



---

# Analisi dei Requisiti

v0.46

---

## Registro delle Modifiche

Data	Versione	Descrizione	Redattore	Verificatore
2026/02/18	0.47.0	Refactoring generale di tutti casi d'uso con riscrittura di molti di essi	Basso Kevin	
2026/02/16	0.46.0	Inserimento UC 47-53 e requisiti	Sandu Antonio	
2026/02/15	0.45.1	Fix UC20-30, eliminazione UC23	Sgreva Andrea	
2026/02/15	0.45.0	Modifica UC 16 e 19, aggiunta UC 41-46 e requisiti	Sandu Antonio	
2026/02/13	0.44.7	Fix UC6, UC37-41	Sgreva Andrea	
2026/02/13	0.44.6	Fix UC5, UC9-11	Sandu Antonio	
2026/02/10	0.44.5	Fix vari degli UC + fix specifici UC13-15	Sgreva Andrea	
2026/02/10	0.44.4	Fix della posizione del sistema in tutti i diagrammi UC	Sgreva Andrea	
2026/02/10	0.44.3	Primo fix generale UC	Sgreva Andrea	
2026/02/09	0.44.2	Sistemato formato dei link al glossario	Sandu Antonio	
2026/02/09	0.44.1	Fix definizione attori	Sgreva Andrea	
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	
2026/02/04	0.43.0	Classificazione Requisiti per priorità	Zago Alice	
2026/02/04	0.42.1	Sistemata la sezione Attori + immagini separate per Front-end e Back-end	Sgreva Andrea	
2026/02/03	0.42.0	Aggiunta diagrammi UC16-30	Sgreva Andrea	

Data	Versione	Descrizione	Redattore	Verificatore
2026/02/02	0.41.0	Fix e aggiunta diagrammi mancanti UC6, UC9, UC10, UC12, UC13, UC14, UC15	Sgreva Andrea	
2026/02/02	0.40.0	Fix e aggiunta diagrammi mancanti UC1-3	Sgreva Andrea	
2026/02/01	0.39.0	Aggiunta Requisiti di Qualità e di Vincolo	Zago Alice	
2026/01/27	0.38.0	Aggiunta dei requisiti funzionali UC36-UC29	Sgreva Andrea	
2026/01/25	0.37.2	Fix alla struttura delle precondizioni, modifica a UC1-3 e relativi requisiti	Sandu Antonio	
2026/01/24	0.37.1	Fix alla struttura di inclusioni ed estensioni	Sandu Antonio	
2026/01/24	0.37.0	Inserimento diagrammi per UC36-41	Sgreva Andrea	
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	
2026/01/21	0.35.0	Inserimento diagrammi aggiornati per UC1-5 e UC26-37	Sandu Antonio	
2026/01/21	0.34.0	Aggiunta di sottocasi di UC21 e 30 e altri fix	Berengan Riccardo	
2026/01/19	0.33.1	Aggiunti requisiti funzionali UC12 e UC13, UC16-UC20 e UC20-UC20. Modifica requisiti UC5-UC15	Zago Alice	
2026/01/18	0.32.1	Riorganizzazione requisiti funzionali	Zago Alice	

Data	Versione	Descrizione	Redattore	Verificatore
		relativi ai casi d'uso da UC1 a UC4		
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	
2026/01/17	0.30.1	Modifica UC22. Aggiunta UC23, UC24	Berengan Riccardo	
2026/01/16	0.29.0	Aggiunta UC36, UC28, UC28.1, UC29	Sgreva Andrea	
2026/01/16	0.28.0	Aggiunta UC26, UC27, UC36 e UC37	Sandu Antonio	
2026/01/16	0.27.0	Aggiunta UC21 e UC22	Berengan Riccardo	
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	
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
2026/01/09	0.20.0	Requisiti da UC6 a UC8	Zago Alice	

Data	Versione	Descrizione	Redattore	Verificatore
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	
2026/01/06	0.17.0	Casi d'uso UC14, UC14.1, UC14.1.1 e UC14.2. Requisiti relativi a UC14	Zago Alice	
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. Rivalutare UC5 per maggiore chiarezza	Suar Alberto	Basso Kevin

Data	Versione	Descrizione	Redattore	Verificatore
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 (compresi di estensioni)	Suar Alberto	Basso Kevin

Data	Versione	Descrizione	Redattore	Verificatore
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

<b>Introduzione .....</b>	<b>15</b>
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
<b>Casi d'Uso .....</b>	<b>18</b>
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 .....	34

---

UC5.1: Visualizzazione informazioni identificative repository .....	35
UC6: Visualizzazione report di analisi repository .....	35
UC6.1: Selezione sezioni del report .....	36
UC6.1.1: Visualizzazione informativa nessuna sezione selezionata .....	36
UC6.2: Visualizzazione metadati del report .....	37
UC6.2.1: Visualizzazione data report .....	37
UC6.2.2: Visualizzazione commit analizzato .....	38
UC6.2.3: Visualizzazione richiedente report .....	38
UC6.3: Visualizzazione sezioni analitiche e remediation .....	38
UC6.3.1: Visualizzazione lista remediation .....	39
UC6.3.1.1: Visualizzazione messaggio assenza criticità .....	40
UC7: Selezione intervallo temporale per confronto report .....	40
UC7.0.1: Visualizzazione errore intervallo non inserito .....	41
UC7.0.2: Visualizzazione informativa assenza report nel periodo .....	41
UC7.0.3: Visualizzazione errore intervallo incoerente .....	41
UC7.0.4: Visualizzazione errore intervallo troppo ampio .....	42
UC8: Visualizzazione metriche comparative tra report .....	42
UC9: Visualizzazione sezione analisi del codice .....	42
UC9.1: Visualizzazione sezione analisi statica del codice .....	43
UC9.2: Visualizzazione sezione test di unità .....	43
UC9.3: Visualizzazione remediation sezione codice .....	44
UC9.3.1: Visualizzazione informativa assenza remediation codice .....	44
UC10: Visualizzazione sezione analisi della sicurezza .....	45
UC10.1: Visualizzazione sezione analisi librerie e dipendenze .....	45
UC10.2: Visualizzazione sezione analisi sicurezza OWASP .....	46
UC10.3: Visualizzazione remediation sezione sicurezza .....	46
UC10.3.1: Visualizzazione informativa assenza remediation sicurezza .....	46
UC11: Visualizzazione sezione analisi della documentazione .....	47
UC11.1: Visualizzazione sezione errori di sintassi .....	48
UC11.2: Visualizzazione completezza della documentazione .....	48
UC11.3: Visualizzazione remediation sezione documentazione .....	48
UC11.3.1: Visualizzazione informativa assenza remediation documentazione .....	49
UC12: Visualizzazione ranking dei repository analizzati .....	49
UC12.1: Visualizzazione informativa assenza dati per ranking .....	50
UC13: Disconnessione account GitHub da CodeGuardian .....	50
UC14: Esportazione report di analisi .....	51
UC14.1: Selezione formato di esportazione .....	51
UC14.1.1: Visualizzazione errore formato mancante .....	52
UC14.2: Conferma esportazione .....	52
UC15: Modifica password profilo .....	53
UC15.1: Inserimento password corrente .....	53
UC15.1.1: Visualizzazione errore password corrente mancante .....	54
UC15.1.2: Visualizzazione errore password corrente errata .....	54
UC15.2: Inserimento nuova password .....	55
UC15.2.1: Visualizzazione errore nuova password mancante .....	55
UC15.2.2: Visualizzazione errore password non conforme .....	56
UC15.2.3: Visualizzazione errore password identica alla precedente .....	56
UC15.3: Conferma modifica password .....	56
UC15.4: Notifica avvenuta modifica password .....	57

---

UC16: Visualizzazione singola remediation di sezione generica .....	57
UC17: Verifica accessibilità repository GitHub .....	58
UC17.1: Comunicazione con GitHub .....	58
UC17.1.1: Errore di comunicazione con GitHub .....	59
UC17.2: Ricerca del repository .....	59
UC17.2.1: Accesso a repository privato .....	60
UC17.2.1.1: Repository inaccessibile .....	60
UC18: Accettazione di una singola remediation .....	61
UC19: Rifiuto di una singola remediation .....	62
UC20: Creazione raccolta report di analisi .....	63
UC20.0.1: Visualizzazione errore campi obbligatori mancanti .....	63
UC20.1: Inserimento nome raccolta .....	64
UC20.1.1: Visualizzazione errore nome non conforme .....	64
UC20.2: Inserimento URL repository GitHub .....	65
UC20.2.1: Visualizzazione errore URL non conforme .....	65
UC20.2.2: Visualizzazione errore repository non accessibile .....	66
UC20.2.3: Visualizzazione errore URL non inserito .....	66
UC20.3: Inserimento descrizione raccolta .....	66
UC21: Avvio analisi .....	67
UC21.1: Richiesta di clonazione del repository .....	67
UC21.1.1: Errore durante la clonazione del repository .....	68
UC21.2: Richiesta di analisi del codice .....	68
UC21.3: Richiesta di analisi della documentazione .....	68
UC21.4: Richiesta di analisi degli standard OWASP .....	69
UC22: Salvataggio stato analisi nel sistema di persistenza .....	69
UC22.0.1: Errore durante il salvataggio dello stato dell'analisi .....	69
UC23: Recupero dei risultati dagli strumenti di analisi .....	70
UC23.1: Fallimento parziale nel recupero dei risultati .....	71
UC24: Generazione del report finale .....	71
UC25: Salvataggio di un report .....	72
UC25.1: Errore durante il salvataggio del report .....	72
UC26: Invio notifica completamento dell'analisi del repository .....	73
UC26.1: Errore durante l'invio della notifica .....	73
UC27: Ricezione notifica completamento analisi .....	73
UC27.0.1: Notifica completamento analisi non ricevuta .....	74
UC28: Gestione errore critico durante l'analisi .....	74
UC28.0.1: Notifica errore critico non ricevuta .....	74
UC29: Gestione del codice OAuth GitHub .....	75
UC29.0.1: Fallimento della procedura di scambio OAuth .....	75
UC30: Visualizzazione singola remediation riguardante l'analisi del codice .....	76
UC31: Visualizzazione singola remediation riguardante l'analisi della sicurezza .....	76
UC32: Visualizzazione singola remediation riguardante l'analisi della documentazione .....	76
UC33: Accettazione singola remediation riguardante l'analisi del codice .....	77
UC33.0.1: Errore nell'applicazione della remediation codice .....	77
UC34: Rifiuto singola remediation riguardante l'analisi del codice .....	78
UC35: Accettazione singola remediation riguardante l'analisi della sicurezza .....	78
UC35.0.1: Errore nell'applicazione della remediation sicurezza .....	78
UC36: Rifiuto singola remediation riguardante l'analisi della sicurezza .....	79
UC37: Accettazione singola remediation riguardante l'analisi della documentazione .....	79

---

UC37.0.1: Errore nell'applicazione della remediation documentale .....	80
UC38: Rifiuto singola remediation riguardante l'analisi della documentazione .....	80
UC39: Richiesta analisi repository GitHub privato autorizzato .....	80
UC40: Inserimento di un proprio repository privato .....	81
UC40.0.1: Visualizzazione errore repository già presente .....	81
UC41: Visualizzazione catalogo repository privati inseriti .....	82
UC41.0.1: Visualizzazione informativa catalogo vuoto .....	82
UC42: Rimozione di un proprio repository privato .....	82
UC42.1: Conferma rimozione repository .....	83
UC42.1.1: Annullamento rimozione repository .....	83
UC43: Gestione permessi di accesso al repository privato .....	83
UC43.0.1: Visualizzazione informativa assenza utenti autorizzati .....	84
UC44: Aggiunta utente autorizzato .....	84
UC44.1: Inserimento credenziale utente da autorizzare .....	84
UC44.1.1: Visualizzazione errore formato identificativo non valido .....	85
UC44.1.2: Visualizzazione errore utente inesistente .....	85
UC44.1.3: Visualizzazione errore utente già autorizzato .....	85
UC44.1.4: Visualizzazione errore campo identificativo vuoto .....	85
UC45: Rimozione utente autorizzato .....	85
UC45.1: Conferma revoca autorizzazione .....	86
UC46: Rimozione di una raccolta di report .....	86
UC46.1: Conferma rimozione raccolta .....	86
UC46.1.1: Annullamento rimozione raccolta .....	87
UC47: Cancellazione profilo CodeGuardian .....	87
UC47.1: Conferma definitiva cancellazione profilo .....	88
<b>Requisiti di Sistema .....</b>	<b>89</b>
Requisiti Funzionali (FR) .....	89
Requisiti di Qualità (QR) .....	118
Requisiti di Vincolo (VR) .....	119

## Indice immagini

<b>Figure 1 UC1 - Registrazione .....</b>	<b>20</b>
<b>Figure 2 UC1.1 - Inserimento username .....</b>	<b>21</b>
<b>Figure 3 UC1.2 - Inserimento email .....</b>	<b>22</b>
<b>Figure 4 UC1.3 - Inserimento password .....</b>	<b>24</b>
<b>Figure 5 UC2 - Autenticazione .....</b>	<b>25</b>
<b>Figure 6 UC2.1 - Inserimento username .....</b>	<b>26</b>
<b>Figure 7 UC2.2 - Inserimento password .....</b>	<b>27</b>
<b>Figure 8 UC3 - Collegamento account GitHub .....</b>	<b>28</b>
<b>Figure 9 UC3.1 - Collegamento account GitHub .....</b>	<b>29</b>
<b>Figure 10 UC3.2 - Collegamento account GitHub .....</b>	<b>30</b>
<b>Figure 11 UC4 - Richiesta analisi repository GitHub .....</b>	<b>32</b>
<b>Figure 12 UC4.1 - Selezione aree di interesse .....</b>	<b>33</b>
<b>Figure 13 UC5 - Visualizzazione lista repository .....</b>	<b>34</b>
<b>Figure 14 UC6 - Visualizzazione report di analisi .....</b>	<b>35</b>
<b>Figure 15 UC6.1 - Selezione sezioni del report .....</b>	<b>36</b>
<b>Figure 16 UC6.2 - Visualizzazione metadati del report .....</b>	<b>37</b>
<b>Figure 17 UC6.3 - Visualizzazione sezioni analitiche e remediation .....</b>	<b>38</b>
<b>Figure 18 UC6.3.1 - Visualizzazione lista remediation .....</b>	<b>39</b>
<b>Figure 19 UC7 - Selezione intervallo temporale .....</b>	<b>40</b>
<b>Figure 20 UC9 - Visualizzazione sezione analisi del codice .....</b>	<b>42</b>
<b>Figure 21 UC9.3 - Visualizzazione remediation sezione codice .....</b>	<b>44</b>
<b>Figure 22 UC10 - Visualizzazione sezione analisi della sicurezza .....</b>	<b>45</b>
<b>Figure 23 UC10.3 - Visualizzazione remediation sezione sicurezza .....</b>	<b>46</b>
<b>Figure 24 UC11 - Visualizzazione sezione analisi della documentazione .....</b>	<b>47</b>
<b>Figure 25 UC11.3 - Visualizzazione remediation sezione documentazione .....</b>	<b>48</b>
<b>Figure 26 UC12 - Visualizzazione ranking dei repository analizzati .....</b>	<b>49</b>
<b>Figure 27 UC14 - Esportazione report .....</b>	<b>51</b>
<b>Figure 28 UC14.1 - Selezione formato di esportazione .....</b>	<b>51</b>
<b>Figure 29 UC15 - Modifica password .....</b>	<b>53</b>
<b>Figure 30 UC15.1 - Inserimento password corrente .....</b>	<b>53</b>
<b>Figure 31 UC15.2 - Inserimento nuova password .....</b>	<b>55</b>
<b>Figure 32 UC16 - Visualizzazione singola remediation di sezione generica .....</b>	<b>57</b>

---

<b>Figure 33 UC17 - Verifica accessibilità repository .....</b>	<b>58</b>
<b>Figure 34 UC17.1 - Comunicazione con GitHub .....</b>	<b>58</b>
<b>Figure 35 UC17.2 - Ricerca del repository .....</b>	<b>59</b>
<b>Figure 36 UC17.2.1 - Accesso a repository privato .....</b>	<b>60</b>
<b>Figure 37 UC18 - Accettazione di una singola remediation .....</b>	<b>61</b>
<b>Figure 38 UC19 - Rifiuto singola remediation generica .....</b>	<b>62</b>
<b>Figure 39 UC20 - Creazione raccolta report di analisi .....</b>	<b>63</b>
<b>Figure 40 UC20.1 - Inserimento nome raccolta .....</b>	<b>64</b>
<b>Figure 41 UC20.2 - Inserimento URL repository GitHub .....</b>	<b>65</b>
<b>Figure 42 UC21 - Avvio analisi .....</b>	<b>67</b>
<b>Figure 43 UC22 - Salvataggio stato analisi .....</b>	<b>69</b>
<b>Figure 44 UC23 - Recupero dei risultati dagli strumenti di analisi .....</b>	<b>70</b>
<b>Figure 45 UC25 - Salvataggio di un report .....</b>	<b>72</b>
<b>Figure 46 UC26 - Invio notifica completamento analisi .....</b>	<b>73</b>
<b>Figure 47 UC29 - Gestione OAuth .....</b>	<b>75</b>
<b>Figure 48 UC40 - Inserimento repository privato .....</b>	<b>81</b>

## Indice tabelle

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

## Introduzione

### Contesto del Progetto

Il presente documento descrive l'Analisi dei Requisiti<sup>G</sup> relativo al progetto Code Guardian<sup>G</sup>, commissionato dall'azienda Var Group<sup>G</sup> e realizzato dal gruppo di studenti Skarab Group<sup>G</sup> 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<sup>G</sup> e remediation<sup>G</sup> delle vulnerabilità del software. L'architettura si basa sul paradigma degli agenti<sup>G</sup> 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<sup>G</sup>).

