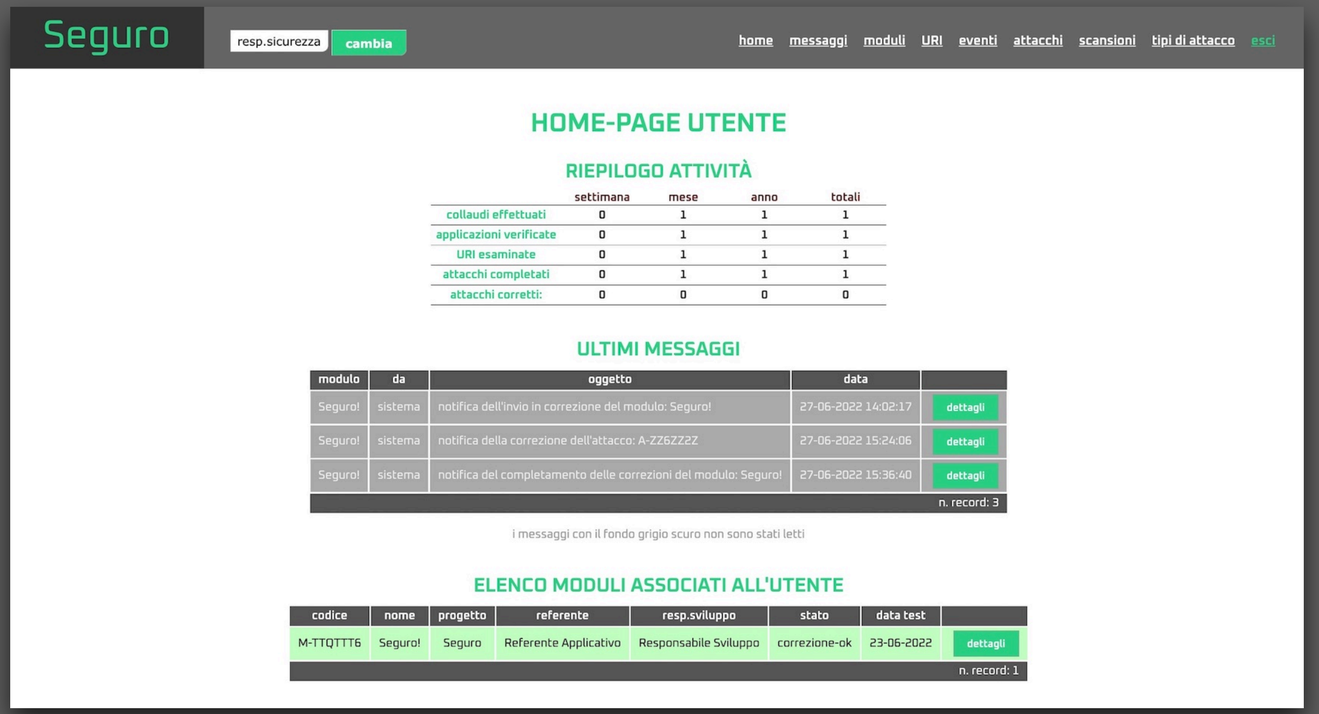
# Seguro!

## Presentazione del sistema

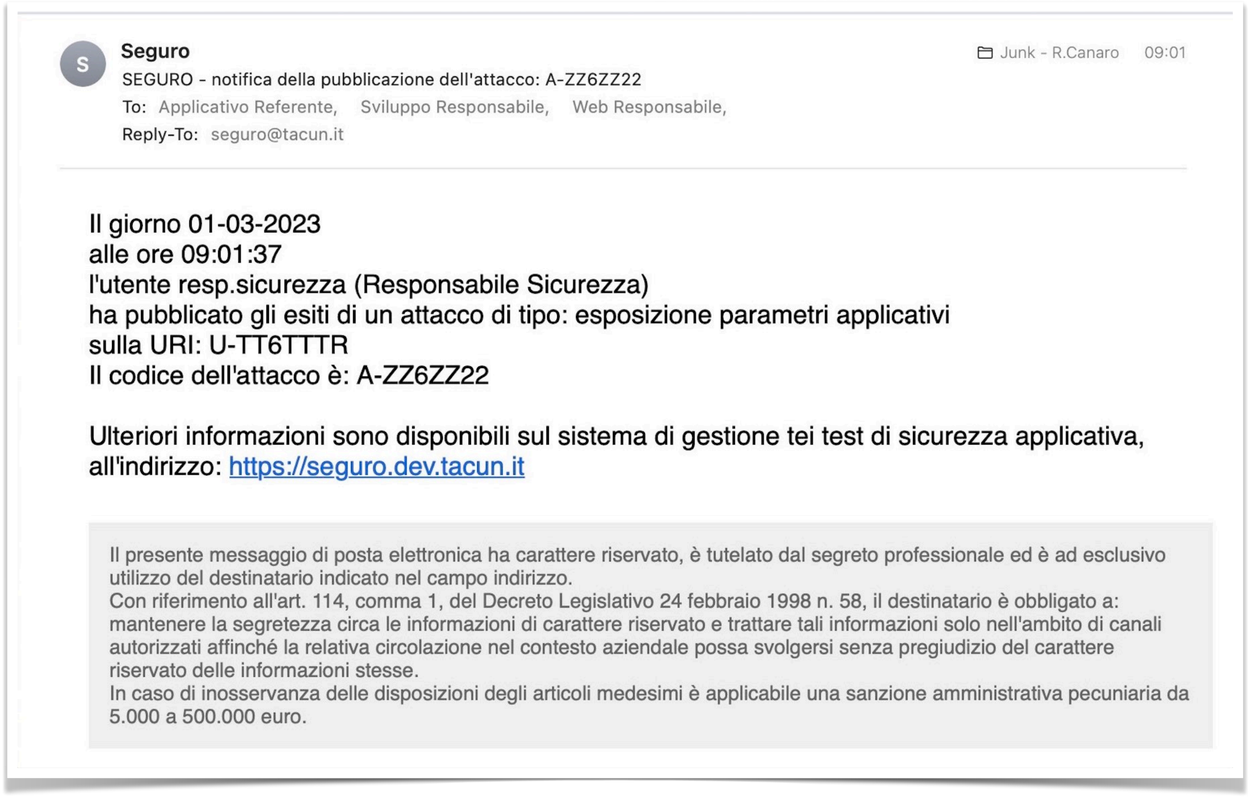
### Versione 1.7- Febbraio 2023




Tacun - 2023

# Seguro!

## Executive summary



**Seguro**
SEGURO - notifica della pubblicazione dell'attacco: A-ZZ6ZZ22
Junk - R.Canaro 09:01
To: Applicativo Referente, Sviluppo Responsabile, Web Responsabile,
Reply-To: seguro@tacun.it

Il giorno 01-03-2023
alle ore 09:01:37
l'utente resp.sicurezza (Responsabile Sicurezza)
ha pubblicato gli esiti di un attacco di tipo: esposizione parametri applicativi
sulla URI: U-TT6TTTR
Il codice dell'attacco è: A-ZZ6ZZ22

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa,
all'indirizzo: https://seguro.dev.tacun.it



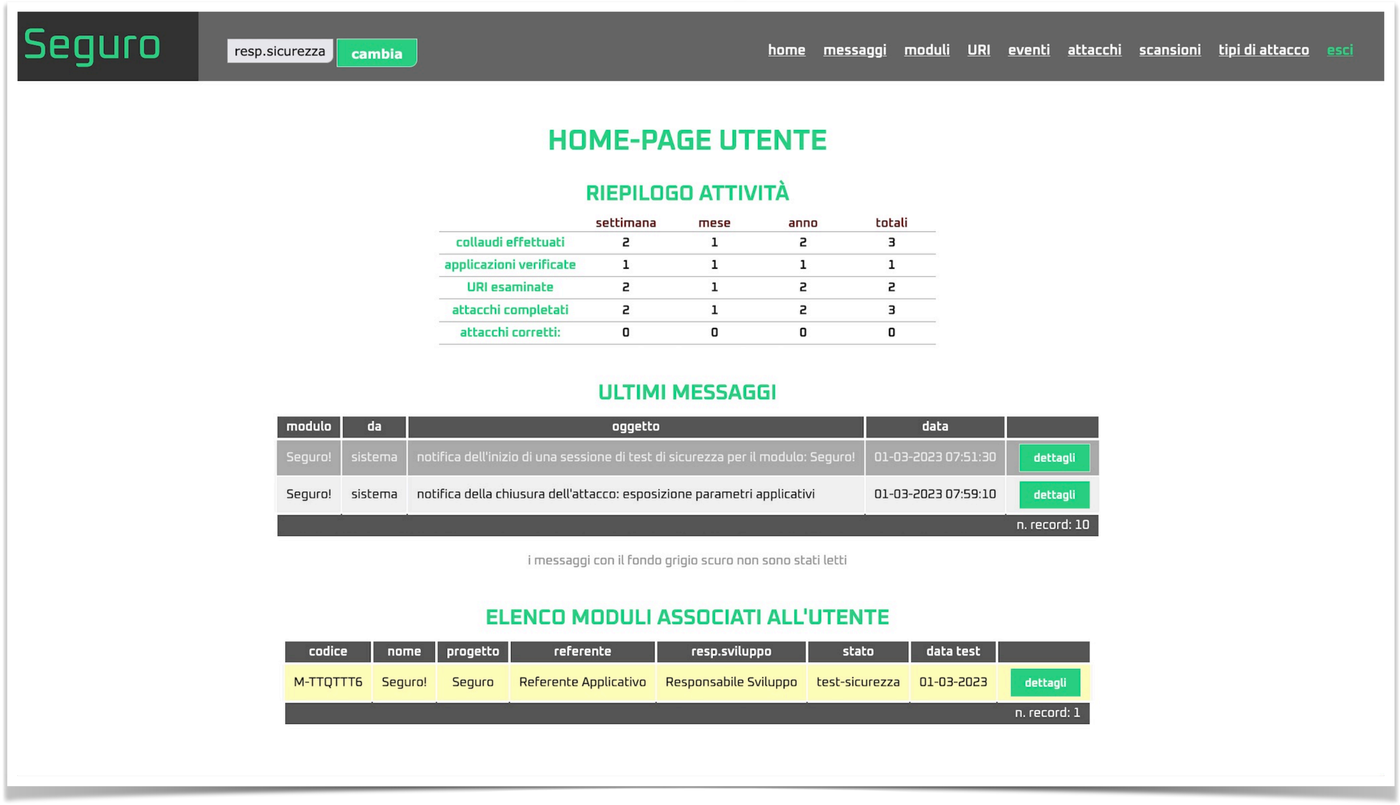
**Seguro!** permette di eseguire i test di sicurezza delle applicazioni Web **senza alcuno scambio di documenti** relativi alle eventuali vulnerabilità rilevate.

I messaggi inviati dal sistema **non contengono alcuna informazione** sulla URL, sul sistema in esame o sull'esito di un attacco, ma solo dei codici identificativi.

Le informazioni relative alle applicazioni in esame **restano all'interno del sistema.**

# Seguro!

## Executive summary



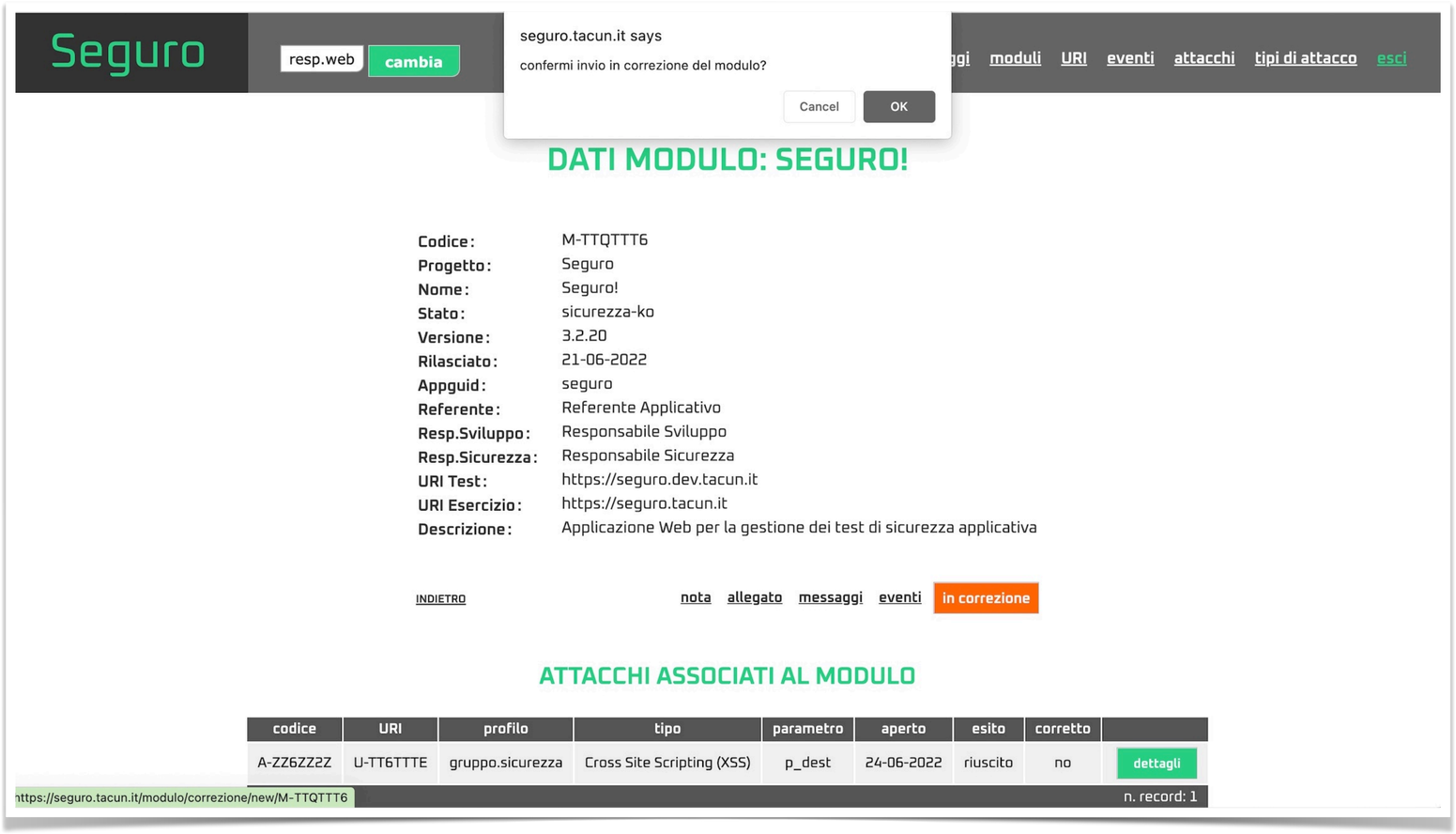

Grazie a **Seguro!** è possibile:

- definire e applicare un processo chiaro e immutabile per la gestione dei test;
- identificare le responsabilità dei singoli attori;
- tenere traccia di ogni evento occorso, in modo che sia sempre possibile capire chi ha fatto (o non ha fatto) cosa.

# Caratteristiche del sistema

# Seguro!

## Caratteristiche del sistema




È un'applicazione Web, scritta in linguaggio **PHP**.

Ha un'interfaccia utente intuitiva, che ne facilita l'utilizzo anche al personale non tecnico.

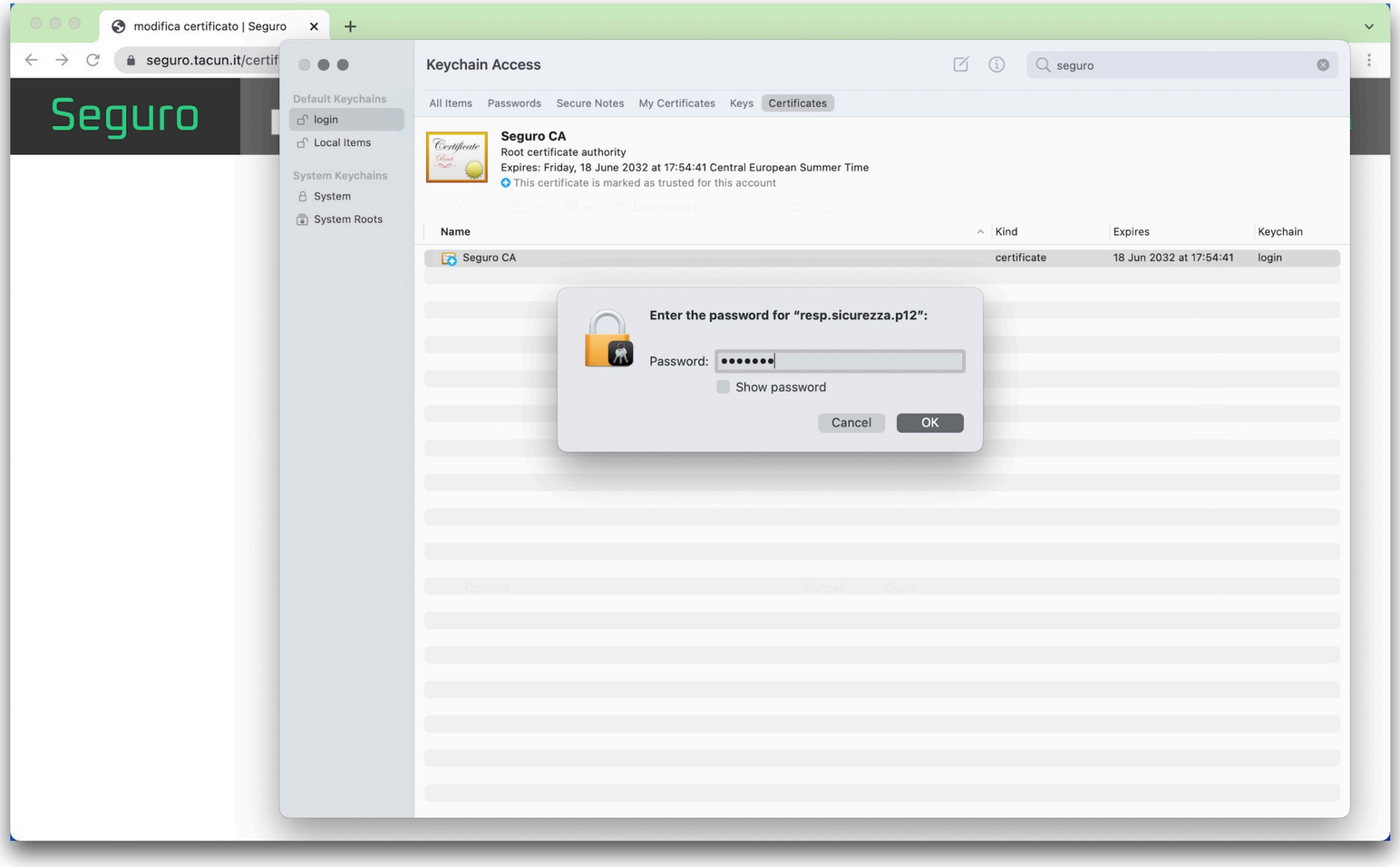
L'accesso degli utenti può avvenire o con **utenze locali** o con **utenze LDAP.**

L'autenticazione può avvenire o con **username** e **password** o con un **certificato digitale** generato dal sistema e una password.

Il sistema ha un **doppio sistema di log** degli eventi, che vengono salvati sia nella base-dati del sistema che su un file esterno.

# Caratteristiche del sistema

## Accesso con certificati

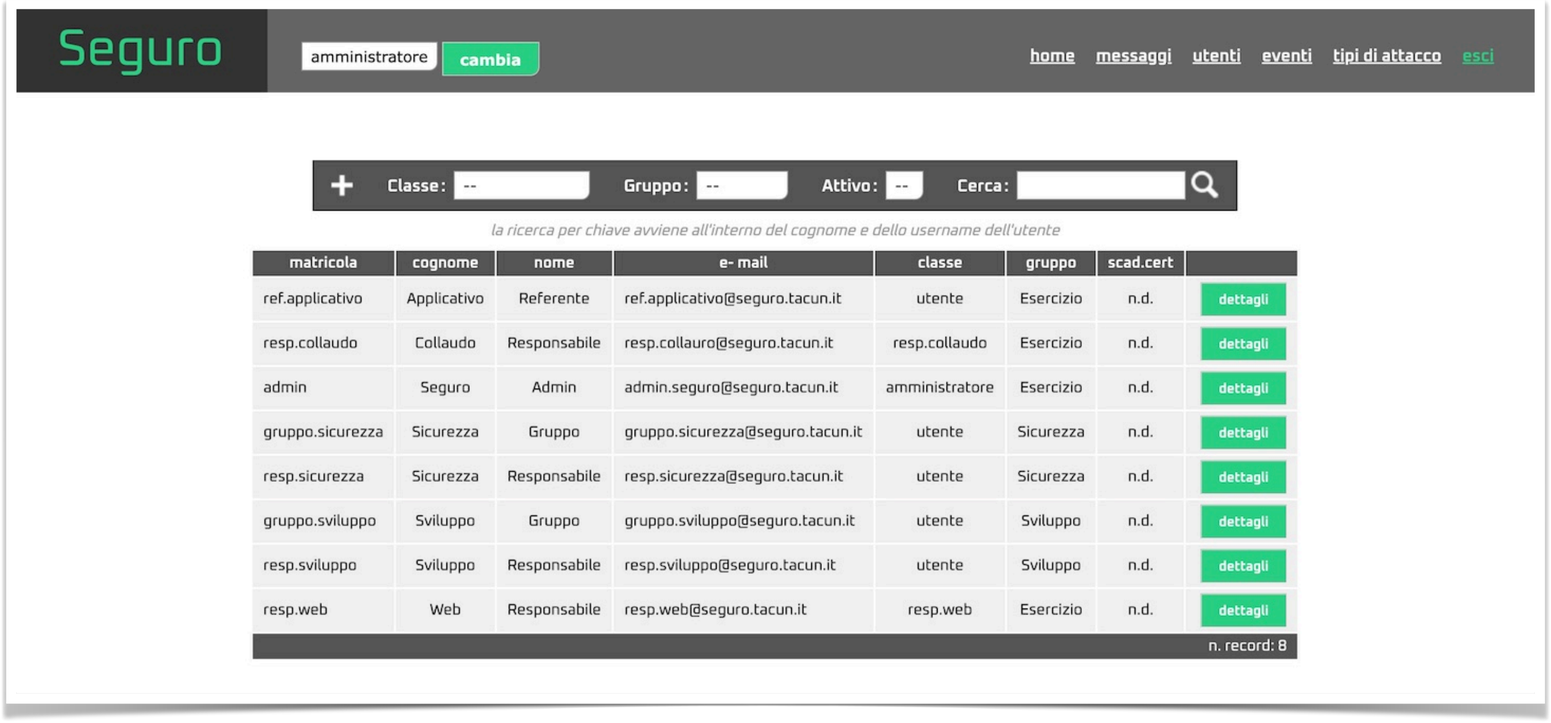



L'accesso con certificato aumenta la sicurezza del sistema e rende **non ripudiabili** le azioni intraprese dagli utenti.

Il sistema ha una **CA interna** per la generazione e la gestione dei certificati.

# Seguro!

## Utenze e gruppi di utenza




La suddivisione molto granulare dei ruoli permette di concedere sempre il minimo dei privilegi possibili a ciascun utente.

Gli utenti sono suddivisi in tre gruppi:

**esercizio:** responsabili dell'esercizio dei sistemi;

**sicurezza:** utenti che si occupano della sicurezza dei sistemi;

**sviluppo:** utenti che si occupano dello sviluppo applicativo dei sistemi.

# Seguro!

## Utenze - Gruppo Esercizio

Al **Gruppo di Esercizio** appartengono i ruoli:

**amministratore:** inserisce gli utenti, genera i certificati e gestisce la documentazione sui tipi di attacco; **non ha** visibilità sui test o sui moduli;

**responsabile collaudo:** inserisce nel sistema i nuovi moduli applicativi;

**responsabile Web:** decide se un modulo possa andare o meno in esercizio;

**referente applicativo:** sono i responsabili dei moduli applicativi esaminati;

**supervisore:** ruolo con funzioni di sola lettura, destinato ai Dirigenti.

# Seguro!

## Utenze - Gruppo Sicurezza

Al **Gruppo di Sicurezza** appartengono i ruoli:

**responsabile del Gruppo Sicurezza:** avvia i test di sicurezza dei sistemi, assegna i moduli in test ai membri del Gruppo Sicurezza, verifica gli esiti dei test effettuati, rende visibili gli attacchi effettuati al Gruppo di Sviluppo, dichiara chiusi i test per un determinato modulo;

**membro del Gruppo Sicurezza:** riporta nel sistema gli esiti dei test effettuati sull'applicazione, verifica l'effettiva correzione delle vulnerabilità da parte del Gruppo di Sviluppo;

**responsabile scansioni:** ha il compito di inserire nel sistema gli esiti delle scansioni automatiche dei moduli applicativi.

# Seguro!

## Utenze - Gruppo Sviluppo

Al **Gruppo di Sviluppo** appartengono i ruoli:

**responsabile dello Sviluppo:** assegna i moduli in correzione ai membri del Gruppo di Sviluppo, verifica gli esiti delle correzioni, dichiara corretto un determinato modulo rimandandolo in test al Gruppo Sicurezza;

**membro del Gruppo di Sviluppo:** analizza le segnalazioni del Gruppo Sicurezza; riporta nel sistema le correzioni delle vulnerabilità rilevate.

# Flusso del programma

# Flusso del programma

## Test di sicurezza

Il flusso del programma può essere così schematizzato:

1. il **responsabile del Collaudo** crea un nuovo modulo e lo rilascia per i test;

2. il **responsabile del Gruppo Sicurezza** avvia il test del modulo;

3. i **membri del Gruppo Sicurezza** verificano le diverse URL del modulo e riportano nel sistema l'esito degli attacchi;

4. il **responsabile del Gruppo Sicurezza** chiude i test con esito **OK** o **KO**;

5. il **responsabile Web** esamina gli esiti del test e decide se mandarlo in esercizio o se rimandarlo al Gruppo di Sviluppo per la correzione.

# Flusso del programma

## Correzione

Se il modulo è vulnerabile, viene sottomesso al Gruppo di Sviluppo per le correzioni del caso:

1. i **membri del Gruppo di Sviluppo** correggono gli errori rilevati;

2. il **responsabile dello Sviluppo** chiude la fase di correzione e il modulo torna al Gruppo Sicurezza per la verifica delle correzioni.

