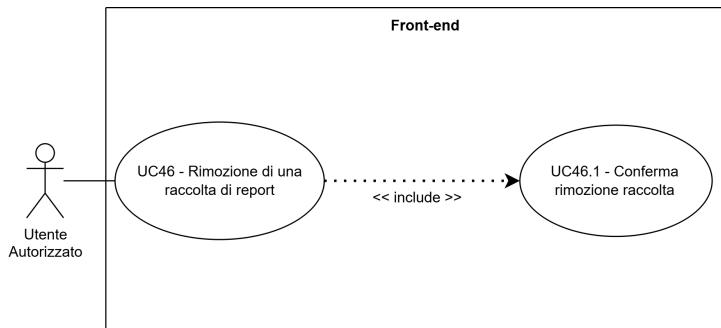


Figure 63: UC46 - Rimozione di una raccolta di report

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza l'elenco delle proprie raccolte di report [UC20]
- **Post-condizioni:**
 - L'utente visualizza l'esito della rimozione della raccolta dal proprio profilo
 - I report precedentemente contenuti nella raccolta rimangono consultabili tramite altri percorsi previsti dal sistema
- **Scenario principale:**
 - L'utente seleziona una raccolta e avvia la funzione di rimozione
 - L'utente conferma o annulla la rimozione [UC46.1]
- **Inclusioni:**
 - [UC46.1]
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede l'eliminazione di una collezione di report dal proprio profilo

UC46.1: Conferma rimozione raccolta

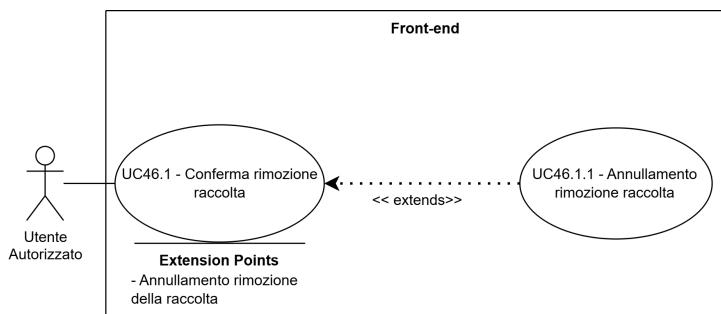


Figure 64: UC46 - Conferma rimozione raccolta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - La procedura di rimozione della raccolta è stata inizializzata [UC46]
- **Post-condizioni:**
 - L'utente conferma o annulla la rimozione della raccolta
- **Scenario principale:**
 - L'utente conferma la rimozione definitiva della raccolta

- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - [UC46.1.1]
- **Trigger:** Visualizzazione dell'avviso di conferma rimozione collezione

UC46.1.1: Annullamento rimozione raccolta

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente visualizza la richiesta di conferma [UC46.1]
- **Post-condizioni:**
 - L'utente annulla l'operazione e la raccolta rimane visibile nel proprio profilo
- **Scenario principale:**
 - L'utente seleziona il comando di annullamento della rimozione
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente aziona il comando di annullamento dell'operazione

UC47: Cancellazione profilo CodeGuardian

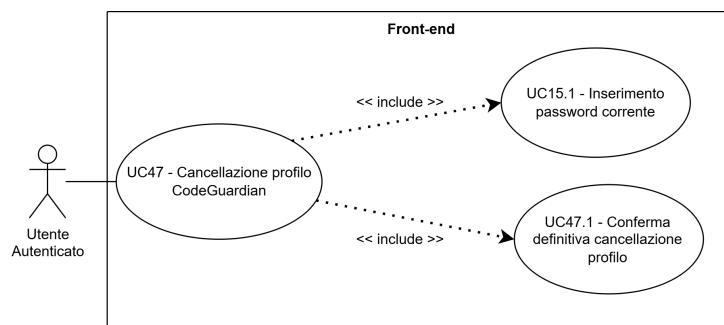


Figure 65: UC47 - Cancellazione profilo CodeGuardian

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha effettuato l'accesso alla piattaforma [UC2]
 - L'utente visualizza la sezione di gestione avanzata del profilo
- **Post-condizioni:**
 - L'utente visualizza l'esito della cancellazione del profilo e non può più accedere al sistema con le credenziali precedenti
 - Le associazioni OAuth e i dati personali risultano rimossi dai registri di persistenza
- **Scenario principale:**
 - L'utente avvia la richiesta di cancellazione del profilo
 - L'utente inserisce la password attuale per conferma identità [UC15.1]
 - L'utente conferma la cancellazione definitiva [UC47.1]
- **Inclusioni:**

- [\[UC15.1\]](#)
- [\[UC47.1\]](#)
- **Estensioni:**
 - Nessuna
- **Trigger:** L'utente richiede la chiusura permanente del proprio account CodeGuardian

UC47.1: Conferma definitiva cancellazione profilo

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
 - L'utente ha completato la verifica dell'identità tramite password [\[UC47\]](#)
- **Post-condizioni:**
 - L'utente conferma la comprensione dell'irreversibilità dell'operazione e procede con la cancellazione oppure annulla l'operazione
- **Scenario principale:**
 - L'utente conferma la cancellazione definitiva del profilo dopo la visualizzazione dell'avviso di irreversibilità
- **Inclusioni:**
 - Nessuna
- **Estensioni:**
 - Nessuna
- **Trigger:** Visualizzazione dell'avviso di avvertimento circa l'irreversibilità della cancellazione

Requisiti di Sistema

In questa sezione sono elencati i requisiti del sistema CodeGuardian individuati da *Skarab Group*.

Per la nomenclatura utilizzata si consiglia di leggere la sezione 2.1.6.3.2 delle [Norme di Progetto](#).

