

# Seguro!

## Presentazione del sistema

### Versione 1.7- Febbraio 2023

The screenshot displays the user interface of the Seguro! system. At the top, there is a navigation bar with the logo 'Seguro!' and a dropdown menu for 'resp.sicurezza' with a 'cambia' button. A navigation menu includes links for 'home', 'messaggi', 'moduli', 'URI', 'eventi', 'attacchi', 'scansioni', 'tipi di attacco', and 'esci'.

### HOME-PAGE UTENTE

#### RIEPILOGO ATTIVITÀ

	settimana	mese	anno	totali
collaudi effettuati	0	1	1	1
applicazioni verificate	0	1	1	1
URI esaminate	0	1	1	1
attacchi completati	0	1	1	1
attacchi corretti:	0	0	0	0

#### ULTIMI MESSAGGI

modulo	da	oggetto	data	
Seguro!	sistema	notifica dell'invio in correzione del modulo: Seguro!	27-06-2022 14:02:17	<a href="#">dettagli</a>
Seguro!	sistema	notifica della correzione dell'attacco: A-ZZ6ZZZZ	27-06-2022 15:24:06	<a href="#">dettagli</a>
Seguro!	sistema	notifica del completamento delle correzioni del modulo: Seguro!	27-06-2022 15:36:40	<a href="#">dettagli</a>

n. record: 3

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-ok	23-06-2022	<a href="#">dettagli</a>

n. record: 1

Tacun - 2023

# Seguro!

## Executive summary

**S** Seguro Junk - R.Canaro 09:01  
SEGURO - notifica della pubblicazione dell'attacco: A-ZZ6ZZ22  
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 dei test di sicurezza applicativa,  
all'indirizzo: <https://seguro.dev.tacun.it>

Il presente messaggio di posta elettronica ha carattere riservato, è tutelato dal segreto professionale ed è ad esclusivo utilizzo del destinatario indicato nel campo indirizzo.  
Con riferimento all'art. 114, comma 1, del Decreto Legislativo 24 febbraio 1998 n. 58, il destinatario è obbligato a: mantenere la segretezza circa le informazioni di carattere riservato e trattare tali informazioni solo nell'ambito di canali autorizzati affinché la relativa circolazione nel contesto aziendale possa svolgersi senza pregiudizio del carattere riservato delle informazioni stesse.  
In caso di inosservanza delle disposizioni degli articoli medesimi è applicabile una sanzione amministrativa pecuniaria da 5.000 a 500.000 euro.

**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

The screenshot displays the Seguro! user interface. At the top, there is a navigation bar with the logo 'Seguro!' and a dropdown menu for 'resp.sicurezza' with a 'cambia' button. The main content area is titled 'HOME-PAGE UTENTE' and contains three sections:

- RIEPILOGO ATTIVITÀ**: A table showing activity counts for the week, month, and year.
- ULTIMI MESSAGGI**: A table of recent messages with columns for 'modulo', 'da', 'oggetto', and 'data', including a 'dettagli' button for each.
- ELENCO MODULI ASSOCIATI ALL'UTENTE**: A table listing modules with columns for 'codice', 'nome', 'progetto', 'referente', 'resp.sviluppo', 'stato', and 'data test', including a 'dettagli' button.

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

The screenshot shows the Seguro! web application interface. At the top left is the logo "Seguro". A navigation bar contains "resp.web" and a "cambia" button. A confirmation dialog box is open, asking "seguro.tacun.it says confermi invio in correzione del modulo?" with "Cancel" and "OK" buttons. Below the dialog, the heading "DATI MODULO: SEGURO!" is displayed. A list of module details follows:

- Codice: M-TTQTTT6
- Progetto: Seguro
- Nome: Seguro!
- Stato: sicurezza-ko
- Versione: 3.2.20
- Rilasciato: 21-06-2022
- Appguid: seguro
- Referente: Referente Applicativo
- Resp.Sviluppo: Responsabile Sviluppo
- Resp.Sicurezza: Responsabile Sicurezza
- URI Test: https://seguro.dev.tacun.it
- URI Esercizio: https://seguro.tacun.it
- Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

Navigation links include "INDIETRO", "nota", "allegato", "messaggi", "eventi", and "in correzione". Below this is the heading "ATTACCHI ASSOCIATI AL MODULO" and a table:

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	no	<a href="#">dettagli</a>

At the bottom left, the URL "https://seguro.tacun.it/modulo/correzione/new/M-TTQTTT6" is visible. At the bottom right, it says "n. record: 1".