# Flusso del programma

## Verifica delle correzioni

Quando il modulo torna al Gruppo di Sicurezza per la verifica delle correzioni:

1. i **membri del Gruppo Sicurezza** verificano che gli attacchi riusciti nella fase precedente non siano più possibili;

2. il **responsabile del Gruppo Sicurezza** verifica gli esiti dei controlli effettuati, li ripete o li approfondisce, se necessario e quando tutte le vulnerabilità rilevate sono state sottoposte a controllo, chiude il test con esito **OK** o **KO**, a seconda dell'esito delle verifiche;

3. il **responsabile Web** esamina gli esiti della verifica e, di nuovo, decide se mandarlo in esercizio o se rimandarlo al Gruppo di Sviluppo per la correzione.

# Flusso del programma

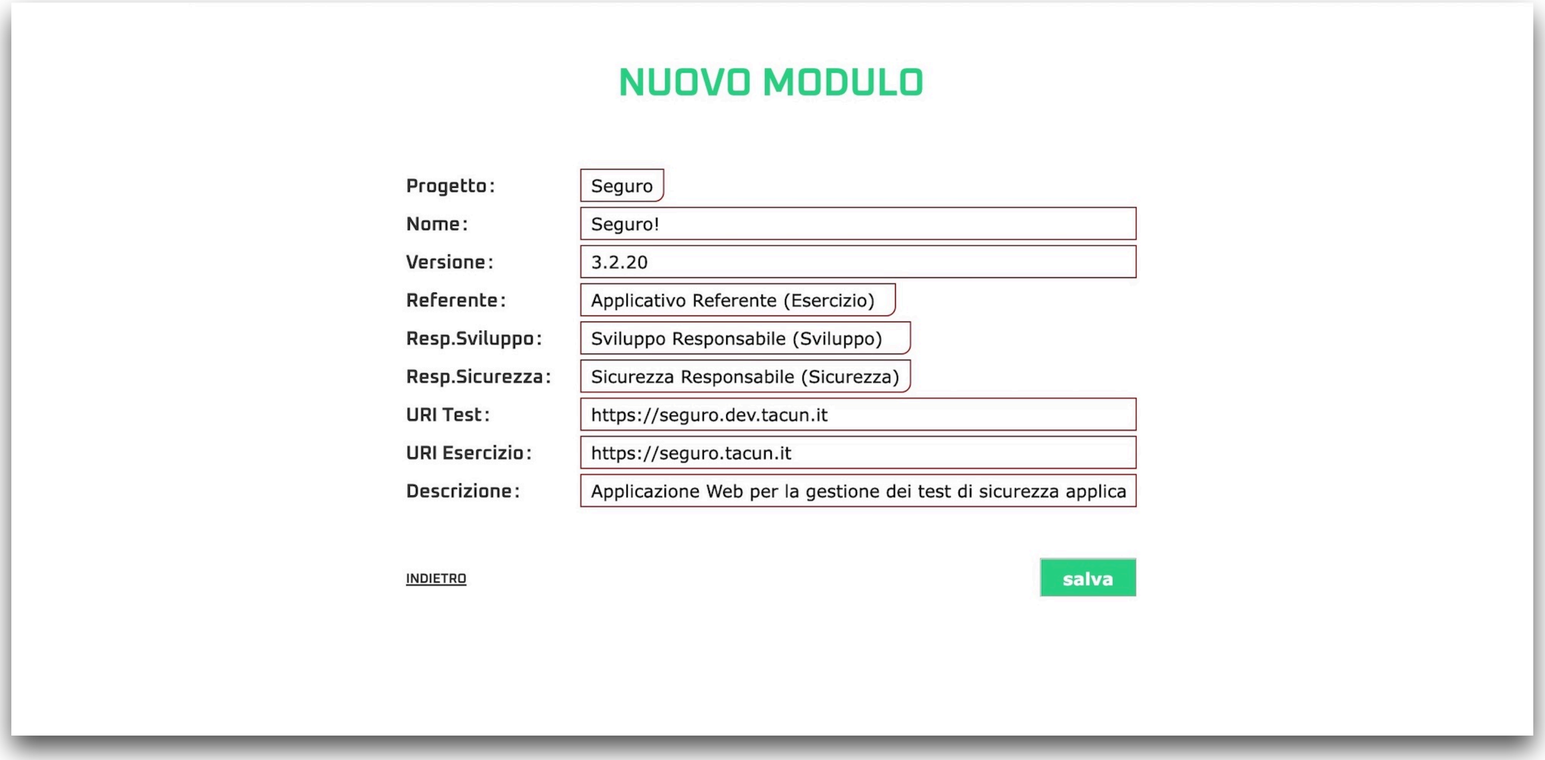
## Punti salienti del processo

Riassumiamo, nelle schede successive, i principali passi del processo di gestione dei test di sicurezza tramite l'applicazione **Seguro!**

Per una descrizione dettagliata dei singoli passi del processo, si veda, sotto, l'**Esempio di test applicativo**

# Flusso del programma

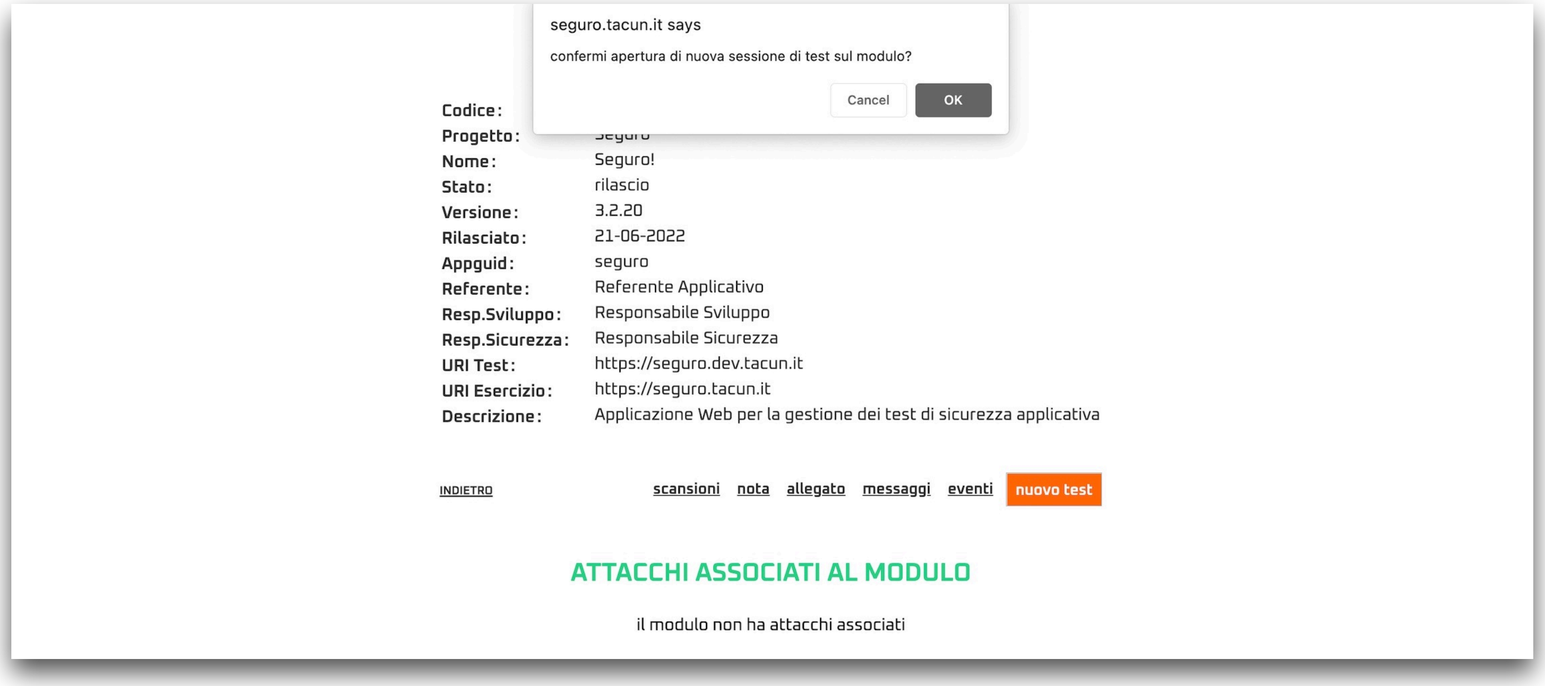
## Nuovo modulo




Il Responsabile Collaudo inserisce i dati di un nuovo modulo applicativo e lo rilascia per i test di sicurezza applicativa.

# Flusso del programma

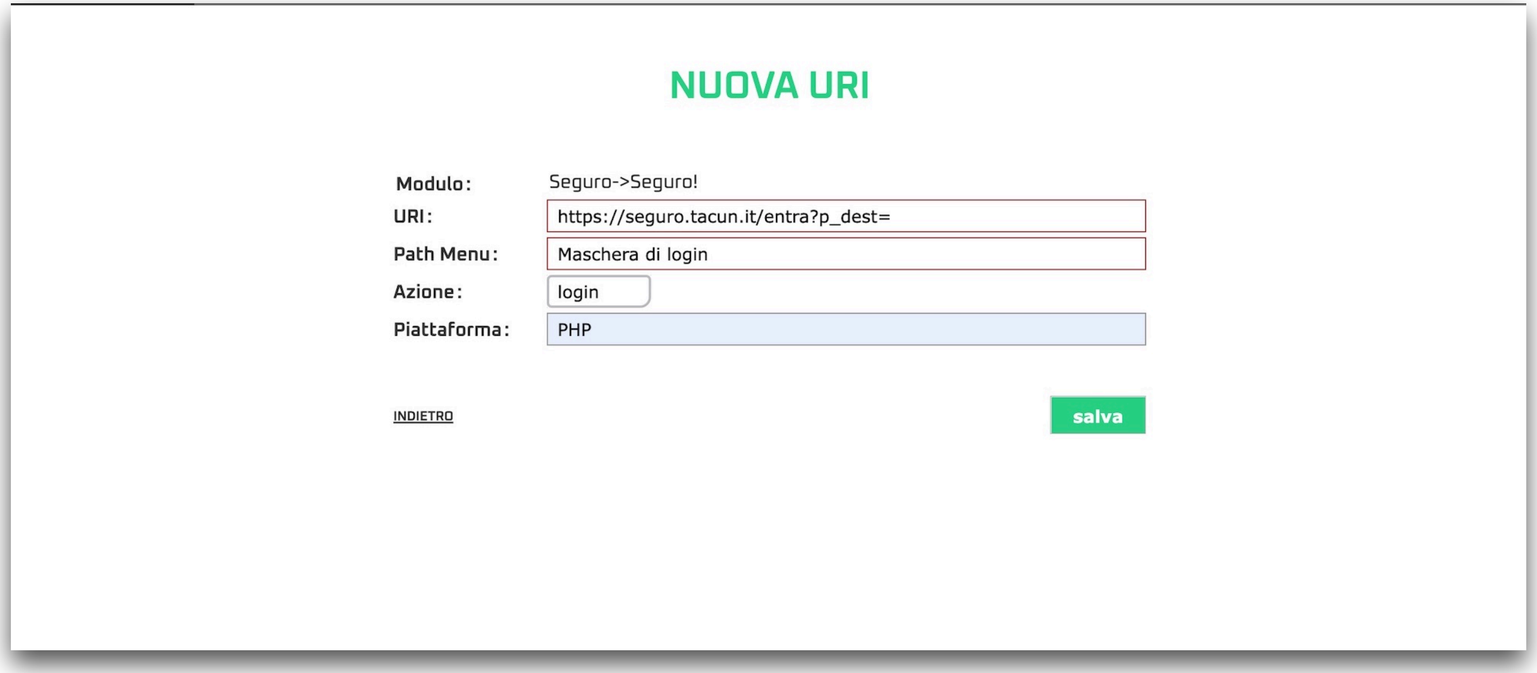
## Avvio nuovo test




Il **Responsabile del Gruppo Sicurezza** associa uno o più membri del Gruppo Sicurezza al modulo applicativo, poi avvia una nuova sessione di test.

# Flusso del programma

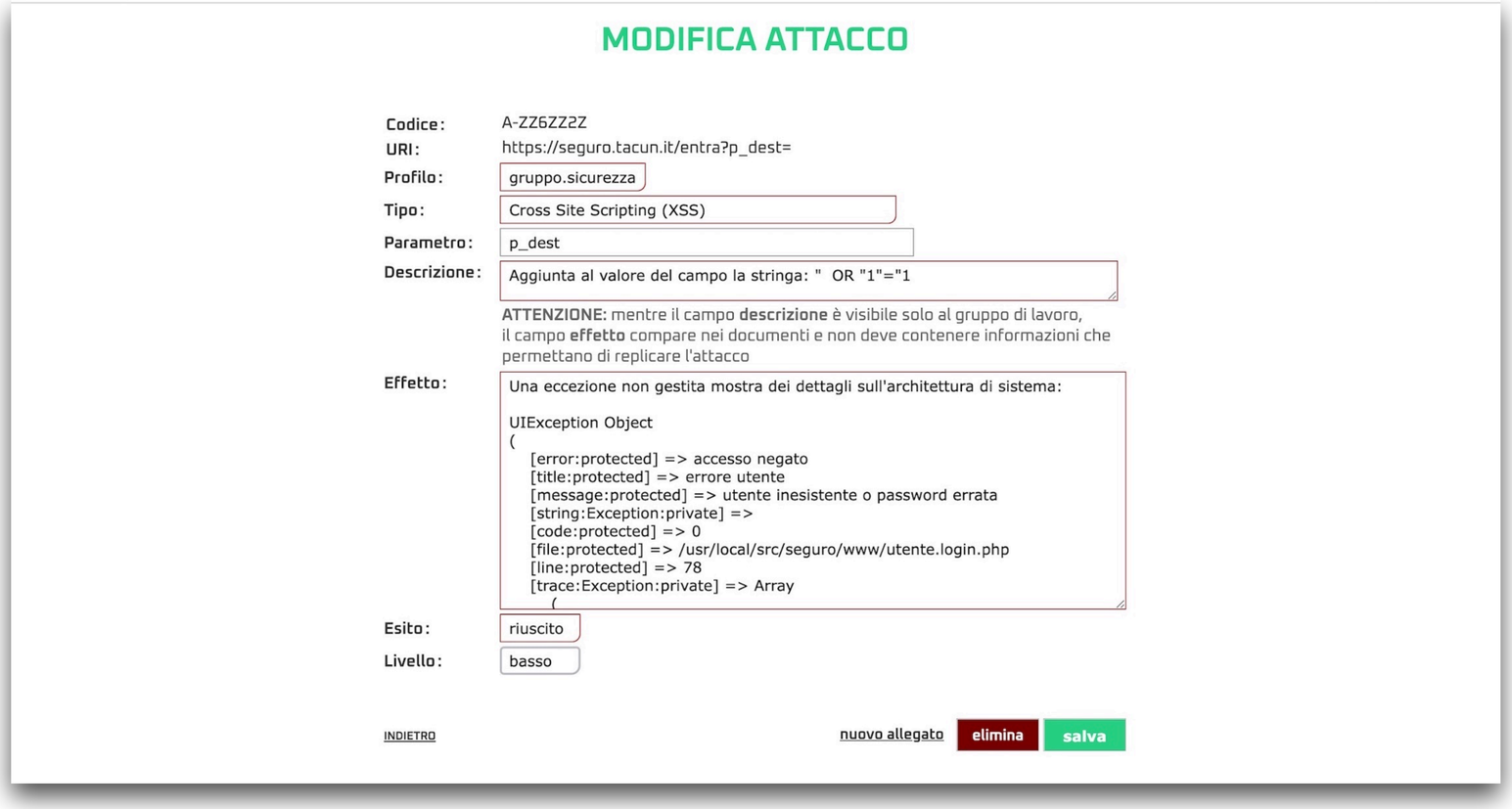
## Nuova URL




Un membro del Gruppo Sicurezza associa al modulo applicativo le URL su cui sono stati eseguiti i test di sicurezza.

# Flusso del programma

## Modifica dati attacco

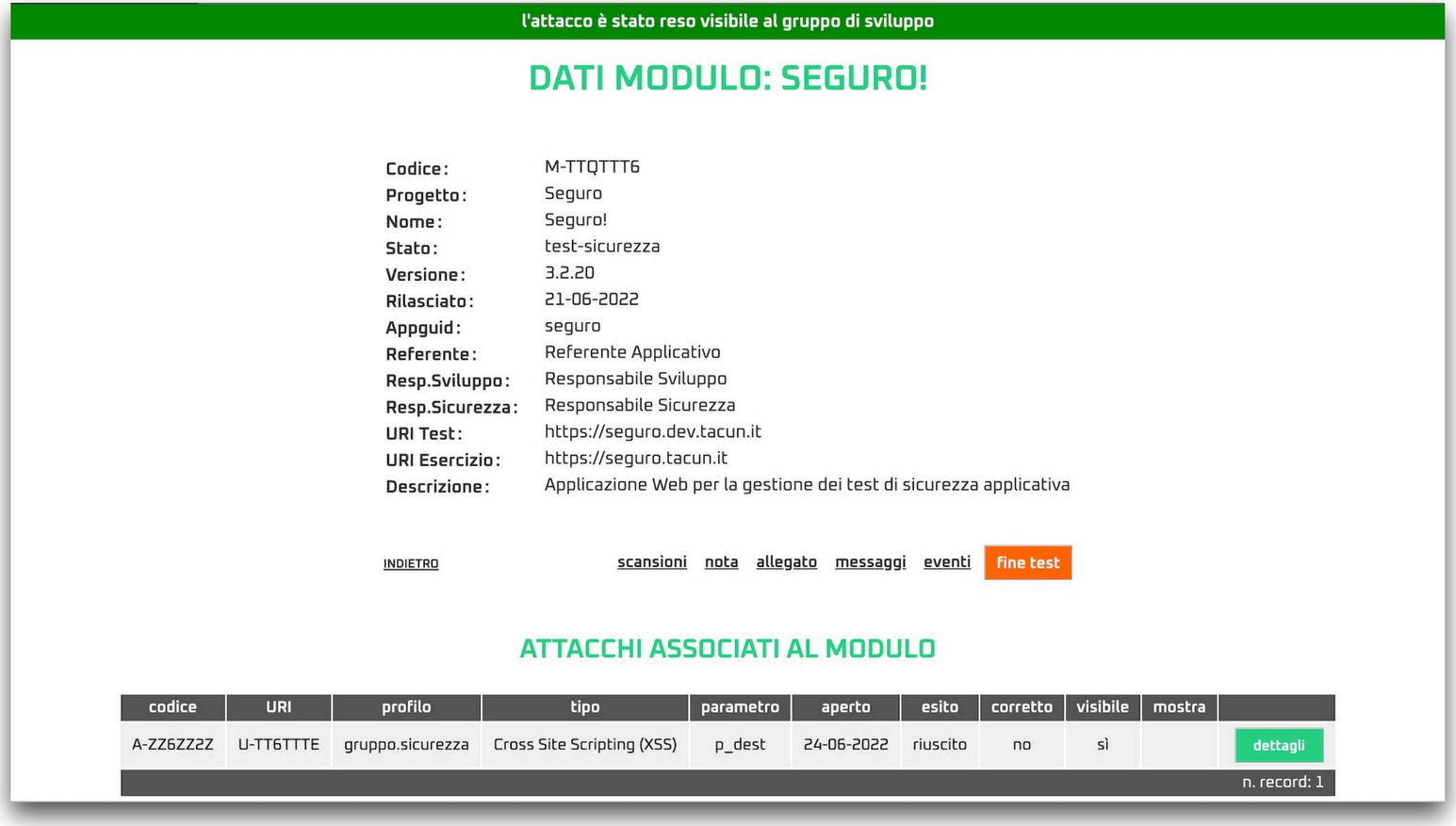



A ciascuna URI sono associati uno o più attacchi.

La maschera di gestione dell'attacco permette di definire le condizioni in cui è avvenuta la prova (URL, parametri, utenza ecc.), gli esiti dell'attacco (riuscito, fallito, nessuno) e il livello di rischio dell'eventuale vulnerabilità riscontrata.

# Flusso del programma

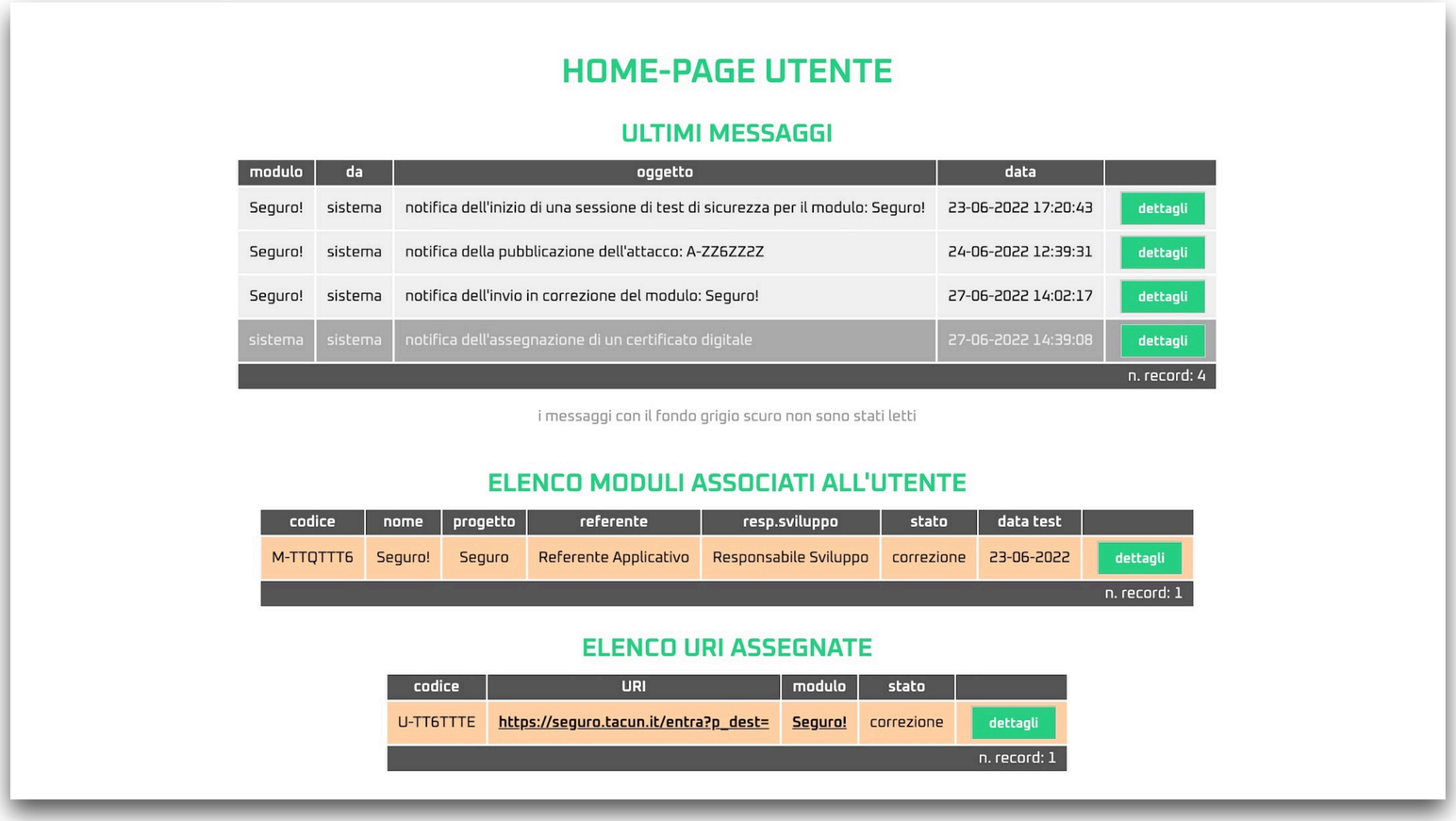
## Pubblicazione attacco




Il Responsabile del Gruppo Sicurezza verifica che l'attacco non sia un falso positivo, poi lo rende visibile al gruppo di sviluppo per le opportune correzioni.

# Flusso del programma

## Correzione delle vulnerabilità



HOME-PAGE UTENTE

ULTIMI MESSAGGI

| modulo | da | oggetto | data | |
|---|---|---|---|---|
| Seguro! | sistema | notifica dell'inizio di una sessione di test di sicurezza per il modulo: Seguro! | 23-06-2022 17:20:43 | dettagli |
| Seguro! | sistema | notifica della pubblicazione dell'attacco: A-ZZ6ZZ2Z | 24-06-2022 12:39:31 | dettagli |
| Seguro! | sistema | notifica dell'invio in correzione del modulo: Seguro! | 27-06-2022 14:02:17 | dettagli |
| sistema | sistema | notifica dell'assegnazione di un certificato digitale | 27-06-2022 14:39:08 | dettagli |

n. record: 4

i messaggi con il fondo grigio scuro non sono stati letti

ELENCO MODULI ASSOCIATI ALL'UTENTE

| codice | nome | progetto | referente | resp.sviluppo | stato | data test | |
|---|---|---|---|---|---|---|---|
| M-TTQTTT6 | Seguro! | Seguro | Referente Applicativo | Responsabile Sviluppo | correzione | 23-06-2022 | dettagli |

n. record: 1

ELENCO URI ASSEGNATE

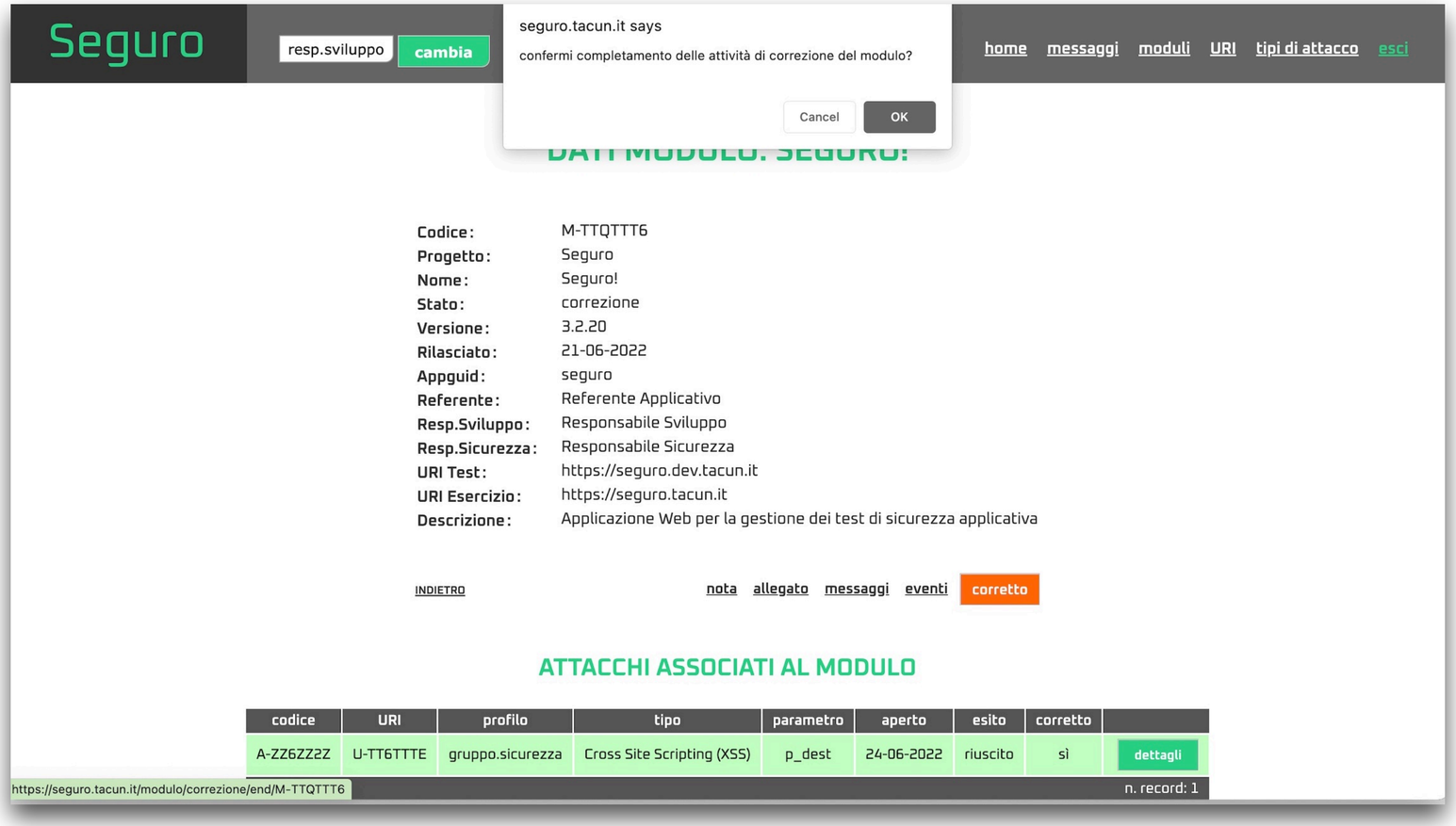
| codice | URI | modulo | stato | |
|---|---|---|---|---|
| U-TT6TTTE | https://seguro.tacun.it/entra?p_dest= | Seguro! | correzione | dettagli |

n. record: 1

Il Gruppo di Sviluppo riceve la segnalazione delle vulnerabilità e apporta le necessarie correzioni o modifiche al sistema.