Requisiti Funzionali (FR)

ID	Descrizione	Rif.
FROb1	Il Sistema deve consentire all'Utente non registrato l'accesso alla sezione di creazione account.	[UC1]
FROb2	Il Sistema deve predisporre un comando di conferma per l'invio del modulo di registrazione.	[UC1]
FROb3	Il Sistema deve eseguire la validazione completa dei campi obbligatori (presenza, formato, conformità ai vincoli e univocità) al momento dell'invio del modulo di registrazione.	[UC1]
FROb4	Il Sistema deve permettere la finalizzazione della registrazione solo a seguito della validazione positiva di tutti i campi obbligatori.	[UC1]
FROb5	Il Sistema deve creare e memorizzare un record account che includa almeno username, email, hash della password e salt associato a seguito di registrazione completata con esito positivo.	[UC1]
FROb6	Il Sistema deve memorizzare le chiavi di accesso esclusivamente in forma cifrata tramite un algoritmo di hashing sicuro e generare un salt univoco per ciascun account.	[UC1]
FROb7	Il Sistema deve garantire l'atomicità della procedura di registrazione: in caso di fallimento della persistenza, nessun record parziale deve essere mantenuto nel database.	[UC1]
FROb8	Il Sistema deve visualizzare un messaggio di conferma esplicito a seguito della creazione corretta dell'account CodeGuardian.	[UC1]
FROb9	Il Sistema deve rilevare il tentativo di invio del modulo di registrazione in presenza di campi obbligatori vuoti.	[UC1.0.1]
FROb10	Il Sistema deve inibire la registrazione e notificare l'utente indicando specificamente quali dati obbligatori non sono stati inseriti.	[UC1.0.1]

ID	Descrizione	Rif.
FROb11	Il Sistema deve consentire l'immissione di un username alfanumerico con lunghezza compresa tra 4 e 20 caratteri.	[UC1.1]
FROb12	Il Sistema deve verificare l'univocità dello username rispetto agli account esistenti nel database.	[UC1.1]
FROb13	Il Sistema deve imporre vincoli di unicità lato persistenza su username per prevenire registrazioni duplicate anche in presenza di richieste concorrenti.	[UC1.1.2]
FROb14	In caso di violazione del vincolo di unicità in fase di persistenza, il Sistema deve annullare la registrazione e notificare l'utente con il messaggio previsto per username già in uso.	[UC1.1.2]
FROb15	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora lo username inserito non rispetti i vincoli sintattici previsti.	[UC1.1.1]
FROb16	Il Sistema deve consentire l'immissione di un indirizzo email conforme allo standard RFC 5322.	[UC1.2]
FROb17	Il Sistema deve rifiutare indirizzi email contenenti spazi o privi del carattere "@".	[UC1.2.1]
FROb18	Il Sistema deve verificare l'univocità dell'indirizzo email rispetto agli account esistenti nel database.	[UC1.2]
FROb19	Il Sistema deve imporre vincoli di unicità lato persistenza su indirizzo email per prevenire registrazioni duplicate.	[UC1.2.2]
FROb20	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora l'indirizzo email inserito non sia conforme ai requisiti sintattici.	[UC1.2.1]
FROb21	Il Sistema deve accettare una password solo se di lunghezza pari o superiore ad 8 caratteri.	[UC1.3]
FROb22	Il Sistema deve accettare una password solo se include almeno una lettera maiuscola, una lettera minuscola, una cifra e un carattere speciale.	[UC1.3]
FROb23	Il Sistema deve rifiutare password che coincidono con lo username o che contengono lo username come sottostringa.	[UC1.3.1]

ID	Descrizione	Rif.
FROb24	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio che specifichi i requisiti di sicurezza non soddisfatti.	[UC1.3.1]
FROb25	Il Sistema deve consentire all'Utente non autenticato l'accesso alla sezione di autenticazione (Login).	[UC2]
FROb26	Il Sistema deve predisporre un comando di conferma per finalizzare la procedura di accesso.	[UC2]
FROb27	Il Sistema deve eseguire la validazione completa delle credenziali (presenza, formato e corrispondenza) al momento dell'invio del modulo.	[UC2]
FROb28	Il Sistema deve garantire l'accesso alle funzionalità riservate esclusivamente a seguito di una corretta validazione delle credenziali.	[UC2]
FROb29	Il Sistema deve reindirizzare l'Utente verso la dashboard principale a seguito di autenticazione avvenuta con successo.	[UC2]
FROb30	Il Sistema deve utilizzare protocolli di comunicazione sicuri (HTTPS) per il trasferimento delle credenziali durante il login.	[UC2]
FROb31	Il Sistema deve utilizzare lo username fornito per recuperare dalla persistenza il record account associato.	[UC2]
FROb32	Il Sistema deve verificare la password inserita confrontando l'hash calcolato con l'hash memorizzato tramite la medesima funzione di hashing e salt.	[UC2]
FROb33	Il Sistema deve implementare meccanismi di rate limiting o lockout temporaneo a seguito di ripetuti tentativi di autenticazione falliti.	[UC2]
FROb34	Il Sistema deve visualizzare un indicatore di caricamento (spinner) durante la validazione delle credenziali per prevenire invii multipli.	[UC2]
FROb35	Il Sistema deve rilevare campi incompleti nel login e inibire l'accesso notificando l'utente tramite avviso specifico.	[UC2.0.1]

ID	Descrizione	Rif.
FROb36	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora lo username inserito non rispetti i vincoli sintattici.	[UC2.1.1]
FROb37	Il Sistema deve notificare l'utente qualora l'identificativo (username) inserito non risulti censito nel sistema.	[UC2.1.2]
FROb38	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora la password inserita non sia formalmente conforme.	[UC2.2.1]
FROb39	Il Sistema deve notificare l'utente qualora la password inserita non corrisponda a quella registrata.	[UC2.2.2]
FROb40	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione dedicata al collegamento del profilo GitHub.	[UC3]
FROb41	Il Sistema deve impedire l'avvio della procedura di collegamento qualora un profilo GitHub risulti già associato all'account CodeGuardian dell'utente.	[UC3]
FROb42	Il Sistema deve utilizzare un parametro di stato (state) per prevenire attacchi di tipo Cross-Site Request Forgery (CSRF) durante il flusso OAuth2.	[UC3]
FROb43	Il Sistema deve memorizzare i token di accesso ottenuti da GitHub esclusivamente in forma cifrata tramite algoritmi di crittografia forte (es. AES-256).	[UC3]
FROb44	Il Sistema deve evitare la persistenza di token o associazioni qualora la procedura di collegamento non termini con esito positivo.	[UC3]
FROb45	Il Sistema deve mostrare un avviso informativo obbligatorio prima di procedere al reindirizzamento verso il dominio esterno GitHub.	[UC3.1]
FROb46	Il Sistema deve consentire all'utente di annullare il reindirizzamento, ripristinando lo stato della sezione integrazioni senza alcuna modifica.	[UC3.1.1]
FROb47	Il Sistema deve elaborare l'esito della procedura di collegamento al ritorno dell'utente su CodeGuardian e visualizzare un messaggio di esito.	[UC3.2]