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

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

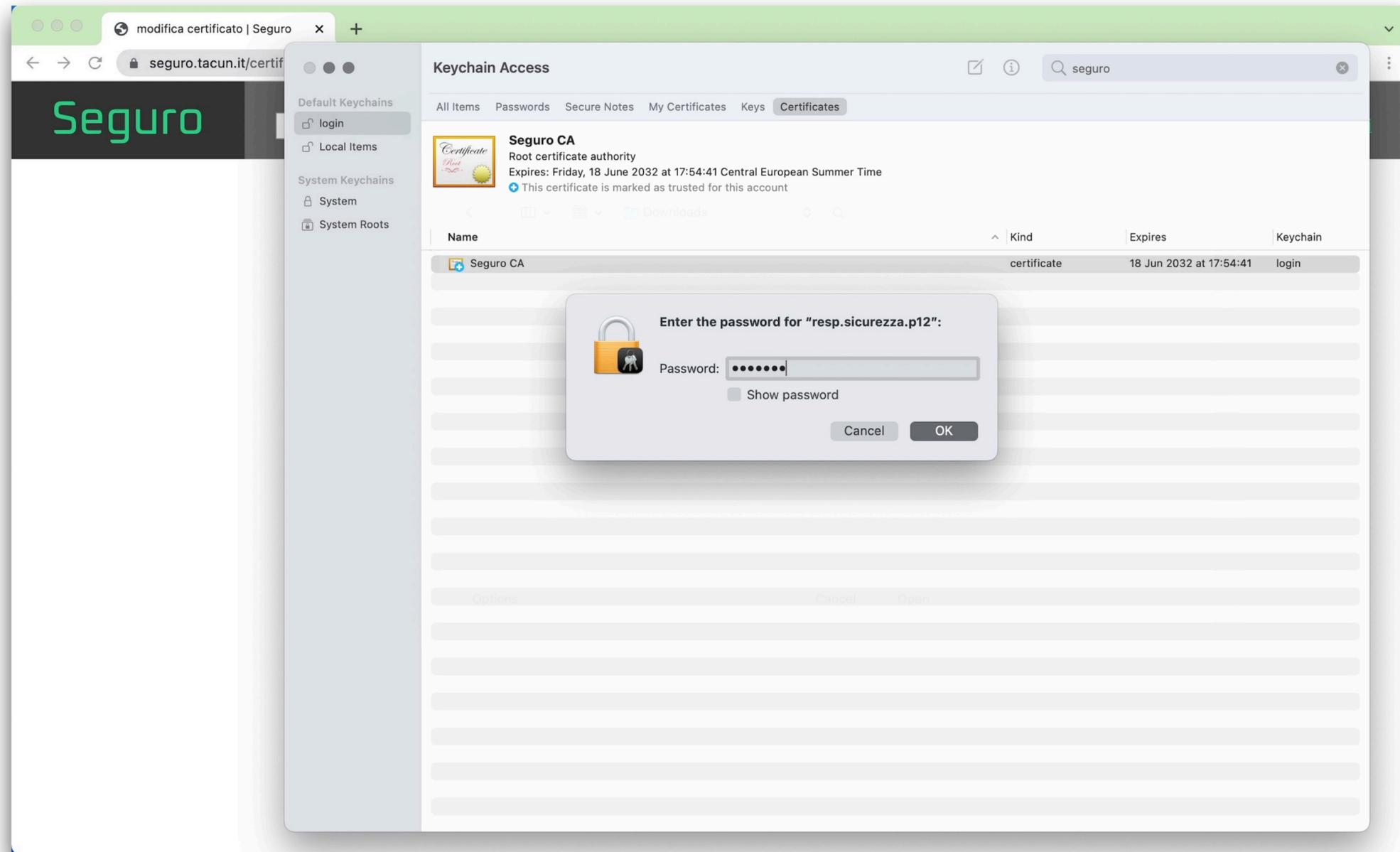
L'accesso degli utenti può avvenire o con **utenze locali** o con **utenze LDAP**.