# Flusso del programma

## Correzione del modulo




Quando tutte le URL e tutti gli attacchi sono stati corretti, il Responsabile del Gruppo di Sviluppo rimanda il modulo al test di sicurezza per le opportune verifiche.

# Gestione dei test

# Gestione dei test

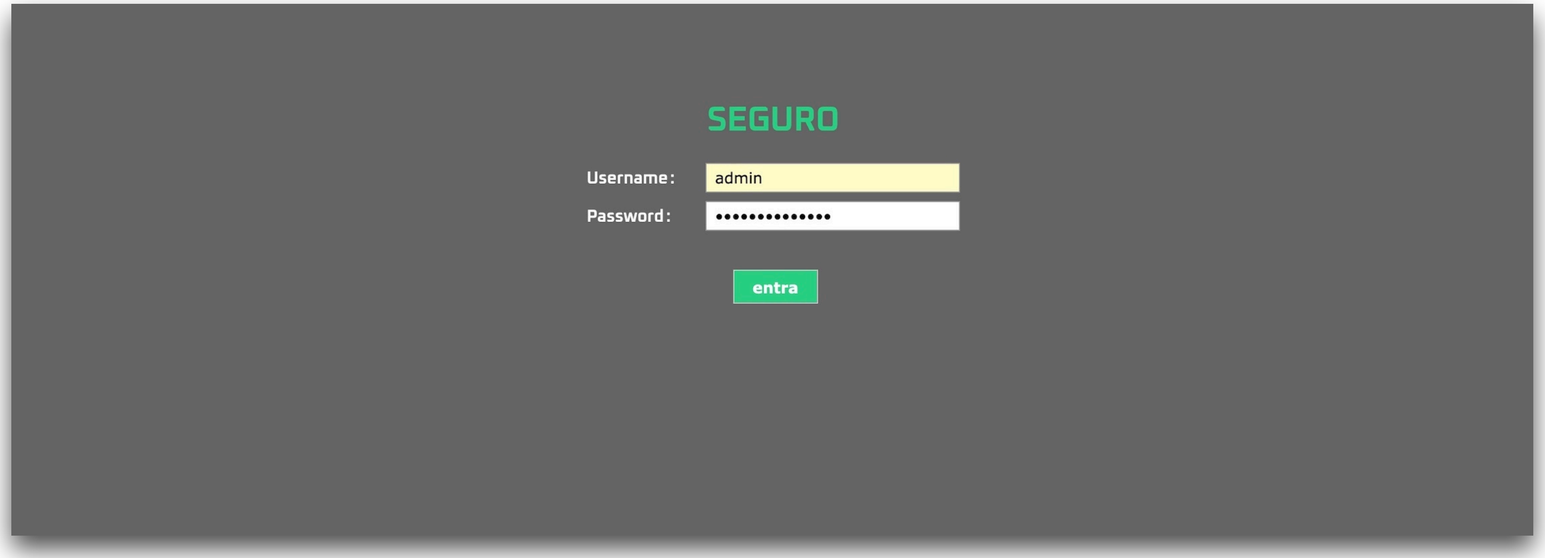
## Esempio di test applicativo

Le schede successive illustrano il modo in cui Seguro! permette di gestire le tre fasi descritte sopra.

Il modulo applicativo in esame, è **Seguro!** stesso.

# Utente amministratore

## Accesso al sistema




L’utente amministratore accede al sistema.

In questo caso, lo fa con username e password locali, ma solo a titolo di esempio.

È bene che tutte le utenze si autentichino con certificato digitale e password, in modo da garantire la non-ripudiabilità delle azioni intraprese.

# Utente amministratore

## Elenco utenti


Facendo click sulla voce di menu **utenti**, l'amministratore accede all'elenco utenti.

Facendo click sul bottone **dettagli**, a destra nell'elenco, va alla maschera di modifica dati utente.

# Utente amministratore

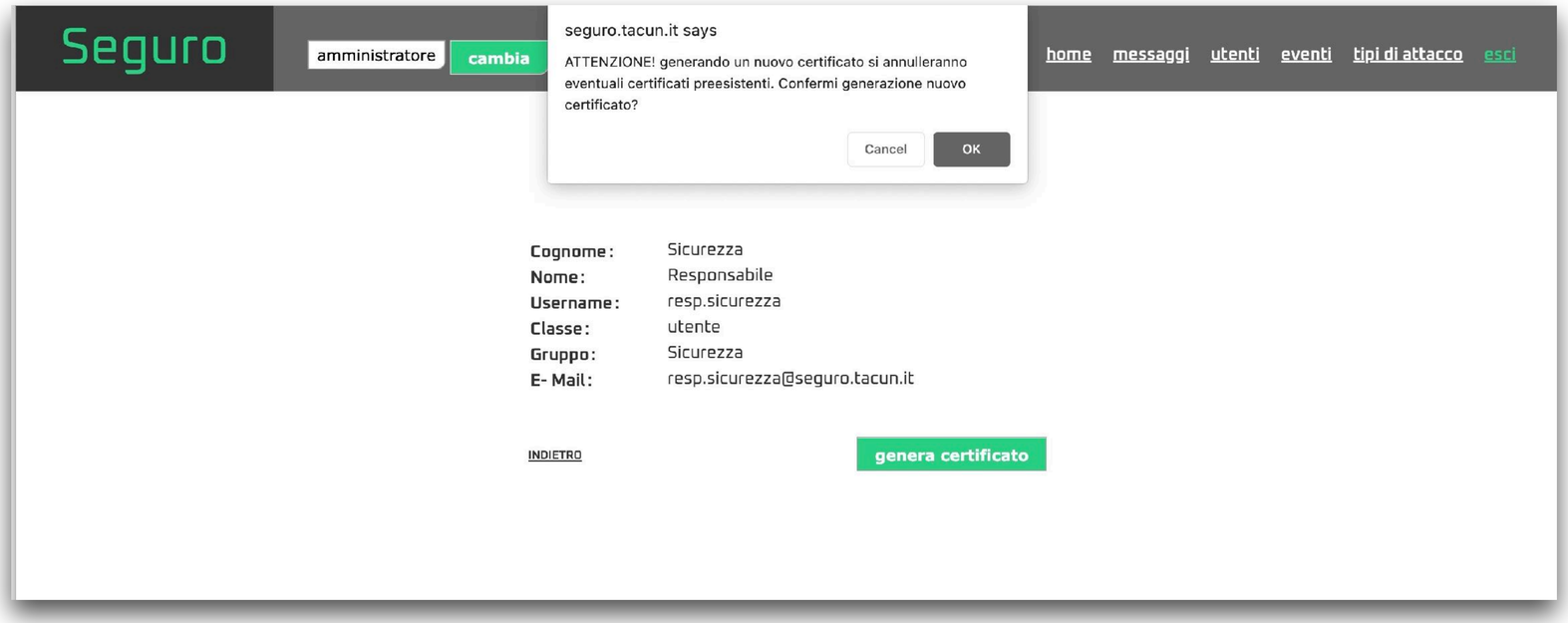
## Modifica dati utente


In questa maschera, l'amministratore può modificare i dati dell'utente.

Facendo click sul link **nuovo certificato**, si apre la maschera di generazione nuovo certificato.

# Utente amministratore

## Generazione nuovo certificato




Facendo click sul bottone **genera certificato**, un messaggio pop-up ricorda che la generazione di un nuovo certificato invalida tutti i certificati precedenti.

Se l'amministratore fa click sul bottone **OK**, il sistema genera un nuovo certificato per l'utente.

# Utente amministratore

## Modifica certificato

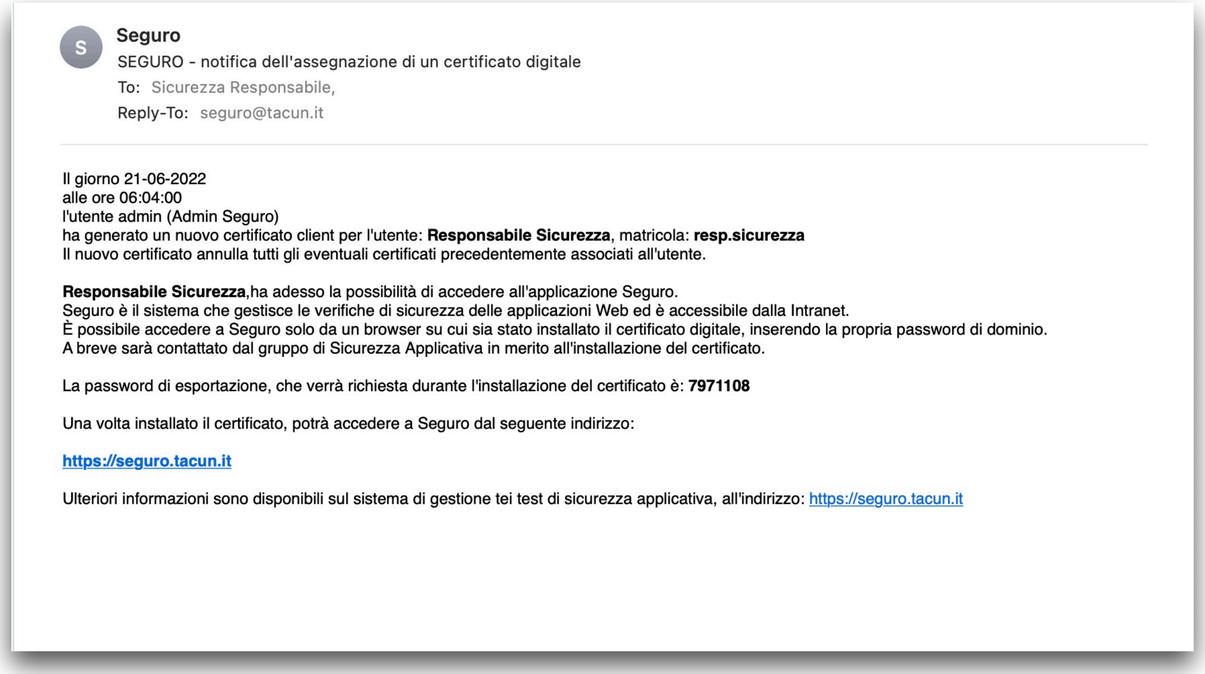

Il sistema apre la maschera di modifica certificato.

Selezionando il radiobutton Attivo **No**, si può disabilitare temporaneamente l'accesso con questo certificato, senza però invalidarlo.

Facendo click sul link **scarica certificato**, si scarica il nuovo certificato.

# Utente amministratore

## Messaggio per certificato



**Seguro**
SEGURO - notifica dell'assegnazione di un certificato digitale
To: Sicurezza Responsabile,
Reply-To: seguro@tacun.it

Il giorno 21-06-2022
alle ore 06:04:00
l'utente admin (Admin Seguro)
ha generato un nuovo certificato client per l'utente: **Responsabile Sicurezza**, matricola: **resp.sicurezza**
Il nuovo certificato annulla tutti gli eventuali certificati precedentemente associati all'utente.

**Responsabile Sicurezza**,ha adesso la possibilità di accedere all'applicazione Seguro.
Seguro è il sistema che gestisce le verifiche di sicurezza delle applicazioni Web ed è accessibile dalla Intranet.
È possibile accedere a Seguro solo da un browser su cui sia stato installato il certificato digitale, inserendo la propria password di dominio.
A breve sarà contattato dal gruppo di Sicurezza Applicativa in merito all'installazione del certificato.

La password di esportazione, che verrà richiesta durante l'installazione del certificato è: **7971108**

Una volta installato il certificato, potrà accedere a Seguro dal seguente indirizzo:

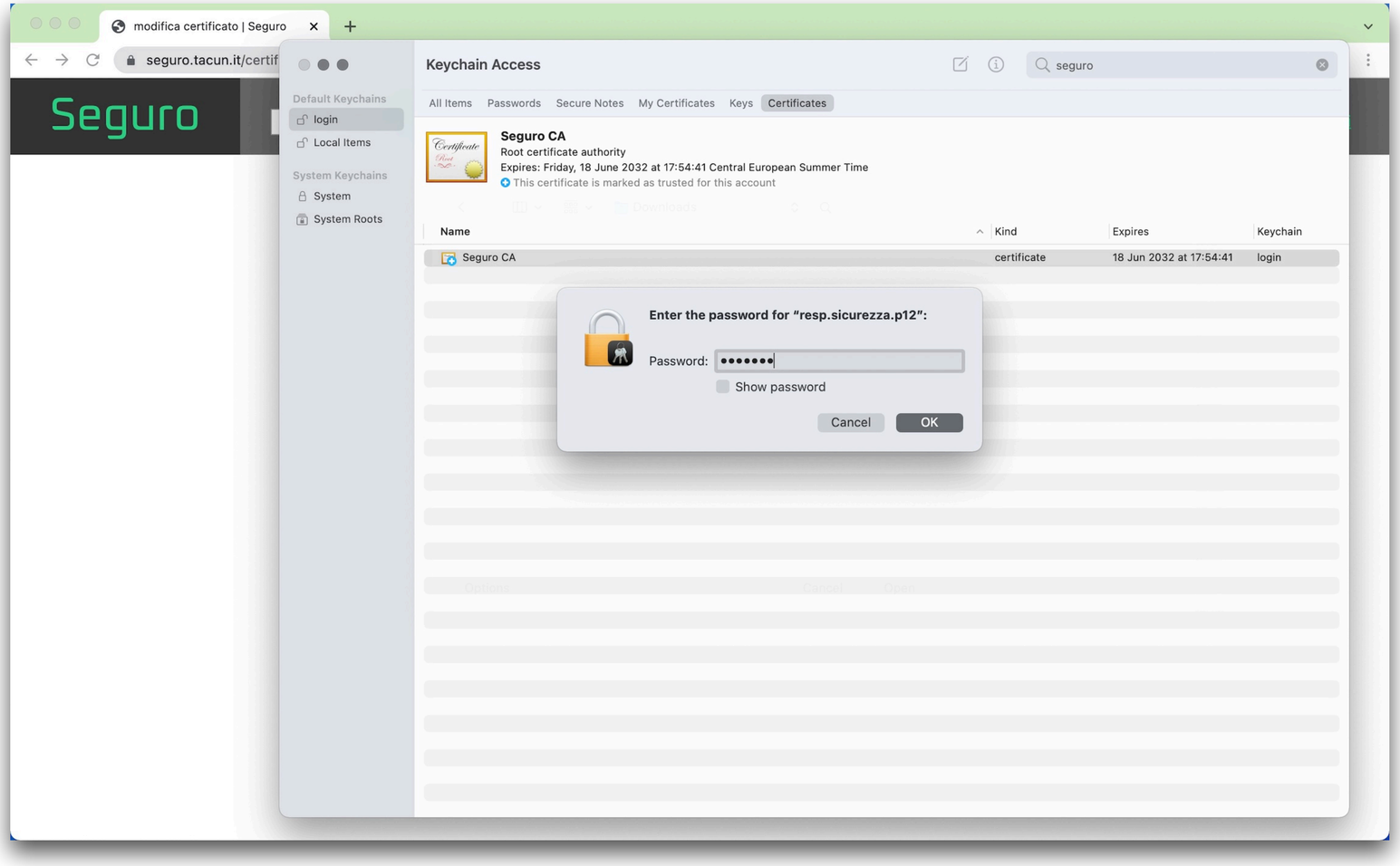
**https://seguro.tacun.it**

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando si genera un nuovo certificato, il sistema gli invia all’utente un messaggio di notifica che contiene la password di importazione e le istruzioni per l’accesso al sistema.

# Utente amministratore

## Importazione certificato

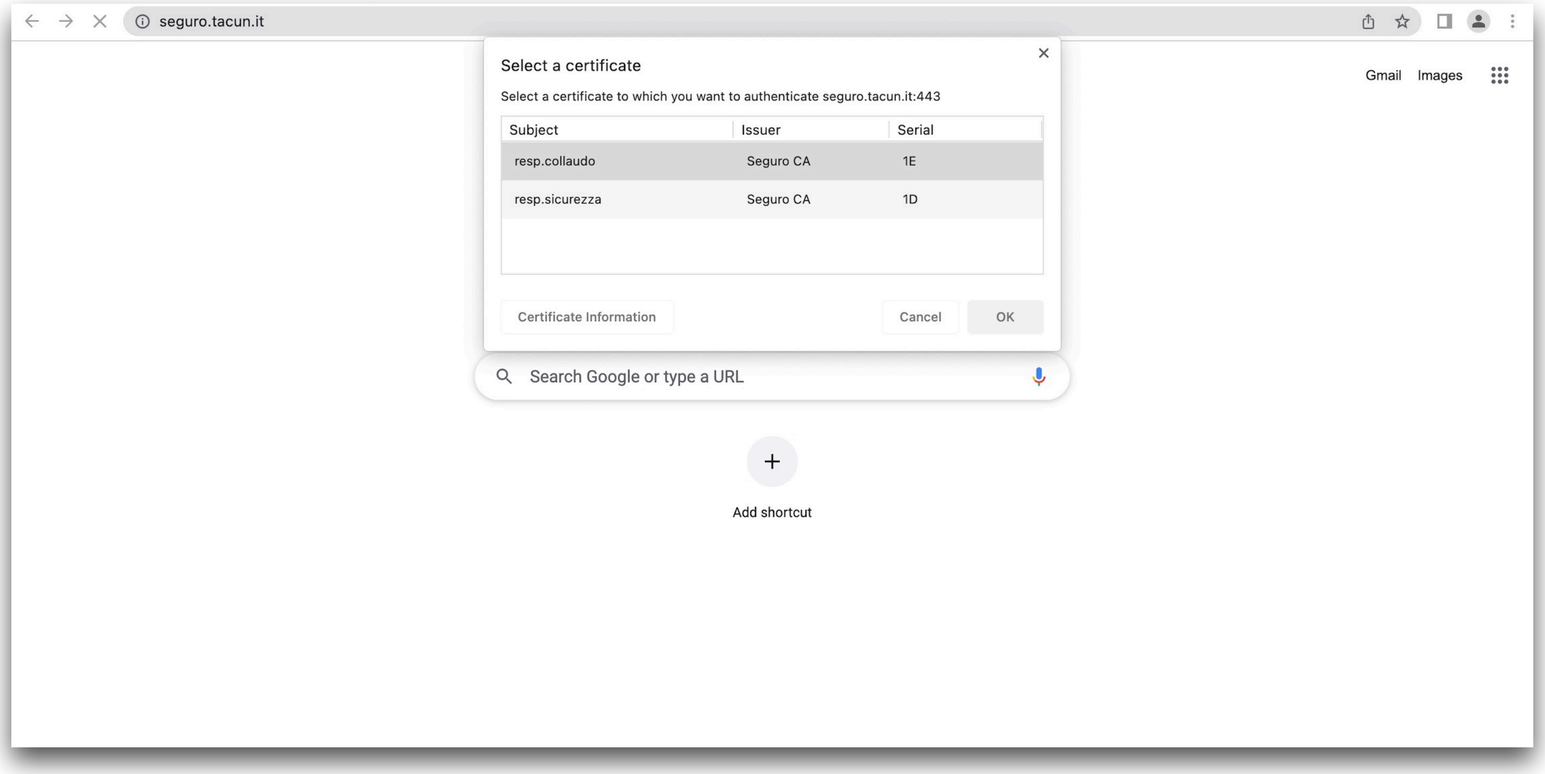



Il certificato viene consegnato **personalmente** all'utente dal Gruppo Sicurezza.

Per poter accedere al sistema, l'utente deve importare il certificato sul suo computer, utilizzando la password ricevuta con il messaggio di notifica.

# Responsabile collaudo

## Login con certificato

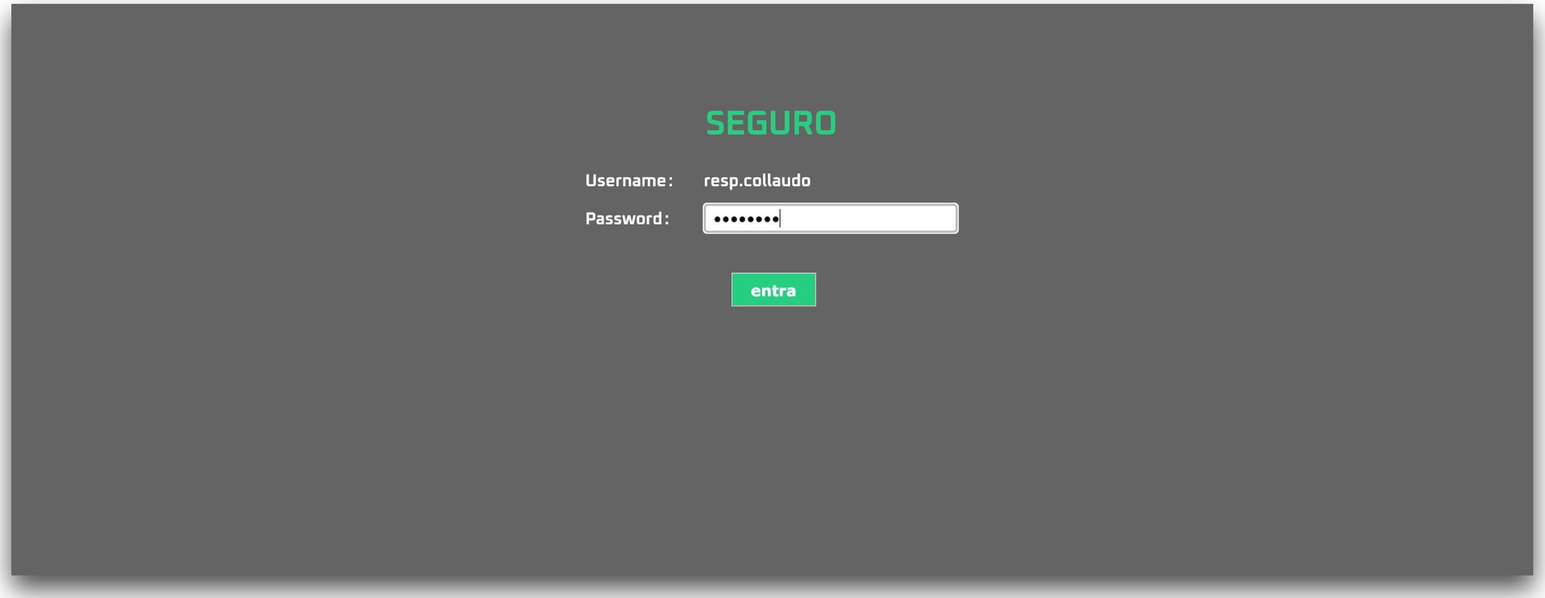



Quando l'utente accede al sistema, il browser permette di scegliere quale certificato utilizzare per l'accesso.

Questa immagine ha unicamente valore dimostrativo: non è bene che ci siano due certificati su uno stesso computer.

# Responsabile collaudo

## Login con certificato




Se il sistema rileva la presenza di un certificato utente sul computer, usa il CN associato come username in sola lettura e richiede l'inserimento della password, che può essere quella locale o quella di dominio, nel caso di utenze LDAP.