ID	Descrizione	Rif.
FROb48	Il Sistema deve gestire i timeout nelle chiamate verso le API di GitHub durante lo scambio del token, notificando l'utente del fallimento temporaneo.	[UC3.2.1]
FROb49	Il Sistema deve inibire il collegamento qualora il profilo GitHub risulti già associato a un altro account CodeGuardian.	[UC3.2.2]
FROb50	Il Sistema deve mostrare un messaggio di errore specifico qualora l'utente neghi il consenso alla condivisione dei dati su GitHub.	[UC3.2.3]
FROb51	Il Sistema deve consentire l'immissione dell'URL del repository GitHub nel modulo di richiesta analisi.	[UC4]
FROb52	Il Sistema deve validare che l'URL del repository GitHub inserito utilizzi il protocollo "https://" e punti al dominio "github.com".	[UC4]
FROb53	Il Sistema deve verificare la dimensione del repository tramite API GitHub e inibire l'analisi qualora questa superi i limiti tecnici prestabiliti.	[UC4]
FROb54	Il Sistema deve impedire l'avvio di una nuova analisi e informare l'utente se il report esistente risulta già aggiornato.	[UC4.0.1]
FROb55	Il Sistema deve disabilitare il comando di conferma dell'invio a seguito della pressione dell'utente per prevenire richieste duplicate.	[UC4]
FROb56	Il Sistema deve impedire l'invio di una nuova richiesta se un'analisi per il medesimo repository è già in fase di elaborazione.	[UC4.0.2]
FROb57	Il Sistema deve inibire la richiesta di analisi qualora non venga selezionata almeno un'area di interesse.	[UC4.1.1]
FROb58	Il Sistema deve ordinare l'elenco dei repository analizzati in ordine decrescente rispetto alla data dell'ultima analisi disponibile.	[UC5]
FROb59	Il Sistema deve esporre per ogni elemento della lista: nome del repository, URL di riferimento e data dell'ultima analisi.	[UC5.1]

ID	Descrizione	Rif.
FROb60	Il Sistema deve inibire la visualizzazione della lista e mostrare un'informativa specifica qualora non risultino repository analizzati.	[UC5.0.1]
FROb61	Il Sistema deve inibire il rendering della lista e mostrare una notifica di errore qualora i servizi di persistenza non siano raggiungibili.	[UC5.0.2]
FROb62	Il Sistema deve fornire un comando di aggiornamento (Refresh) per consentire un nuovo tentativo di caricamento in caso di errore tecnico.	[UC5.0.2]
FROb63	Il Sistema deve consentire la selezione di un repository dalla lista per il recupero del report di dettaglio associato.	[UC6]
FROb64	Il Sistema deve validare lato server che il report richiesto appartenga al repository associato all'account dell'Utente Autorizzato prima del rendering.	[UC6]
FROb65	Il Sistema deve inibire il rendering e mostrare un errore di autorizzazione qualora l'utente tenti di accedere a un report di un repository non associato al proprio profilo.	[UC6]
FROb66	Il Sistema deve gestire i timeout nel recupero dei dati analitici dalla persistenza, notificando l'utente in caso di indisponibilità temporanea del report.	[UC6]
FROb67	Il Sistema deve permettere la selezione o deselectazione dinamica delle aree analitiche (Codice, Sicurezza, Documentazione) tramite interfaccia utente.	[UC6.1]
FROb68	Il Sistema deve aggiornare dinamicamente il contenuto a video in base ai filtri applicati senza richiedere il ricaricamento dell'intera pagina.	[UC6.1]
FROb69	Il Sistema deve inibire la visualizzazione delle aree analitiche e mostrare un avviso informativo qualora non risulti selezionata alcuna area nei filtri.	[UC6.1.1]
FROb70	Il Sistema deve esporre i metadati identificativi del report recuperati in fase di caricamento.	[UC6.2]
FROb71	Il Sistema deve esporre il timestamp (data e ora ISO 8601) relativo alla generazione del report.	[UC6.2.1]

ID	Descrizione	Rif.
FROb72	Il Sistema deve visualizzare l'identificativo SHA del commit GitHub analizzato, fornendo un link diretto al commit sulla piattaforma esterna.	[UC6.2.2]
FROb73	Il Sistema deve esporre lo username o l'identificativo dell'account che ha originato la scansione.	[UC6.2.3]
FROb74	Il Sistema deve presentare le metriche tecniche aggregate (es. punteggi di qualità, numero bug, vulnerabilità) per ogni sezione attiva.	[UC6.3]
FROb75	Il Sistema deve caricare e visualizzare la lista delle azioni correttive (remediation) associate univocamente alle criticità rilevate nel report.	[UC6.3.1]
FROb76	Il Sistema deve consentire l'espansione dei dettagli di ogni singola remediation per la visualizzazione della proposta di risoluzione tecnica.	[UC6.3.1]
FROb77	Il Sistema deve visualizzare un messaggio di conferma esito positivo (badge “Clean” o simile) qualora il motore di analisi non rilevi criticità nella sezione.	[UC6.3.1.1]
FROb78	Il Sistema deve consentire la selezione di un intervallo temporale tramite input di data (inizio e fine) per l'estrazione dei report storici dal database.	[UC7]
FROb79	Il Sistema deve predisporre un comando di conferma per l'invio della richiesta di confronto dei dati.	[UC7]
FROb80	Il Sistema deve inibire il caricamento dei dati e visualizzare un avviso specifico qualora i campi relativi alle date non risultino popolati.	[UC7.0.1]
FROb81	Il Sistema deve impedire l'invio della richiesta qualora la data di inizio sia cronologicamente successiva alla data di fine, segnalando l'errore di coerenza.	[UC7.0.3]
FROb82	Il Sistema deve limitare l'ampiezza dell'intervallo temporale a un massimo di 12 mesi solari, inibendo la richiesta e notificando l'utente in caso di superamento.	[UC7.0.4]
FROb83	Il Sistema deve gestire l'assenza di dati nel periodo selezionato visualizzando un'informativa di “Nessun report trovato” senza interrompere la sessione utente.	[UC7.0.2]