### 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<sup>G</sup>) e per gli stakeholder<sup>G</sup>, perseguendo i seguenti obiettivi:

- modellare le interazioni tra gli utenti e il sistema attraverso la definizione formale dei casi d'uso<sup>G</sup>
- individuare e dettagliare i requisiti di sistema, distinguendo tra requisiti funzionali<sup>G</sup>, di qualità<sup>G</sup> e di vincolo<sup>G</sup>
- classificare i requisiti in base alla priorità negoziale e strategica (obbligatori<sup>G</sup>, opzionali<sup>G</sup>, desiderabili<sup>G</sup>), 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<sup>G</sup> sviluppa è un sistema software<sup>G</sup> multiagente<sup>G</sup> per l'analisi di repository<sup>G</sup> GitHub<sup>G</sup>. 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<sup>G</sup> 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<sup>G</sup>):

- **Audit del Codice:** Esecuzione di analisi statica<sup>G</sup> 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<sup>G</sup>.
- **Audit della Documentazione:** Controllo della completezza e della coerenza semantica della documentazione tecnica rispetto al codice sorgente, effettuato tramite LLM<sup>G</sup>.
- **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<sup>G</sup> 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 nel documento Norme di Progetto. Si rimanda a tale documento per la descrizione dettagliata della struttura dei campi (precondizioni, postcondizioni, scenari) e della sintassi UML<sup>G</sup> utilizzata.

### Attori

Gli attori<sup>G</sup> rappresentano le entità che interagiscono con il sistema Code Guardian<sup>G</sup>. 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
<b>Attori Primari (Utenti Umani)</b>	
<b>Utente non Registrato</b>	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.
<b>Utente non Autenticato</b>	Utente generico che accede alle funzionalità pubbliche della piattaforma (es. Home Page, Login, Registrazione) senza possedere o aver attivato una sessione valida.
<b>Utente Autorizzato</b>	Utente che ha completato con successo la procedura di autenticazione. Può configurare nuove analisi, consultare lo storico dei report e gestire il proprio profilo.
<b>Utente Avanzato</b>	Specializzazione dell'Utente Autorizzato che ha collegato il proprio account al provider GitHub <sup>G</sup> , abilitando l'accesso ai repository privati e funzionalità di integrazione avanzata.
<b>Attori Primari (Sistemi Interni)</b>	
<b>OrCHEstratore</b>	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.
<b>Attori Secondari (Sistemi Esterni)</b>	
<b>GitHub</b>	Piattaforma di hosting esterna. Interagisce con il sistema per fornire l'accesso al codice sorgente (via API o clone) e ai metadati dei repository.
<b>Servizi AWS</b>	Infrastruttura cloud esterna di Amazon Web Service <sup>G</sup> utilizzata dal sistema come ambiente di calcolo e storage per l'esecuzione delle analisi intensive.
<b>Servizio LLM</b>	Servizio esterno di Intelligenza Artificiale interrogato per l'analisi semantica della documentazione e la generazione dei suggerimenti di remediation.
<b>Strumenti di Analisi</b>	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

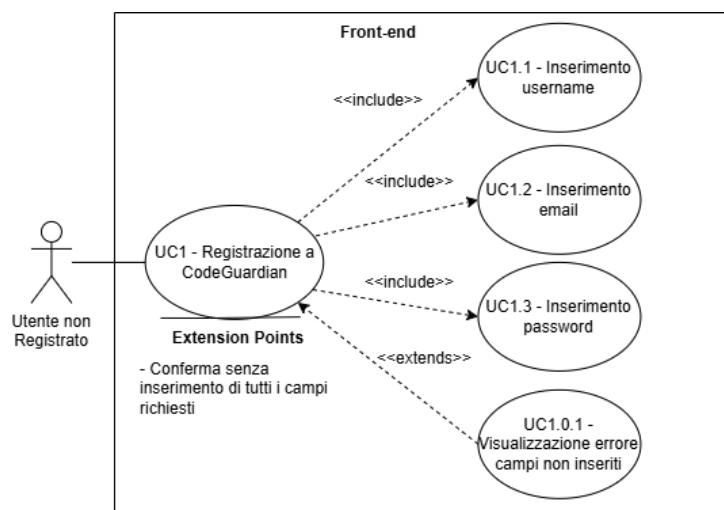


Figure 1: UC1 - Registrazione

- **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

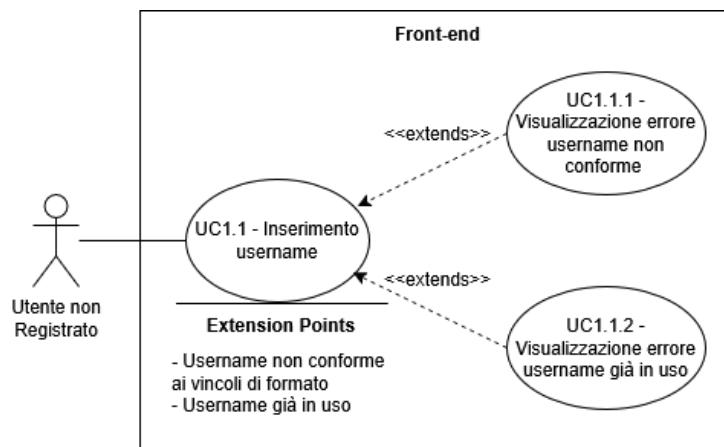


Figure 2: UC1.1 - Inserimento username

- **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**

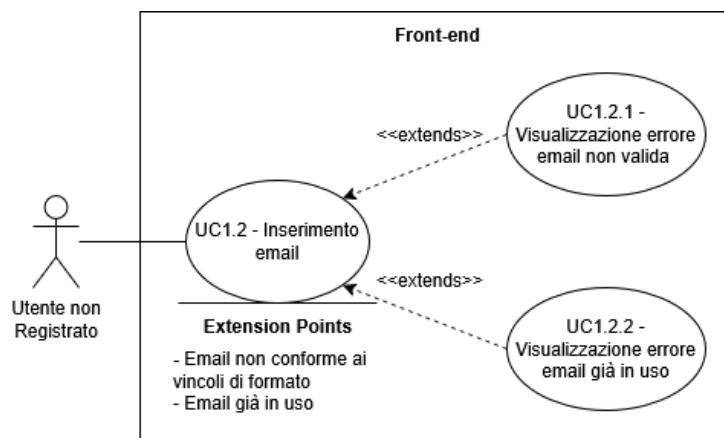


Figure 3: UC1.2 - Inserimento email

- **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

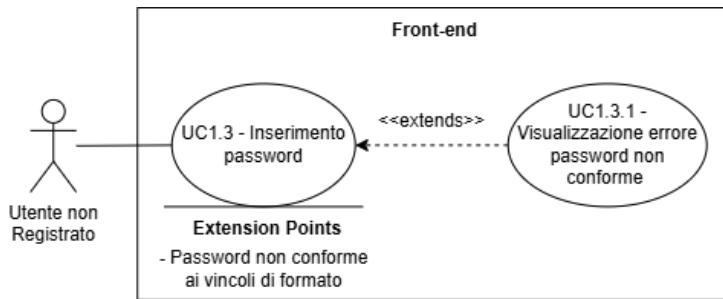


Figure 4: UC1.3 - Inserimento password

- **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

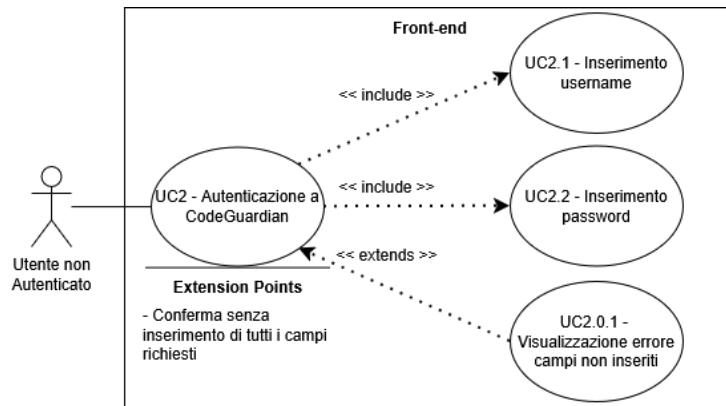


Figure 5: UC2 - Autenticazione

- **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

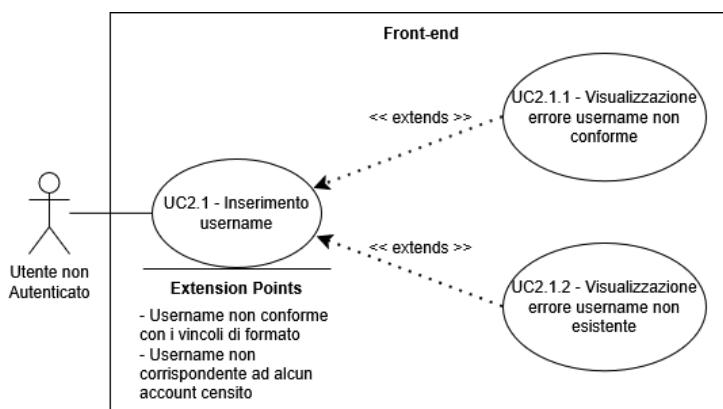


Figure 6: UC2.1 - Inserimento username

- **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**

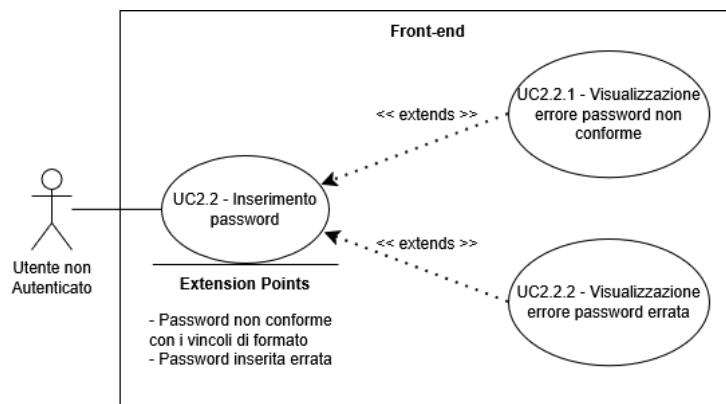


Figure 7: UC2.2 - Inserimento password

- **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

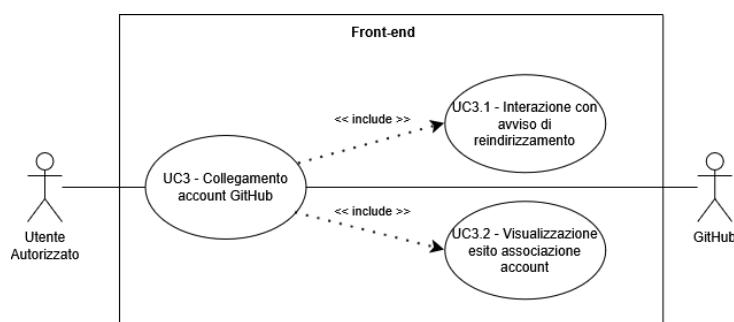
**UC3: Collegamento account GitHub**

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

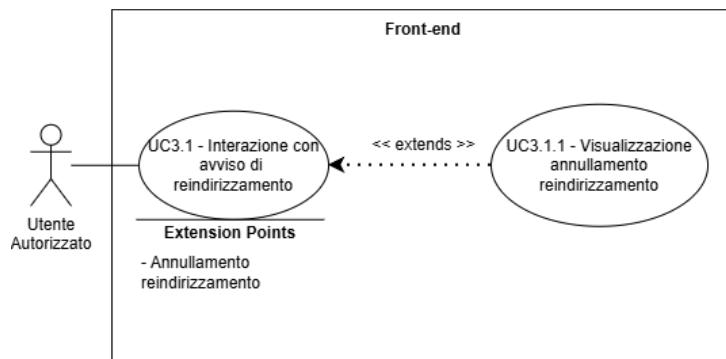


Figure 9: UC3.1 - Collegamento account GitHub

- **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

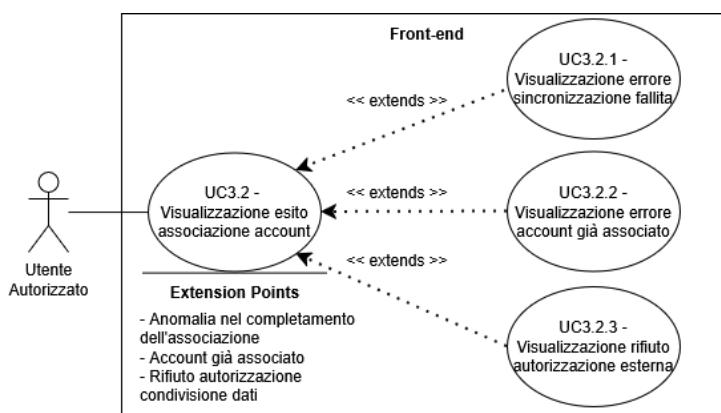


Figure 10: UC3.2 - Collegamento account GitHub

- **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

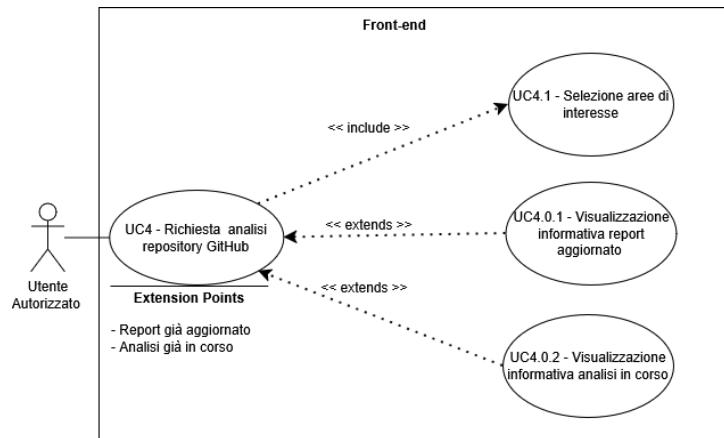


Figure 11: UC4 - Richiesta analisi repository GitHub

- **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 visualizza l'avviso di analisi già pendente per il medesimo repository
- **Scenario principale:**
  - L'utente visualizza un messaggio circa l'impossibilità di avviare un nuovo audit simultaneo
- **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