# Responsabile collaudo

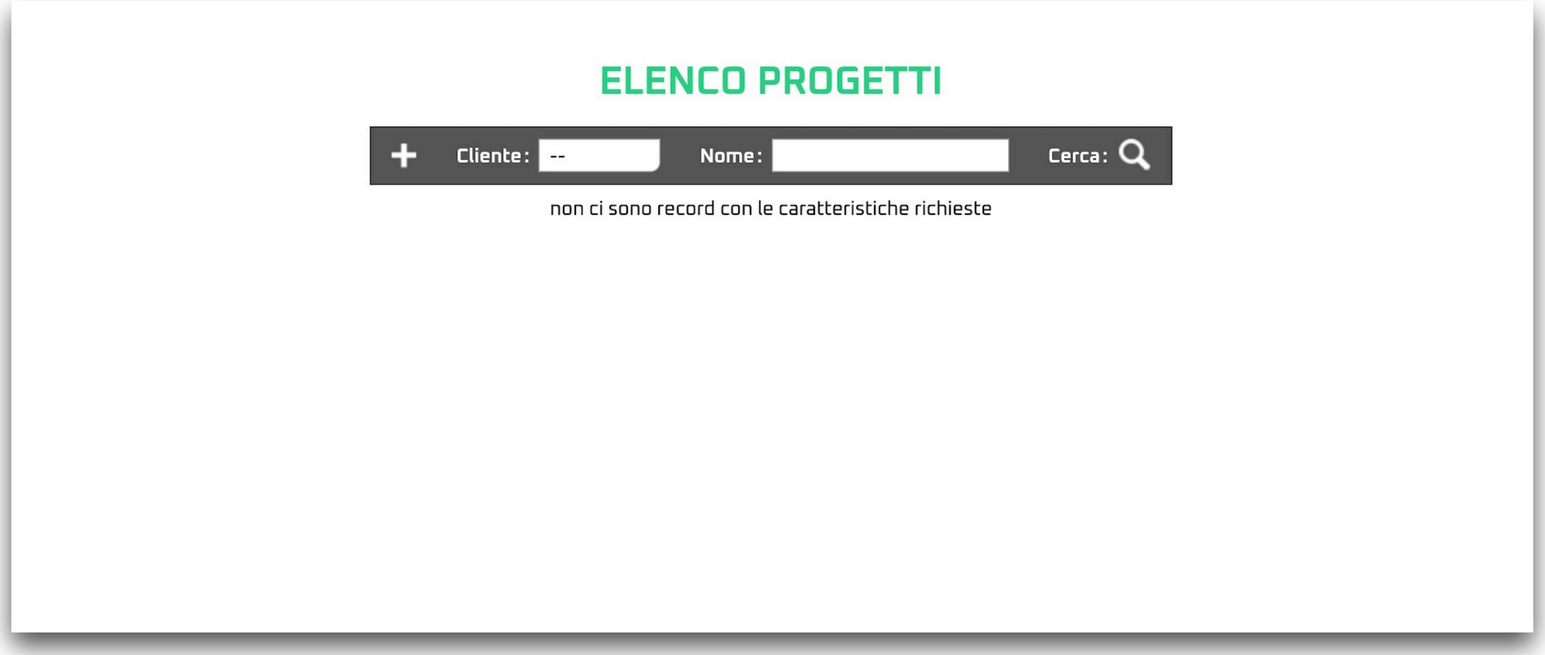
## Login con certificato


Nella home-page, il Responsabile Collaudo ha un elenco dei messaggi ricevuti.

Facendo click sulla voce di **menu progetti**, si accede all'elenco progetti.

# Responsabile collaudo

## Elenco progetti

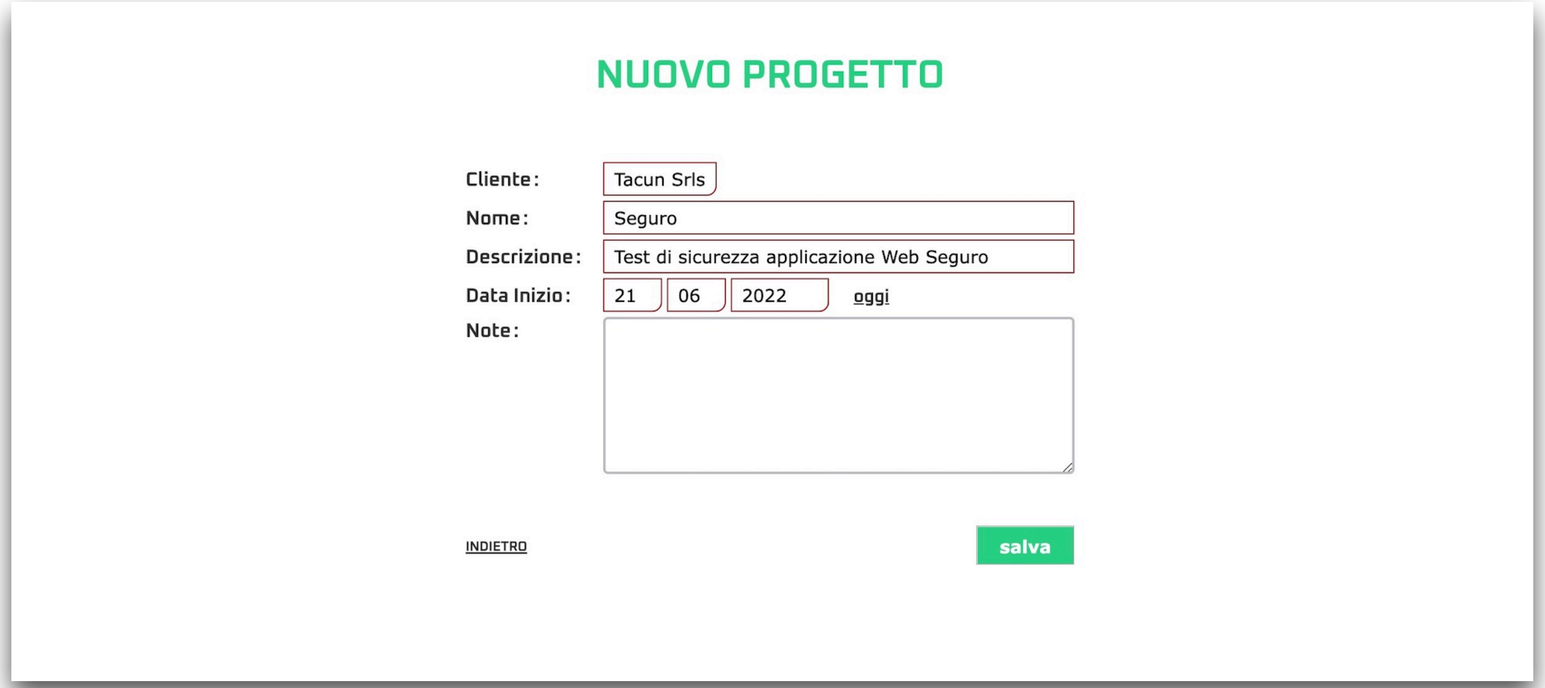



Inizialmente, l'elenco progetti è vuoto.

Facendo click sul simbolo **+**, in alto a sinistra nella barra di ricerca, si apre la maschera di inserimento nuovo progetto.

# Responsabile collaudo

## Nuovo progetto




L’utente inserisce i dati del progetto, poi fa click sul bottone **salva.**

Si apre così la pagina di modifica dati progetto.

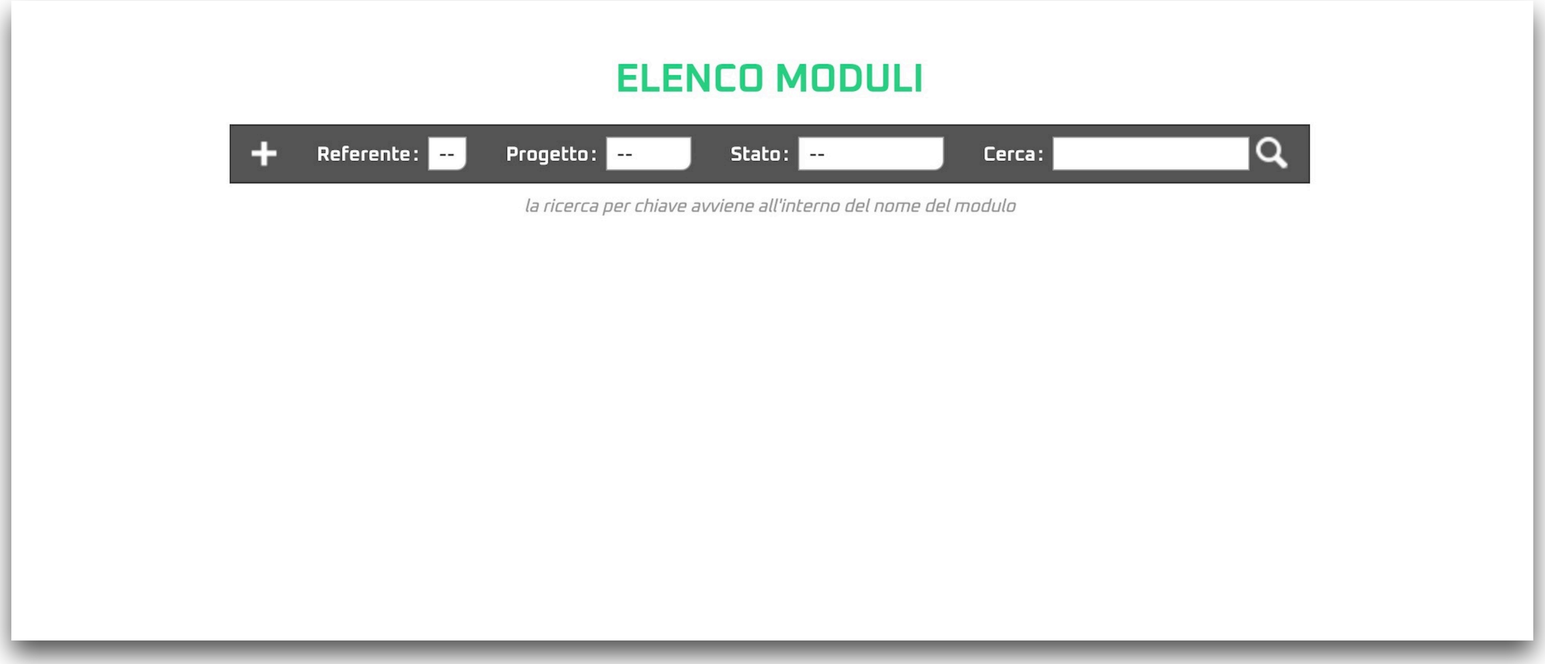
# Responsabile collaudo

## Modifica progetto


Rispetto alla maschera di inserimento, la maschera di modifica dati progetto ha, in più, il campo per l'inserimento della data di fine del progetto e l'elenco dei moduli applicativi e degli utenti associati al progetto.

# Responsabile collaudo

## Elenco moduli applicativi




Facendo click sulla voce di menu **moduli**, si apre l’elenco moduli applicativi.

Inizialmente, l’elenco progetti è vuoto.

Facendo click sul simbolo **+**, in alto a sinistra nella barra di ricerca, si apre la maschera di inserimento nuovo modulo.

# Responsabile collaudo

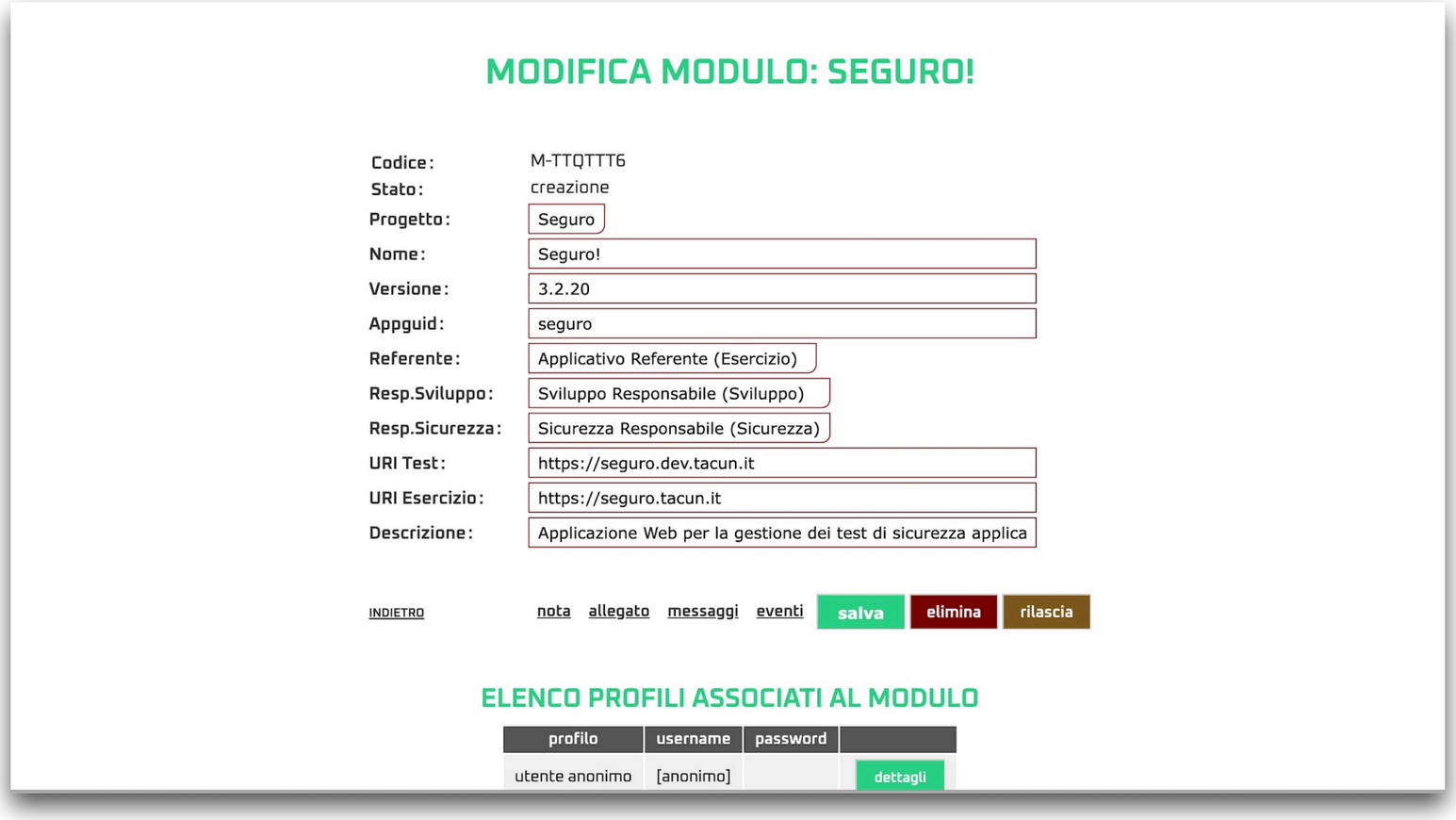
## Nuovo modulo


L'utente riempie i campi della maschera e poi li salva facendo click sul bottone **salva**.

Si apre così la maschera di modifica dati modulo.

# Responsabile collaudo

## Modifica dati modulo - 1




La maschera di modifica dati modulo ha dei link per l'aggiunta di allegati o di note e una serie di elenchi per le diverse entità associate al modulo.

Lo stato corrente del modulo è visualizzato in sola lettura in alto sotto al codice.

# Responsabile collaudo

## Modifica dati modulo - 2

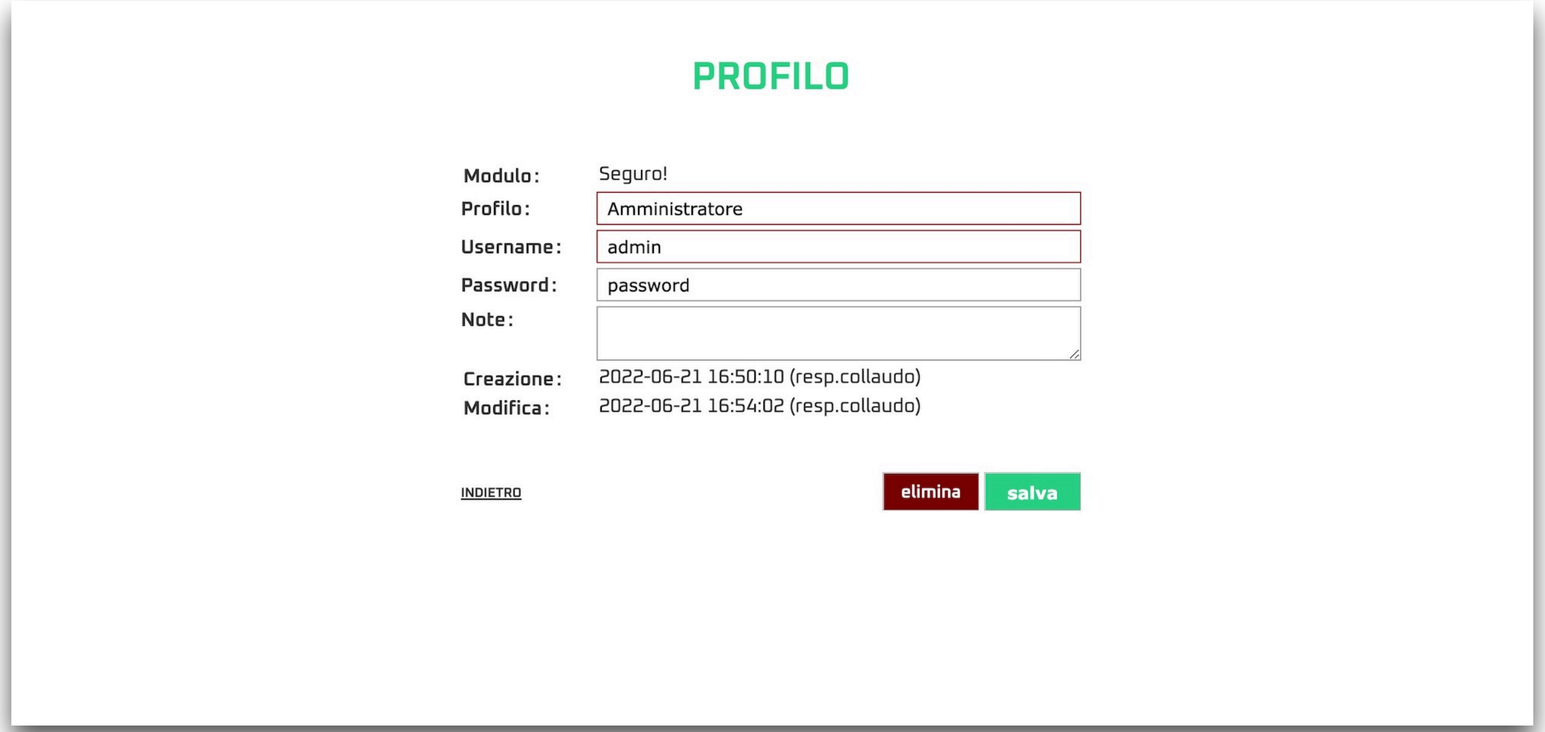

Il primo elenco contiene i profili utente associati al modulo.

Il secondo elenco, contiene gli attributi del modulo.

Il terzo elenco riporta il nome degli utenti associati al modulo e un’eventuale data di fine associazione.

# Responsabile collaudo

## Modifica profili utente



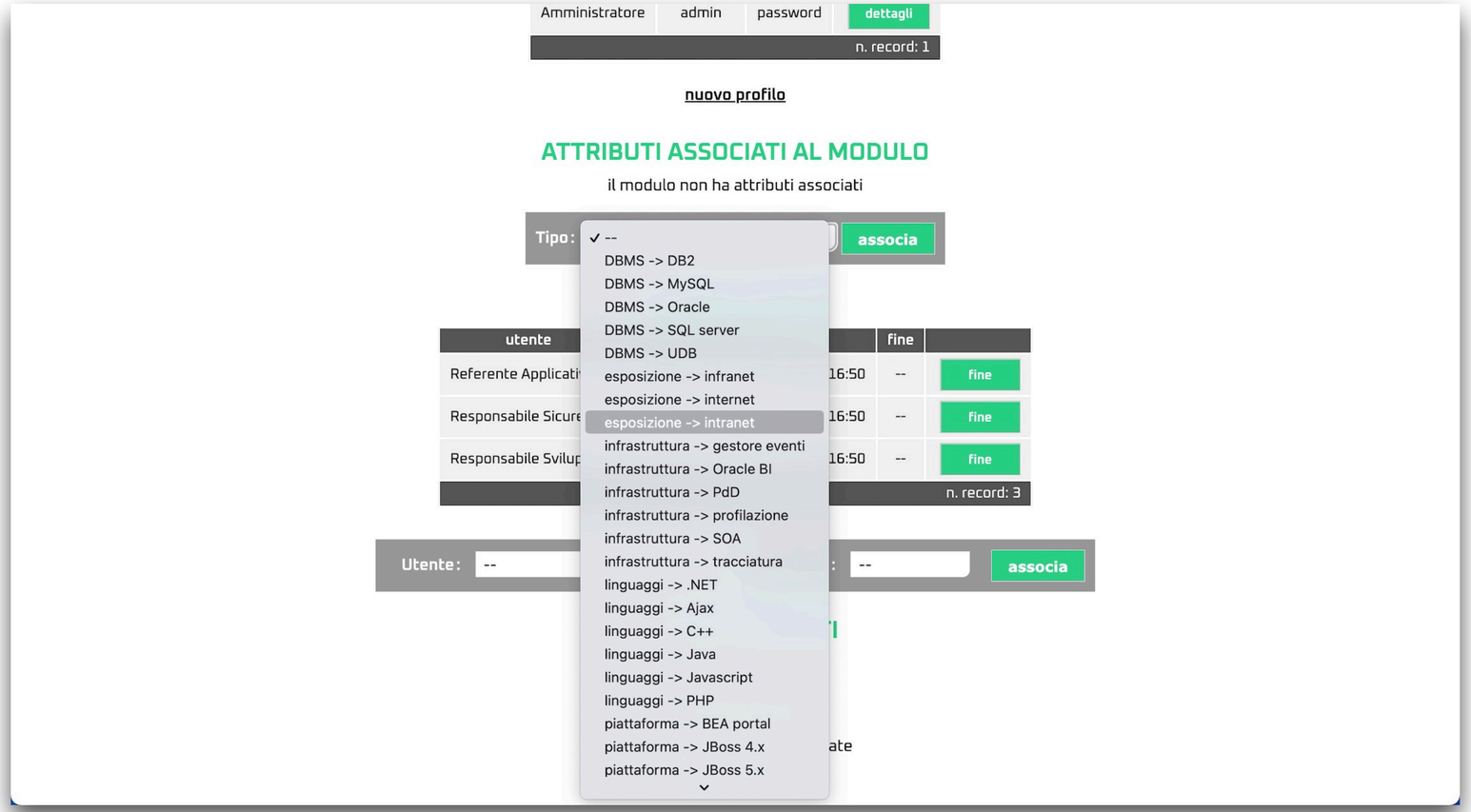

Il sistema associa a ogni nuovo modulo un profilo di utenza di default.

Facendo click sul bottone **dettagli** a destra nell'elenco, si apre la maschera di modifica dati profilo.

Dato che **Seguro!** non ha utenze anonime, modifichiamo il profilo per gestire l'utenza di amministrazione.

# Responsabile collaudo

## Aggiunta attributi




Selezionando un attributo dalla casella a discesa e facendo click sul bottone **associa**, si associa l'attributo al modulo applicativo.

Non è possibile associare due volte lo stesso attributo a uno stesso modulo.

# Responsabile collaudo

## Aggiunta attributi


Per rimuovere un attributo del modulo, si deve fare click sul bottone **elimina** a destra nell'elenco.

# Responsabile collaudo

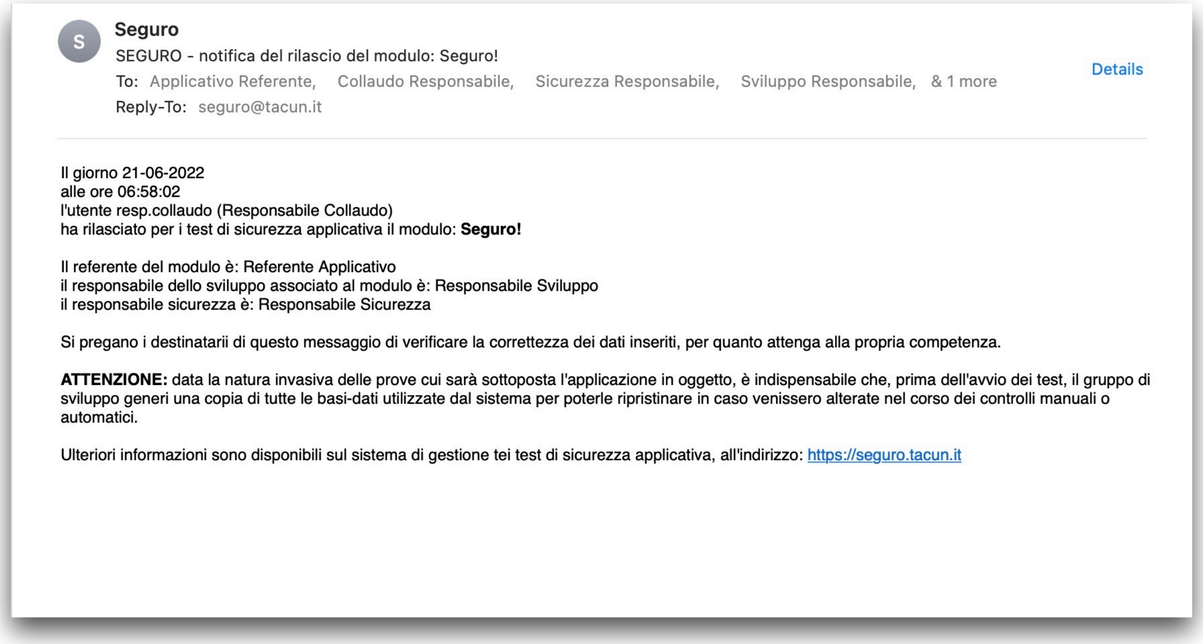
## Rilascio del modulo


Quando sono state inserite tutte le informazioni sul modulo, lo si può rilasciare per i test di sicurezza facendo click sul bottone **rilascia** nella barra sotto alla form.

Lo stato del modulo passa da **creazione** a **rilascio**.

# Responsabile collaudo

## Messaggio per rilascio modulo



**Seguro**
SEGURO - notifica del rilascio del modulo: Seguro!
To: Applicativo Referente, Collaudo Responsabile, Sicurezza Responsabile, Sviluppo Responsabile, & 1 more
Details
Reply-To: seguro@tacun.it

Il giorno 21-06-2022
alle ore 06:58:02
l'utente resp.collaudo (Responsabile Collaudo)
ha rilasciato per i test di sicurezza applicativa il modulo: **Seguro!**

Il referente del modulo è: Referente Applicativo
il responsabile dello sviluppo associato al modulo è: Responsabile Sviluppo
il responsabile sicurezza è: Responsabile Sicurezza

Si pregano i destinatarii di questo messaggio di verificare la correttezza dei dati inseriti, per quanto attenga alla propria competenza.