ID	Descrizione	Rif.
FRDe84	Il Sistema deve generare rappresentazioni grafiche dinamiche (es. grafici a linee o istogrammi) per illustrare l'evoluzione temporale delle metriche analitiche.	[UC8]
FRDe85	Il Sistema deve abilitare tooltips informativi al passaggio del cursore (hover) sui punti dati dei grafici per mostrare i valori esatti e l'hash del commit associato.	[UC8]
FROb86	Il Sistema deve presentare una tabella comparativa che elenchi i report selezionati in ordine cronologico crescente.	[UC8]
FROb87	Il Sistema deve calcolare e visualizzare gli indicatori di variazione (trend incrementali o decrementali) tra ogni analisi e quella immediatamente precedente.	[UC8]
FROb88	Il Sistema deve garantire l'allineamento dei dati tra la vista grafica e la vista tabellare, effettuando una singola operazione di fetch atomica per l'intero intervallo.	[UC8]
FROb89	Il Sistema deve gestire eventuali errori di rendering dei grafici (es. mancanza di librerie client-side) mostrando in alternativa i dati grezzi in formato tabellare.	[UC8]
FROb90	Il Sistema deve caricare e visualizzare i dati relativi alla sezione "Codice" esclusivamente se l'area risulta attiva nei filtri di visualizzazione del report.	[UC9]
FROb91	Il Sistema deve esporre i risultati dell'analisi statica (bug, code smell) indicando per ogni rilievo la gravità e la posizione nel file sorgente.	[UC9.1]
FROb92	Il Sistema deve esporre la percentuale di copertura dei test (Code Coverage) e il rapporto tra test superati e falliti rispetto al totale eseguito.	[UC9.2]
FROb93	Il Sistema deve presentare la lista delle remediation specifiche per il codice, permettendo la navigazione verso il dettaglio della singola azione.	[UC9.3]
FROb94	Il Sistema deve visualizzare un'informativa di "Codice Conforme" qualora non siano rilevati bug o violazioni degli standard qualitativi.	[UC9.3.1]

ID	Descrizione	Rif.
FROb95	Il Sistema deve caricare i dati della sezione “Sicurezza” in modo asincrono rispetto alle altre sezioni per ottimizzare i tempi di risposta.	[UC10]
FROb96	Il Sistema deve esporre l’elenco delle dipendenze vulnerabili indicando il codice CVE, il grado di severità (CVSS) e la versione sicura consigliata.	[UC10.1]
FROb97	Il Sistema deve mappare i rilievi di sicurezza rispetto alle categorie della Top 10 OWASP per facilitare la valutazione della conformità.	[UC10.2]
FROb98	Il Sistema deve presentare le remediation di sicurezza, ordinandole prioritariamente in base alla criticità della vulnerabilità associata.	[UC10.3]
FROb99	Il Sistema deve visualizzare un’informativa di “Repository Sicuro” qualora non siano rilevate vulnerabilità note nelle dipendenze o nel codice.	[UC10.3.1]
FROb100	Il Sistema deve caricare e visualizzare i dati della sezione “Documentazione” analizzando la presenza e la sintassi dei file Markdown e testuali.	[UC11]
FROb101	Il Sistema deve segnalare gli errori sintattici e i link interrotti individuati all’interno della documentazione del repository.	[UC11.1]
FROb102	Il Sistema deve calcolare e mostrare un indice di completezza documentale basato sulla copertura delle interfacce pubbliche descritte.	[UC11.2]
FROb103	Il Sistema deve esporre suggerimenti testuali per l’integrazione delle parti di documentazione mancanti o incomplete.	[UC11.3]
FROb104	Il Sistema deve visualizzare un’informativa di “Documentazione Completa” qualora non siano rilevati errori o mancanze informative.	[UC11.3.1]
FROb105	Il Sistema deve calcolare un punteggio di qualità globale (0-100) per ogni repository analizzato, basandosi sulle metriche pesate di codice, sicurezza e documentazione.	[UC12]
FROb106	Il Sistema deve generare una graduatoria dinamica dei repository associati all’account dell’Utente Autorizzato, ordinata per punteggio di qualità decrescente.	[UC12]

ID	Descrizione	Rif.
FROb107	Il Sistema deve esporre, per ogni riga del ranking: posizione in classifica, nome del repository, punteggio globale e un indicatore di trend rispetto al mese precedente.	[UC12]
FROb108	Il Sistema deve inibire il rendering del ranking e visualizzare un'informativa specifica qualora non risultino analisi completate per l'account utente.	[UC12.1]
FROb109	Il Sistema deve consentire la rimozione dell'integrazione GitHub esclusivamente previa conferma esplicita dell'Utente Avanzato.	[UC13]
FROb110	Il Sistema deve inviare una richiesta di revoca del token OAuth alle API di GitHub al momento della conferma della disconnessione.	[UC13]
FROb111	Il Sistema deve eliminare definitivamente dal database i token (access e refresh) e l'ID utente GitHub associato all'account CodeGuardian.	[UC13]
FROb112	Il Sistema deve gestire eventuali errori di comunicazione con GitHub durante la revoca, procedendo comunque alla cancellazione locale dei dati sensibili.	[UC13]
FRDe113	Il Sistema deve rendere disponibile il file generato tramite un link di download	[UC14]
FRDe114	Il Sistema deve consentire l'esportazione dei report nei formati PDF (per consultazione) e JSON (per interoperabilità dati).	[UC14.1]
FRDe115	Il Sistema deve inibire l'invio della richiesta di generazione file qualora l'utente non selezioni formalmente uno dei formati previsti.	[UC14.1.1]
FRDe116	Il Sistema deve generare il documento includendo i metadati del report (timestamp, commit hash) e i risultati delle sezioni effettivamente analizzate.	[UC14.2]
FRDe117	Il Sistema deve gestire il processo di generazione del file asincronamente per evitare il blocco dell'interfaccia utente durante il parsing di report voluminosi.	[UC14.2]