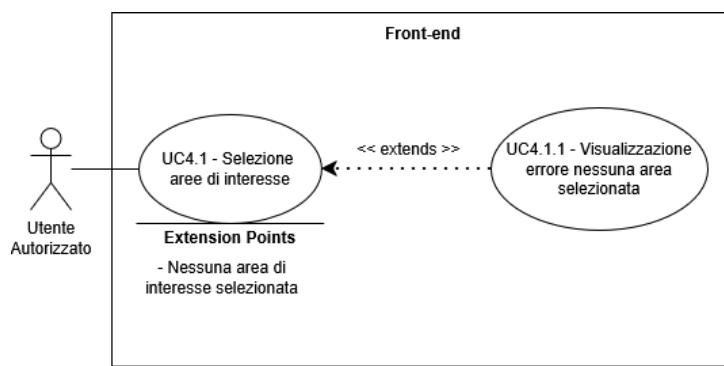


Figure 12: UC4.1 - Selezione aree di interesse

- **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

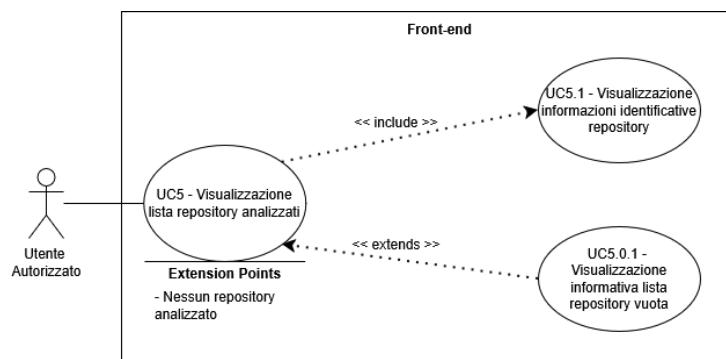
**UC5: Visualizzazione lista repository analizzati**

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
- **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]
- **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

#### UC5.1: 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

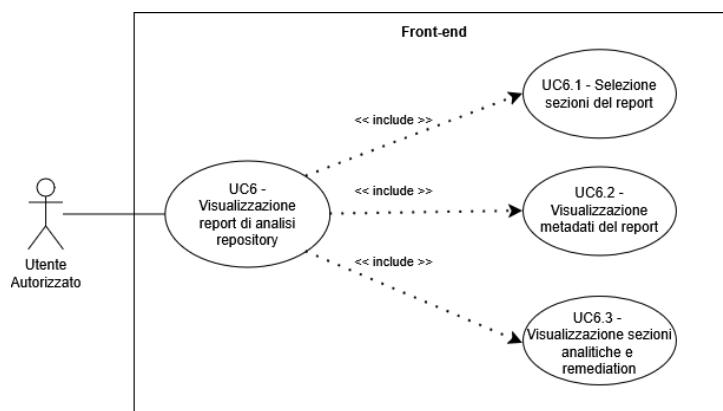


Figure 14: UC6 - Visualizzazione report di analisi

- **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

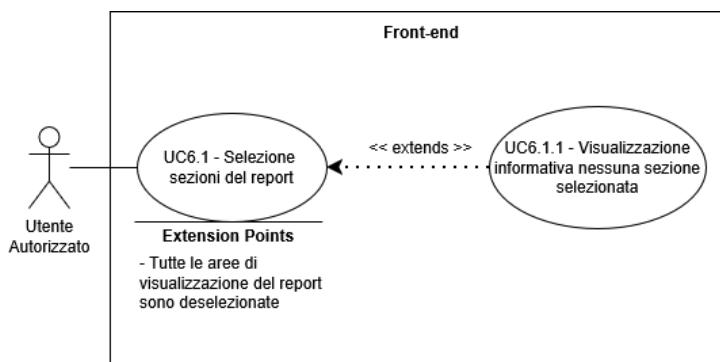


Figure 15: UC6.1 - Selezione sezioni del report

- 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 deseleziona 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 deseleziona tutte le aree di visualizzazione del report

### UC6.2: Visualizzazione metadati del report

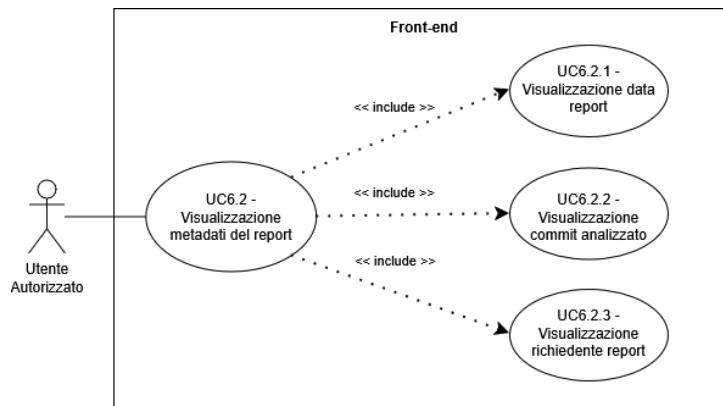


Figure 16: UC6.2 - Visualizzazione metadati del report

- **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 espone 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
- **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**

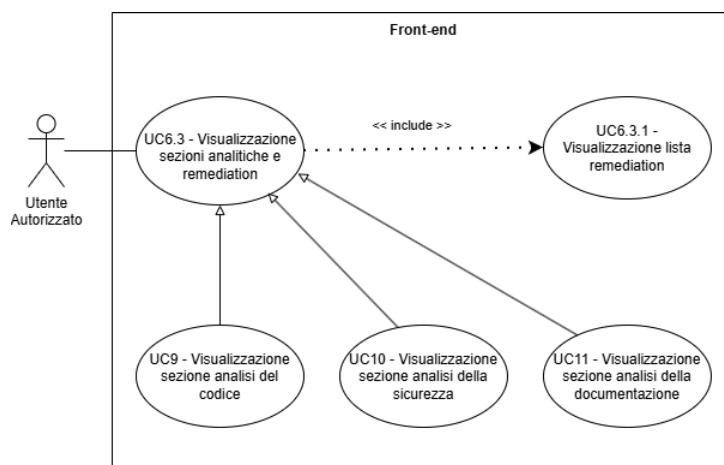


Figure 17: UC6.3 - Visualizzazione sezioni analitiche e remediation

- **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

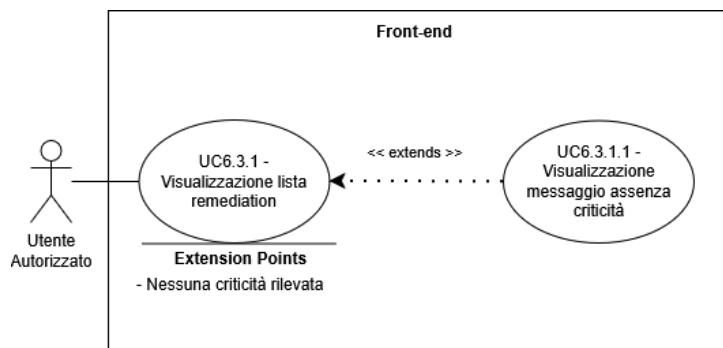


Figure 18: UC6.3.1 - Visualizzazione lista remediation

- **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
- **Trigger:** Il sistema non individua criticità o suggerimenti per la sezione selezionata

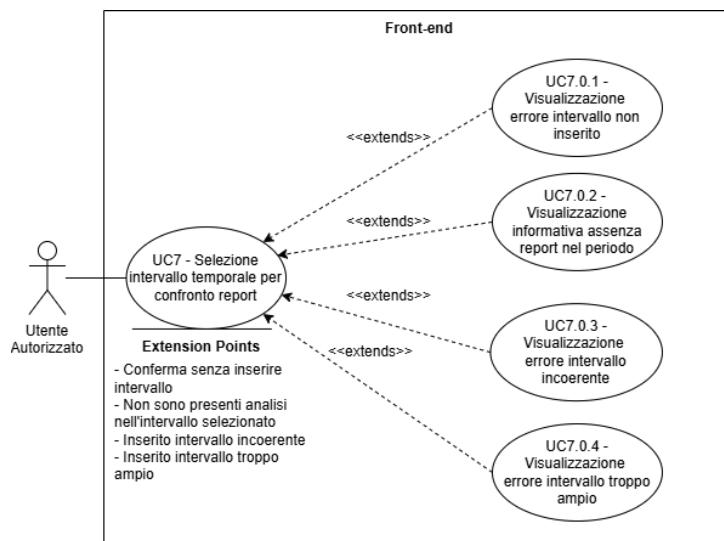
**UC7: Selezione intervallo temporale per confronto report**