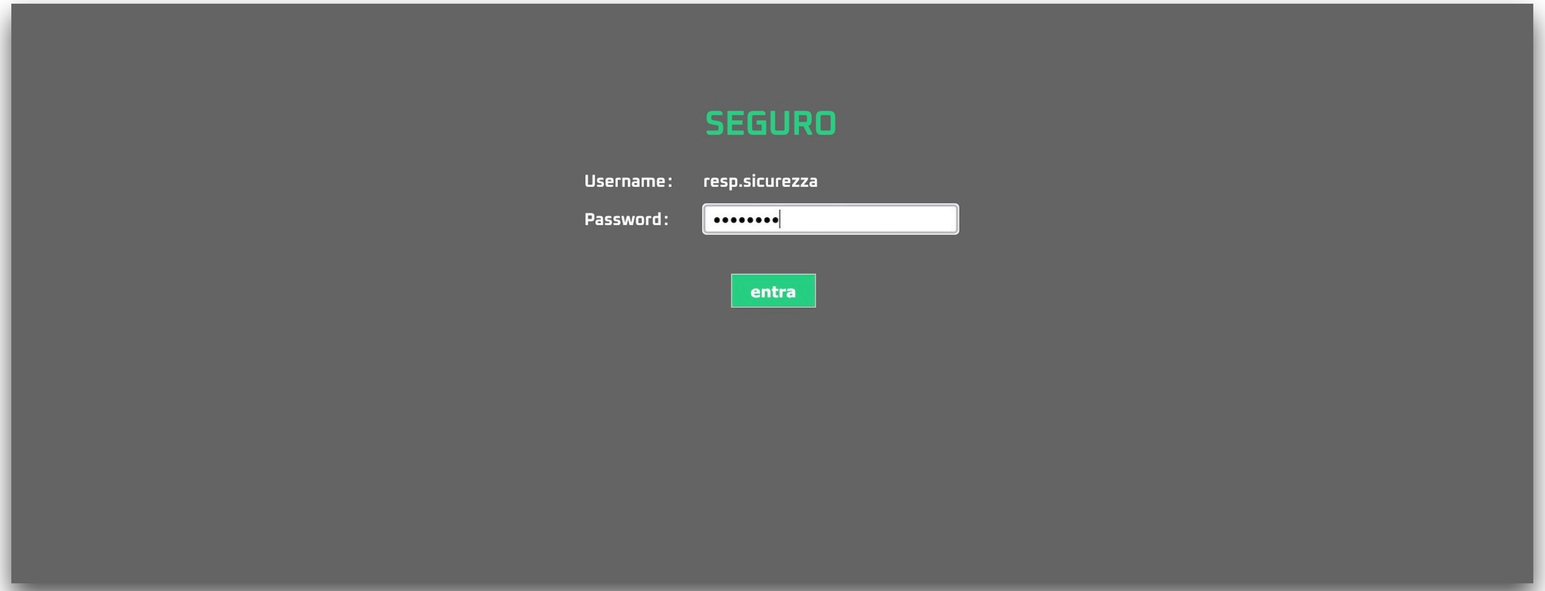
**ATTENZIONE:** data la natura invasiva delle prove cui sarà sottoposta l'applicazione in oggetto, è indispensabile che, prima dell'avvio dei test, il gruppo di sviluppo generi una copia di tutte le basi-dati utilizzate dal sistema per poterle ripristinare in caso venissero alterate nel corso dei controlli manuali o automatici.

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando un modulo viene rilasciato, il sistema invia a tutti gli utenti coinvolti un messaggio contenente le informazioni necessarie all’esecuzione dei test.

# Responsabile sicurezza

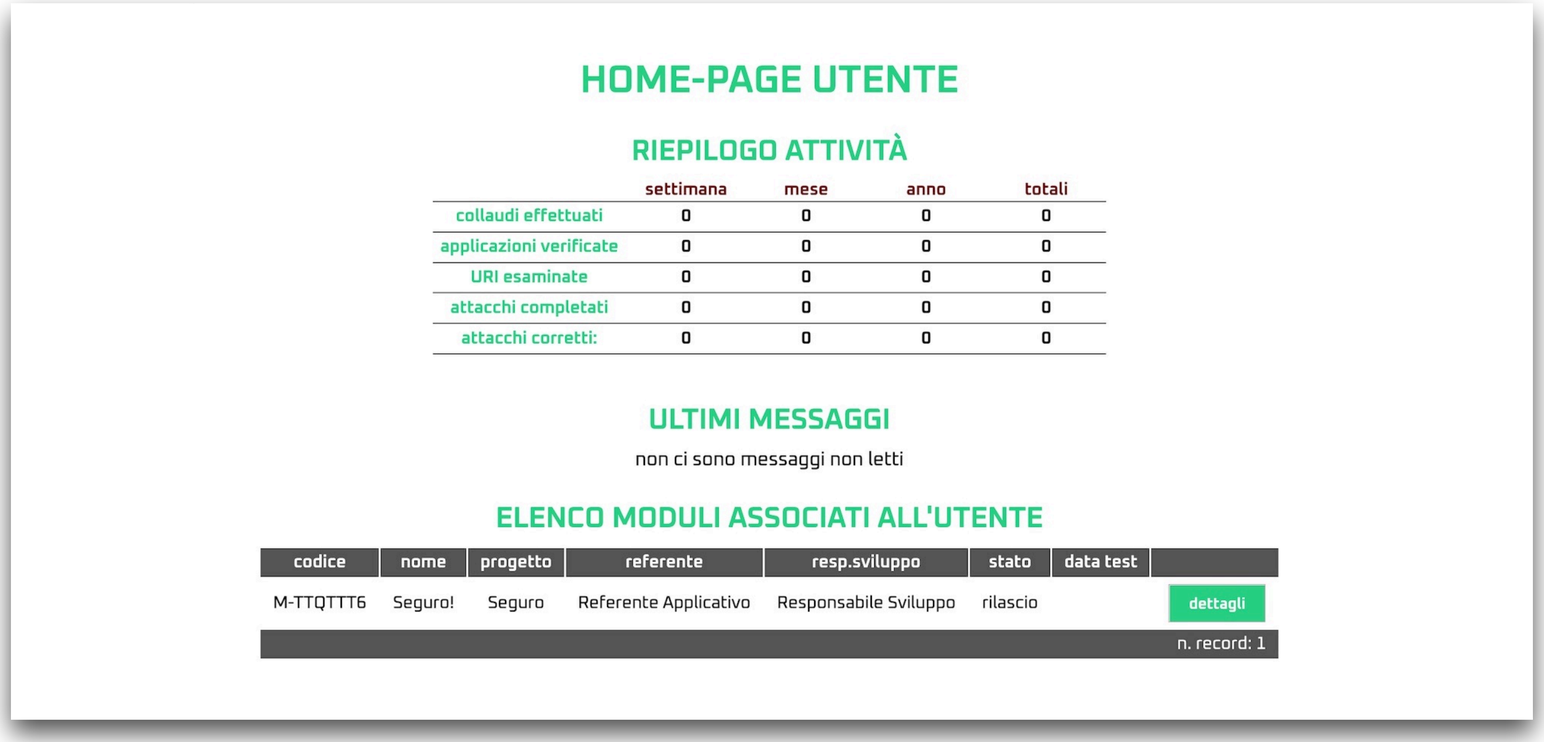
## Login con certificato




Il responsabile del Gruppo Sicurezza accede con il certificato e inserisce la sua password.

# Responsabile sicurezza

## Home page




Nella home-page del responsabile del Gruppo Sicurezza c'è un riepilogo delle attività svolte, un elenco dei messaggi ricevuti e l'elenco dei moduli associati.

Facendo click sul bottone **dettagli** a destra nell'elenco moduli, si apre la maschera di gestione del modulo.

# Responsabile sicurezza

## Gestione modulo - 1


La maschera di gestione de dati modulo ha i link per l'aggiunta di allegati o di note, ma i dati del modulo sono visualizzati in sola lettura.

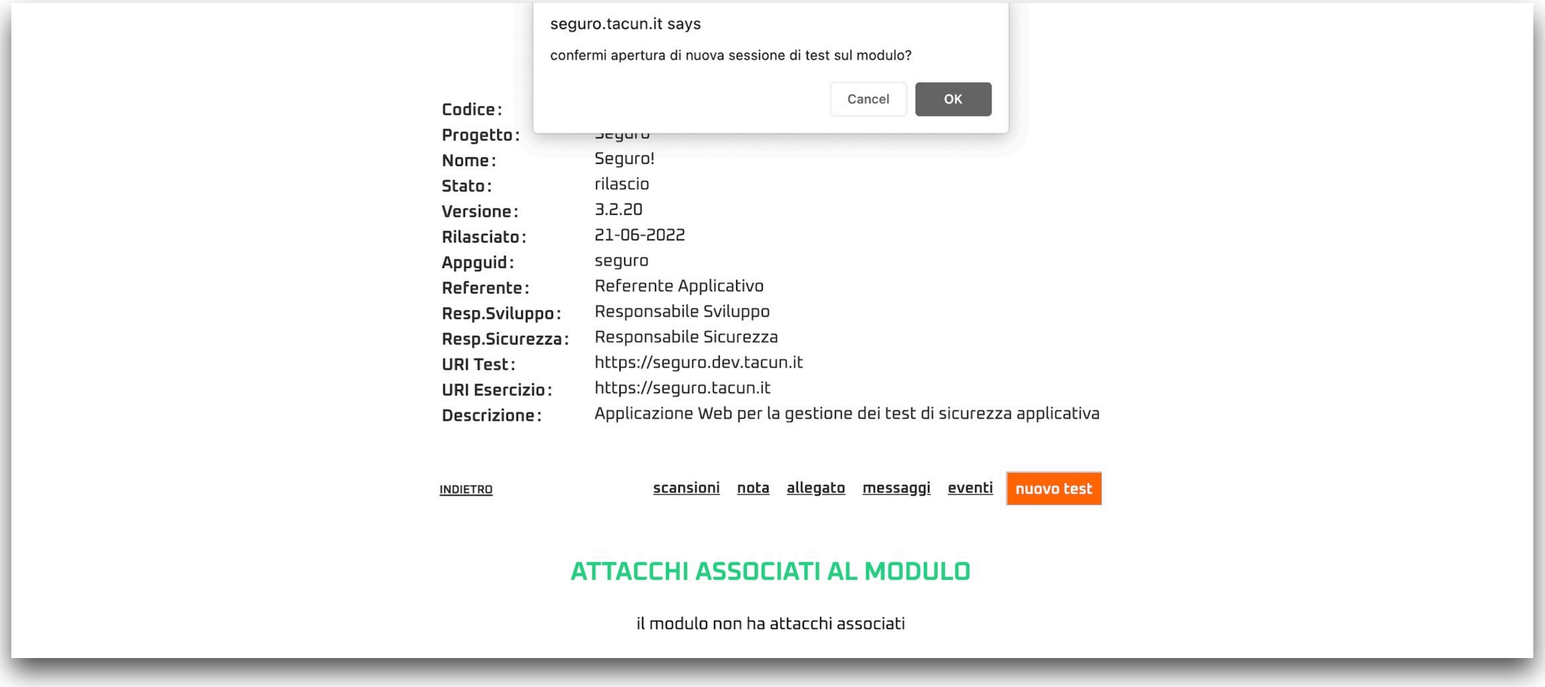
# Responsabile sicurezza

## Gestione modulo - 2


Al contrario, gli attributi e le utenze possono essere modificati anche dal responsabile Gruppo Sicurezza, con le stesse modalità viste in precedenza.

# Responsabile sicurezza

## Avvio nuovo test



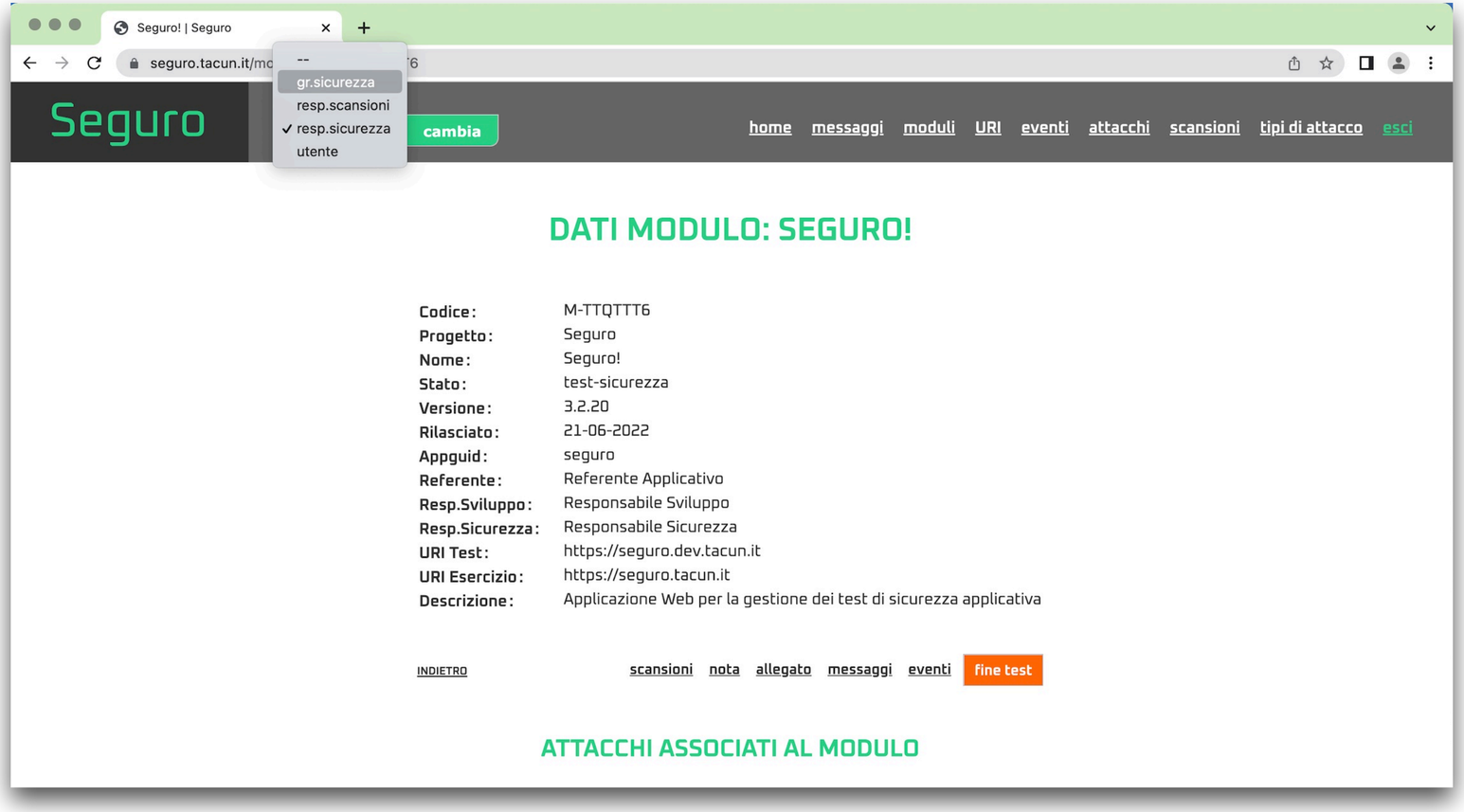

Facendo click sul bottone **nuovo test**, nella barra sotto ai dati anagrafici del modulo, si avvia una nuova sessione di test.

Il sistema chiede conferma della richiesta con un messaggio pop-up.

Se l'utente conferma, Lo stato del modulo passa da **rilascio** a **test-sicurezza**.

# Responsabile sicurezza

## Cambio ruolo

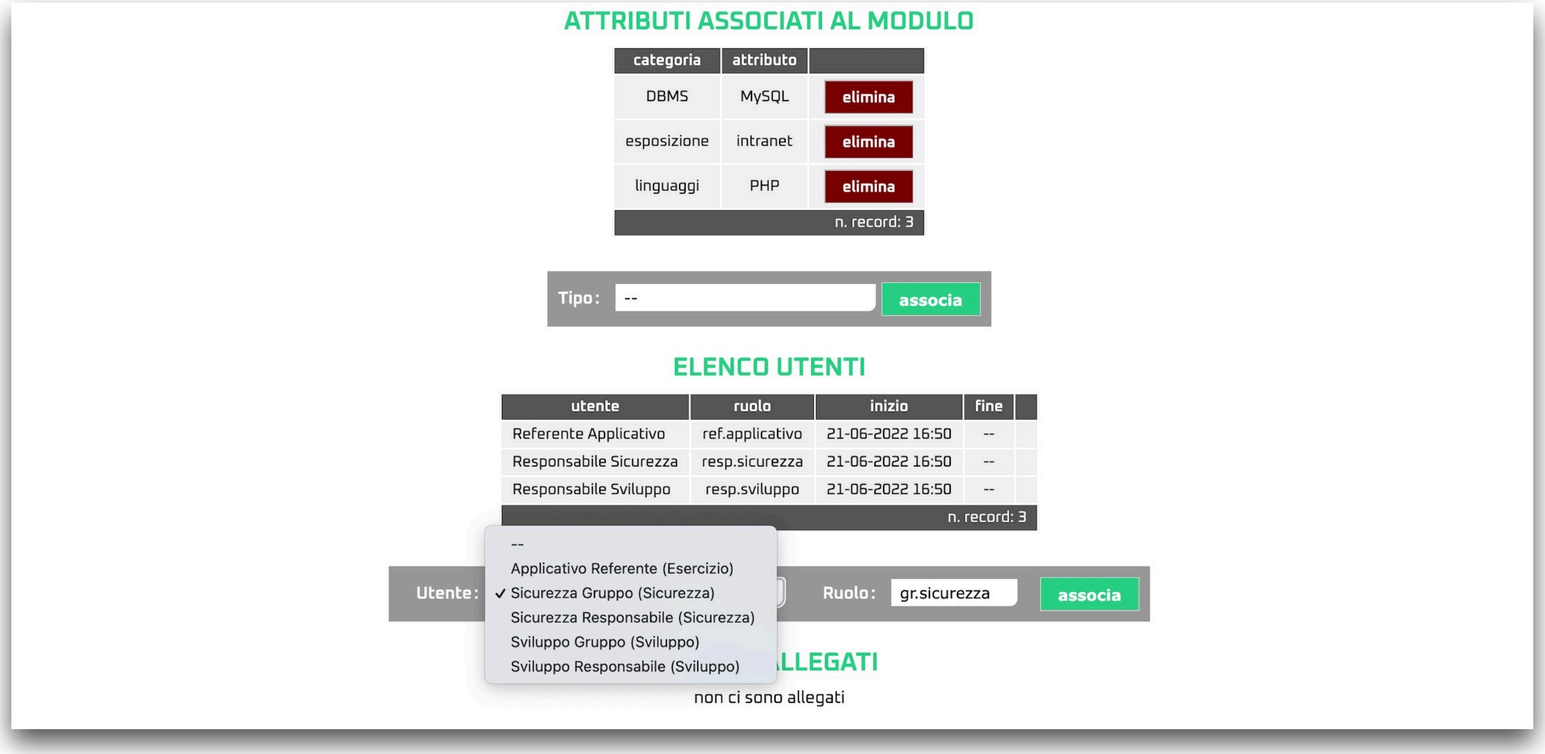



Per eseguire i test, il responsabile del Gruppo Sicurezza può modificare temporaneamente il proprio ruolo a **Gruppo Sicurezza**, o può associare degli utenti con questo ruolo al modulo.

Questo permette di portare a termine il processo di test anche in caso di assenze per malattia o nei periodi di ferie.

# Responsabile sicurezza

## Associazione utenti a modulo

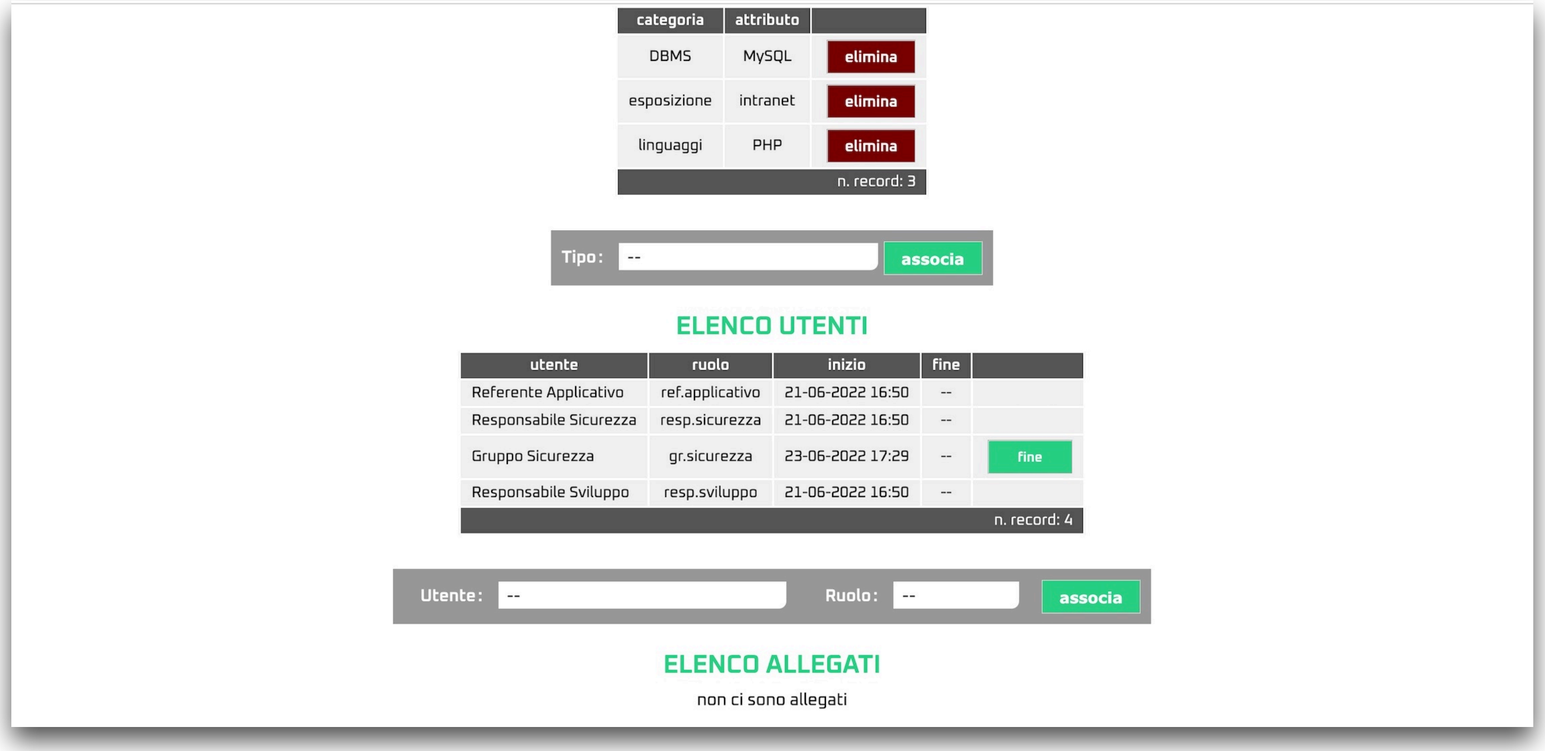



Per associare un utente al modulo, si deve:

1. selezionare il nome dell'utente nella casella a discesa nella form sotto all'elenco utenti;
2. associargli il ruolo **gruppo sicurezza** o **responsabile scansioni**;
3. fare click sul bottone **associa**.

# Responsabile sicurezza

## Rimozione utenti associati a un modulo

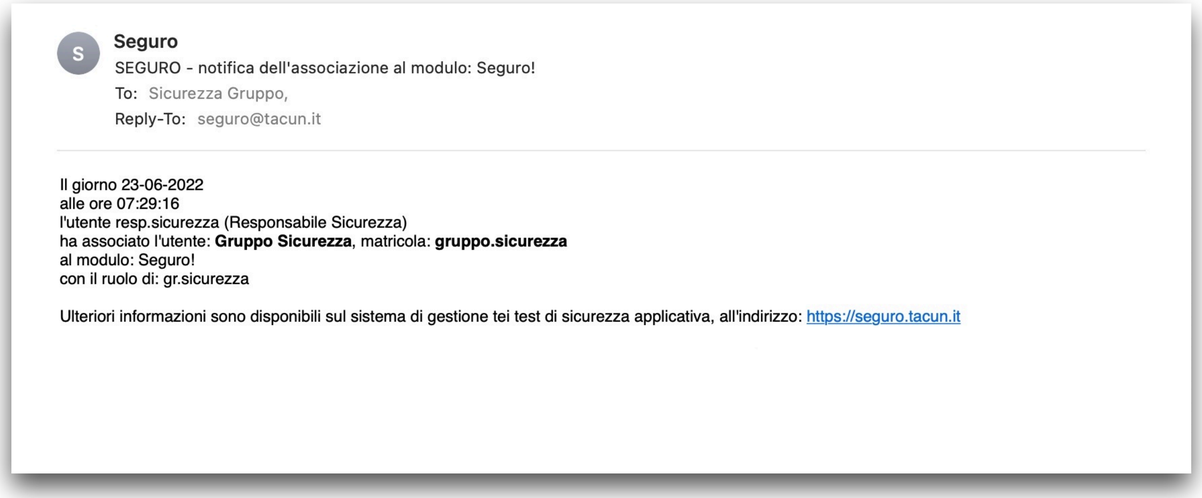



Per terminare l'associazione di un utente al modulo, si deve fare click sul bottone **fine** a destra nell'elenco.

Nella colonna **fine** comparirà la data di termine dell'associazione.

# Gruppo sicurezza

## Messaggio per associazione a modulo



**Seguro**
SEGURO - notifica dell'associazione al modulo: Seguro!
To: Sicurezza Gruppo,
Reply-To: seguro@tacun.it

Il giorno 23-06-2022
alle ore 07:29:16
l'utente resp.sicurezza (Responsabile Sicurezza)
ha associato l'utente: **Gruppo Sicurezza**, matricola: **gruppo.sicurezza**
al modulo: Seguro!
con il ruolo di: gr.sicurezza

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando un utente viene associato a un modulo, il sistema gli invia un messaggio contenente le informazioni necessarie all’esecuzione dei test.

# Gruppo Sicurezza

## Login con certificato


Ricevuto il messaggio, il membro del Gruppo Sicurezza accede al sistema con il suo certificato.