ID	Descrizione	Rif.
FROb118	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione dedicata alla modifica della chiave di accesso.	[UC15]
FROb119	Il Sistema deve richiedere l'immissione della password attualmente in uso e validarne la corrispondenza con l'hash memorizzato prima di procedere alla variazione.	[UC15.1]
FROb120	Il Sistema deve inibire la procedura e mostrare un errore specifico qualora la password corrente non venga inserita o risulti errata.	[UC15.1.1], [UC15.1.2]
FROb121	Il Sistema deve validare che la nuova password rispetti i vincoli di complessità stabiliti per la registrazione iniziale.	[UC15.2.2]
FROb122	Il Sistema deve confrontare l'hash della nuova password con quello attuale e impedire la modifica qualora i valori coincidano.	[UC15.2.3]
FROb123	Il Sistema deve aggiornare la password nella persistenza esclusivamente tramite un nuovo processo di hashing sicuro e generazione di un nuovo salt univoco.	[UC15]
FROb124	Il Sistema deve inviare una notifica email automatica all'indirizzo associato al profilo a seguito dell'avvenuta modifica delle credenziali.	[UC15.4]
FROb125	Il Sistema deve invalidare tutte le sessioni attive dell'utente (ad eccezione di quella corrente) a seguito del cambio password avvenuto con successo.	[UC15.4]
FROb126	Il Sistema deve consentire la visualizzazione dei dettagli tecnici di una specifica remediation selezionata dall'utente.	[UC16]
FROb127	Il Sistema deve esporre per ogni remediation: descrizione del difetto, snippet di codice interessato (se applicabile), grado di severità e proposta di risoluzione.	[UC16]
FROb128	Il Sistema deve includere riferimenti o link a documentazione esterna (es. CWE, OWASP) qualora la remediation riguardi una vulnerabilità di sicurezza nota.	[UC16]

ID	Descrizione	Rif.
FROb129	L'Orchestratore deve gestire il ciclo di vita della verifica accessibilità tramite chiamate asincrone verso le API REST di GitHub.	[UC17]
FROb130	L'Orchestratore deve implementare un meccanismo di "Exponential Backoff" per gestire i tentativi di riconnessione in caso di errori di rete temporanei verso GitHub.	[UC17.1.1]
FROb131	L'Orchestratore deve validare la raggiungibilità dell'endpoint API di GitHub inviando una richiesta di "Heartbeat" prima di tentare il fetch del repository.	[UC17.1]
FROb132	L'Orchestratore deve prima tentare l'accesso al repository senza intestazioni di autorizzazione per verificare se la risorsa è di dominio pubblico.	[UC17.2]
FROb133	In caso di errore HTTP 404 o 403 sulla risorsa pubblica, l'Orchestratore deve tentare una seconda richiesta iniettando nel modulo di autorizzazione il "Personal Access Token" (PAT) o il token OAuth dell'utente.	[UC17.2.1]
FROb134	L'Orchestratore deve verificare che il token fornito disponga degli "scopes" (permessi) minimi di lettura (repo o public_repo) necessari per il clonaggio.	[UC17.2.1]
FROb135	In caso di fallimento definitivo (es. token scaduto o repository eliminato), l'Orchestratore deve inviare un segnale di interruzione al modulo di notifica e aggiornare lo stato dell'audit in "FAILED_ACCESS".	[UC17.2.1.1]
FRDe136	Il Sistema deve consentire l'applicazione automatica delle modifiche al repository tramite l'integrazione GitHub a seguito dell'accettazione della remediation.	[UC18]
FRDe137	Il Sistema deve eseguire una validazione di integrità sulla proposta correttiva prima dell'invio del commit verso il repository esterno.	[UC18]
FRDe138	Il Sistema deve aggiornare lo stato della remediation in "Applied" o "Dismissed" nel database di persistenza a seguito dell'azione dell'utente.	[UC18] [UC19]
FRDe139	Il Sistema deve notificare l'utente in caso di fallimento del processo di scrittura (commit) sul repository remoto durante l'accettazione.	[UC18]

ID	Descrizione	Rif.
FROb140	Il Sistema deve consentire all'Utente Autorizzato la definizione di un nome univoco per la raccolta di report all'interno del proprio account.	[UC20.1]
FROb141	Il Sistema deve validare la sintassi dell'URL GitHub fornito, assicurando l'uso del protocollo HTTPS e la corretta struttura del path user/repo.	[UC20.2.1]
FROb142	Il Sistema deve interrogare le API di GitHub per confermare l'esistenza e la raggiungibilità del repository indicato prima di finalizzare la raccolta.	[UC20.2.2]
FROb143	Il Sistema deve gestire i casi di inaccessibilità del repository (es. repository privato senza permessi) notificando l'utente tramite avviso specifico.	[UC20.2.2]
FROb144	Il Sistema deve impedire la creazione di raccolte duplicate che puntano al medesimo repository per lo stesso utente.	[UC20]
FROb145	Il Sistema deve memorizzare la descrizione facoltativa della raccolta supportando la codifica UTF-8 per caratteri speciali e simboli.	[UC20.3]
FROb146	L'Orchestratore deve parallelizzare le richieste di analisi verso i diversi strumenti per ottimizzare il tempo complessivo di esecuzione dell'audit.	[UC21]
FROb147	L'Orchestratore deve includere nella richiesta verso gli strumenti esterni i parametri di configurazione definiti dall'utente durante la fase di richiesta.	[UC21]
FROb148	L'Orchestratore deve trasmettere in modo sicuro (tramite secret manager) le credenziali o i token di accesso al servizio AWS incaricato della clonazione.	[UC21.1]
FROb149	L'Orchestratore deve monitorare il completamento della clonazione e gestire eventuali timeout o errori di spazio disco insufficiente sul volume di destinazione.	[UC21.1.1]
FROb150	In caso di errore durante la clonazione, l'Orchestratore deve inibire l'invio delle richieste agli strumenti di analisi e liberare immediatamente le risorse allocate.	[UC21.1.1]
FROb151	L'Orchestratore deve inoltrare la codebase o i file specifici agli strumenti di analisi esterna (Codice,	[UC21.2] [UC21.3] [UC21.4]