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

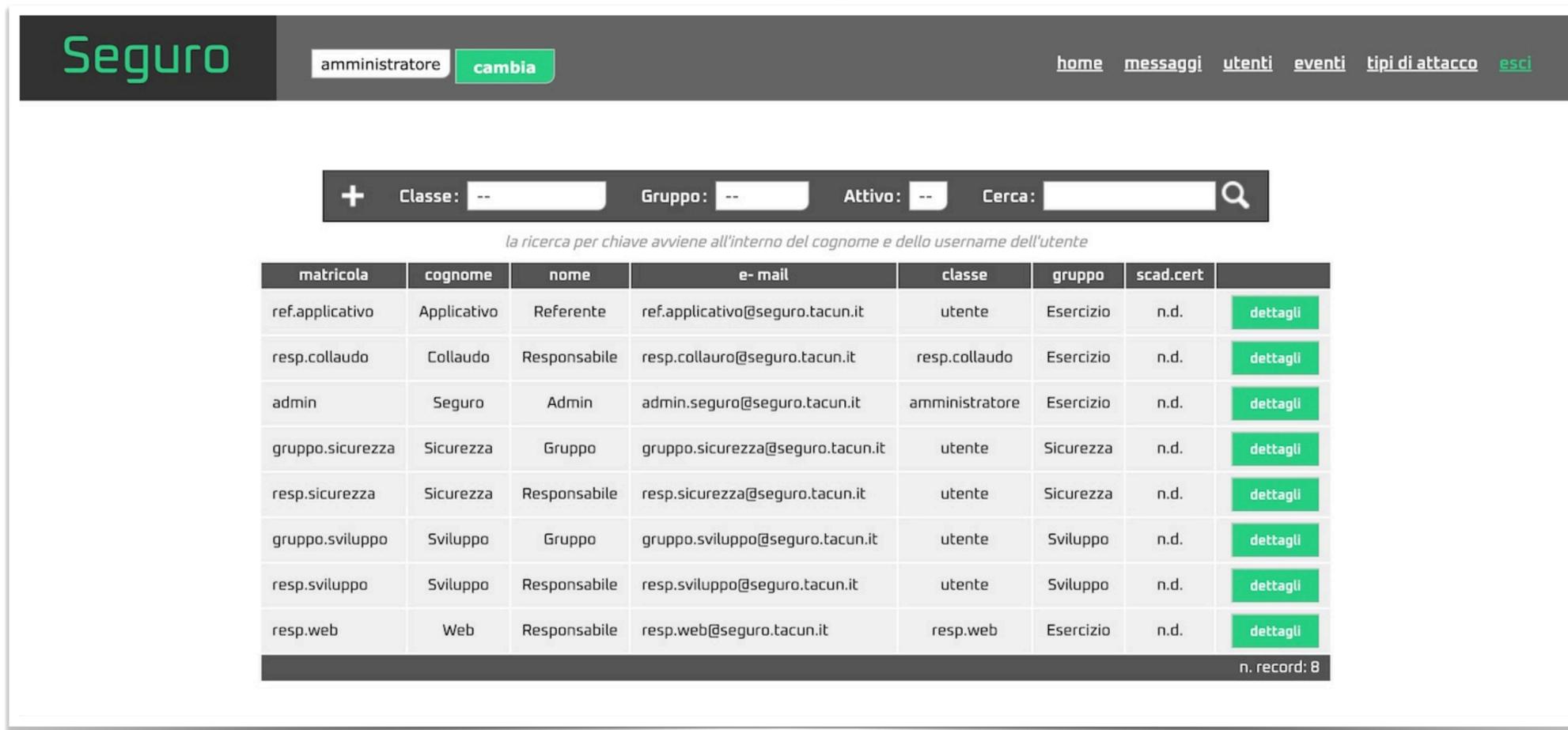


L'accesso con certificato aumenta la sicurezza del sistema e rende **non ripudiabili** le azioni intraprese dagli utenti.

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

# Seguro!

## Utenze e gruppi di utenza



The screenshot shows the Seguro user management interface. At the top, there is a navigation bar with the Seguro logo, a user role indicator 'amministratore' with a 'cambia' button, and a menu with links for 'home', 'messaggi', 'utenti', 'eventi', 'tipi di attacco', and 'esci'. Below the navigation bar is a search and filter section with a plus sign, dropdown menus for 'Classe' and 'Gruppo', a radio button for 'Attivo', and a search input field with a magnifying glass icon. A note below the search section states: 'la ricerca per chiave avviene all'interno del cognome e dello username dell'utente'. The main content is a table with 8 columns: 'matricola', 'cognome', 'nome', 'e-mail', 'classe', 'gruppo', 'scad.cert', and 'dettagli'. The table contains 8 rows of user and group information. At the bottom right of the table, it says 'n. record: 8'.

matricola	cognome	nome	e-mail	classe	gruppo	scad.cert	dettagli
ref applicativo	Applicativo	Referente	ref applicativo@seguro.tacun.it	utente	Esercizio	n.d.	dettagli
resp collaudo	Collaudo	Responsabile	resp collauro@seguro.tacun.it	resp collaudo	Esercizio	n.d.	dettagli
admin	Seguro	Admin	admin.seguro@seguro.tacun.it	amministratore	Esercizio	n.d.	dettagli
gruppo sicurezza	Sicurezza	Gruppo	gruppo.sicurezza@seguro.tacun.it	utente	Sicurezza	n.d.	dettagli
resp sicurezza	Sicurezza	Responsabile	resp.sicurezza@seguro.tacun.it	utente	Sicurezza	n.d.	dettagli
gruppo sviluppo	Sviluppo	Gruppo	gruppo.sviluppo@seguro.tacun.it	utente	Sviluppo	n.d.	dettagli
resp sviluppo	Sviluppo	Responsabile	resp.sviluppo@seguro.tacun.it	utente	Sviluppo	n.d.	dettagli
resp.web	Web	Responsabile	resp.web@seguro.tacun.it	resp.web	Esercizio	n.d.	dettagli