# Gruppo Sicurezza

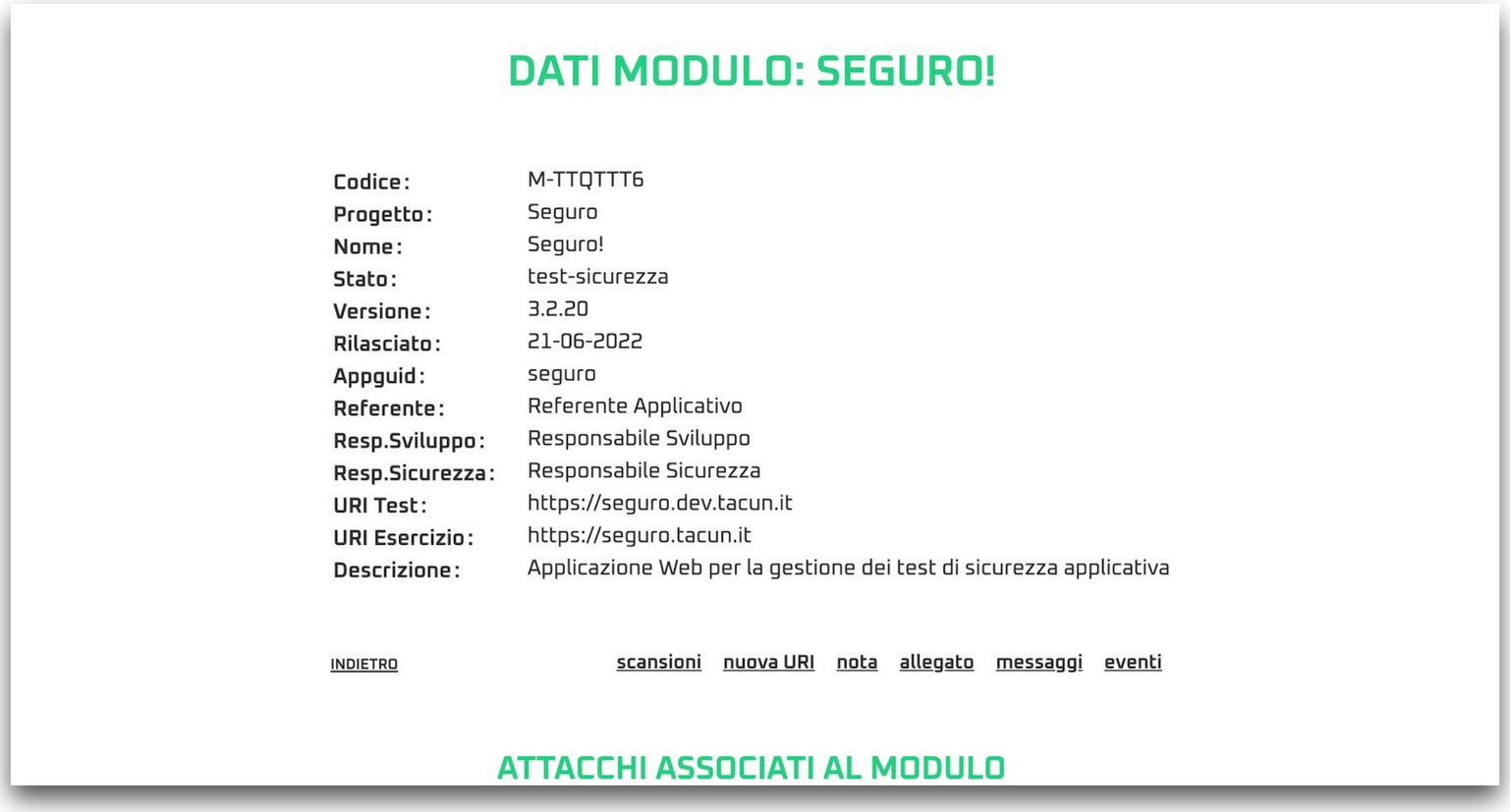
## Home-page


Nella home-page del membro del Gruppo Sicurezza c'è l'elenco dei messaggi ricevuti, l'elenco dei moduli associati e l'elenco delle URI assegnate.

Facendo click sul bottone **dettagli** a destra nell'elenco moduli, l'utente apre la maschera di gestione del modulo.

# Gruppo Sicurezza

## Gestione modulo - 1




Nella maschera, i dati del modulo sono visualizzati in sola lettura. Nella barra sotto ai dati anagrafici, compaiono i link:

- elenco scansioni;
- nuova URI;
- nuova nota;
- nuovo allegato;
- elenco messaggi;
- elenco eventi.

# Gruppo Sicurezza

## Gestione modulo - 2

URI ASSOCIATE AL MODULO

il modulo non ha URI associate

ELENCO PROFILI ASSOCIATI AL MODULO

| profilo | username | password | |
|---|---|---|---|
| Amministratore | admin | password | dettagli |
| | | | n. record: 1 |

ATTRIBUTI ASSOCIATI AL MODULO

| categoria | attributo |
|---|---|
| DBMS | MySQL |
| esposizione | intranet |
| linguaggi | PHP |
| | n. record: 3 |

ELENCO UTENTI

| utente | ruolo | inizio | fine | |
|---|---|---|---|---|
| Referente Applicativo | ref.applicativo | 21-06-2022 16:50 | -- | |
| Responsabile Sicurezza | resp.sicurezza | 21-06-2022 16:50 | -- | |
| Gruppo Sicurezza | gr.sicurezza | 23-06-2022 17:29 | -- | |
| Responsabile Sviluppo | resp.sviluppo | 21-06-2022 16:50 | -- | |
| | | | | n. record: 4 |

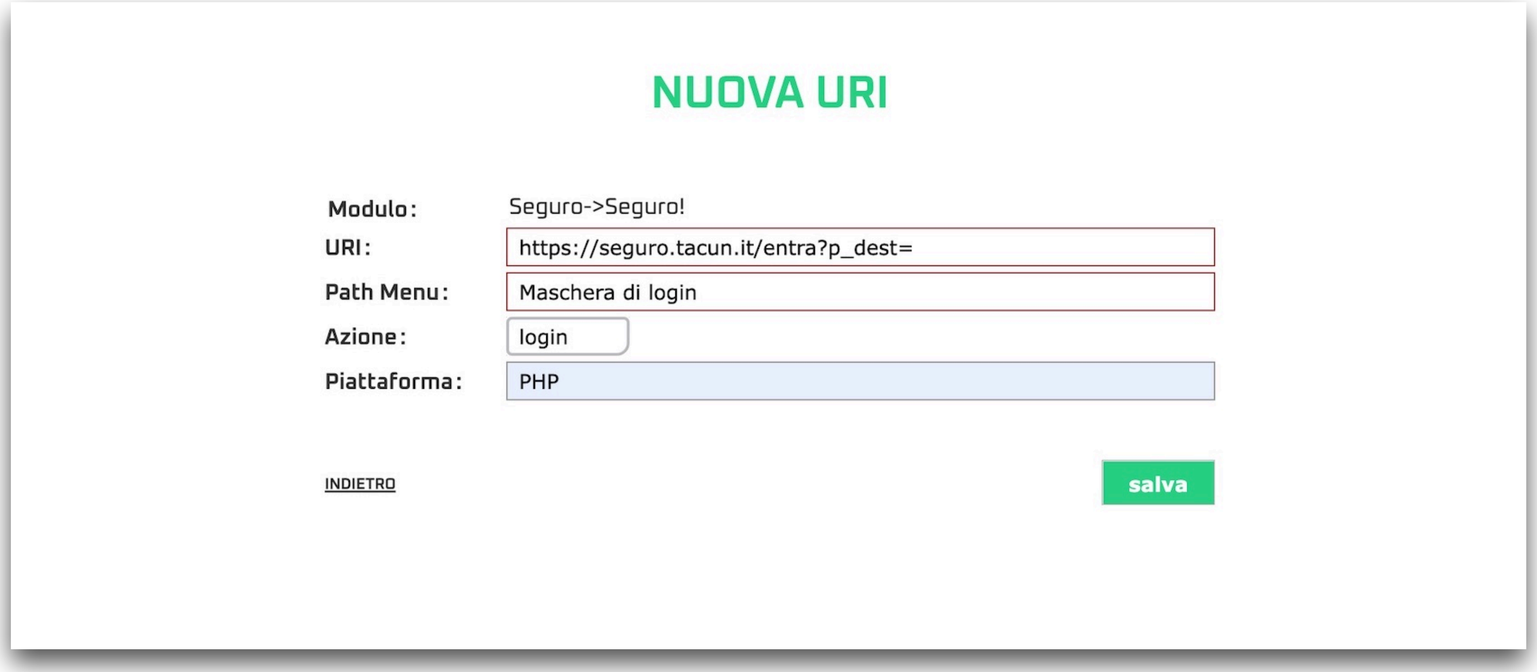
ELENCO ALLEGATI

non ci sono allegati

L’utente può leggere e modificare i dati dei profili, ma gli attributi del modulo sono visualizzati in sola lettura.

# Gruppo Sicurezza

## Nuova URL




Facendo click sul link **nuova URI**, sotto ai dati del modulo, l'utente apre la maschera di inserimento nuova URI.

I dati richiesti identificano la URI e specificano quale sia la sua funzione.

# Gruppo Sicurezza

## Maschera di modifica dati URI


Una volta salvata la URI, l'utente può associarle un nuovo attacco facendo click sul link **nuovo attacco**.

# Gruppo Sicurezza

## Nuovo attacco

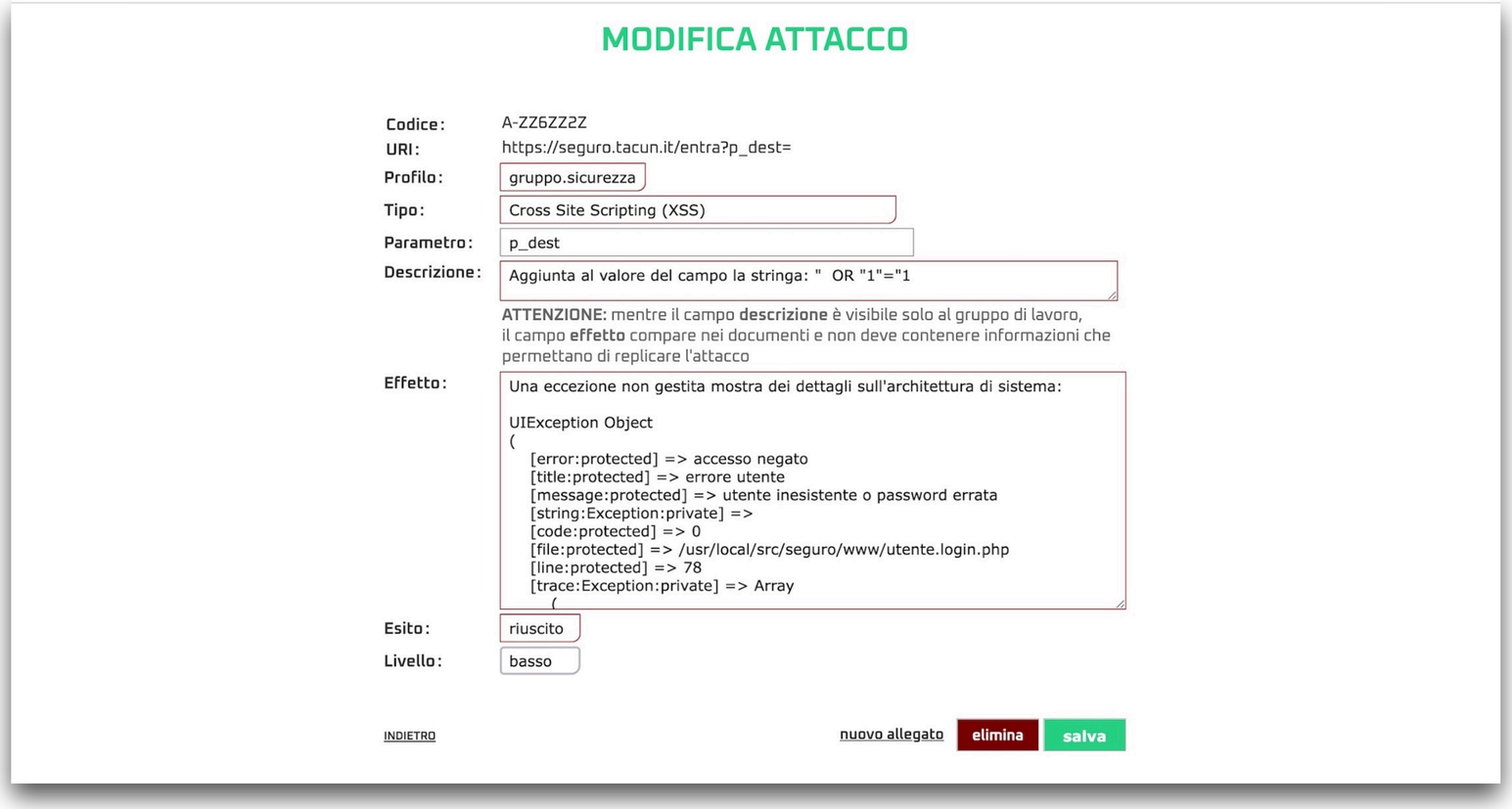

La maschera di inserimento nuovo attacco richiede le seguenti informazioni:

- profilo utente;
- tipologia di attacco;
- eventuale parametro sfruttato.

Facendo click sul bottone **salva**, si inserisce nel DB il nuovo attacco e si passa alla maschera di modifica.

# Gruppo Sicurezza

## Modifica dati attacco

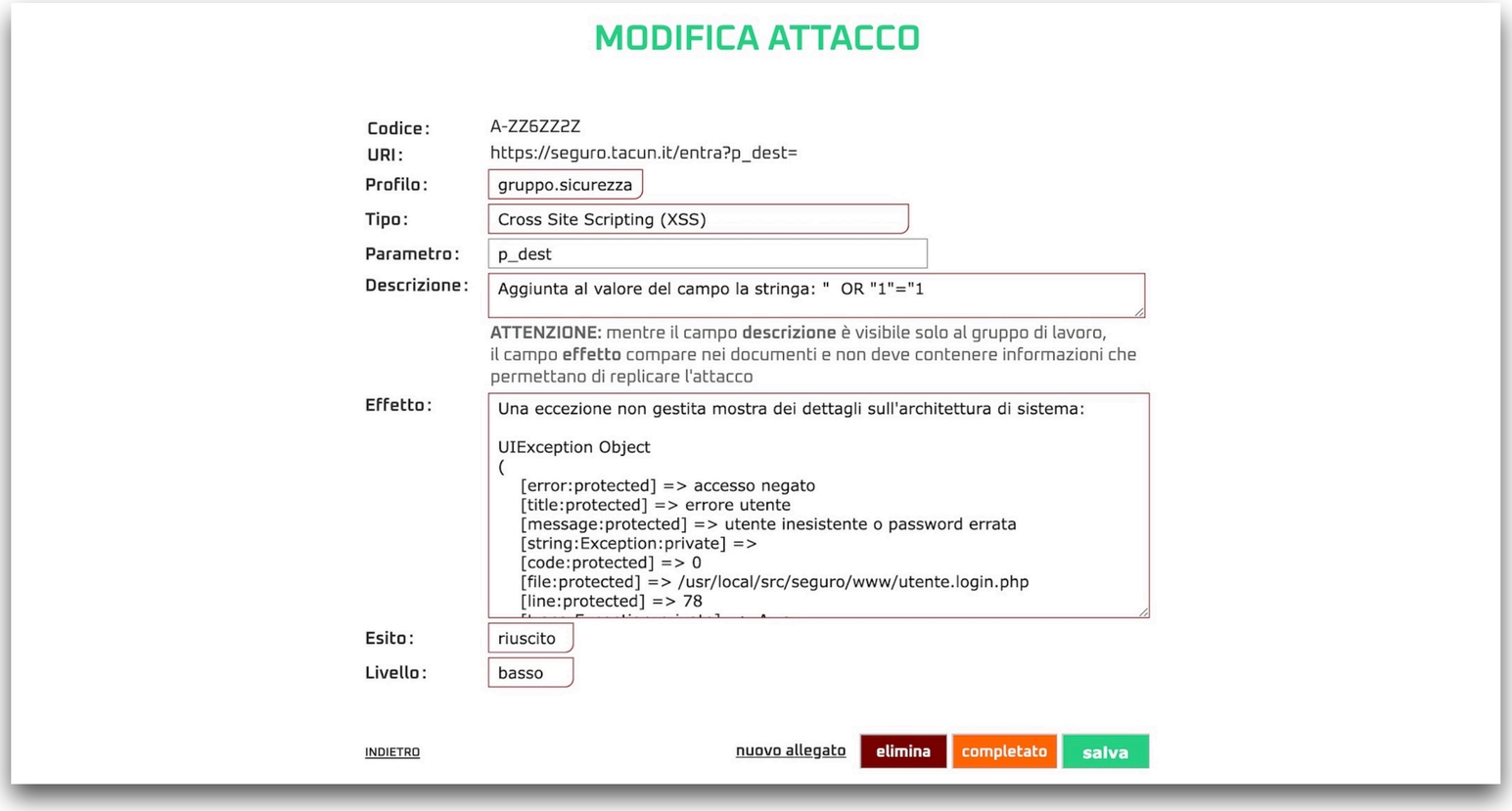



La maschera di modifica dati attacco permette di inserire una descrizione dell'attacco effettuato, gli esiti dell'attacco e di selezionare l'esito dell'attacco: riuscito, fallito, nessuno.

Un altro campo permette di definire il livello di rischio dell'eventuale vulnerabilità riscontrata: alto, basso, nessuno.

# Gruppo Sicurezza

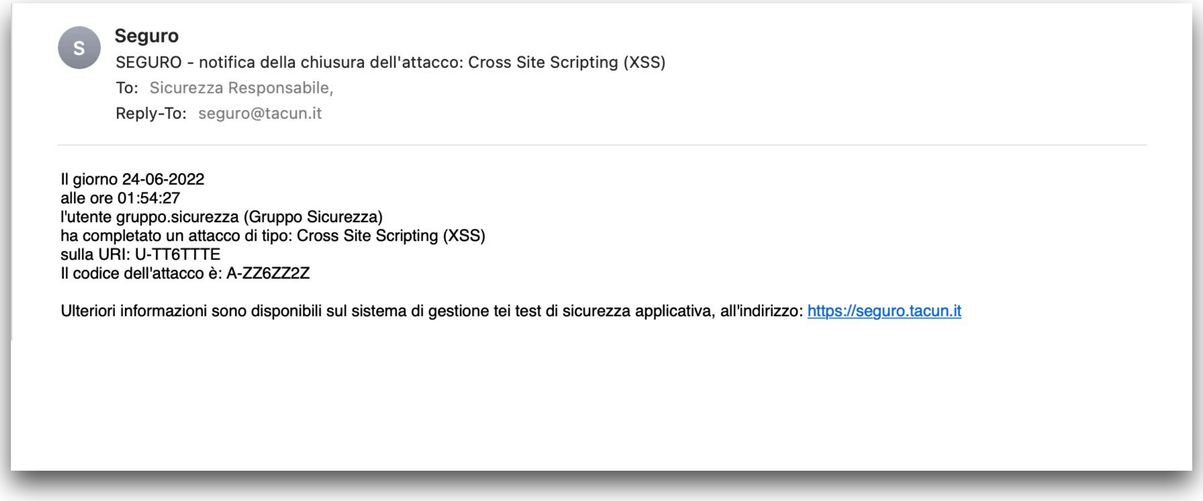
## Attacco completato




Se è definito un esito, per l'attacco, l'utente ha la possibilità di dichiarare completato l'attacco facendo click sul bottone **completato**.

# Gruppo Sicurezza

## Messaggio attacco completato



**Seguro**
SEGURO - notifica della chiusura dell'attacco: Cross Site Scripting (XSS)
To: Sicurezza Responsabile,
Reply-To: seguro@tacun.it

Il giorno 24-06-2022
alle ore 01:54:27
l'utente gruppo.sicurezza (Gruppo Sicurezza)
ha completato un attacco di tipo: Cross Site Scripting (XSS)
sulla URI: U-TT6TTTE
Il codice dell'attacco è: A-ZZ6ZZ2Z

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando l'utente segna un attacco come completato, il sistema invia al responsabile del Gruppo Sicurezza un messaggio di notifica.

I messaggi non rivelano alcun dettaglio sul modulo applicativo o sulla URI vulnerabile.

Non è specificato nemmeno se l'attacco sia andato a buon fine.

# Responsabile Sicurezza

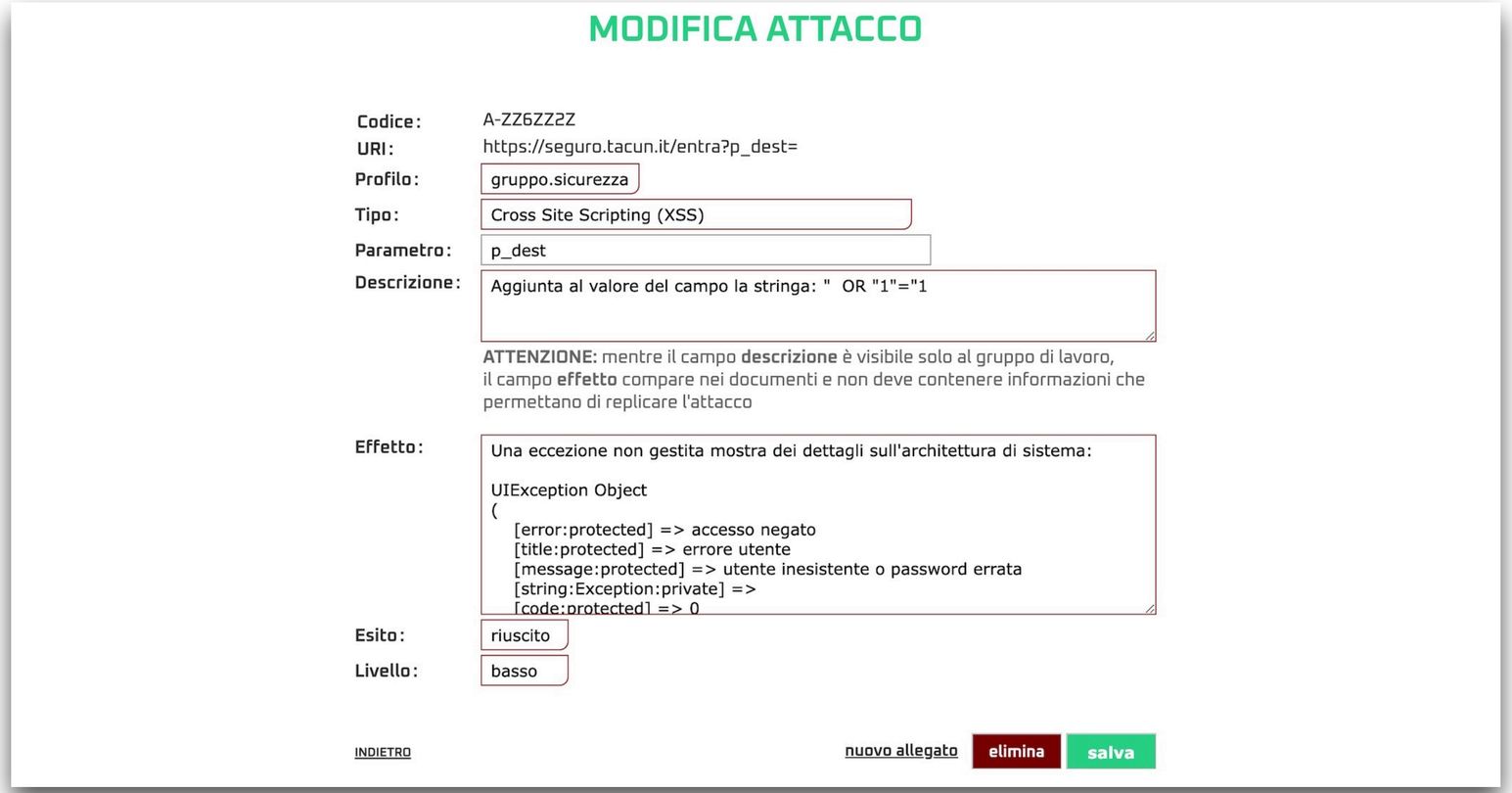
## Elenco attacchi modulo


Il responsabile del Gruppo Sicurezza riceve il messaggio di chiusura dell'attacco e apre la scheda del modulo.

Nell'elenco attacchi compare il nuovo attacco.
Facendo click sul bottone **dettagli**, va alla maschera di dettaglio attacco.

# Responsabile Sicurezza

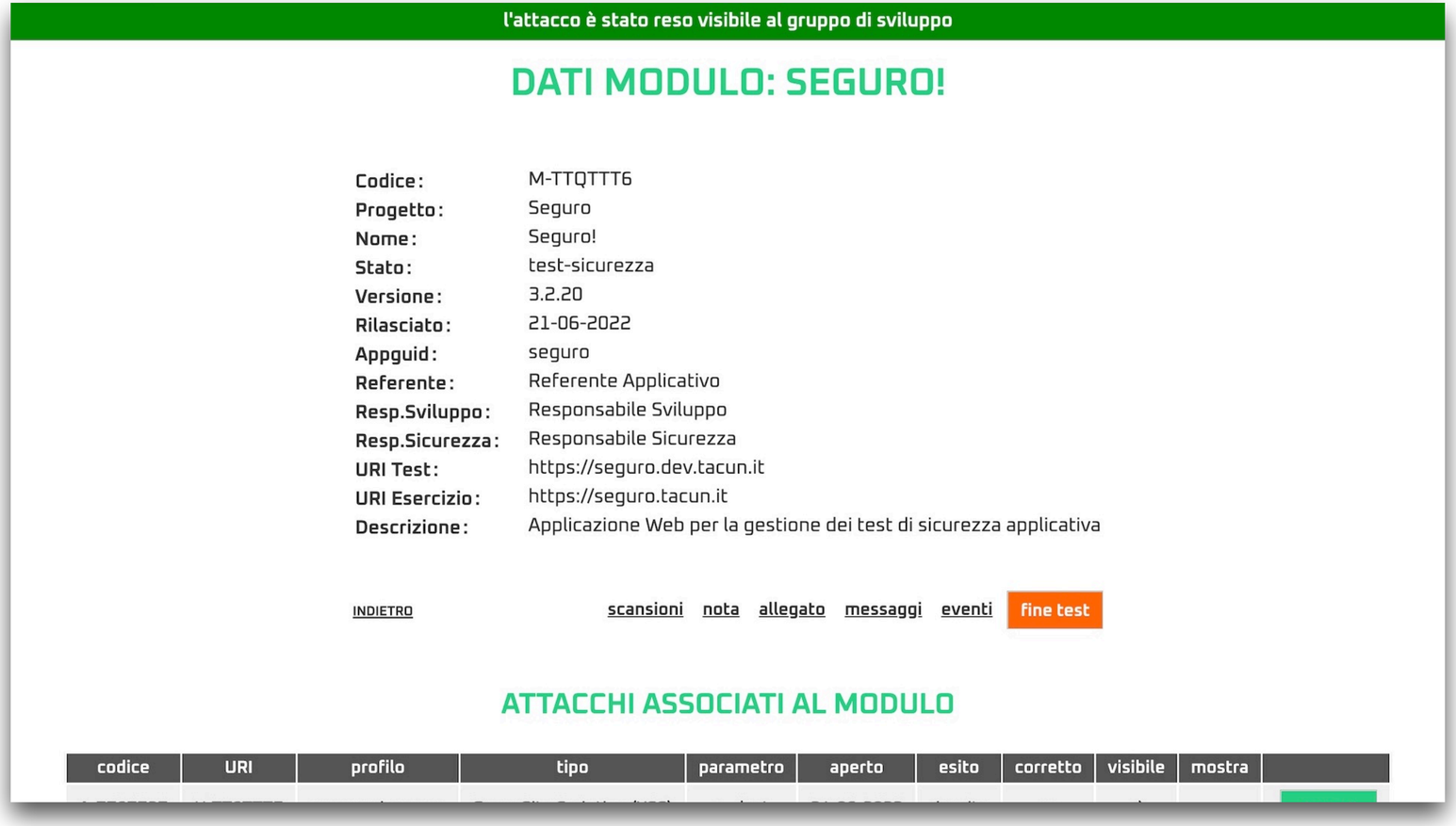
## Maschera dettaglio dati attacco




Il responsabile del Gruppo Sicurezza può modificare i dati dell'attacco, correggendo eventuali errori e cambiando il livello di rischio se lo ritiene necessario.