ID	Descrizione	Rif.
	Sicurezza, Documentazione) tramite protocolli di trasferimento sicuri.	
FROb152	Il Sistema deve registrare lo stato dell'analisi nel sistema di persistenza impostandolo a "PENDING" a seguito dell'inizializzazione corretta di tutti i servizi esterni.	[UC22]
FROb153	Il Sistema deve associare univocamente l'ID dell'analisi al repository oggetto dell'audit e all'identificativo dell'utente richiedente.	[UC22]
FROb154	Il Sistema deve persistere i metadati di avvio, inclusi l'hash del commit analizzato e il timestamp di sistema.	[UC22]
FROb155	In caso di errore critico durante la scrittura dello stato (UC22.0.1), l'Orchestratore deve tentare una procedura di "Rollback" informando gli strumenti esterni di annullare l'analisi.	[UC22.0.1]
FROb156	Il Sistema deve registrare nei log di audit ogni fallimento di persistenza dello stato, includendo lo stack trace dell'errore per finalità diagnostiche.	[UC22.0.1]
FROb157	L'Orchestratore deve verificare regolarmente se gli strumenti esterni hanno terminato l'analisi del repository.	[UC23.1]
FROb158	L'Orchestratore deve scaricare i risultati delle analisi non appena questi vengono messi a disposizione dagli strumenti esterni.	[UC23.2]
FROb159	L'Orchestratore deve controllare che i file ricevuti siano completi e leggibili prima di utilizzarli.	[UC23.2]
FROb160	Il Sistema deve poter proseguire con la creazione del report anche se uno degli strumenti fallisce, utilizzando solo i dati recuperati con successo.	[UC23.0.1]
FROb161	L'Orchestratore deve impostare un tempo massimo di attesa per le analisi, oltre il quale smette di aspettare lo strumento ritardatario.	[UC23.0.1]
FROb162	Il Sistema deve segnalare all'interno del database se il report finale contiene solo dati parziali a causa di un problema tecnico.	[UC23.0.1]

ID	Descrizione	Rif.
FROb163	Il Sistema deve unificare i dati provenienti dai diversi strumenti (codice, sicurezza, documentazione) in un unico documento di sintesi.	[UC24]
FROb164	Il Sistema deve convertire i diversi formati dei dati ricevuti dagli strumenti esterni in un modello standard comune.	[UC24]
FROb165	Il Sistema deve verificare che il report finale contenga tutte le informazioni essenziali (risultati, data, versione del codice) prima di procedere al salvataggio.	[UC24]
FROb166	Il Sistema deve calcolare i punteggi di riepilogo generali basandosi sui singoli risultati ottenuti nelle varie aree analizzate.	[UC24]
FROb167	Il Sistema deve archiviare il report in modo permanente, collegandolo correttamente al repository dell'utente.	[UC25]
FROb168	Il Sistema deve modificare lo stato dell'analisi in "Completato" solo dopo aver confermato che il salvataggio dei dati è andato a buon fine.	[UC25]
FROb169	Il Sistema deve informare l'utente con un messaggio di errore se un problema tecnico impedisce il salvataggio definitivo del report.	[UC25.0.1]
FROb170	Il Sistema deve tenere traccia internamente dei motivi del fallimento del salvataggio per permettere controlli tecnici successivi.	[UC25.0.1]
FROb171	In caso di errore nel salvataggio, il Sistema deve tentare di mantenere una copia temporanea del report per evitare la perdita totale dei dati elaborati.	[UC25.0.1]
FROb172	Il Sistema deve generare automaticamente un avviso per l'utente non appena il report di analisi è pronto e salvato correttamente.	[UC26]
FROb173	La notifica inviata deve contenere un link o un pulsante che permetta all'utente di accedere direttamente alla visualizzazione del report.	[UC26]
FROb174	Il Sistema deve includere nella notifica informazioni di base per identificare l'analisi, come il nome del repository e la data di esecuzione.	[UC26]

ID	Descrizione	Rif.
FROb175	Il Sistema deve garantire che l'invio della notifica non interferisca con lo stato dell'analisi: se la notifica fallisce, il report deve comunque rimanere disponibile.	[UC26.0.1]
FROb176	In caso di errore nell'invio del messaggio (es. email non raggiungibile), il Sistema deve segnare l'anomalia nei registri interni per permettere verifiche tecniche.	[UC26.0.1]
FROb177	Il Sistema deve tentare nuovamente l'invio della notifica per un numero limitato di volte in caso di problemi temporanei di rete.	[UC26.0.1]
FROb178	Il Sistema deve consegnare la notifica di fine analisi attraverso i canali scelti dall'utente (es. email o notifiche app).	[UC27]
FROb179	Il Sistema deve mostrare i dettagli dell'analisi (nome progetto e ora) direttamente nell'avviso ricevuto dall'utente.	[UC27]
FROb180	Il Sistema deve garantire che l'utente possa consultare i risultati nella propria area personale anche se la notifica via email non viene recapitata.	[UC27.0.1]
FROb181	Il Sistema deve inviare un avviso immediato se un'analisi si interrompe per un errore imprevisto, spiegandone brevemente il motivo.	[UC28]
FROb182	Il Sistema deve contrassegnare l'analisi come "Fallita" nella lista dei progetti dell'utente se il processo non può essere completato.	[UC28]
FROb183	Il Sistema deve rendere visibili le cause del fallimento all'interno della dashboard, indipendentemente dall'invio o dalla ricezione dell'avviso di errore.	[UC28.0.1]
FROb184	Il Sistema deve trasformare il codice provvisorio fornito da GitHub in una chiave di accesso permanente per poter leggere i repository.	[UC29]
FROb185	Il Sistema deve proteggere la chiave di accesso di GitHub nascondendola tramite cifratura prima di salvarla nei propri archivi.	[UC29]
FROb186	Il Sistema deve collegare la chiave di GitHub in modo esclusivo al profilo dell'utente che ha autorizzato l'operazione.	[UC29]