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

### NUOVO MODULO

Progetto:	<input type="text" value="Seguro"/>
Nome:	<input type="text" value="Seguro!"/>
Versione:	<input type="text" value="3.2.20"/>
Referente:	<input type="text" value="Applicativo Referente (Esercizio)"/>
Resp.Sviluppo:	<input type="text" value="Sviluppo Responsabile (Sviluppo)"/>
Resp.Sicurezza:	<input type="text" value="Sicurezza Responsabile (Sicurezza)"/>
URI Test:	<input type="text" value="https://seguro.dev.tacun.it"/>
URI Esercizio:	<input type="text" value="https://seguro.tacun.it"/>
Descrizione:	<input type="text" value="Applicazione Web per la gestione dei test di sicurezza applica"/>

[INDIETRO](#)

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



seguro.tacun.it says  
confermi apertura di nuova sessione di test sul modulo?

Cancel OK

Codice:  
Progetto: seguro  
Nome: Seguro!  
Stato: rilascio  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#) [scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [nuovo test](#)

### ATTACCHI ASSOCIATI AL MODULO

il modulo non ha attacchi associati

**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

### NUOVA URI

Modulo:	Seguro->Seguro!
URI:	<input "="" type="text" value="https://seguro.tacun.it/entra?p_dest="/>
Path Menu:	<input type="text" value="Maschera di login"/>
Azione:	<input type="text" value="login"/>
Piattaforma:	<input type="text" value="PHP"/>

[INDIETRO](#)

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

### MODIFICA ATTACCO

**Codice:** A-ZZ6ZZZZ

**URI:** https://seguro.tacun.it/entra?p\_dest=

**Profilo:** gruppo.sicurezza

**Tipo:** Cross Site Scripting (XSS)

**Parametro:** p\_dest

**Descrizione:** Aggiunta al valore del campo la stringa: " OR "1"="1

**ATTENZIONE:** mentre il campo **descrizione** è visibile solo al gruppo di lavoro, il campo **effetto** compare nei documenti e non deve contenere informazioni che permettano di replicare l'attacco

**Effetto:** Una eccezione non gestita mostra dei dettagli sull'architettura di sistema:  
UIException Object  
(  
[error:protected] => accesso negato  
[title:protected] => errore utente  
[message:protected] => utente inesistente o password errata  
[string:Exception:private] =>  
[code:protected] => 0  
[file:protected] => /usr/local/src/seguro/www/utente.login.php  
[line:protected] => 78  
[trace:Exception:private] => Array  
(

**Esito:** riuscito

**Livello:** basso

[INDIETRO](#) [nuovo allegato](#) [elimina](#) [salva](#)

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

**l'attacco è stato reso visibile al gruppo di sviluppo**

### DATI MODULO: SEGURO!

Codice: M-TTQTTT6  
Progetto: Seguro  
Nome: Seguro!  
Stato: test-sicurezza  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#)      [scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [fine test](#)

### ATTACCHI ASSOCIATI AL MODULO

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	visibile	mostra	
A-ZZ6ZZ2Z	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	no	sì		<a href="#">dettagli</a>

n. record: 1

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	<a href="#">dettagli</a>
Seguro!	sistema	notifica della pubblicazione dell'attacco: A-ZZ6ZZZZ	24-06-2022 12:39:31	<a href="#">dettagli</a>
Seguro!	sistema	notifica dell'invio in correzione del modulo: Seguro!	27-06-2022 14:02:17	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	27-06-2022 14:39:08	<a href="#">dettagli</a>

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	<a href="#">dettagli</a>

n. record: 1

#### ELENCO URI ASSEGNATE

codice	URI	modulo	stato	
U-TT6TTTE	<a href="https://seguro.tacun.it/entra?p_dest=">https://seguro.tacun.it/entra?p_dest=</a>	Seguro!	correzione	<a href="#">dettagli</a>

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

The screenshot shows the 'Seguro' web application interface. At the top left, the logo 'Seguro' is displayed. A navigation bar contains the text 'resp.sviluppo' and a 'cambia' button. A confirmation dialog box is open, asking 'seguro.tacun.it says confermi completamento delle attività di correzione del modulo?' with 'Cancel' and 'OK' buttons. Below the dialog, the page title 'DATI MODULO. SEGURO!' is visible. The main content area displays the following details:

- Codice: M-TTQTTT6
- Progetto: Seguro
- Nome: Seguro!
- Stato: correzione
- Versione: 3.2.20
- Rilasciato: 21-06-2022
- Appguid: seguro
- Referente: Referente Applicativo
- Resp.Sviluppo: Responsabile Sviluppo
- Resp.Sicurezza: Responsabile Sicurezza
- URI Test: https://seguro.dev.tacun.it
- URI Esercizio: https://seguro.tacun.it
- Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

Navigation links include 'INDIETRO', 'nota', 'allegato', 'messaggi', 'eventi', and a highlighted 'corretto' button.