# Responsabile Sicurezza

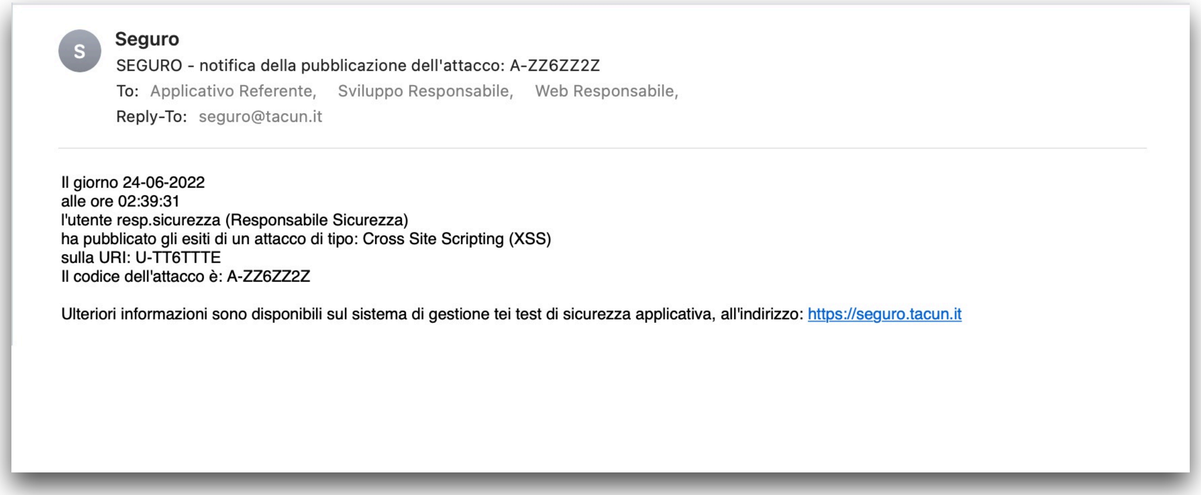
## Pubblicazione attacco




Quando il Responsabile del Gruppo Sicurezza è sicuro che l'attacco non sia un falso positivo, fa click sul bottone **mostra**, nell'elenco attacchi e lo rende visibile al gruppo di sviluppo.

# Responsabile Sicurezza

## Messaggio pubblicazione attacco



S **Seguro**

SEGURO - notifica della pubblicazione dell'attacco: A-ZZ6ZZ2Z

To: Applicativo Referente, Sviluppo Responsabile, Web Responsabile,

Reply-To: seguro@tacun.it

Il giorno 24-06-2022
alle ore 02:39:31
l'utente resp.sicurezza (Responsabile Sicurezza)
ha pubblicato gli esiti di un attacco di tipo: Cross Site Scripting (XSS)
sulla URI: U-TT6TTTE
Il codice dell'attacco è: A-ZZ6ZZ2Z

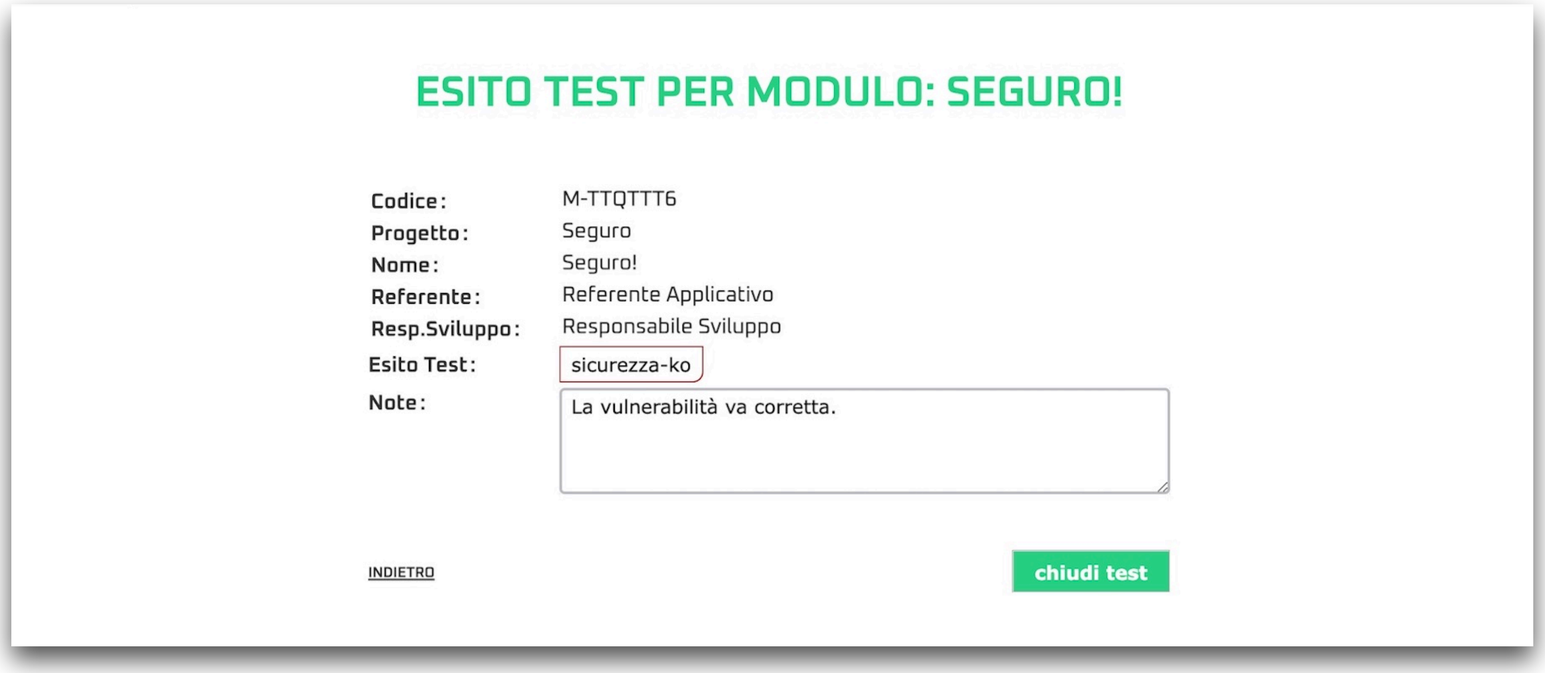
Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando l'attacco viene pubblicato, il sistema invia un messaggio di notifica al responsabile dello sviluppo, al referente dell'applicazione e al responsabile delle applicazioni Web.

Anche in questo caso, non ci sono informazioni sulla URL o sul sistema in oggetto.

# Responsabile Sicurezza

## Chiusura test di sicurezza

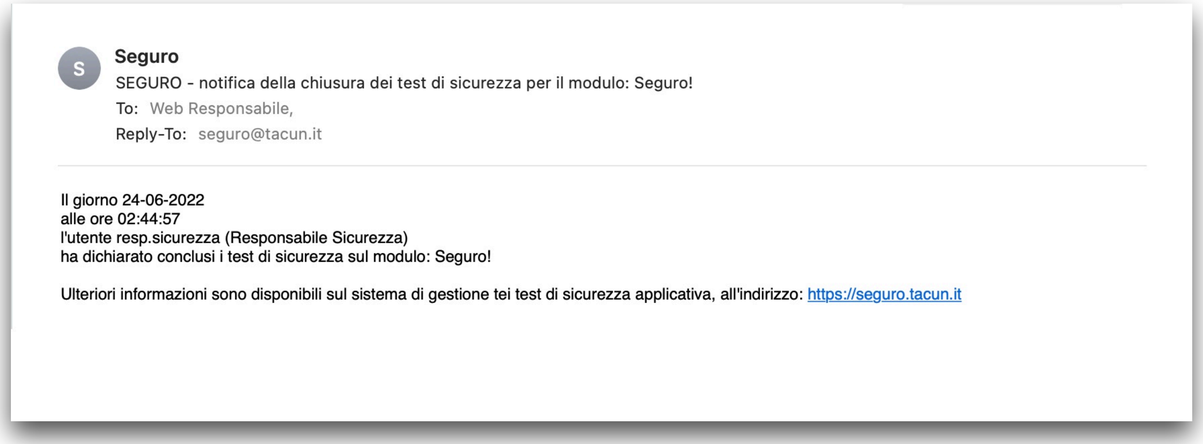



Quando tutti gli attacchi sono stati verificati ed eventualmente pubblicati, il responsabile del Gruppo Sicurezza fa click sul bottone **chiudi test** e accede alla maschera di chiusura del test.

Qui inserisce l'esito del test (OK/KO) e delle eventuali note conclusive, poi salva i dati facendo click sul bottone **chiudi test**.

# Responsabile Sicurezza

## Verifica esito test



**Seguro**
SEGURO - notifica della chiusura dei test di sicurezza per il modulo: Seguro!
To: Web Responsabile,
Reply-To: seguro@tacun.it

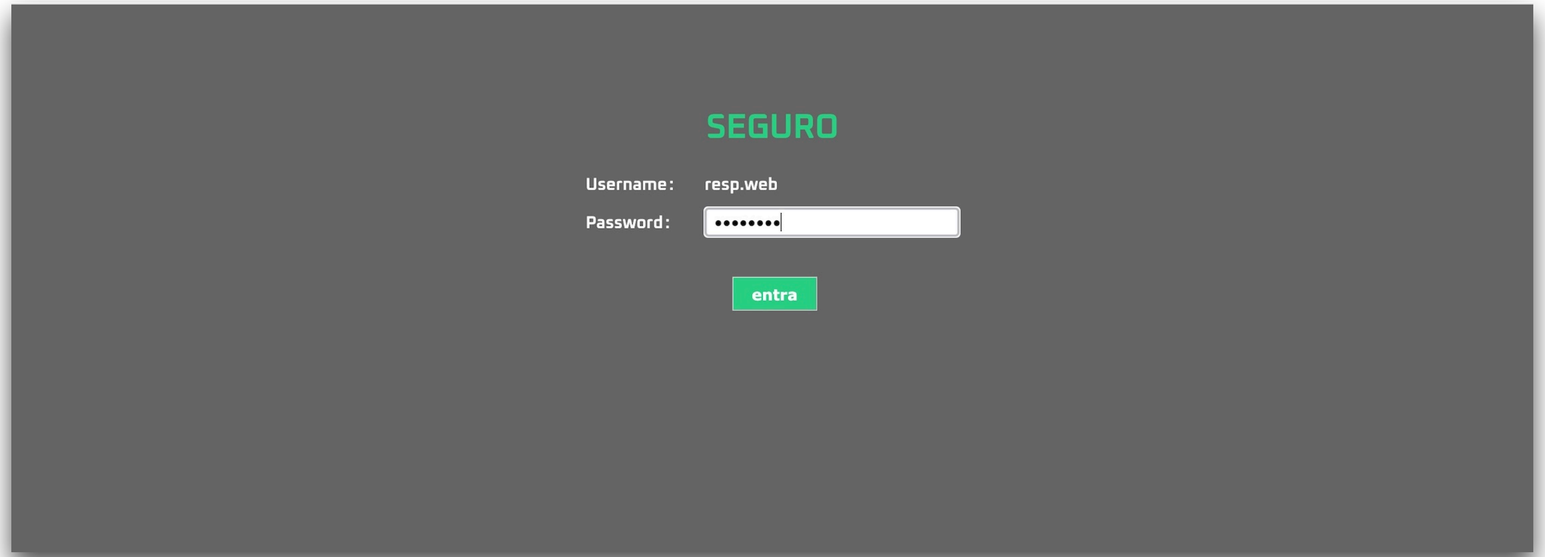
Il giorno 24-06-2022
alle ore 02:44:57
l'utente resp.sicurezza (Responsabile Sicurezza)
ha dichiarato conclusi i test di sicurezza sul modulo: Seguro!

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando il responsabile del Gruppo Sicurezza dichiara chiusi i test su un modulo applicativo, il sistema invia un messaggio informativo al responsabile Web, che, a seconda dell'esito, decide se inoltrare il modulo in correzione o mandarlo in esercizio.

# Responsabile Web

## Login




Ricevuto il messaggio di fine test, il responsabile Web accede al sistema.

# Responsabile Web

## Home page


Nella home-page del responsabile Web c’è il riepilogo delle attività svolte e l’elenco dei messaggi ricevuti.

Facendo click sulla voce di menu **moduli**, l’utente accede all’elenco moduli.

# Responsabile Web

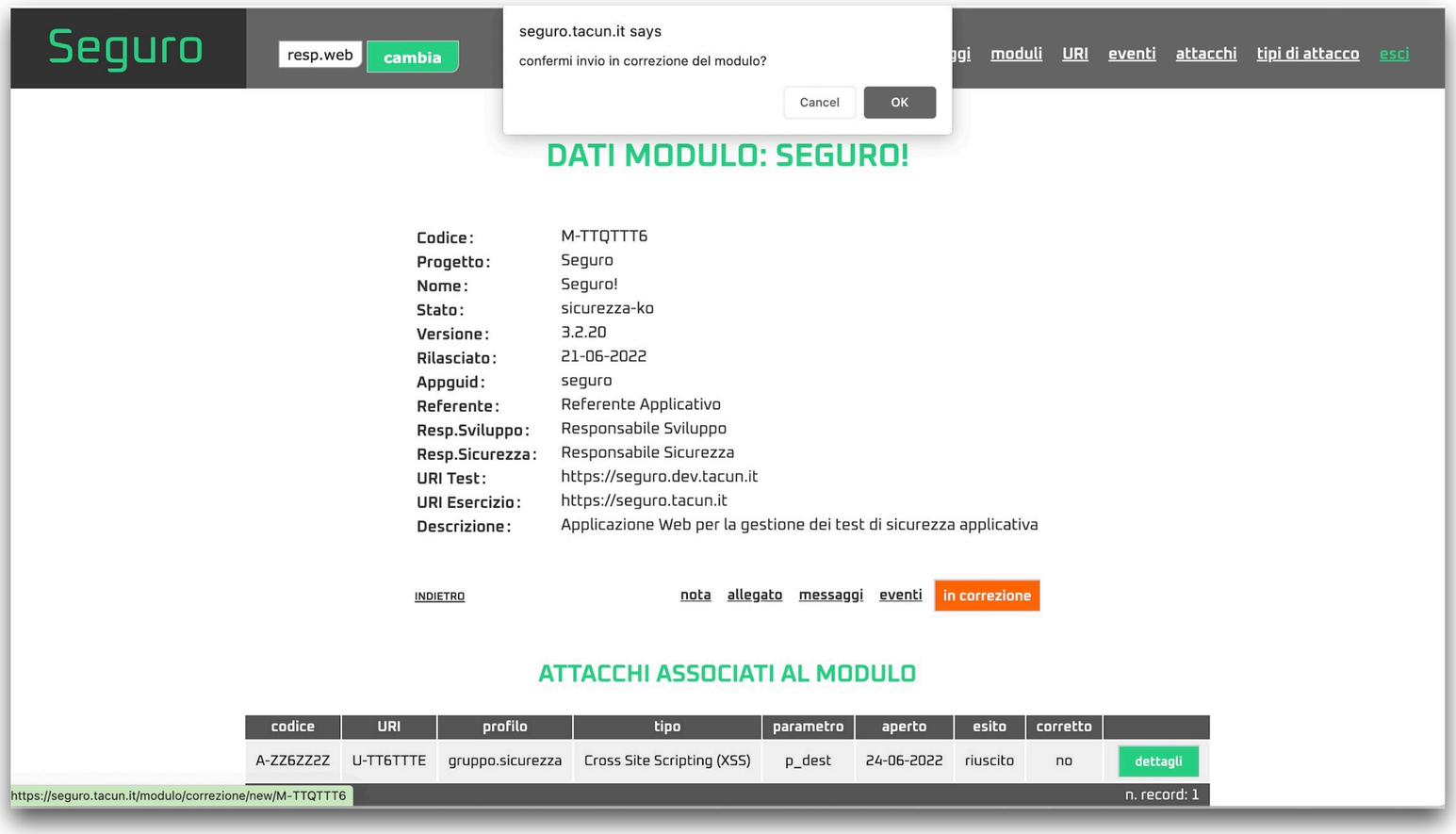
## Elenco moduli


Nell'elenco, la riga del modulo appare con il fondo rosso perché il test si è chiuso con esito negativo.

Facendo click sul bottone **dettagli**, a destra nell'elenco, l'utente apre la maschera di gestione del modulo.

# Responsabile Web

## Dettagli modulo




Il responsabile Web può vedere i dettagli di tutte le entità legate al modulo, ma non le può modificare.

Facendo click sul bottone **in correzione**, in basso a destra, sotto ai dati anagrafici, si invia il modulo in correzione.

Il sistema chiede conferma prima di eseguire l'operazione.

# Responsabile Web

## Modulo in correzione

**Seguro**
SEGURO - notifica dell'invio in correzione del modulo: Seguro!
To: Applicativo Referente, Sicurezza Responsabile, Sviluppo Responsabile, Web Responsabile,
Reply-To: seguro@tacun.it

Il giorno 27-06-2022
alle ore 04:02:17
l'utente resp.web (Responsabile Web)
ha inviato in correzione il modulo: Seguro!

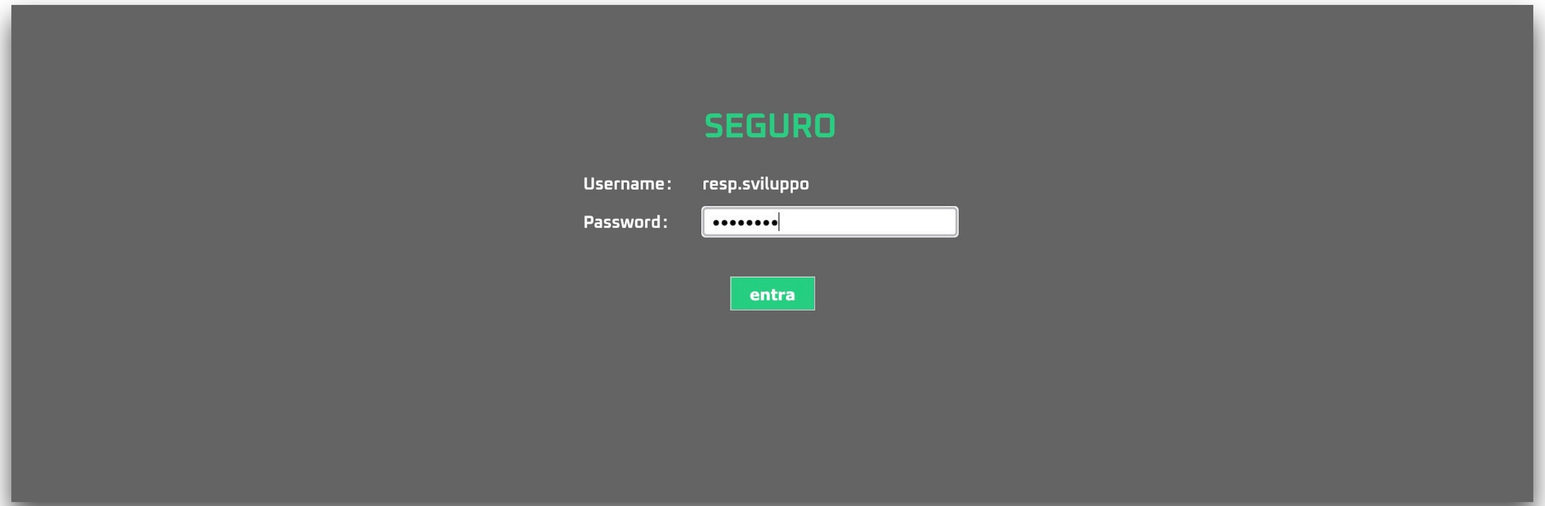
Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando un modulo è inviato in correzione, il sistema invia a tutti i responsabili un messaggio di notifica.

Il responsabile dello sviluppo adesso deve intervenire per correggere le vulnerabilità.

# Responsabile gruppo di Sviluppo

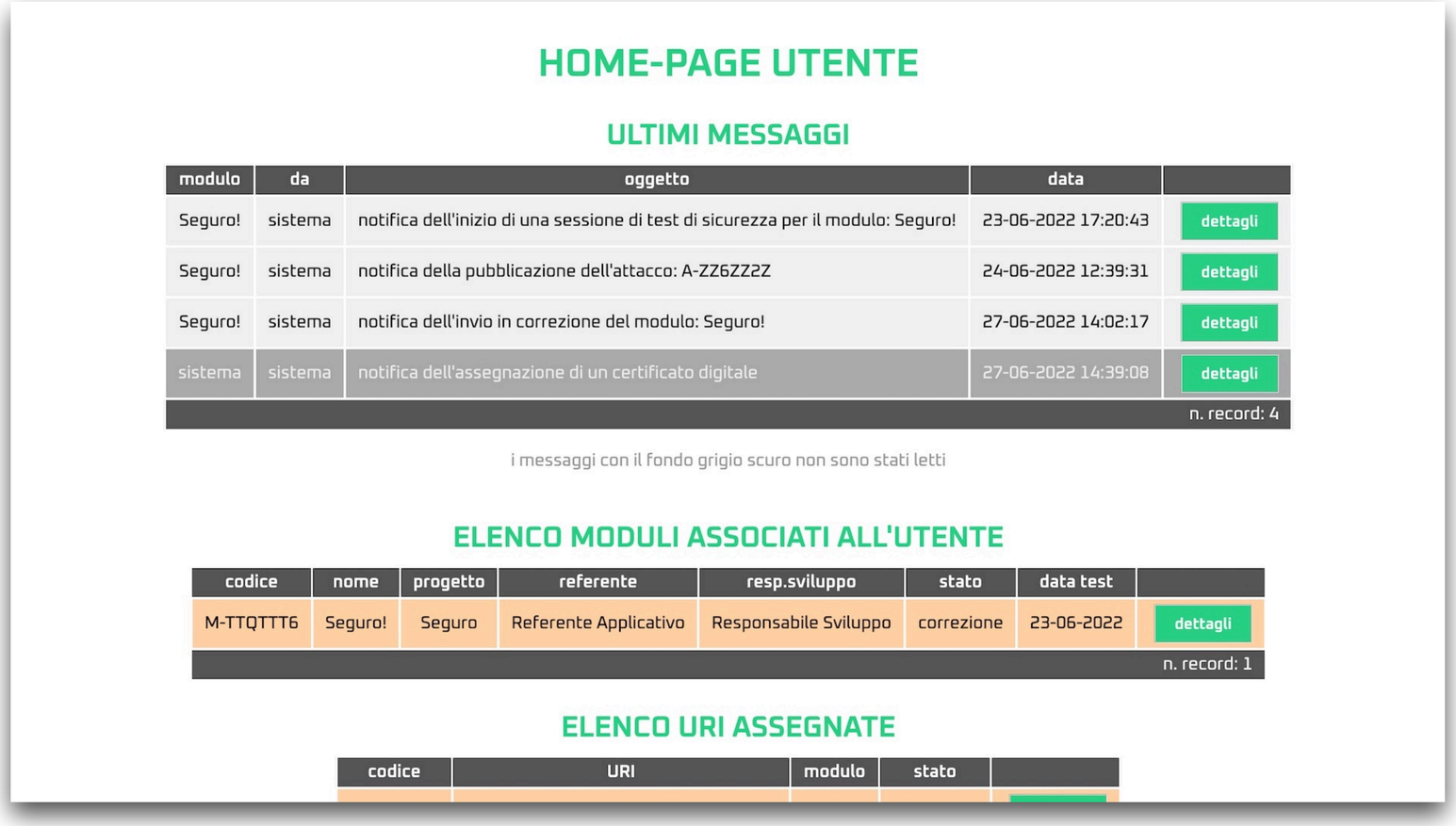
## Login




Il responsabile dello sviluppo accede al sistema.