Figure 19: UC7 - Selezione intervallo temporale

- **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**

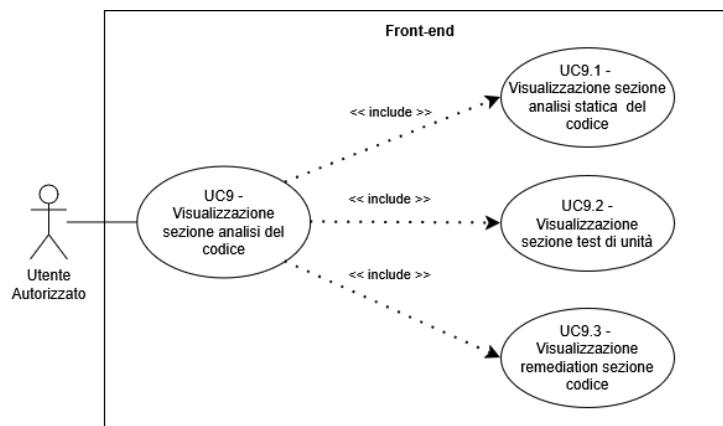


Figure 20: UC9 - Visualizzazione sezione analisi del codice

- **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

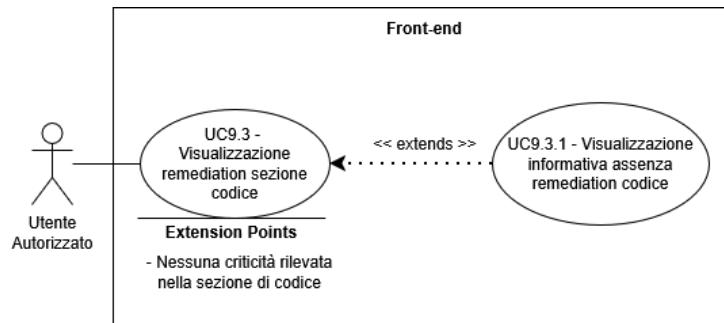


Figure 21: UC9.3 - Visualizzazione remediation sezione codice

- **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

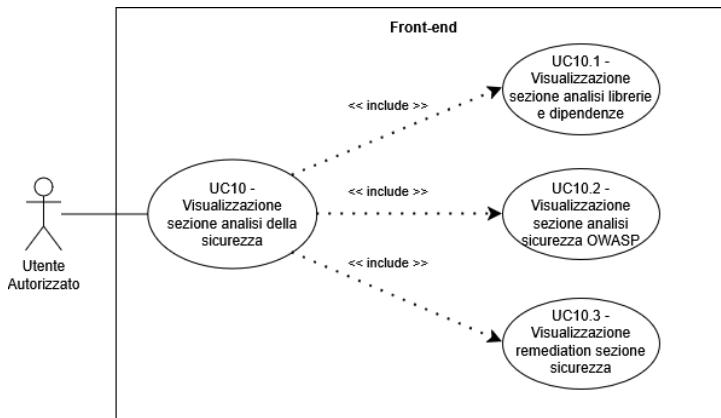


Figure 22: UC10 - Visualizzazione sezione analisi della sicurezza

- **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**

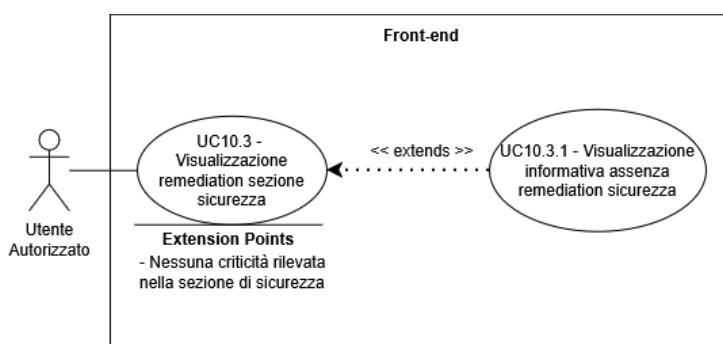


Figure 23: UC10.3 - Visualizzazione remediation sezione sicurezza

- **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

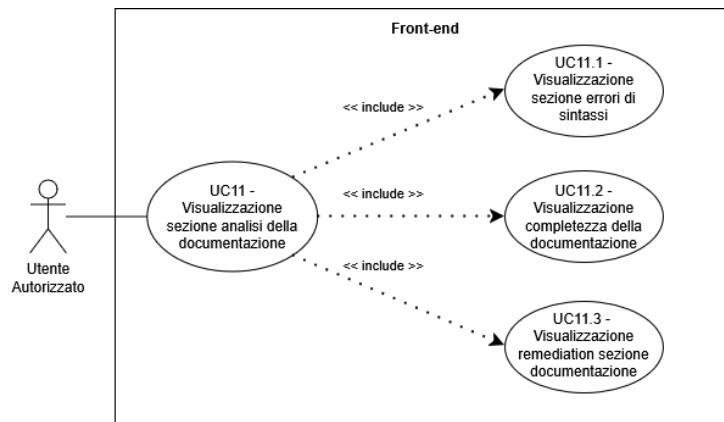


Figure 24: UC11 - Visualizzazione sezione analisi della documentazione

- **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**

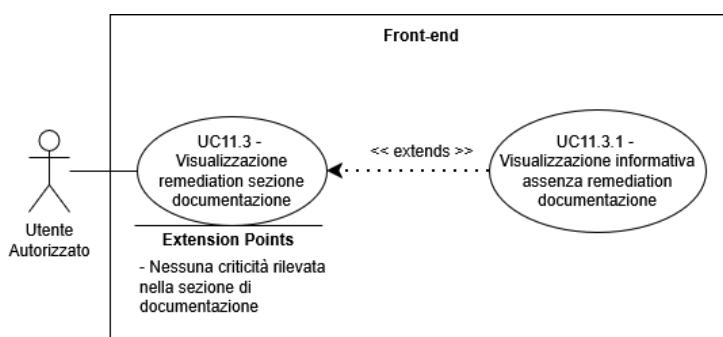


Figure 25: UC11.3 - Visualizzazione remediation sezione documentazione

- **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**

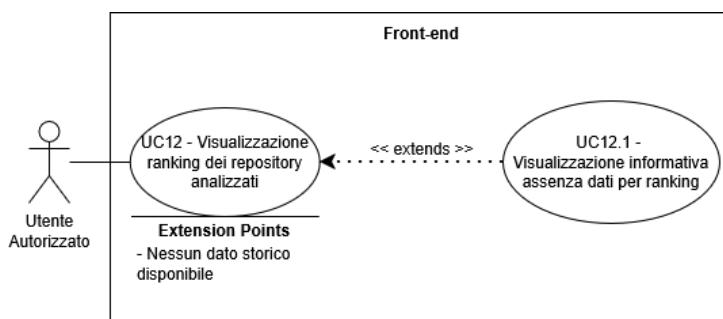


Figure 26: UC12 - Visualizzazione ranking dei repository analizzati

- **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

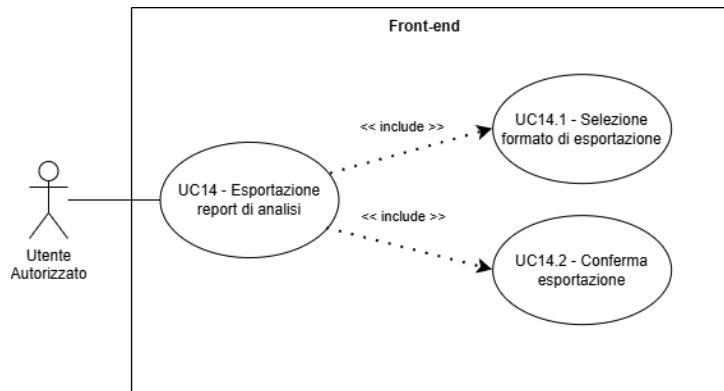


Figure 27: UC14 - Esportazione report

- **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

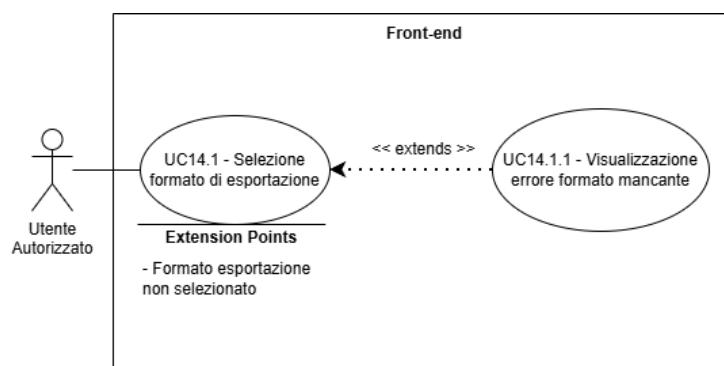


Figure 28: UC14.1 - Selezione formato di esportazione

- **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

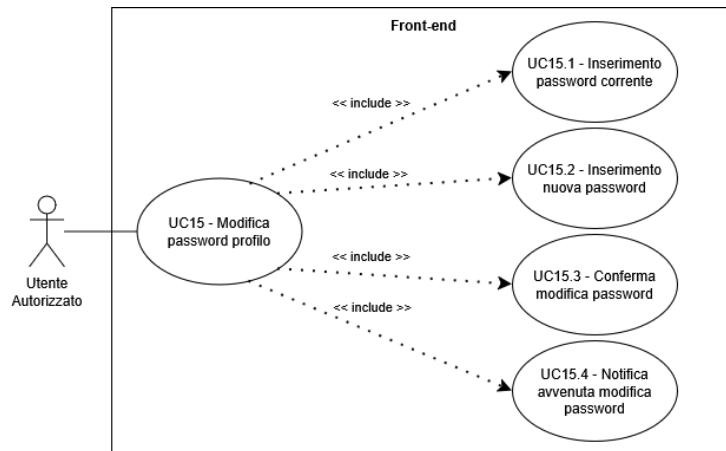


Figure 29: UC15 - Modifica password

- **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

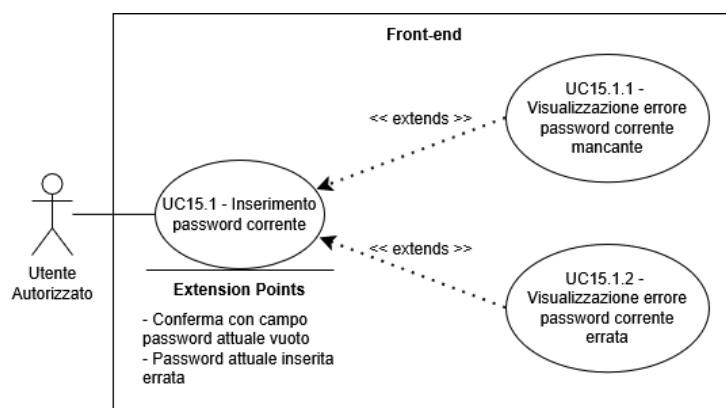


Figure 30: UC15.1 - Inserimento password corrente

- **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

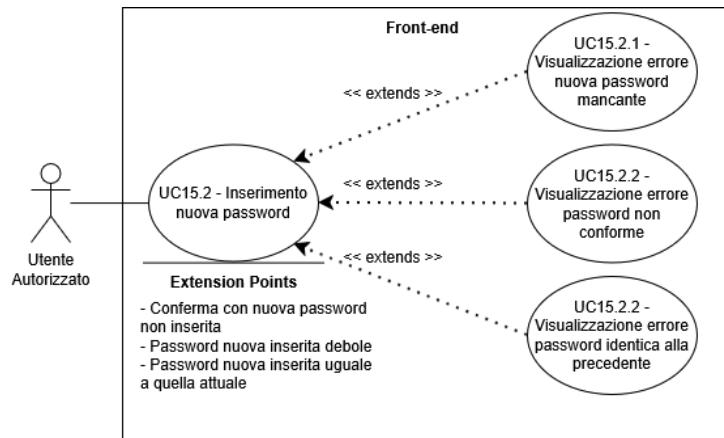


Figure 31: UC15.2 - Inserimento nuova password

- **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

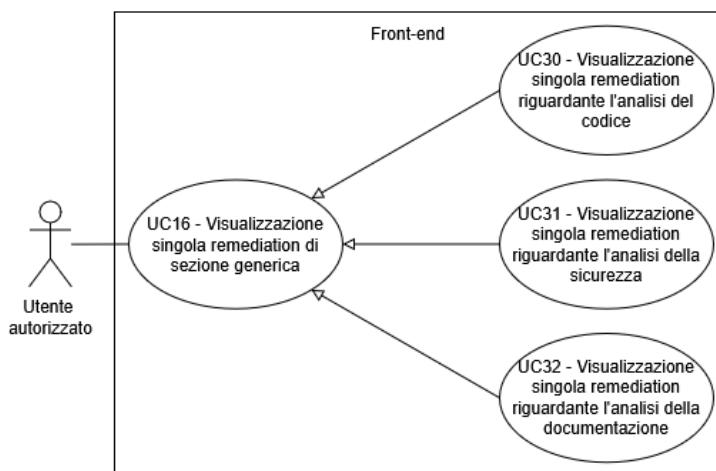
**UC16: Visualizzazione singola remediation di sezione generica**

Figure 32: UC16 - Visualizzazione singola remediation di sezione generica

- **Attore principale:** Utente Autorizzato
- **Pre-condizioni:**
  - L'utente sta visualizzando la lista delle remediation [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

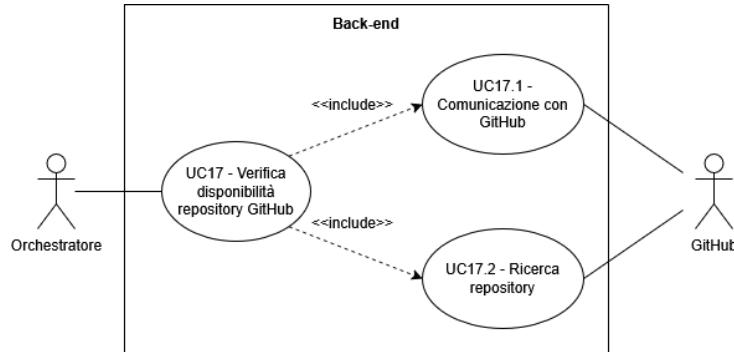


Figure 33: UC17 - Verifica accessibilità repository

- **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

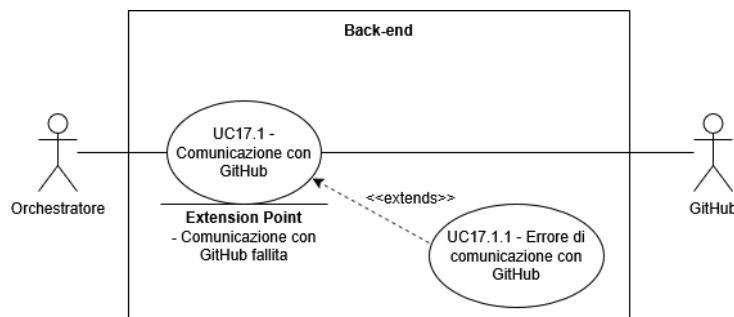


Figure 34: UC17.1 - Comunicazione con GitHub

- **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**

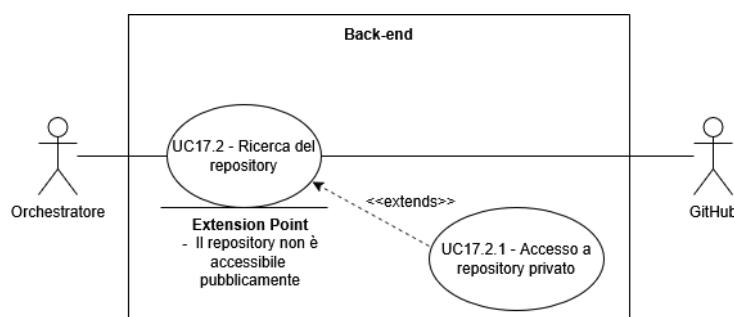


Figure 35: UC17.2 - Ricerca del repository

- **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

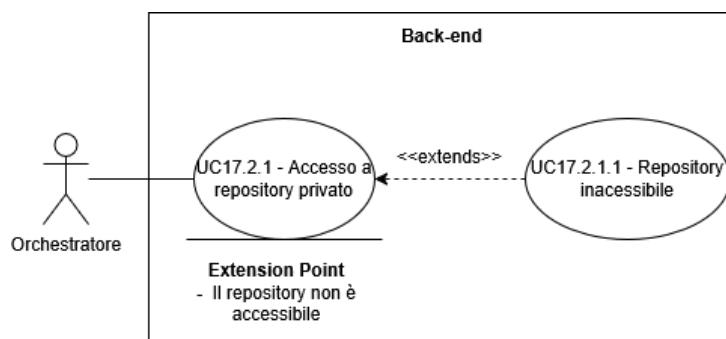


Figure 36: UC17.2.1 - Accesso a repository privato

- **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

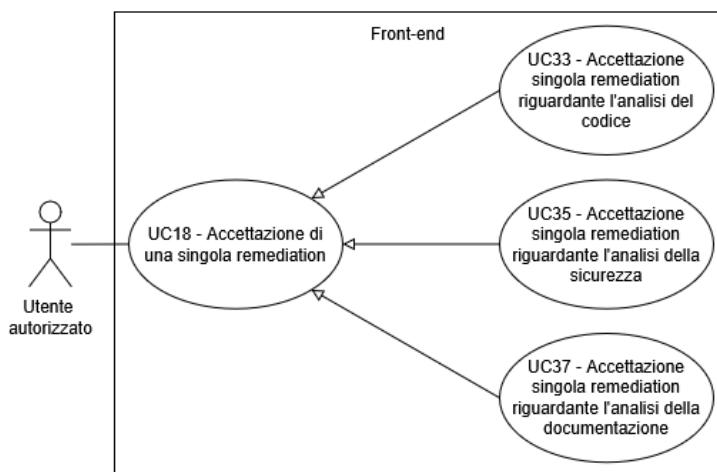


Figure 37: UC18 - Accettazione di una singola remediation

- **Attore principale:** Utente Autorizzato
- **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

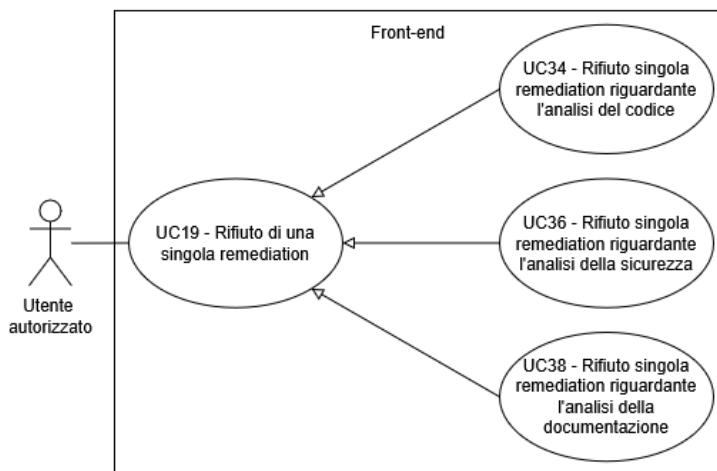


Figure 38: UC19 - Rifiuto singola remediation generica

- **Attore principale:** Utente Autorizzato
- **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

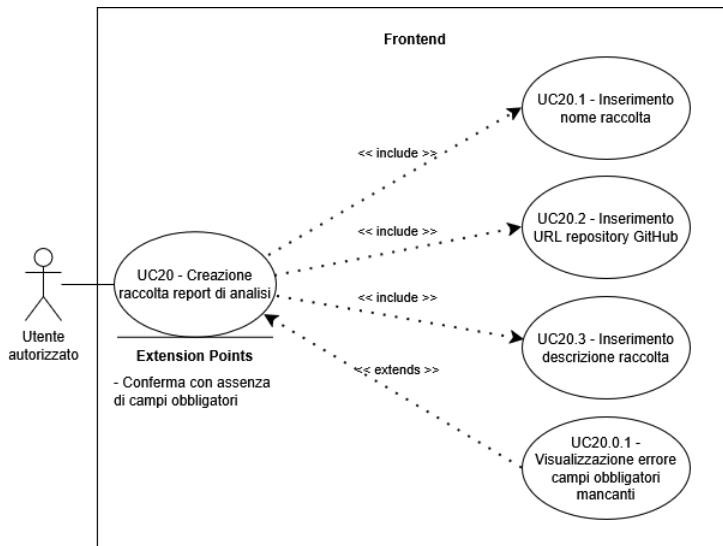


Figure 39: UC20 - Creazione raccolta report di analisi

- 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

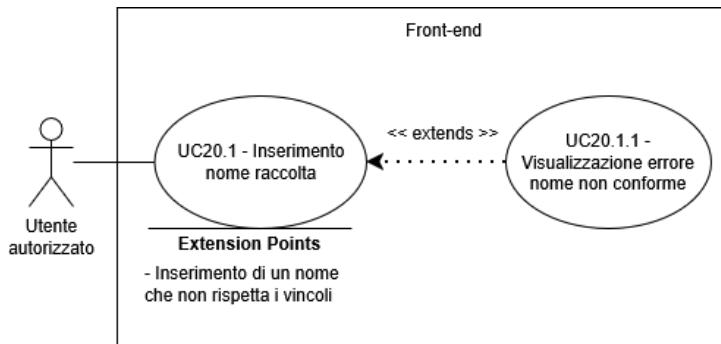


Figure 40: UC20.1 - Inserimento nome raccolta

- **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

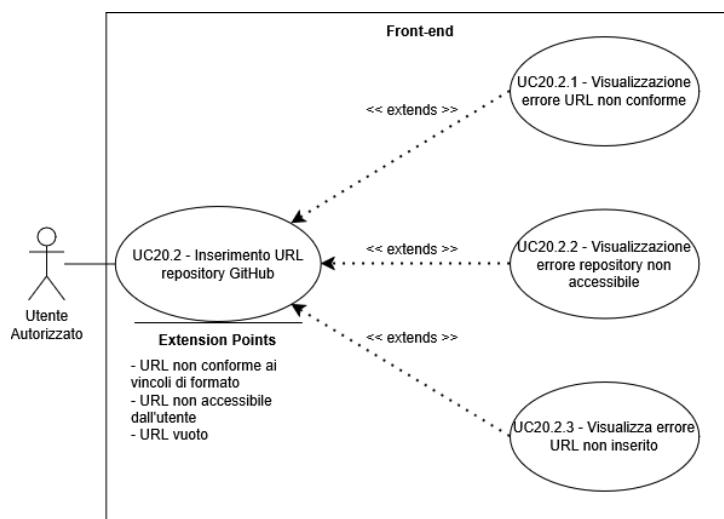


Figure 41: UC20.2 - Inserimento URL repository GitHub

- **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

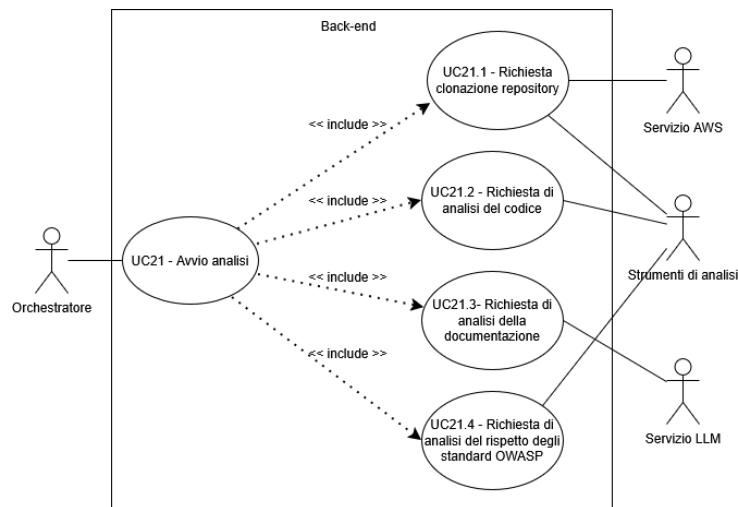


Figure 42: UC21 - Avvio analisi

- **Attore principale:** Orchestratore
- **Attore secondario:** Servizio AWS
- **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 gli standard OWASP [UC21.4]
- **Inclusioni:**
  - ▶ [UC21.1]
  - ▶ [UC21.2]
  - ▶ [UC21.3]
  - ▶ [UC21.4]
- **Trigger:** Convalida positiva delle autorizzazioni di accesso al repository remoto