The section 'ATTACCHI ASSOCIATI AL MODULO' contains a table with the following data:

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	sì	<a href="#">dettagli</a>

The footer shows the URL 'https://seguro.tacun.it/modulo/correzione/end/M-TTQTTT6' and 'n. record: 1'.

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

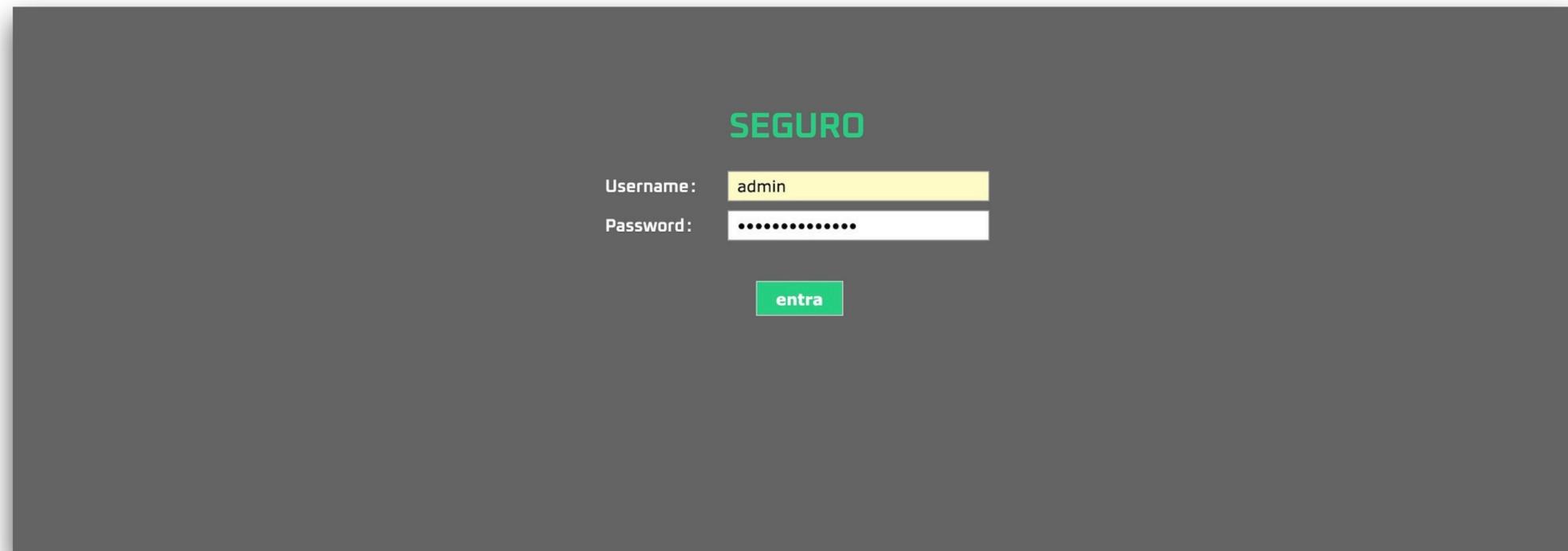
## Esempio di test applicativo

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



The screenshot shows a login form on a dark grey background. At the top center, the word "SEGURO" is written in green. Below it, there are two input fields: "Username:" with the text "admin" and "Password:" with a series of dots. A green button labeled "entra" is positioned below the password field.

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

+ Classe: -- Gruppo: -- Attivo: -- Cerca:

*la ricerca per chiave avviene all'interno del cognome e dello username dell'utente*

matricola	cognome	nome	e- mail	classe	gruppo	scad.cert	
ref applicativo	Applicativo	Referente	ref applicativo@seguro.tacun.it	utente	Esercizio	n.d.	<a href="#">dettagli</a>
resp.collaudo	Collaudo	Responsabile	resp.collaudo@seguro.tacun.it	resp.collaudo	Esercizio	n.d.	<a href="#">dettagli</a>
admin	Seguro	Admin	admin.seguro@seguro.tacun.it	amministratore	Esercizio	n.d.	<a href="#">dettagli</a>
gruppo.sicurezza	Sicurezza	Gruppo	gruppo.sicurezza@seguro.tacun.it	utente	Sicurezza	n.d.	<a href="#">dettagli</a>
resp.sicurezza	Sicurezza	Responsabile	resp.sicurezza@seguro.tacun.it	utente	Sicurezza	n.d.	<a href="#">dettagli</a>
gruppo.sviluppo	Sviluppo	Gruppo	gruppo.sviluppo@seguro.tacun.it	utente	Sviluppo	n.d.	<a href="#">dettagli</a>
resp.sviluppo	Sviluppo	Responsabile	resp.sviluppo@seguro.tacun.it	utente	Sviluppo	n.d.	<a href="#">dettagli</a>
resp.web	Web	Responsabile	resp.web@seguro.tacun.it	resp.web	Esercizio	n.d.	<a href="#">dettagli</a>

n. record: 8

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

### DATI UTENTE

Username:	<input type="text" value="resp.sicurezza"/>
Classe:	<input type="text" value="utente"/>
Gruppo:	<input type="text" value="Sicurezza"/>
E- Mail:	<input type="text" value="resp.sicurezza@seguro.tacun.it"/>
Cognome:	<input type="text" value="Sicurezza"/>
Nome:	<input type="text" value="Responsabile"/>