# Responsabile gruppo di Sviluppo

## Home-page



HOME-PAGE UTENTE

ULTIMI MESSAGGI

| modulo | da | oggetto | data | |
|---|---|---|---|---|
| Seguro! | sistema | notifica dell'inizio di una sessione di test di sicurezza per il modulo: Seguro! | 23-06-2022 17:20:43 | dettagli |
| Seguro! | sistema | notifica della pubblicazione dell'attacco: A-ZZ6ZZ2Z | 24-06-2022 12:39:31 | dettagli |
| Seguro! | sistema | notifica dell'invio in correzione del modulo: Seguro! | 27-06-2022 14:02:17 | dettagli |
| sistema | sistema | notifica dell'assegnazione di un certificato digitale | 27-06-2022 14:39:08 | dettagli |

n. record: 4

i messaggi con il fondo grigio scuro non sono stati letti

ELENCO MODULI ASSOCIATI ALL'UTENTE

| codice | nome | progetto | referente | resp.sviluppo | stato | data test | |
|---|---|---|---|---|---|---|---|
| M-TTQTTT6 | Seguro! | Seguro | Referente Applicativo | Responsabile Sviluppo | correzione | 23-06-2022 | dettagli |

n. record: 1

ELENCO URI ASSEGNATE

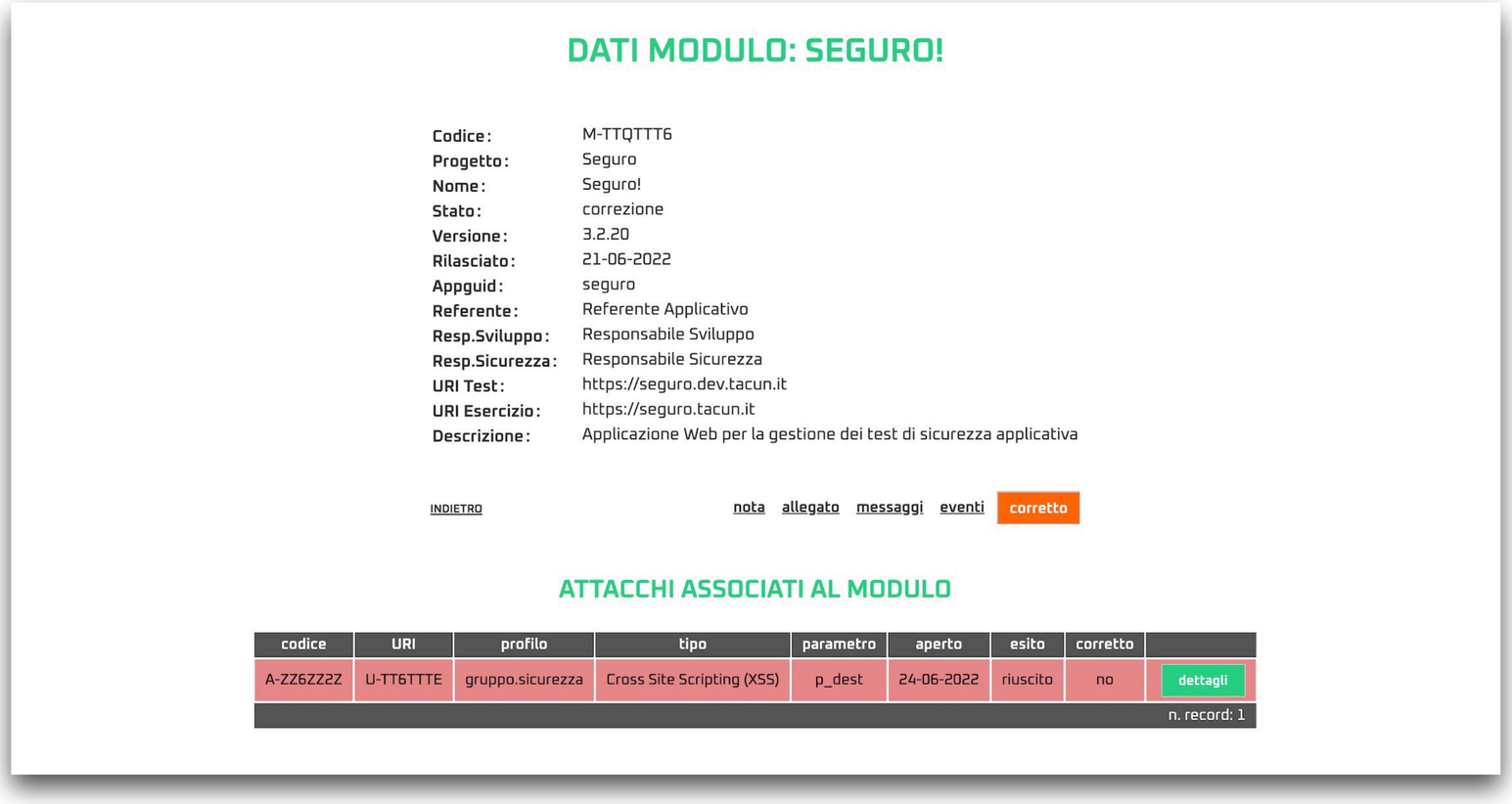
| codice | URI | modulo | stato | |
|---|---|---|---|---|

Nella sua home-page c'è l'elenco dei messaggi ricevuti, l'elenco dei moduli e quello delle URI a cui è associato.

Sia il modulo che la URI compaiono con il fondo arancio perché devono essere corretti.

# Responsabile gruppo di Sviluppo

## Dettagli modulo in correzione




Nei dettagli del modulo, la riga relativa all'attacco riuscito appare con lo sfondo rosso perché ha un alto indice di rischio.

Facendo click sul bottone **dettagli**, a destra nell'elenco, l'utente apre la maschera con i dettagli dell'attacco.

# Responsabile gruppo di Sviluppo

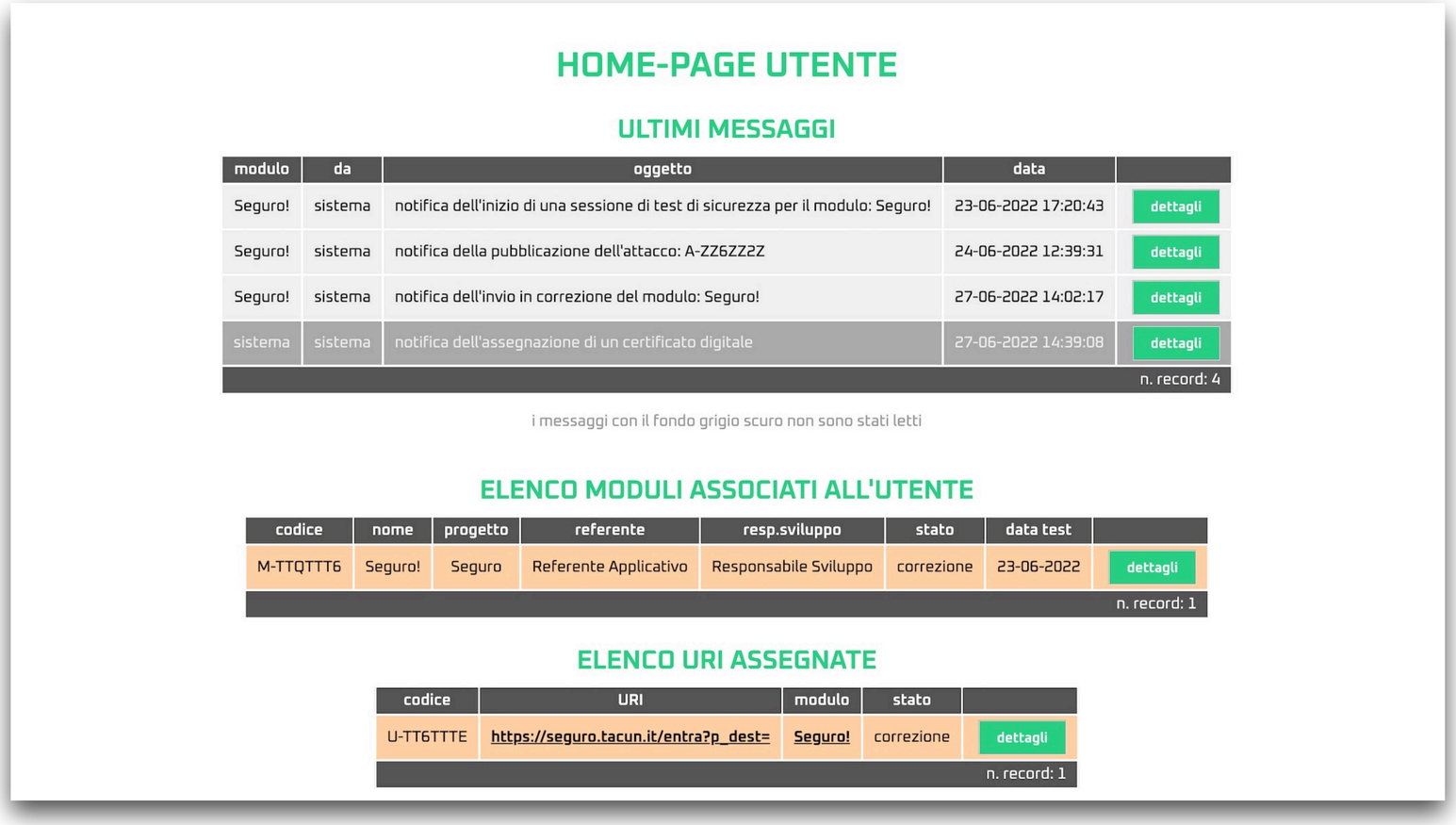
## Cambio di ruolo


Esaminando i dettagli dell'attacco, il responsabile dello sviluppo si accorge che la vulnerabilità dipende da un errore di configurazione.

Decide perciò di correggere personalmente l'errore e modifica temporaneamente il suo ruolo "degradandosi" a membro del Gruppo Sviluppo.

# Membro gruppo di Sviluppo

## Home page



HOME-PAGE UTENTE

ULTIMI MESSAGGI

| modulo | da | oggetto | data | |
|---|---|---|---|---|
| Seguro! | sistema | notifica dell'inizio di una sessione di test di sicurezza per il modulo: Seguro! | 23-06-2022 17:20:43 | dettagli |
| Seguro! | sistema | notifica della pubblicazione dell'attacco: A-ZZ6ZZ2Z | 24-06-2022 12:39:31 | dettagli |
| Seguro! | sistema | notifica dell'invio in correzione del modulo: Seguro! | 27-06-2022 14:02:17 | dettagli |
| sistema | sistema | notifica dell'assegnazione di un certificato digitale | 27-06-2022 14:39:08 | dettagli |

n. record: 4

i messaggi con il fondo grigio scuro non sono stati letti

ELENCO MODULI ASSOCIATI ALL'UTENTE

| codice | nome | progetto | referente | resp.sviluppo | stato | data test | |
|---|---|---|---|---|---|---|---|
| M-TTQTTT6 | Seguro! | Seguro | Referente Applicativo | Responsabile Sviluppo | correzione | 23-06-2022 | dettagli |

n. record: 1

ELENCO URI ASSEGNATE

| codice | URI | modulo | stato | |
|---|---|---|---|---|
| U-TT6TTTE | https://seguro.tacun.it/entra?p_dest= | Seguro! | correzione | dettagli |

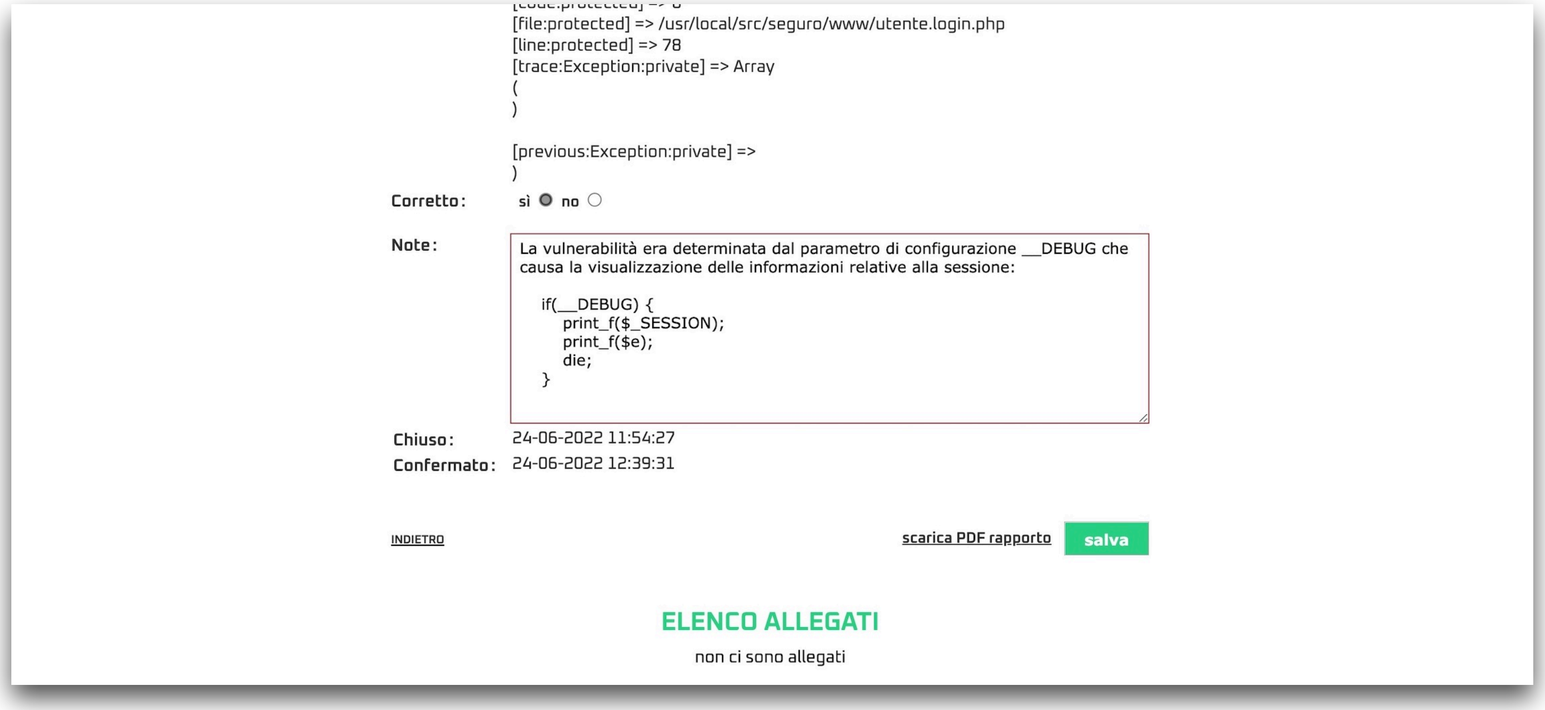
n. record: 1

Il sistema, da questo momento in poi, gestisce l'utente come se fosse un membro del Gruppo di Sviluppo.

Questa funzione è particolarmente utile in periodi di ferie, perché consente di gestire il processo in maniera omogenea anche se mancano degli elementi del gruppo di lavoro.

# Membro gruppo di Sviluppo

## Modifica dati attacco

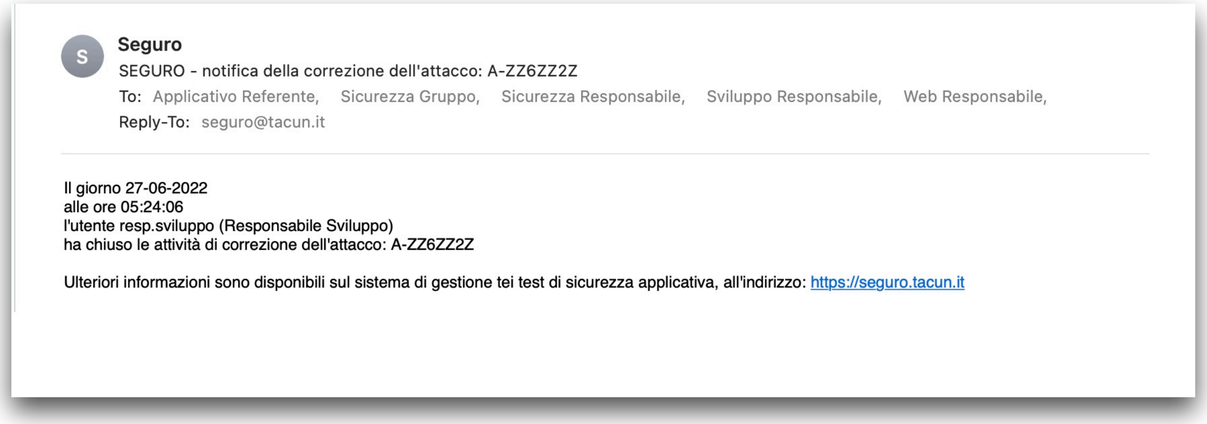



Dopo aver corretto la vulnerabilità, l'utente apre la maschera di dettaglio della URI vulnerabile e da lì va alla maschera di dettaglio dell'attacco.

Inserisce una nota relativa alla correzione, poi segna l'attacco come **corretto** e salva i dati.

# Membro gruppo di Sviluppo

## Messaggio correzione attacco



**Seguro**
SEGURO - notifica della correzione dell'attacco: A-ZZ6ZZ2Z
To: Applicativo Referente, Sicurezza Gruppo, Sicurezza Responsabile, Sviluppo Responsabile, Web Responsabile,
Reply-To: seguro@tacun.it

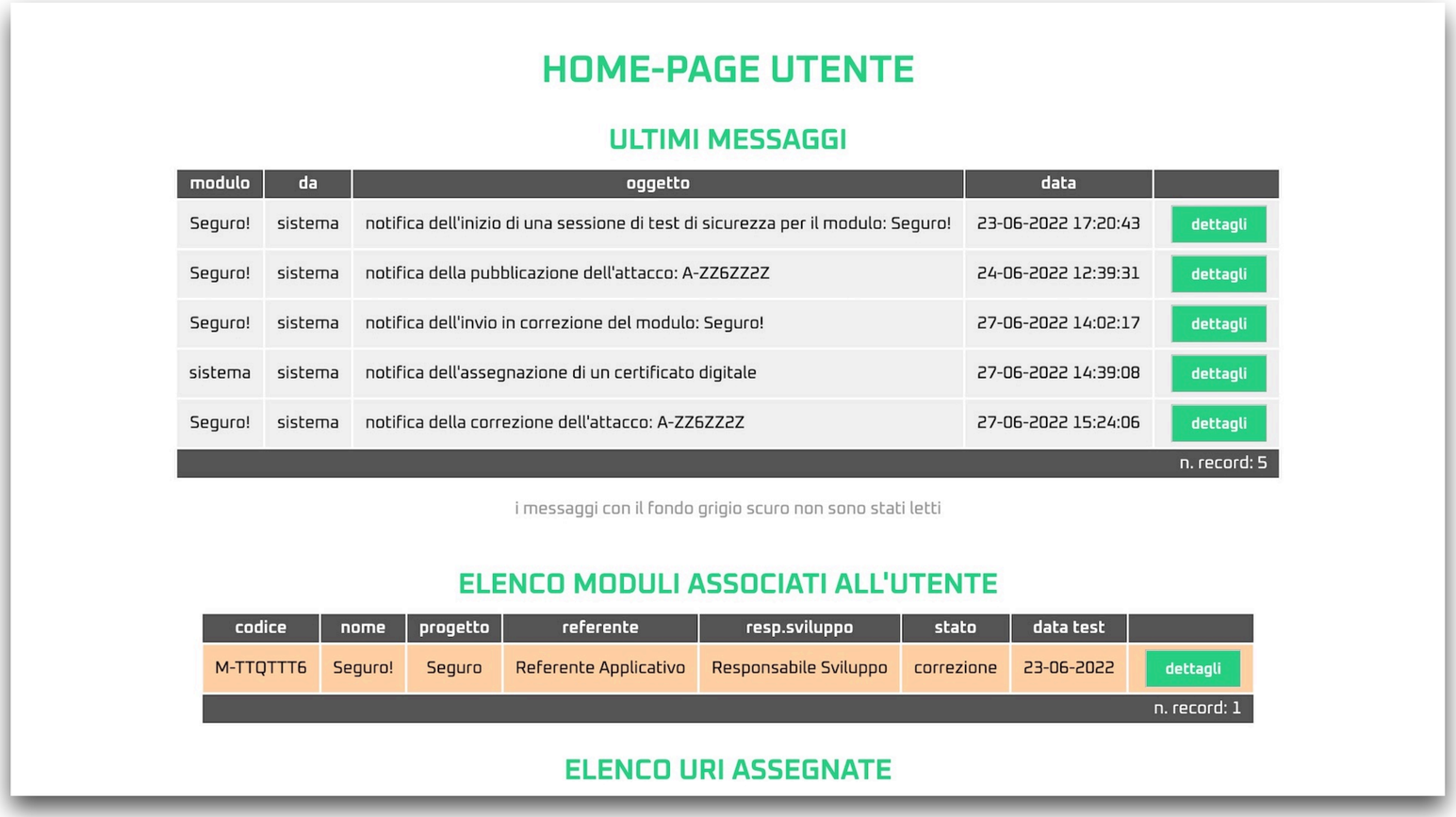
Il giorno 27-06-2022
alle ore 05:24:06
l'utente resp.sviluppo (Responsabile Sviluppo)
ha chiuso le attività di correzione dell'attacco: A-ZZ6ZZ2Z

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando l'utente segna l'attacco come corretto, il sistema invia a tutti i responsabili un messaggio di notifica.

# Responsabile gruppo di Sviluppo

## Ripristino ruolo originario



HOME-PAGE UTENTE

ULTIMI MESSAGGI

| modulo | da | oggetto | data | |
|---|---|---|---|---|
| Seguro! | sistema | notifica dell'inizio di una sessione di test di sicurezza per il modulo: Seguro! | 23-06-2022 17:20:43 | dettagli |
| Seguro! | sistema | notifica della pubblicazione dell'attacco: A-ZZ6ZZ2Z | 24-06-2022 12:39:31 | dettagli |
| Seguro! | sistema | notifica dell'invio in correzione del modulo: Seguro! | 27-06-2022 14:02:17 | dettagli |
| sistema | sistema | notifica dell'assegnazione di un certificato digitale | 27-06-2022 14:39:08 | dettagli |
| Seguro! | sistema | notifica della correzione dell'attacco: A-ZZ6ZZ2Z | 27-06-2022 15:24:06 | dettagli |

n. record: 5

i messaggi con il fondo grigio scuro non sono stati letti

ELENCO MODULI ASSOCIATI ALL'UTENTE

| codice | nome | progetto | referente | resp.sviluppo | stato | data test | |
|---|---|---|---|---|---|---|---|
| M-TTQTTT6 | Seguro! | Seguro | Referente Applicativo | Responsabile Sviluppo | correzione | 23-06-2022 | dettagli |

n. record: 1

ELENCO URI ASSEGNATE

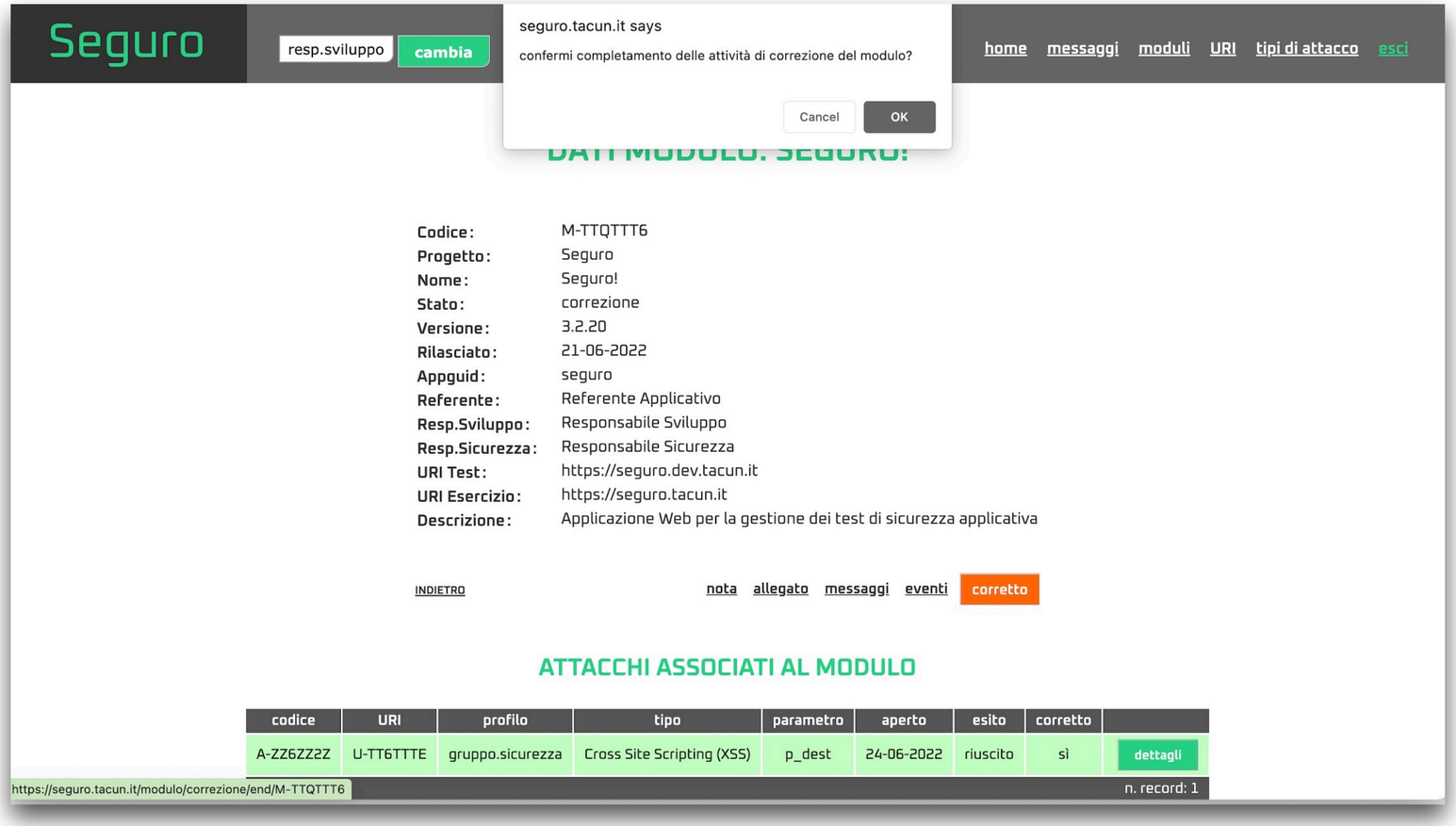
Con lo stesso meccanismo visto in precedenza, il responsabile del Gruppo di Sviluppo riacquisisce il suo ruolo originario.

Da notare come, nell’elenco in basso, non compaia più la URI appena corretta.

Il modulo, però, risulta ancora in correzione.

# Responsabile gruppo di Sviluppo

## Correzione del modulo




L'utente accede alla maschera di modifica dati modulo.

Tutte le URL e tutti gli attacchi hanno sfondo verde perché corretti.

L'utente allora fa click sul bottone **corretto** e rimanda il modulo al test di sicurezza.

Come sempre, il sistema chiede conferma.

# Responsabile gruppo di Sviluppo

## Messaggio correzione modulo

**Seguro**
SEGURO - notifica del completamento delle correzioni del modulo: Seguro!
To: Applicativo Referente, Sicurezza Gruppo, Sicurezza Responsabile, Sviluppo Responsabile, Web Responsabile,
Reply-To: seguro@tacun.it

Il giorno 27-06-2022
alle ore 05:36:40
l'utente resp.sviluppo (Responsabile Sviluppo)
ha chiuso le attività di correzione del modulo: Seguro!

Ulteriori informazioni sono disponibili sul sistema di gestione tei test di sicurezza applicativa, all'indirizzo: https://seguro.tacun.it

Quando un modulo è segnalato come corretto, il sistema invia un messaggio di notifica a tutti i responsabili.

# Seguro!

## Tacun Srls

https://tacun.it/it/prodotti/seguro.html