### 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
- **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
- **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
- **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 all'agente incaricato dell'analisi qualitativa
- **Trigger:** Disponibilità locale dei sorgenti per l'audit documentale

#### **UC21.4: Richiesta di analisi degli standard OWASP**

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

#### **UC22: Salvataggio stato analisi nel sistema di persistenza**

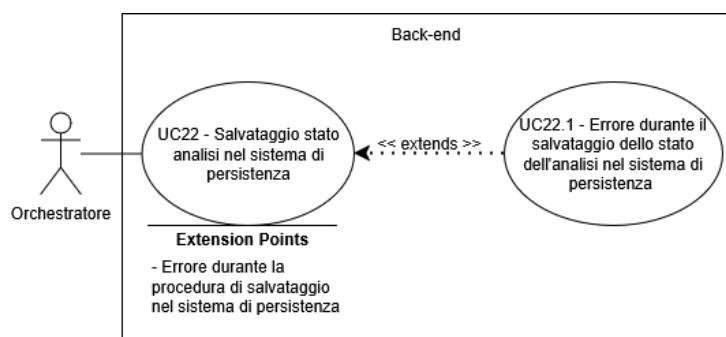


Figure 43: UC22 - Salvataggio stato analisi

- **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'utente visualizza 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

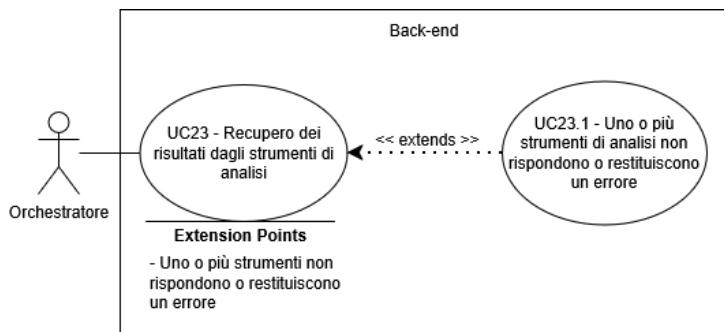


Figure 44: UC23 - Recupero dei risultati dagli strumenti di analisi

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
  - Gli strumenti esterni di analisi risultano in fase di esecuzione [UC21]
  - Lo stato dell'analisi risulta registrato come "pending" [UC22]
- **Post-condizioni:**
  - L'orchestratore dispone della totalità dei dati grezzi prodotti dagli strumenti di analisi consultati
- **Scenario principale:**
  - L'orchestratore monitora il completamento delle attività presso gli strumenti esterni
  - L'orchestratore acquisisce i file di output e i metadati generati da ciascuno strumento di analisi
- **Inclusioni:**
  - Nessuna
- **Estensioni:**
  - [UC23.1]
- **Trigger:** Gli strumenti esterni di analisi notificano la disponibilità dei risultati o concludono l'elaborazione

**UC23.1: Fallimento parziale nel recupero dei risultati**

- **Attore principale:** Orchestratore
- **Attore secondario:** Strumenti di Analisi
- **Pre-condizioni:**
  - L'orchestratore è in attesa dei dati dagli strumenti esterni [UC23]
- **Post-condizioni:**
  - La procedura di analisi prosegue utilizzando esclusivamente i risultati parziali ottenuti correttamente
  - L'utente viene informato circa l'incompletezza del report finale
- **Scenario principale:**
  - L'orchestratore rileva il superamento del tempo massimo di attesa (timeout) o riceve un messaggio di errore da uno o più strumenti
  - L'orchestratore registra l'anomalia specifica per lo strumento non rispondente
  - L'orchestratore genera una segnalazione per l'utente riguardante la parzialità dei dati acquisiti
- **Inclusioni:**
  - Nessuna
- **Estensioni:**
  - Nessuna
- **Trigger:** Mancata risposta o restituzione di un codice di errore da parte di uno strumento esterno entro i termini previsti

**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

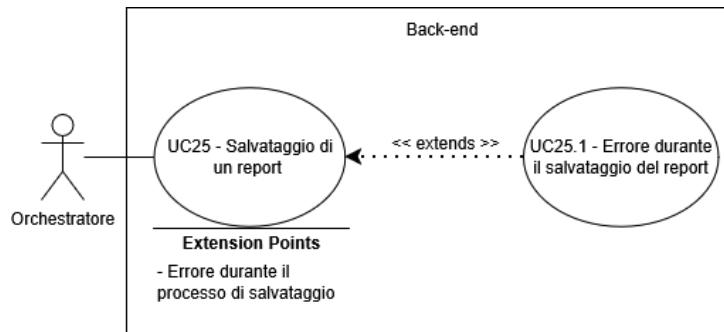


Figure 45: UC25 - Salvataggio di un report

- **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:**
  - [UC25.1]
- **Trigger:** Completamento delle operazioni di sintesi e aggregazione del report finale

#### UC25.1: 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

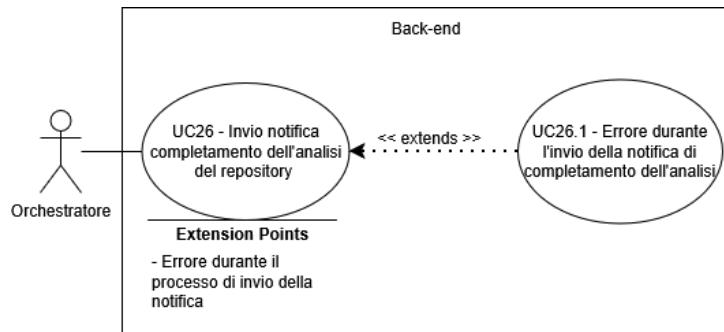


Figure 46: UC26 - Invio notifica completamento analisi

- **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:**
  - [UC26.1]
- **Trigger:** Avvenuto aggiornamento dello stato dell'analisi a 'completed' nel sistema di persistenza

#### UC26.1: 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

- **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
- **Trigger:** Mancata consegna o ricezione del messaggio informativo a seguito dell'invio

#### **UC28: Gestione 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:**
- **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
- **Trigger:** Mancata ricezione della comunicazione di errore

#### UC29: Gestione del codice OAuth GitHub

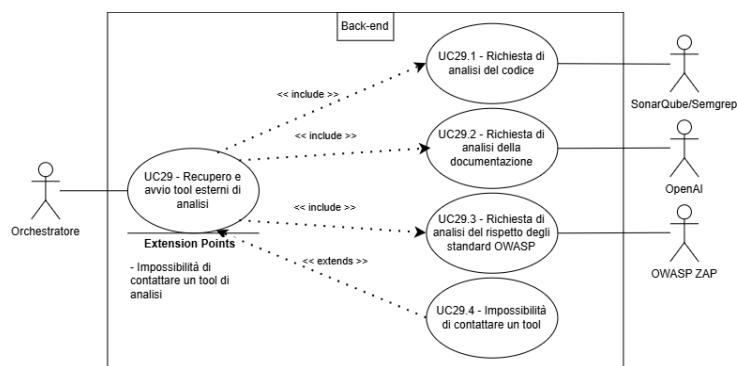


Figure 47: UC29 - Gestione OAuth

- **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

- **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]
- **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:**
  - [UC16]
- **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 Autorizzato
- **Pre-condizioni:**
  - L'utente visualizza l'elenco delle remediation nella sezione di analisi della sicurezza [UC10.3]
- **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:**
  - [UC16]
- **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 Autorizzato
- **Pre-condizioni:**
  - L'utente visualizza l'elenco delle remediation nella sezione di analisi della documentazione [UC11.3]
- **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:**
  - [\[UC16\]](#)
- **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**

- **Attore principale:** Utente Autorizzato
- **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 Autorizzato
- **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 Autorizzato
- **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 impartisce 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 impartisce il comando di rifiuto della remediation del codice
- **Specializzazione:**
  - [\[UC19\]](#)

**UC35: Accettazione singola remediation riguardante l'analisi della sicurezza**

- **Attore principale:** Utente Autorizzato
- **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 Autorizzato
- **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 Autorizzato
- **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 impedisce 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**

- **Attore principale:** Utente Autorizzato
- **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 Autorizzato
- **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 Autorizzato
- **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**

- **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
- **Specializzazione:**
  - [UC4]

#### **UC40: Inserimento di un proprio repository privato**

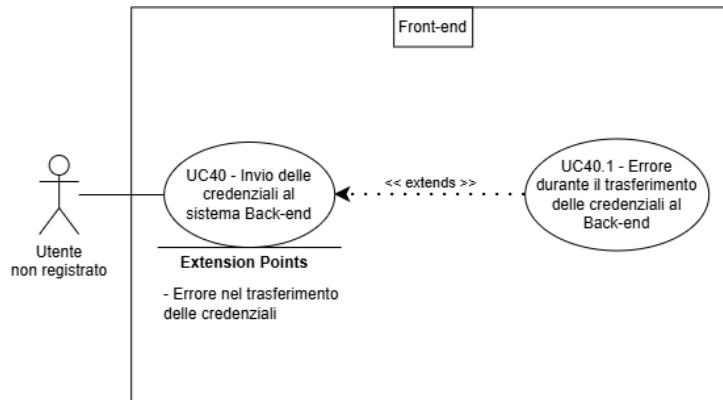


Figure 48: UC40 - Inserimento repository privato

- **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
- **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**

- **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**

- **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**

- **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**

- **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**

- **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**

- **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
- **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
- **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
- **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
- **Trigger:** Conferma con campo identificativo non popolato

**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**

- **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**

- **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**

- **Attore principale:** Utente Autenticato
- **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 Autenticato
- **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 *Requisiti* 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	L'utente deve visualizzare un messaggio di conferma esplicito a seguito della creazione corretta dell'account CodeGuardian.	[UC1]
FROb8	Il Sistema deve rilevare il tentativo di invio del modulo di registrazione in presenza di campi obbligatori vuoti.	[UC1.0.1]
FROb9	Il Sistema deve inibire la registrazione e notificare l'utente indicando specificamente quali dati obbligatori non sono stati inseriti.	[UC1.0.1]
FROb10	Il Sistema deve consentire l'immissione di un username alfanumerico con lunghezza compresa tra 4 e 20 caratteri.	[UC1.1]

ID	Descrizione	Rif.
FROb11	Il Sistema deve verificare l'univocità dello username rispetto agli account esistenti nel database.	[UC1.1]
FROb12	Il Sistema deve imporre vincoli di unicità lato persistenza su username per prevenire registrazioni duplicate anche in presenza di richieste concorrenti.	[UC1.1.2]
FROb13	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]
FROb14	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]
FROb15	Il Sistema deve consentire l'immissione di un indirizzo email composto da una parte locale, il carattere “@”, e un dominio contenente almeno un “.” con un TLD di lunghezza maggiore o uguale a 2 caratteri.	[UC1.2]
FROb16	Il Sistema deve rifiutare indirizzi email contenenti spazi o privi del carattere “@”.	[UC1.2.1]
FROb17	Il Sistema deve verificare l'univocità dell'indirizzo email rispetto agli account esistenti nel database.	[UC1.2]
FROb18	Il Sistema deve imporre vincoli di unicità lato persistenza su indirizzo email per prevenire registrazioni duplicate anche in presenza di richieste concorrenti.	[UC1.2.2]
FROb19	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 email già in uso.	[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 previsti.	[UC1.2.1]
FROb21	Il Sistema deve accettare una password solo se di lunghezza pari o superiore ad 8 caratteri.	[UC1.3]

ID	Descrizione	Rif.
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]
FROb24	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio che specifichi i requisiti di sicurezza non soddisfatti qualora la password inserita non rispetti i criteri stabiliti.	[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 con i dati registrati) al momento dell'invio del modulo di autenticazione.	[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 visualizzare un messaggio di conferma esplicito 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 nel record account recuperato tramite lo username, utilizzando la medesima funzione di hashing e il salt associato.	[UC2]

ID	Descrizione	Rif.
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 notificare l'utente dell'avvenuto lockout temporaneo e impedire ulteriori tentativi di autenticazione fino alla scadenza del periodo di blocco.	[UC2]
FROb35	Il Sistema deve rilevare campi incompleti nel login e inibire l'accesso notificando l'utente tramite avviso specifico che indichi i dati mancanti.	[UC2.0.1]
FROb36	Il Sistema deve consentire l'immissione di uno username conforme ai vincoli sintattici stabiliti per gli identificativi utente.	[UC2.1]
FROb37	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora lo username inserito non rispetti i vincoli sintattici previsti.	[UC2.1.1]
FROb38	Il Sistema deve notificare l'utente qualora l'identificativo (username) inserito non risulti censito nel sistema.	[UC2.1.2]
FROb39	Il Sistema deve accettare la password nel modulo di autenticazione solo se formalmente conforme ai vincoli di sistema stabiliti.	[UC2.2]
FROb40	Il Sistema deve inibire l'avanzamento della procedura e mostrare un messaggio di errore qualora la password inserita non sia formalmente conforme ai vincoli previsti.	[UC2.2.1]
FROb41	Il Sistema deve notificare l'utente qualora la password inserita non corrisponda a quella registrata e inibire l'accesso.	[UC2.2.2]
FROb42	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione dedicata al collegamento del profilo GitHub.	[UC3]
FROb43	Il Sistema deve consentire l'avvio della procedura di collegamento GitHub esclusivamente in presenza di una sessione attiva.	[UC3]

ID	Descrizione	Rif.
FROb44	Il Sistema deve impedire l'avvio della procedura di collegamento qualora un profilo GitHub risulti già associato all'account CodeGuardian dell'utente.	[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 confermare la volontà di procedere con il collegamento esterno.	[UC3.1]
FROb47	Il Sistema deve consentire all'utente di annullare il reindirizzamento tornando alla sezione integrazioni, annullando la procedura di collegamento.	[UC3.1.1]
FROb48	Il Sistema deve reindirizzare l'utente verso GitHub esclusivamente a seguito della conferma esplicita dell'avviso di reindirizzamento.	[UC3.1]
FROb49	Il Sistema deve elaborare l'esito della procedura di collegamento al ritorno dell'utente su CodeGuardian e visualizzare un messaggio di esito.	[UC3.2]
FROb50	In caso di esito positivo, il Sistema deve visualizzare la conferma dell'avvenuta sincronizzazione tra l'account CodeGuardian e il profilo GitHub.	[UC3.2]
FROb51	In caso di esito positivo, il Sistema deve memorizzare l'associazione tra l'account CodeGuardian e l'identificativo del profilo GitHub collegato.	[UC3]
FROb52	In caso di esito positivo, il Sistema deve autorizzare l'interazione con i repository GitHub dell'utente tramite le API GitHub utilizzando le credenziali ottenute in fase di autorizzazione.	[UC3]
FROb53	Il Sistema deve memorizzare i token di accesso ottenuti da GitHub esclusivamente in forma cifrata all'interno del database e associarli univocamente all'account CodeGuardian dell'utente.	[UC3]
FROb54	Il Sistema deve evitare la persistenza di token o associazioni qualora la procedura di collegamento non termini con esito positivo.	[UC3]