[INDIETRO](#)      [nuovo certificato](#)    [salva](#)    [elimina](#)

### CERTIFICATI ASSOCIATI ALL'UTENTE

l'utente non ha certificati associati

### MODULI ASSOCIATI ALL'UTENTE

l'utente non ha moduli associati

### EVENTI ASSOCIATI ALL'UTENTE

non ci sono record con le caratteristiche richieste

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

The screenshot shows the Seguro web interface. At the top left, the logo "Seguro" is displayed. Below it, there is a navigation bar with "amministratore" and a "cambia" button. A confirmation dialog box is open, titled "seguro.tacun.it says", with the text: "ATTENZIONE! generando un nuovo certificato si annulleranno eventuali certificati preesistenti. Confermi generazione nuovo certificato?". The dialog has "Cancel" and "OK" buttons. Below the dialog, the user details are listed:

Cognome:	Sicurezza
Nome:	Responsabile
Username:	resp.sicurezza
Classe:	utente
Gruppo:	Sicurezza
E- Mail:	resp.sicurezza@seguro.tacun.it

At the bottom left, there is a link labeled "INDIETRO". At the bottom right, there is a green button labeled "genera 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

### MODIFICA CERTIFICATO

Utente: resp.sicurezza  
Seriale: 29  
Scadenza: 21-06-2023 00:00:00  
Attivo: sì  no

[INDIETRO](#) [scarica certificato](#) [salva](#)

### EVENTI ASSOCIATI AL CERTIFICATO

data	utente	tipo	classe	esito
21-06-2022 16:25:43	Admin Seguro	creazione	certificato	OK

n. record: 1

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**

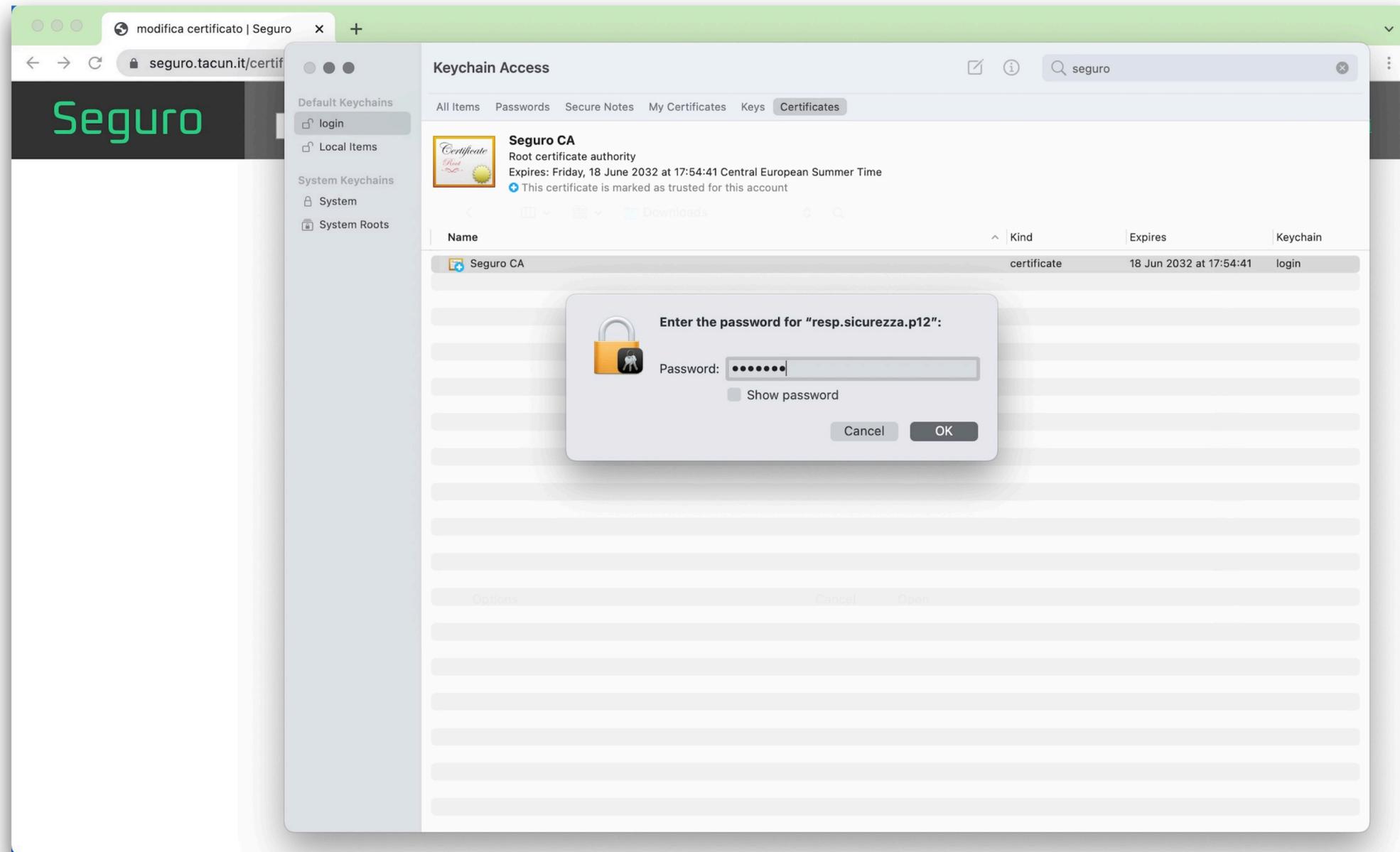
Una volta installato il certificato, potrà accedere a Seguro dal seguente indirizzo:  
<https://seguro.tacun.it>