ID	Descrizione	Rif.
FROb187	Il Sistema deve annullare il collegamento e chiedere all’utente di rifare la procedura se la chiave provvisoria risulta scaduta o non valida.	[UC29.0.1]
FROb188	Il Sistema deve consentire all’Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all’analisi del codice.	[UC30]
FROb189	Il Sistema deve includere nel dettaglio della remediation del codice il titolo, la descrizione, la tipologia di criticità e il livello di severità.	[UC30]
FROb190	Il Sistema deve consentire all’Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all’analisi della sicurezza.	[UC31]
FROb191	Il Sistema deve includere nel dettaglio della remediation di sicurezza il titolo, la descrizione, la tipologia di vulnerabilità e il livello di severità.	[UC31]
FROb192	Il Sistema deve consentire all’Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all’analisi della documentazione.	[UC32]
FROb193	Il Sistema deve includere nel dettaglio della remediation documentale il titolo, la descrizione e la tipologia di rilievo documentale.	[UC32]
FROb194	Il Sistema deve consentire all’Utente Autorizzato di accettare una remediation relativa all’analisi del codice.	[UC33]
FROb195	Il Sistema deve applicare automaticamente alla codebase le modifiche previste dalla remediation del codice accettata.	[UC33]
FROb196	Il Sistema deve aggiornare lo stato della remediation del codice come “eseguita” nella dashboard a seguito dell’applicazione riuscita.	[UC33]
FROb197	Il Sistema deve gestire errori durante l’applicazione della remediation del codice notificando il fallimento all’utente e mantenendo invariata la codebase.	[UC33.0.1]
FROb198	Il Sistema deve consentire all’Utente Autorizzato di rifiutare una remediation relativa all’analisi del codice.	[UC34]

ID	Descrizione	Rif.
FROb199	Il Sistema deve aggiornare lo stato della remediation del codice come “rifiutata” nella dashboard senza apportare modifiche al repository.	[UC34]
FROb200	Il Sistema deve consentire all’Utente Autorizzato di accettare una remediation relativa all’analisi della sicurezza.	[UC35]
FROb201	Il Sistema deve applicare le patch o le configurazioni di sicurezza previste dalla remediation di sicurezza accettata.	[UC35]
FROb202	Il Sistema deve aggiornare lo stato della remediation di sicurezza come “eseguita” nella dashboard a seguito dell’applicazione riuscita.	[UC35]
FROb203	Il Sistema deve gestire errori durante l’applicazione della remediation di sicurezza notificando il fallimento all’utente.	[UC35.0.1]
FROb204	Il Sistema deve consentire all’Utente Autorizzato di rifiutare una remediation relativa all’analisi della sicurezza.	[UC36]
FROb205	Il Sistema deve aggiornare lo stato della remediation di sicurezza come “rifiutata” nella dashboard senza modificare il repository.	[UC36]
FROb206	Il Sistema deve consentire all’Utente Autorizzato di accettare una remediation relativa all’analisi della documentazione.	[UC37]
FROb207	Il Sistema deve applicare automaticamente ai file documentali le modifiche previste dalla remediation documentale accettata.	[UC37]
FROb208	Il Sistema deve aggiornare lo stato della remediation documentale come “eseguita” nella dashboard a seguito dell’applicazione riuscita.	[UC37]
FROb209	Il Sistema deve gestire errori durante l’applicazione della remediation documentale notificando il fallimento all’utente.	[UC37.0.1]
FROb210	Il Sistema deve consentire all’Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all’analisi della documentazione.	[UC38]

ID	Descrizione	Rif.
FROb211	Il Sistema deve consentire all'Utente Autorizzato di rifiutare una remediation relativa all'analisi della documentazione.	[UC38]
FROb212	Il Sistema deve aggiornare lo stato della remediation documentale come "rifiutata" nella dashboard a seguito del rifiuto confermato dall'utente.	[UC38]
FROb213	Il Sistema deve garantire che il rifiuto di una remediation documentale non comporti alcuna modifica ai file sorgente o di documentazione del repository.	[UC38]
FROb214	Il Sistema deve rimuovere la remediation rifiutata dalla lista delle azioni pendenti dell'area "Documentazione" o marcarla visivamente come scartata.	[UC38]
FROb215	Il Sistema deve mostrare all'Utente Autorizzato una conferma visiva dell'avvenuto rifiuto della proposta correttiva.	[UC38]
FROb216	Il Sistema deve consentire all'Utente Avanzato di richiedere un'analisi per un repository GitHub privato a condizione che l'integrazione GitHub sia attiva.	[UC39]
FROb217	Il Sistema deve validare la presenza di un'integrazione GitHub valida prima di accettare la richiesta di analisi per una risorsa privata.	[UC39]
FROb218	Il Sistema deve inibire la richiesta di analisi privata se l'utente non seleziona almeno un'area di interesse (Codice, Sicurezza, Documentazione).	[UC39]
FROb219	Il Sistema deve consentire all'Utente Avanzato di inserire l'URL di un repository privato di sua proprietà nel proprio catalogo personale.	[UC40]
FROb220	Il Sistema deve impedire l'inserimento di un URL repository già presente nel catalogo personale dell'Utente Avanzato, notificando la duplicazione.	[UC40.0.1]
FROb221	Il Sistema deve esporre all'Utente Avanzato la lista dei repository privati registrati, includendo per ciascuno il nome e l'URL della risorsa.	[UC41]
FROb222	Il Sistema deve visualizzare un'informativa specifica che suggerisce l'inserimento della prima risorsa qualora il catalogo privato risulti vuoto.	[UC41.0.1]