ID	Descrizione	Rif.
FROb55	Il Sistema deve notificare l'utente qualora la procedura di sincronizzazione fallisca per anomalie tecniche nella ricezione o nell'elaborazione dei dati di GitHub.	[UC3.2.1]
FROb56	Il Sistema deve consentire all'utente di ripetere la procedura di collegamento a seguito di fallimento tecnico della sincronizzazione.	[UC3.2.1]
FROb57	Il Sistema deve inibire il collegamento qualora il profilo GitHub risulti già associato a un altro account CodeGuardian e visualizzare un messaggio di errore dedicato.	[UC3.2.2]
FROb58	Il Sistema deve mostrare un messaggio di errore specifico qualora l'utente neghi il consenso alla condivisione dei dati su GitHub e considerare la procedura di collegamento come non completata.	[UC3.2.3]
FROb59	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione di configurazione dell'analisi del repository.	[UC4]
FROb60	Il Sistema deve consentire l'immissione dell'URL del repository GitHub nel modulo di richiesta analisi.	[UC4]
FROb61	Il Sistema deve inibire l'invio della richiesta e notificare l'utente qualora il campo URL non venga compilato.	[UC4]
FROb62	Il Sistema deve validare che l'URL del repository GitHub inserito utilizzi il protocollo "https://" e punti al dominio "github.com".	[UC4]
FROb63	Il Sistema deve inibire l'invio della richiesta e notificare l'utente qualora l'URL inserito non risulti valido secondo i vincoli di sistema.	[UC4]
FROb64	Il Sistema deve inibire l'invio della richiesta e notificare l'utente qualora il repository risulti inesistente o non accessibile dal sistema.	[UC4]
FROb65	Il Sistema deve validare lato server la titolarità o autorizzazione dell'utente sul repository GitHub prima di avviare l'analisi.	[UC4]
FROb66	Il Sistema deve impedire l'avvio di una nuova analisi e informare l'utente se il report esistente risulta già aggiornato rispetto allo stato corrente del repository.	[UC4.0.1]

ID	Descrizione	Rif.
FROb67	Il Sistema deve impedire l'invio di una nuova richiesta se un'analisi per il medesimo repository è già in fase di elaborazione e informare l'utente con un messaggio dedicato.	[UC4.0.2]
FROb68	Il Sistema deve permettere la selezione multipla delle aree di interesse tra test, sicurezza e documentazione.	[UC4.1]
FROb69	Il Sistema deve inibire la richiesta di analisi qualora non venga selezionata almeno un'area di interesse e notificare l'utente con un messaggio dedicato.	[UC4.1.1]
FROb70	Il Sistema deve consentire la navigazione verso la sezione riepilogativa dei repository analizzati.	[UC5]
FROb71	Il Sistema deve mostrare all'Utente Autorizzato l'elenco dei repository per i quali è stato generato almeno un report.	[UC5]
FROb72	Il Sistema deve ordinare l'elenco dei repository analizzati in ordine decrescente rispetto alla data dell'ultima analisi disponibile.	[UC5]
FROb73	Il Sistema deve esporre per ogni elemento della lista: nome del repository, URL di riferimento e data dell'ultima analisi.	[UC5.1]
FROb74	Il Sistema deve inibire la visualizzazione della lista e mostrare un'informativa specifica qualora non risultino repository analizzati.	[UC5.0.1]
FROb75	Il Sistema deve consentire la selezione di un repository dalla lista per aprire il report di dettaglio associato.	[UC6]
FROb76	Il Sistema deve consentire l'accesso al report di dettaglio esclusivamente per repository associati all'account dell'Utente Autorizzato.	[UC6]
FROb77	Il Sistema deve visualizzare il contenuto dettagliato del report di analisi relativo al repository selezionato.	[UC6]
FROb78	Il Sistema deve permettere di selezionare o deselectionare le aree analitiche (Codice, Sicurezza, Documentazione) da mostrare a video.	[UC6.1]

ID	Descrizione	Rif.
FROb79	Il Sistema deve aggiornare dinamicamente la visualizzazione del report in base alle sezioni selezionate o deselectionate dall'utente.	[UC6.1]
FROb80	Il Sistema deve inibire il rendering dei risultati analitici e mostrare un avviso informativo se nessuna area risulta selezionata.	[UC6.1.1]
FROb81	Il Sistema deve esporre i metadati generali del report selezionato.	[UC6.2]
FROb82	Il Sistema deve esporre il timestamp (data e ora) relativo al completamento dell'attività di audit.	[UC6.2.1]
FROb83	Il Sistema deve visualizzare l'identificativo univoco (hash) del commit GitHub oggetto dell'analisi.	[UC6.2.2]
FROb84	Il Sistema deve indicare lo username dell'Utente Autorizzato che ha sottomesso la richiesta di analisi.	[UC6.2.3]
FROb85	Il Sistema deve esporre metriche tecniche e criticità rilevate per ciascuna sezione selezionata dall'utente.	[UC6.3]
FROb86	Il Sistema deve presentare la lista delle azioni correttive (remediation) suggerite per i difetti individuati nelle sezioni selezionate.	[UC6.3.1]
FROb87	Il Sistema deve mostrare un messaggio informativo di esito positivo (assenza di criticità) qualora non risultino remediation necessarie per la sezione selezionata.	[UC6.3.1.1]
FROb88	Il Sistema deve consentire la selezione di un intervallo temporale (data inizio e data fine) per la generazione dell'analisi comparativa tra report.	[UC7]
FROb89	Il Sistema deve predisporre un comando di conferma per aggiornare la vista di confronto tra il report corrente e quelli compresi nell'intervallo selezionato.	[UC7]
FROb90	Il Sistema deve eseguire la validazione completa dell'intervallo temporale (presenza delle date, coerenza cronologica e rispetto dei limiti di ampiezza) al momento della conferma del confronto.	[UC7]
FROb91	Il Sistema deve notificare l'utente tramite avviso qualora i campi relativi all'intervallo temporale non siano popolati e inibire la generazione del confronto.	[UC7.0.1]

ID	Descrizione	Rif.
FROb92	Il Sistema deve validare la coerenza cronologica dell'intervallo, segnalando come errore una data di inizio successiva a quella di fine e inibendo la generazione del confronto.	[UC7.0.3]
FROb93	Il Sistema deve inibire la richiesta se l'intervallo temporale selezionato eccede l'ampiezza massima prevista e notificare l'utente con un messaggio dedicato.	[UC7.0.4]
FROb94	Il Sistema deve mostrare un'informativa specifica qualora non risultino report archiviati all'interno del periodo selezionato e non generare la vista comparativa.	[UC7.0.2]
FROb95	In caso di validazione positiva e presenza di report nel periodo selezionato, il Sistema deve visualizzare la comparazione tra il report corrente e quelli compresi nell'intervallo temporale definito.	[UC7]
FRDe96	Il Sistema deve generare rappresentazioni grafiche per monitorare l'andamento delle metriche tra i report inclusi nell'intervallo temporale.	[UC8]
FRDe97	Il Sistema deve permettere l'interazione con gli elementi del grafico per l'esposizione dei dati puntuali relativi a ogni singola analisi.	[UC8]
FRDe98	Il Sistema deve predisporre una tabella comparativa per il confronto testuale dei dati estratti dai report selezionati.	[UC8]
FRDe99	Il Sistema deve calcolare e visualizzare, all'interno della tabella, gli indicatori di variazione (trend) rispetto all'analisi cronologicamente precedente.	[UC8]
FRDe100	Il Sistema deve garantire che i dati visualizzati nella vista comparativa (grafici e tabella) siano coerenti con i report effettivamente inclusi nell'intervallo temporale selezionato.	[UC8]
FROb101	Il Sistema deve consentire la visualizzazione della sezione del report dedicata alla qualità del codice sorgente quando l'area "Codice" risulta selezionata nei filtri del report.	[UC9]

ID	Descrizione	Rif.
FROb102	Il Sistema deve esporre i risultati dell'analisi statica, specificando bug, vulnerabilità e code smell rilevati.	[UC9.1]
FROb103	Il Sistema deve esporre le metriche di copertura dei test di unità e l'esito complessivo delle suite di test eseguite.	[UC9.2]
FROb104	Il Sistema deve presentare l'elenco delle azioni correttive (remediation) specifiche per i difetti del codice individuati.	[UC9.3]
FROb105	Il Sistema deve mostrare un'informativa di esito positivo qualora non risultino remediation necessarie per l'area del codice sorgente.	[UC9.3.1]
FROb106	Il Sistema deve consentire la visualizzazione della sezione del report dedicata alla sicurezza del repository quando l'area "Sicurezza" risulta selezionata nei filtri di visualizzazione.	[UC10]
FROb107	Il Sistema deve esporre i risultati dell'analisi delle librerie e dipendenze, indicando dipendenze obsolete o affette da vulnerabilità note (CVE).	[UC10.1]
FROb108	Il Sistema deve mostrare i rilievi di conformità rispetto agli standard OWASP basati sulla Top 10 OWASP.	[UC10.2]
FROb109	Il Sistema deve presentare l'elenco delle azioni correttive (remediation) specifiche per le vulnerabilità rilevate nell'area sicurezza.	[UC10.3]
FROb110	Il Sistema deve mostrare un'informativa di esito positivo qualora non risultino vulnerabilità o minacce alla sicurezza che richiedano remediation.	[UC10.3.1]
FROb111	Il Sistema deve consentire la visualizzazione della sezione del report dedicata alla qualità della documentazione quando l'area "Documentazione" risulta selezionata nei filtri di visualizzazione.	[UC11]
FROb112	Il Sistema deve esporre gli errori sintattici rilevati nei file di documentazione analizzati.	[UC11.1]
FROb113	Il Sistema deve mostrare le metriche di completezza della documentazione in relazione alle componenti e alle interfacce del repository.	[UC11.2]

ID	Descrizione	Rif.
FROb114	Il Sistema deve presentare l'elenco delle azioni correttive (remediation) per il miglioramento della documentazione.	[UC11.3]
FROb115	Il Sistema deve mostrare un'informativa di esito positivo qualora non risultino remediation necessarie per l'area documentazione.	[UC11.3.1]
FROb116	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione dedicata alla visualizzazione del ranking dei repository analizzati.	[UC12]
FROb117	Il Sistema deve generare una graduatoria dei repository analizzati associati all'account dell'Utente Autorizzato.	[UC12]
FROb118	Il Sistema deve ordinare i repository in modo decrescente in base al punteggio di qualità globale calcolato.	[UC12]
FROb119	Il Sistema deve esporre, per ogni elemento del ranking, il punteggio di qualità calcolato e le metriche di sintesi utilizzate per determinarlo.	[UC12]
FROb120	Il Sistema deve inibire la visualizzazione della classifica e mostrare un avviso specifico qualora non risultino repository analizzati associati all'account dell'utente.	[UC12.1]
FROb121	Il Sistema deve consentire all'Utente Avanzato l'accesso alla sezione per la rimozione del collegamento con l'account GitHub.	[UC13]
FROb122	Il Sistema deve predisporre un comando di conferma per la finalizzazione della disconnessione dell'account GitHub.	[UC13]
FROb123	Il Sistema deve rimuovere l'associazione tra l'account CodeGuardian dell'utente e l'identità GitHub collegata a seguito della conferma di disconnessione.	[UC13]
FROb124	Il Sistema deve revocare o invalidare i token di accesso GitHub memorizzati e associati all'account utente a seguito della conferma di disconnessione.	[UC13]
FROb125	Il Sistema deve mostrare un messaggio di conferma esplicito a seguito della disconnessione dell'account GitHub.	[UC13]

ID	Descrizione	Rif.
FRDe126	Il Sistema deve consentire l'avvio della procedura di esportazione dei dati del report di analisi tramite comando dedicato.	[UC14]
FRDe127	Il Sistema deve permettere la selezione di un formato di output valido per il file di esportazione tra le opzioni disponibili.	[UC14.1]
FRDe128	Il Sistema deve mostrare un'informativa di errore e inibire la generazione del file qualora l'utente non selezioni alcun formato.	[UC14.1.1]
FRDe129	Il Sistema deve predisporre un comando di conferma finale per l'attivazione del processo di generazione del file esportato.	[UC14.2]
FRDe130	Il Sistema deve eseguire il parsing dei dati analitici e produrre un documento coerente con il formato selezionato dall'utente.	[UC14.2]
FRDe131	Il Sistema deve rendere disponibile il file generato per il download a seguito del completamento con successo dell'esportazione.	[UC14]
FRDe132	Il Sistema deve includere nel file esportato almeno i metadati del report e i risultati analitici relativi alle sezioni visualizzate o selezionate dall'utente.	[UC14]
FROb133	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla sezione dedicata alla modifica della chiave di accesso.	[UC15]
FROb134	Il Sistema deve permettere l'immissione della password attualmente in uso per finalità di verifica della titolarità prima di accettare la modifica.	[UC15.1]
FROb135	Il Sistema deve segnalare l'obbligatorietà del campo e impedire la modifica qualora la password corrente non venga inserita.	[UC15.1.1]
FROb136	Il Sistema deve inibire la procedura di aggiornamento e notificare l'utente qualora la password attuale inserita sia errata.	[UC15.1.2]
FROb137	Il Sistema deve consentire l'immissione di una nuova chiave di accesso.	[UC15.2]

ID	Descrizione	Rif.
FROb138	Il Sistema deve rilevare e segnalare il mancato inserimento della nuova password durante la fase di conferma.	[UC15.2.1]
FROb139	Il Sistema deve validare che la nuova password rispetti i criteri di complessità stabiliti.	[UC15.2.2]
FROb140	Il Sistema deve verificare che la nuova password sia differente da quella attualmente attiva e segnalare l'eventuale identità.	[UC15.2.3]
FROb141	Il Sistema deve predisporre un comando di conferma per l'invio della richiesta di aggiornamento delle credenziali.	[UC15.3]
FROb142	Il Sistema deve aggiornare la password memorizzata esclusivamente in forma cifrata tramite un algoritmo di hashing sicuro con salt univoco.	[UC15]
FROb143	Il Sistema deve mostrare un messaggio di feedback esplicito a seguito della corretta persistenza della nuova password.	[UC15.4]
FROb144	Il Sistema deve consentire all'Utente Autorizzato la selezione di una remediation dalla lista e la visualizzazione dei relativi dettagli.	[UC16]
FROb145	Il Sistema deve presentare i dettagli della remediation selezionata includendo almeno descrizione, severità o priorità, e indicazioni operative di correzione quando disponibili.	[UC16]
FROb146	Il Sistema deve essere in grado di prendere in carico la richiesta di verifica dell'accessibilità di un repository GitHub per avviare un audit.	[UC17]
FROb147	Il Sistema deve essere in grado di stabilire una comunicazione con i servizi API di GitHub per verificare l'operatività della piattaforma esterna.	[UC17.1]
FROb148	Il Sistema deve avviare la procedura di verifica dell'accessibilità del repository a partire dall'URL recuperato dai metadati della collezione di report.	[UC17]
FROb149	Il Sistema deve rilevare l'eventuale errore di comunicazione con GitHub (timeout o errore di rete) e interrompere la procedura di verifica.	[UC17.1.1]