Ulteriori informazioni sono disponibili sul sistema di gestione dei 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

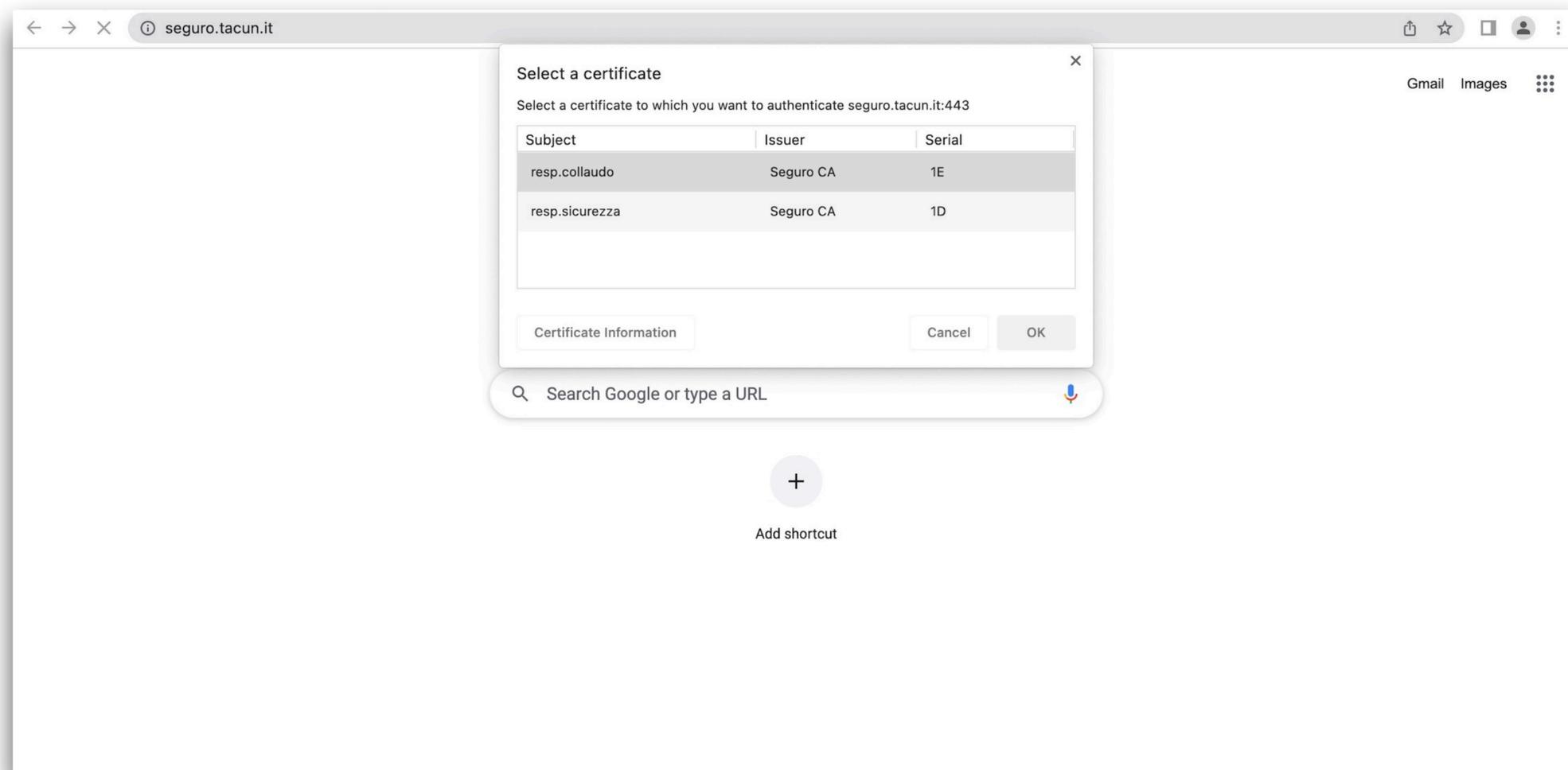


Il certificato viene consegnato **personalmente** all'utente dal Gruppo Sicurezza.