ID	Descrizione	Rif.
FROb223	Il Sistema deve consentire la rimozione di un repository dal catalogo privato previa conferma esplicita dell'utente.	[UC42.1]
FROb224	In caso di annullamento della procedura di rimozione, il Sistema deve garantire l'integrità del catalogo mantenendo la risorsa selezionata.	[UC42.1.1]
FROb225	Il Sistema deve mostrare all'Utente Avanzato l'elenco dei profili autorizzati alla consultazione dei report per un repository privato selezionato.	[UC43]
FROb226	Il Sistema deve informare l'utente proprietario qualora l'accesso ai report di un repository privato sia limitato esclusivamente al suo profilo.	[UC43.0.1]
FROb227	Il Sistema deve consentire l'aggiunta di un utente autorizzato tramite l'inserimento dello username o dell'indirizzo email del profilo destinatario.	[UC44.1]
FROb228	Il Sistema deve validare che l'identificativo inserito corrisponda a un profilo effettivamente registrato nella piattaforma.	[UC44.1.2]
FROb229	Il Sistema deve impedire l'autorizzazione multipla del medesimo profilo per lo stesso repository privato.	[UC44.1.3]
FROb230	Il Sistema deve consentire la revoca dei permessi di consultazione per un utente precedentemente autorizzato a seguito di conferma del proprietario.	[UC45.1]
FROb231	Il Sistema deve consentire la rimozione di una raccolta di report senza che questo comporti l'eliminazione dei singoli report di analisi in essa contenuti.	[UC46]
FROb232	Il Sistema deve richiedere l'inserimento della password attuale come verifica di identità obbligatoria prima di avviare la cancellazione dell'account.	[UC47]
FROb233	Il Sistema deve mostrare un avviso di irreversibilità prima della cancellazione definitiva del profilo, consentendo l'annullamento dell'operazione.	[UC47.1]
FROb234	A seguito della cancellazione del profilo, il Sistema deve rimuovere i dati personali e le associazioni OAuth, invalidando ogni credenziale di accesso precedente.	[UC47]

Requisiti di Qualità (QR)

I seguenti requisiti garantiscono che il sistema sia manutenibile, performante e strutturato secondo gli standard di eccellenza ingegneristica definiti dal team.

ID	Descrizione	Fonti
QROb1	L'architettura deve garantire un'alta coesione e un basso accoppiamento tra l'orchestratore NestJS e gli agenti Python, verificabile tramite revisione dei diagrammi UML2.5.	Interno (Obiettivi di Qualità)
QROb2	Il sistema deve garantire tempi di risposta della dashboard web ottimizzati, minimizzando il carico computazionale lato client durante il rendering dei report di audit.	Interno (Efficienza)
QROb3	Ogni componente software deve essere testabile isolatamente; la logica di business deve essere separata dalle interfacce di comunicazione (API/Database).	Interno (Manutenibilità)
QROb4	È necessario rispettare rigorosamente le metriche di qualità del codice (complessità ciclomatica, duplicazione) definite nelle Norme di Progetto .	Interno

Requisiti di Vincolo (VR)

Requisiti imposti dal committente riguardanti tecnologie, standard di sicurezza e documentazione obbligatoria.

ID	Descrizione	Fonti
VROb1	Il team deve svolgere un'attività di analisi preliminare includendo Design Thinking, User Story Mapping, Business Requirements e Diagrammi UML degli Use Case	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb2	Deve essere fornita documentazione tecnica tramite standard OpenAPI 3.0 (Swagger) per le API e documentazione del codice sorgente tramite TypeDoc	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb3	Deve essere fornito un Manuale Utente e un Manuale Manutentore (installazione e integrazione agenti) come parte integrante della fornitura finale	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb4	Al termine del progetto deve essere consegnato un MVP funzionante accompagnato da una Demo Live e dallo Schema Design relativo alla base dati	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb5	Il codice prodotto deve raggiungere una copertura minima del 70% tramite test di unità automatizzati misurati con Jest	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb6	L'applicativo deve essere creato seguendo principi di modularità per consentire l'estensione delle funzioni e l'aggiunta di nuovi agenti di analisi	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb7	Deve essere fornito un sistema di Bug Reporting strutturato su GitHub Issues per tracciare e gestire le anomalie tramite apposite label	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb8	Il Back-end e l'Orchestratore devono essere sviluppati utilizzando NestJS v10+, il Front-end in React v18.3+ e gli agenti in Python v3.12+	Capitolato di Progetto, Sez. "Tecnologie"
VROb9	L'architettura deve essere ospitata su infrastruttura cloud AWS, utilizzando esclusivamente gli account IAM forniti dall'azienda proponente	Capitolato di Progetto, Sez. "Tecnologie"

ID	Descrizione	Fonti
VROb10	Devono essere utilizzate GitHub Actions per implementare pipeline di Continuous Integration e Continuous Deployment (CI/CD)	Capitolato di Progetto, Sez. "Tecnologie"
VROb11	Il codice sorgente deve essere versionato utilizzando Git (v2.40+) seguendo la branching strategy definita nelle NdP	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb12	L'analisi di sicurezza deve essere conforme agli standard OWASP Top 10 (v2021 o successivi)	Capitolato di Progetto, Sez. "OWASP"
VROb13	L'interfaccia web deve essere compatibile con Windows 10/11, macOS 14+ e distribuzioni Linux (Ubuntu 22.04+) su browser Chrome 120+, Firefox 120+ e Safari 17+	