ID	Descrizione	Rif.
FROb150	Il Sistema deve essere in grado di ricercare il repository come risorsa pubblica e determinare se risulta accessibile in lettura.	[UC17.2]
FROb151	Qualora il repository non risulti accessibile pubblicamente, il Sistema deve tentare la verifica di accesso utilizzando credenziali o token validi associati all'utente richiedente.	[UC17.2.1]
FROb152	Il Sistema deve rilevare il fallimento di tutti i metodi di autorizzazione disponibili e annullare l'audit notificando l'impossibilità di accedere al repository.	[UC17.2.1.1]
FRDe153	Il Sistema deve consentire all'Utente Autorizzato l'interazione con i comandi di accettazione e rifiuto della remediation visualizzata nel dettaglio.	[UC18] [UC19]
FRDe154	Il Sistema deve predisporre un comando di conferma per l'applicazione della remediation selezionata.	[UC18]
FRDe155	Il Sistema deve applicare al repository di riferimento le modifiche previste dalla remediation accettata, coerentemente con i contenuti della proposta correttiva.	[UC18]
FRDe156	Il Sistema deve aggiornare lo stato della remediation accettata nella dashboard dell'Utente Autorizzato.	[UC18]
FRDe157	Il Sistema deve consentire all'Utente Autorizzato di rifiutare la remediation proposta tramite comando dedicato.	[UC19]
FRDe158	Il Sistema deve rimuovere la remediation rifiutata dall'elenco delle azioni pendenti e aggiornare lo stato nella dashboard.	[UC19]
FROb159	Il Sistema deve consentire all'Utente Autorizzato l'accesso alla funzione di creazione di una nuova raccolta di report di analisi.	[UC20]
FROb160	Il Sistema deve predisporre un comando di conferma per finalizzare la creazione della raccolta di report.	[UC20]
FROb161	Il Sistema deve creare e rendere disponibile una nuova collezione di report a seguito della validazione positiva dei dati e della conferma dell'utente.	[UC20]

ID	Descrizione	Rif.
FROb162	Il Sistema deve visualizzare un messaggio di successo a seguito del completamento della procedura di creazione della raccolta.	[UC20]
FROb163	Il Sistema deve inibire la creazione della raccolta e notificare l'utente qualora i campi obbligatori del modulo risultino mancanti al momento della conferma.	[UC20.0.1]
FROb164	Il Sistema deve consentire all'Utente Autorizzato l'immissione del nome identificativo della raccolta di report.	[UC20.1]
FROb165	Il Sistema deve validare che il nome della raccolta rispetti i vincoli di formato previsti e notificare l'utente in caso di non conformità.	[UC20.1.1]
FROb166	Il Sistema deve consentire all'Utente Autorizzato l'immissione dell'URL del repository GitHub associato alla raccolta.	[UC20.2]
FROb167	Il Sistema deve inibire la procedura di creazione e notificare l'utente qualora il campo URL del repository non venga compilato.	[UC20.2.3]
FROb168	Il Sistema deve validare che l'URL del repository GitHub inserito utilizzi il protocollo "https://" e punti al dominio "github.com", notificando l'utente in caso di non conformità.	[UC20.2.1]
FROb169	Il Sistema deve verificare l'esistenza e l'accessibilità del repository indicato e inibire la creazione della raccolta qualora la risorsa risulti inesistente o non accessibile.	[UC20.2.2]
FROb170	Il Sistema deve consentire l'immissione facoltativa di una descrizione testuale della raccolta di report.	[UC20.3]
FROb171	Il sistema deve poter avviare il processo di analisi contattando i servizi per la clonazione del repository	[UC21]
FROb172	Il sistema deve poter avviare il processo di analisi contattando i servizi per l'analisi della documentazione	[UC21]
FROb173	Il sistema deve poter avviare il processo di analisi contattando i servizi per l'analisi degli standard OWASP	[UC21]

ID	Descrizione	Rif.
FROb174	Il sistema deve poter richiedere la clonazione del repository ad un servizio AWS che gestirà la clonazione	[UC21.1]
FROb175	Il sistema deve gestire gli errori durante la richiesta di clonazione di un repository	[UC21.1.1]
FROb176	Il sistema deve poter richiedere l'analisi del codice ad uno strumento di analisi esterno	[UC21.2]
FROb177	Il sistema deve poter trasmettere dei file ad uno strumento di analisi del codice esterno	[UC21.2]
FROb178	Il sistema deve poter richiedere l'analisi della documentazione ad uno strumento di analisi esterno	[UC21.3]
FROb179	Il sistema deve trasmettere dei file o l'intera codebase ad uno strumento di analisi della documentazione esterno	[UC21.3]
FROb180	Il sistema deve poter richiedere l'analisi degli standard OWASP ad uno strumento di analisi esterno	[UC21.4]
FROb181	Il sistema deve trasmettere dei file o l'intera codebase ad uno strumento di analisi degli standard OWASP esterno	[UC21.4]
FROb182	Il Sistema deve registrare lo stato dell'analisi nel sistema di persistenza impostandolo a "pending" a seguito dell'inizializzazione corretta degli strumenti esterni.	[UC22]
FROb183	Il Sistema deve associare univocamente lo stato dell'analisi al repository oggetto dell'audit e all'utente richiedente.	[UC22]
FROb184	Il Sistema deve persistere i dati di tracciamento dell'analisi includendo almeno identificativo della richiesta, riferimento al repository e timestamp di avvio.	[UC22]
FROb185	Il Sistema deve rilevare e gestire errori critici durante la scrittura dei dati di stato nel database, interrompendo la registrazione e notificando l'impossibilità di tracciare l'avanzamento dell'audit.	[UC22.0.1]

ID	Descrizione	Rif.
FROb186	In caso di errore di persistenza dello stato, il Sistema deve registrare l'evento di errore per finalità di diagnosi e audit.	[UC22.0.1]
FROb187	Il Sistema deve monitorare il completamento delle attività presso gli strumenti esterni di analisi fino alla disponibilità dei risultati o al raggiungimento dei limiti di attesa previsti.	[UC23]
FROb188	Il Sistema deve recuperare i file di output e i metadati generati da ciascuno strumento di analisi consultato.	[UC23]
FROb189	Il Sistema deve rendere disponibili i dati grezzi complessivi prodotti dagli strumenti di analisi come input per le successive fasi di elaborazione del report.	[UC23]
FROb190	Il Sistema deve rilevare timeout o codici di errore restituiti da uno o più strumenti esterni e registrare l'anomalia indicando lo strumento non rispondente.	[UC23.1]
FROb191	In caso di fallimento parziale nel recupero dei risultati, il Sistema deve proseguire l'elaborazione utilizzando esclusivamente i risultati acquisiti correttamente.	[UC23.1]
FROb192	In caso di fallimento parziale nel recupero dei risultati, il Sistema deve notificare l'utente circa l'incompletezza dei dati e la conseguente parzialità del report finale.	[UC23.1]
FROb193	Il Sistema deve generare un report finale aggregando i risultati prodotti dagli strumenti di analisi disponibili (codice, sicurezza, documentazione).	[UC24]
FROb194	Il Sistema deve normalizzare metriche, criticità e remediation in un formato strutturato coerente durante la generazione del report finale.	[UC24]
FROb195	Il report finale deve includere le metriche e le criticità rilevate dalle diverse analisi e i relativi metadati minimi di tracciamento (repository, commit, timestamp).	[UC24]
FROb196	Il Sistema deve validare il report finale prodotto per garantirne coerenza e completezza rispetto ai dati disponibili prima della persistenza.	[UC24]
FROb197	Il Sistema deve persistere il report finale nel sistema di persistenza e aggiornare lo stato dell'analisi a	[UC25]

ID	Descrizione	Rif.
	“completed” a seguito del salvataggio avvenuto con successo.	
FROb198	Il Sistema deve associare il report archiviato al repository oggetto dell’analisi e all’utente richiedente in modo univoco e tracciabile.	<a href="#">[UC25]</a>
FROb199	Il Sistema deve aggiornare i metadati dell’analisi per riflettere il completamento della procedura a seguito della persistenza del report.	<a href="#">[UC25]</a>
FROb200	Il Sistema deve rilevare e gestire errori durante il salvataggio del report, notificando l’utente circa il mancato salvataggio dei risultati dell’analisi.	<a href="#">[UC25.1]</a>
FROb201	In caso di errore durante la persistenza del report, il Sistema deve registrare l’evento di errore per finalità di diagnosi e audit interno.	<a href="#">[UC25.1]</a>
FROb202	Il Sistema deve inviare una notifica all’utente a seguito del completamento dell’analisi e della disponibilità del report archiviato.	<a href="#">[UC26]</a>
FROb203	La notifica di completamento deve indicare la disponibilità del nuovo report e fornire un riferimento al report appena generato.	<a href="#">[UC26]</a>
FROb204	Il Sistema deve gestire l’eventuale fallimento dell’invio della notifica registrando la mancata consegna nei log di errore per finalità di audit interno.	<a href="#">[UC26.1]</a>
FROb205	Il Sistema deve consentire all’Utente Autorizzato la ricezione della notifica di completamento dell’analisi tramite i canali di comunicazione configurati.	<a href="#">[UC27]</a>
FROb206	La notifica di completamento deve contenere un riferimento al report generato e le informazioni minime per identificarlo (repository e data/ora di generazione).	<a href="#">[UC27]</a>
FROb207	A seguito della ricezione della notifica, il Sistema deve consentire all’Utente Autorizzato l’accesso al report tramite la sezione dedicata della piattaforma.	<a href="#">[UC27]</a>
FROb208	Il Sistema deve consentire all’Utente Autorizzato di accedere al report tramite la sezione dedicata anche in assenza della ricezione della notifica, qualora l’analisi risulti completata e archiviata.	<a href="#">[UC27.0.1]</a>

ID	Descrizione	Rif.
FROb209	Il Sistema deve gestire la mancata ricezione della notifica dovuta a impedimenti tecnici esterni o di connettività, mantenendo comunque disponibile lo stato dell'analisi e il report nella piattaforma.	<a href="#">[UC27.0.1]</a>
FROb210	Il Sistema deve notificare all'Utente Autorizzato il fallimento critico di un'analisi pendente indicando che l'audit non può proseguire.	<a href="#">[UC28]</a>
descrizione delle cause riscontrate o un codice di errore tracciabile associato alla FROb211	La notifica di errore critico deve includere una specifica analisi.	<a href="#">[UC28]</a>
FROb212	Il Sistema deve aggiornare lo stato dell'analisi nel sistema di persistenza a "failed" o equivalente a seguito del rilevamento di un'anomalia bloccante.	<a href="#">[UC28]</a>
FROb213	Il Sistema deve rendere consultabile nella dashboard lo stato di fallimento dell'analisi e le relative informazioni anche in assenza della ricezione della notifica di errore.	<a href="#">[UC28.0.1]</a>
FROb214	Il Sistema deve gestire la mancata ricezione della notifica di errore critico dovuta a problemi di rete o servizi esterni, registrando l'evento nei log e mantenendo lo stato aggiornato in piattaforma.	<a href="#">[UC28.0.1]</a>
FROb215	Il Sistema deve scambiare il codice OAuth temporaneo ricevuto da GitHub con un token di accesso tramite il protocollo OAuth previsto dal provider esterno.	<a href="#">[UC29]</a>
FROb216	Il Sistema deve crittografare il token di accesso ottenuto prima della memorizzazione nel sistema di persistenza.	<a href="#">[UC29]</a>
FROb217	Il Sistema deve associare il token di accesso GitHub memorizzato all'account dell'Utente Autorizzato che ha richiesto l'integrazione.	<a href="#">[UC29]</a>
FROb218	Il Sistema deve gestire il fallimento della procedura di scambio OAuth dovuto a codice scaduto o non valido annullando l'integrazione e notificando all'utente la necessità di ripetere l'autenticazione.	<a href="#">[UC29.0.1]</a>

ID	Descrizione	Rif.
FROb219	Il Sistema deve consentire all'Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all'analisi del codice.	[UC30]
FROb220	Il dettaglio della remediation del codice deve includere almeno titolo, descrizione, tipologia di criticità e livello di severità.	[UC30]
FROb221	Il Sistema deve consentire all'Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all'analisi della sicurezza.	[UC31]
FROb222	Il dettaglio della remediation di sicurezza deve includere almeno titolo, descrizione, tipologia di vulnerabilità e livello di severità.	[UC31]
FROb223	Il Sistema deve consentire all'Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all'analisi della documentazione.	[UC32]
FROb224	Il dettaglio della remediation documentale deve includere almeno titolo, descrizione e tipologia di rilievo documentale.	[UC32]
FROb225	Il Sistema deve consentire all'Utente Autorizzato di accettare una remediation relativa all'analisi del codice.	[UC33]
FROb226	Il Sistema deve applicare automaticamente alla codebase le modifiche previste dalla remediation del codice accettata.	[UC33]
FROb227	Il Sistema deve aggiornare lo stato della remediation del codice come "eseguita" nella dashboard a seguito dell'applicazione riuscita.	[UC33]
FROb228	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]
FROb229	Il Sistema deve consentire all'Utente Autorizzato di rifiutare una remediation relativa all'analisi del codice.	[UC34]
FROb230	Il Sistema deve aggiornare lo stato della remediation del codice come "rifiutata" senza apportare modifiche al repository.	[UC34]

ID	Descrizione	Rif.
FROb231	Il Sistema deve consentire all'Utente Autorizzato di accettare una remediation relativa all'analisi della sicurezza.	[UC35]
FROb232	Il Sistema deve applicare le patch o le configurazioni di sicurezza previste dalla remediation accettata.	[UC35]
FROb233	Il Sistema deve aggiornare lo stato della remediation di sicurezza come "eseguita" nella dashboard.	[UC35]
FROb234	Il Sistema deve gestire errori durante l'applicazione della remediation di sicurezza notificando il fallimento all'utente.	[UC35.0.1]
FROb235	Il Sistema deve consentire all'Utente Autorizzato di rifiutare una remediation relativa all'analisi della sicurezza senza modificare il repository.	[UC36]
FROb236	Il Sistema deve aggiornare lo stato della remediation di sicurezza come "rifiutata" nella dashboard.	[UC36]
FROb237	Il Sistema deve consentire all'Utente Autorizzato di accettare una remediation relativa all'analisi della documentazione.	[UC37]
FROb238	Il Sistema deve applicare automaticamente le modifiche ai file documentali previste dalla remediation accettata.	[UC37]
FROb239	Il Sistema deve aggiornare lo stato della remediation documentale come "eseguita" nella dashboard.	[UC37]
FROb240	Il Sistema deve gestire errori durante l'applicazione della remediation documentale notificando il fallimento all'utente.	[UC37.0.1]
FROb241	Il Sistema deve consentire all'Utente Autorizzato la visualizzazione del dettaglio di una singola remediation relativa all'analisi della documentazione.	[UC38]
FROb242	Il Sistema deve consentire all'Utente Autorizzato di rifiutare una remediation relativa all'analisi della documentazione.	[UC38]
FROb243	Il Sistema deve aggiornare lo stato della remediation documentale come "rifiutata" nella dashboard a seguito del rifiuto confermato dall'utente.	[UC38]

ID	Descrizione	Rif.
FROb244	Il Sistema deve garantire che il rifiuto di una remediation documentale non modifichi i file di documentazione del repository.	[UC38]
FROb245	Il Sistema deve rimuovere la remediation rifiutata dalla lista delle azioni pendenti dell'area "Documentazione" oppure marcarla come rifiutata mantenendola consultabile.	[UC38]
FROb246	Il Sistema deve mostrare all'Utente Autorizzato una conferma dell'avvenuto rifiuto della remediation documentale.	[UC38]
FROb247	Il Sistema deve registrare nel sistema di persistenza la decisione di rifiuto della remediation documentale associandola all'utente e al repository.	[UC38]
FRDe248	Il Sistema deve consentire all'Utente Autorizzato di consultare in ogni momento il dettaglio di una remediation documentale rifiutata.	[UC38]
FROb249	Il Sistema deve consentire all'Utente Avanzato di inviare una richiesta di analisi per un repository GitHub privato per cui dispone di integrazione GitHub attiva.	[UC39]
FROb250	Il Sistema deve consentire all'Utente Avanzato di inserire l'URL del repository privato da analizzare nella sezione di configurazione dell'analisi.	[UC39]
FROb251	Il Sistema deve consentire all'Utente Avanzato di selezionare una o più aree di interesse per l'audit del repository privato.	[UC39]
FROb252	Il Sistema deve consentire all'Utente Avanzato di confermare l'invio della richiesta di analisi del repository privato.	[UC39]
FROb253	Il Sistema deve validare la presenza dell'integrazione GitHub attiva prima di accettare la richiesta di analisi di un repository privato.	[UC39]
FROb254	Il Sistema deve rifiutare l'invio della richiesta di analisi se l'Utente Avanzato non ha selezionato alcuna area di interesse per l'audit.	[UC39]

ID	Descrizione	Rif.
FROb255	Il Sistema deve mostrare all'Utente Avanzato una conferma di presa in carico della richiesta di analisi del repository privato a seguito dell'invio.	[UC39]
FRDe256	Il Sistema deve associare la richiesta di analisi del repository privato all'identità dell'Utente Avanzato richiedente e all'URL del repository indicato.	[UC39]
FRDe257	Il Sistema deve impedire l'invio della richiesta di analisi se esiste già un'analisi in esecuzione per lo stesso repository e lo stesso utente.	[UC39]
FRDe258	Il Sistema deve consentire all'Utente Avanzato di visualizzare l'esito di presa in carico includendo almeno identificativo della richiesta e timestamp di creazione.	[UC39]
FROb259	Il Sistema deve consentire all'Utente Avanzato di inserire un repository GitHub privato di sua proprietà nel proprio catalogo personale.	[UC40]
FROb260	Il Sistema deve consentire all'Utente Avanzato di inserire l'URL del repository privato di sua proprietà nella sezione di gestione repository privati.	[UC40]
FROb261	Il Sistema deve consentire all'Utente Avanzato di confermare l'aggiunta del repository privato al catalogo personale.	[UC40]
FROb262	Il Sistema deve validare che l'utente abbia collegato GitHub prima di consentire l'inserimento di un repository privato nel catalogo personale.	[UC40]
FROb263	Il Sistema deve registrare il repository privato inserito nel sistema di persistenza associandolo al profilo dell'Utente Avanzato.	[UC40]
FROb264	Il Sistema deve visualizzare all'Utente Avanzato l'esito della registrazione del repository privato nel catalogo personale.	[UC40]
FROb265	Il Sistema deve rilevare il caso di URL già presente nel catalogo personale dell'Utente Avanzato e inibire l'inserimento duplicato.	[UC40.0.1]
FROb266	Il Sistema deve mostrare all'Utente Avanzato un avviso di duplicazione quando l'URL del repository risulta già associato al proprio profilo.	[UC40.0.1]

ID	Descrizione	Rif.
FRDe267	Il Sistema deve mantenere invariato il catalogo personale a seguito del tentativo di inserimento di un repository già presente.	[UC40.0.1]
FROb268	Il Sistema deve consentire all'Utente Avanzato di visualizzare il catalogo dei repository privati registrati nel proprio profilo.	[UC41]
FROb269	Il Sistema deve mostrare all'Utente Avanzato l'elenco dei repository privati presenti nel catalogo personale.	[UC41]
FROb270	Ogni elemento dell'elenco dei repository privati deve includere almeno nome e URL della risorsa.	[UC41]
FROb271	Il Sistema deve consentire all'Utente Avanzato di accedere alla sezione di gestione repository privati a partire dalla propria sessione autenticata.	[UC41]
FROb272	Il Sistema deve gestire il caso di catalogo vuoto mostrando un messaggio informativo all'Utente Avanzato.	[UC41.0.1]
FROb273	Il messaggio informativo di catalogo vuoto deve suggerire all'Utente Avanzato l'inserimento del primo repository privato.	[UC41.0.1]
FRDe274	Il Sistema deve consentire all'Utente Avanzato di selezionare un repository dal catalogo per accedere alle funzionalità di gestione successive.	[UC41]
FROb275	Il Sistema deve consentire all'Utente Avanzato di rimuovere un repository privato dal proprio catalogo personale.	[UC42]
FROb276	Il Sistema deve consentire all'Utente Avanzato di avviare la procedura di rimozione selezionando un repository specifico dal catalogo.	[UC42]
FROb277	Il Sistema deve richiedere conferma esplicita della rimozione del repository prima di procedere.	[UC42.1]
FROb278	Il Sistema deve consentire all'Utente Avanzato di annullare la rimozione del repository durante la fase di conferma.	[UC42.1.1]

ID	Descrizione	Rif.
FROb279	Il Sistema deve rimuovere il repository dal catalogo personale dell'Utente Avanzato solo a seguito di conferma della rimozione.	[UC42.1]
FROb280	Il Sistema deve mostrare all'Utente Avanzato l'esito della rimozione e garantire che la risorsa non sia più presente nel catalogo personale.	[UC42]
FROb281	In caso di annullamento della rimozione, il Sistema deve mantenere il repository nel catalogo personale dell'Utente Avanzato.	[UC42.1.1]
FRDe282	Il Sistema deve revocare i permessi di accesso ai report del repository rimosso per eventuali utenti terzi precedentemente autorizzati.	[UC42]
FRDe283	Il Sistema deve registrare nel sistema di persistenza l'operazione di rimozione del repository associandola all'Utente Avanzato e alla risorsa.	[UC42]
FROb284	Il Sistema deve consentire all'Utente Avanzato di accedere alla sezione di gestione permessi di un repository privato selezionato dal catalogo personale.	[UC43]
FROb285	Il Sistema deve mostrare all'Utente Avanzato la lista degli utenti autorizzati alla consultazione dei report per il repository selezionato.	[UC43]
FROb286	Per ciascun utente autorizzato, il Sistema deve mostrare almeno un identificativo univoco del profilo.	[UC43]
FROb287	Il Sistema deve gestire il caso di lista autorizzazioni vuota mostrando un messaggio informativo all'Utente Avanzato.	[UC43.0.1]
FROb288	Il messaggio informativo di lista autorizzazioni vuota deve indicare che l'accesso è limitato al proprietario del repository.	[UC43.0.1]
FRDe289	Il Sistema deve consentire all'Utente Avanzato di avviare le funzionalità di aggiunta e rimozione utenti autorizzati a partire dalla sezione di gestione permessi.	[UC43]
FROb290	Il Sistema deve consentire all'Utente Avanzato di aggiungere un utente autorizzato per un repository privato selezionato.	[UC44]

ID	Descrizione	Rif.
FROb291	Il Sistema deve consentire all'Utente Avanzato di inserire come credenziale di autorizzazione lo username o l'email del profilo da autorizzare.	[UC44.1]
FROb292	Il Sistema deve validare l'identificativo inserito e mostrare all'Utente Avanzato l'esito della verifica prima della conferma dell'aggiunta.	[UC44.1]
FROb293	Il Sistema deve consentire all'Utente Avanzato di confermare l'aggiunta dell'autorizzazione per il profilo inserito.	[UC44]
FROb294	Il Sistema deve aggiornare la lista degli utenti autorizzati mostrando il nuovo profilo a seguito dell'aggiunta riuscita.	[UC44]
FROb295	Il Sistema deve impedire l'aggiunta di un profilo se lo username o l'email non rispettano i vincoli di formato previsti.	[UC44.1.1]
FROb296	Il Sistema deve mostrare all'Utente Avanzato un errore di formato nel caso di identificativo non valido e consentire la correzione dell'input.	[UC44.1.1]
FROb297	Il Sistema deve impedire l'aggiunta di un profilo se l'identificativo non corrisponde a nessun utente registrato.	[UC44.1.2]
FROb298	Il Sistema deve mostrare all'Utente Avanzato un avviso nel caso di profilo inesistente.	[UC44.1.2]
FROb299	Il Sistema deve impedire l'aggiunta di un profilo già presente tra gli utenti autorizzati del repository.	[UC44.1.3]
FROb300	Il Sistema deve mostrare all'Utente Avanzato un avviso di duplicazione nel caso di utente già autorizzato.	[UC44.1.3]
FROb301	Il Sistema deve impedire la conferma dell'aggiunta nel caso in cui il campo identificativo risulti vuoto.	[UC44.1.4]
FROb302	Il Sistema deve mostrare all'Utente Avanzato un avviso di obbligatorietà del campo nel caso di conferma con campo vuoto.	[UC44.1.4]
FRDe303	Il Sistema deve registrare nel sistema di persistenza l'assegnazione dei permessi al profilo autorizzato associandola al repository e al proprietario.	[UC44]

ID	Descrizione	Rif.
FRDe304	Il profilo autorizzato aggiunto deve poter consultare i report del repository per cui è stato autorizzato, secondo i permessi assegnati.	[UC44]
FROb305	Il Sistema deve consentire all'Utente Avanzato di rimuovere un utente autorizzato dalla lista dei profili autorizzati per un repository privato selezionato.	[UC45]
FROb306	Il Sistema deve consentire all'Utente Avanzato di selezionare un profilo dalla lista degli autorizzati per avviare la procedura di revoca.	[UC45]
FROb307	Il Sistema deve richiedere conferma esplicita della revoca dei permessi prima di procedere con la rimozione dell'autorizzazione.	[UC45.1]
FROb308	Il Sistema deve eseguire la revoca dei permessi per il profilo selezionato solo a seguito di conferma dell'Utente Avanzato.	[UC45.1]
FROb309	Il Sistema deve aggiornare la lista degli autorizzati rimuovendo il profilo revocato a seguito di revoca riuscita.	[UC45]
FRDe310	Il Sistema deve revocare l'accesso del profilo rimosso alla consultazione dei report del repository per cui era autorizzato.	[UC45]
FRDe311	Il Sistema deve registrare nel sistema di persistenza la revoca dei permessi associandola al repository, al profilo revocato e al proprietario.	[UC45]
FROb312	Il Sistema deve consentire all'Utente Autorizzato di rimuovere una raccolta di report dal proprio profilo.	[UC46]
FROb313	Il Sistema deve consentire all'Utente Autorizzato di selezionare una raccolta e avviare la funzione di rimozione.	[UC46]
FROb314	Il Sistema deve richiedere conferma esplicita prima di procedere con la rimozione della raccolta.	[UC46.1]
FROb315	Il Sistema deve consentire all'Utente Autorizzato di annullare la rimozione della raccolta durante la fase di conferma.	[UC46.1.1]

ID	Descrizione	Rif.
FROb316	Il Sistema deve rimuovere la raccolta dal profilo dell'Utente Autorizzato solo a seguito di conferma della rimozione.	[UC46.1]
FROb317	Il Sistema deve mostrare all'Utente Autorizzato l'esito della rimozione della raccolta dal proprio profilo.	[UC46]
FROb318	Il Sistema deve garantire che la rimozione di una raccolta non comporti la cancellazione dei report contenuti, che devono rimanere persistiti e consultabili tramite altri percorsi previsti.	[UC46]
FRDe319	Il Sistema deve registrare nel sistema di persistenza l'operazione di rimozione della raccolta associandola all'utente e alla raccolta rimossa.	[UC46]
FROb320	Il Sistema deve consentire all'Utente Autenticato di avviare la richiesta di cancellazione definitiva del profilo CodeGuardian dalla sezione di gestione avanzata del profilo.	[UC47]
FROb321	Il Sistema deve richiedere all'Utente Autenticato l'inserimento della password attuale per confermare l'identità prima di procedere con la cancellazione del profilo.	[UC47]
FROb322	Il Sistema deve consentire all'Utente Autenticato di confermare la cancellazione definitiva del profilo dopo la verifica dell'identità.	[UC47]
FROb323	Il Sistema deve mostrare all'Utente Autenticato un avviso che descriva l'irreversibilità della cancellazione e richiedere una conferma finale.	[UC47.1]
FROb324	Il Sistema deve consentire all'Utente Autenticato di annullare l'operazione di cancellazione del profilo nella fase di conferma finale.	[UC47.1]
FROb325	Il Sistema deve eliminare in modo permanente il profilo dell'Utente Autenticato solo a seguito di conferma finale della cancellazione.	[UC47.1]
FROb326	Il Sistema deve invalidare la sessione dell'Utente Autenticato e impedire ulteriori accessi con le credenziali precedenti a seguito della cancellazione riuscita.	[UC47]

ID	Descrizione	Rif.
FROb327	Il Sistema deve rimuovere dal sistema di persistenza i dati personali dell'Utente Autenticato associati al profilo cancellato.	[UC47]
FROb328	Il Sistema deve rimuovere dal sistema di persistenza le associazioni OAuth collegate al profilo dell'Utente Autenticato a seguito della cancellazione.	[UC47]
FROb329	Il Sistema deve mostrare all'Utente Autenticato l'esito della cancellazione del profilo a seguito del completamento dell'operazione.	[UC47]
FRDe330	Il Sistema deve registrare nei log applicativi l'operazione di cancellazione del profilo, includendo timestamp e identificativo dell'utente, per finalità di audit interno.	[UC47]

## Requisiti di Qualità (QR)

I seguenti requisiti garantiscono che il sistema non solo funzioni correttamente, ma sia anche manutenibile, performante e ben documentato.

ID	Descrizione	Fonti
QROb1	È necessario fornire un diagramma architettonale completo che illustri la struttura multiagente e le interazioni tra componenti	Capitolato di Progetto, Sez. "Obiettivi"
QROb2	Deve essere fornita documentazione tecnica esaustiva del sistema, includendo swagger Application Programming Interface <sup>G</sup> (API) e documentazione descrittiva del progetto	Capitolato di Progetto, Sez. "Vincoli Generali"
QROb3	Il codice prodotto deve raggiungere una copertura minima del 70% tramite Test di Unità <sup>G</sup> automatizzati	Capitolato di Progetto, Sez. "Vincoli Generali"
QROb4	L'applicativo deve essere creato seguendo principi di modularità per consentire l'aggiunta di nuovi agenti di analisi	Capitolato di Progetto, Sez. "Vincoli Generali"
QROb5	Deve essere fornito un sistema di Bug Reporting strutturato per tracciare e gestire le anomalie riscontrate	Capitolato di Progetto, Sez. "Vincoli Generali"
QROb6	È necessario utilizzare appositi sistemi di versionamento del codice	Capitolato di Progetto, Sez. "Vincoli Generali"
QROb7	È necessario rispettare tutte le norme presenti nelle <b>Norme di Progetto</b>	Interno

## Requisiti di Vincolo (VR)

ID	Descrizione	Fonti
VROb1	Il Back-end e l'Orchestratore devono essere sviluppati utilizzando Node.js <sup>G</sup> o Python <sup>G</sup>	Capitolato di Progetto, Sez. "Tecnologie"
VROb2	Il Front-end deve essere sviluppato utilizzando React <sup>G</sup>	Capitolato di Progetto, Sez. "Tecnologie"
VROb3	Il sistema di persistenza deve essere implementato utilizzando MongoDB o PostgreSQL	Capitolato di Progetto, Sez. "Tecnologie"
VROb4	L'architettura deve essere ospitata su infrastruttura cloud AWS	Capitolato di Progetto, Sez. "Tecnologie"
VROb5	Devono essere utilizzate GitHub Actions per implementare pipeline CI/CD	Capitolato di Progetto, Sez. "Tecnologie"
VROb6	Il codice sorgente deve essere versionato utilizzando sistemi come Git <sup>G</sup> o repository online	Capitolato di Progetto, Sez. "Vincoli Generali"
VROb7	L'analisi di sicurezza deve essere conforme agli standard OWASP Top 10	Capitolato di Progetto, Sez. "OWASP"