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

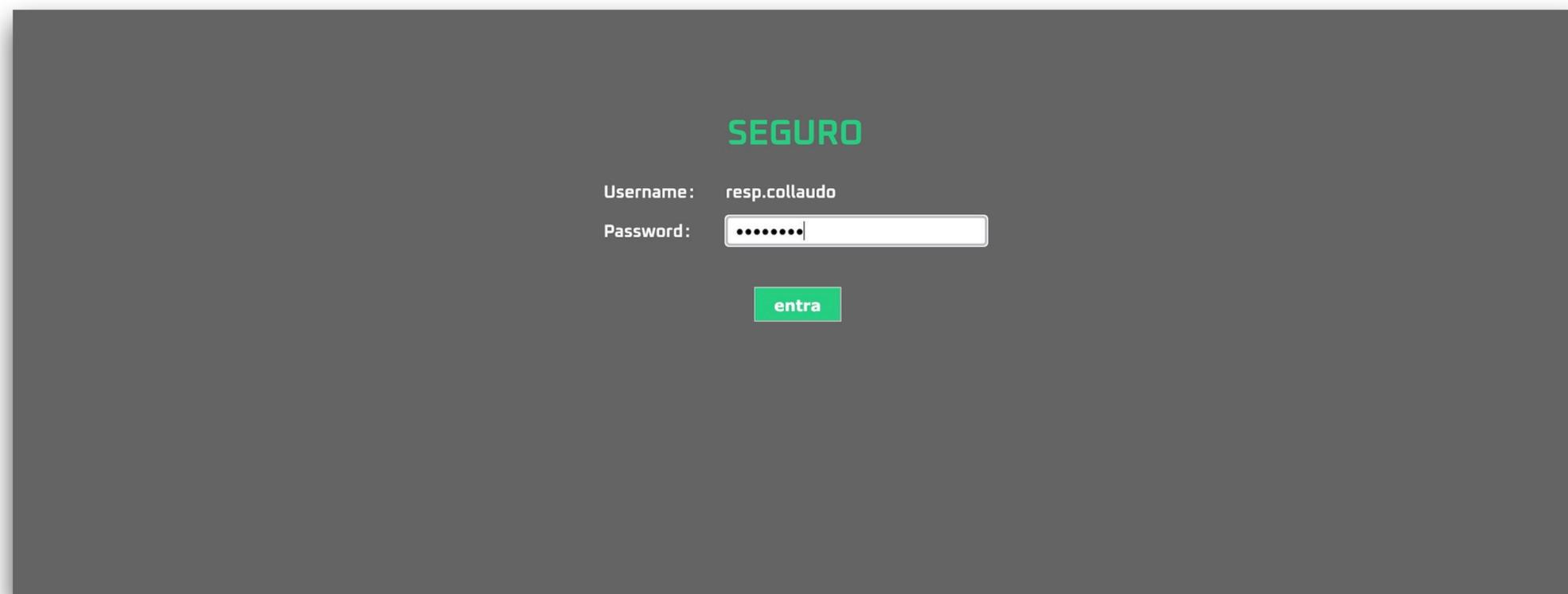


Quando l'utente accede al sistema, il browser permette di scegliere quale certificato utilizzare per l'accesso.

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

# Responsabile collaudo

## Login con certificato



The screenshot shows a login interface on a dark grey background. At the top center, the word "SEGURO" is displayed in green. Below it, the text "Username: resp.collaudo" is shown. Underneath, the text "Password:" is followed by a white input field containing seven black dots. At the bottom center, there is a green button with the white text "entra".

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

### HOME-PAGE UTENTE

#### RIEPILOGO ATTIVITÀ

	settimana	mese	anno	totali
collaudi effettuati	0	1	1	1
applicazioni verificate	0	1	1	1
URI esaminate	0	1	1	1
attacchi completati	0	1	1	1
attacchi corretti:	0	0	0	0

#### ULTIMI MESSAGGI

modulo	da	oggetto	data	
sistema	sistema	notifica dell'assegnazione di un certificato digitale	21-06-2022 16:36:44	<a href="#">dettagli</a>

n. record: 1

i messaggi con il fondo grigio scuro non sono stati letti

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

The screenshot shows a web interface titled "ELENCO PROGETTI" in green. Below the title is a dark grey search bar containing a plus sign (+), a "Cliente:" dropdown menu with "--" selected, a "Nome:" text input field, and a "Cerca:" button with a magnifying glass icon. Below the search bar, the text "non ci sono record con le caratteristiche richieste" is displayed in a small, grey font.

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

**NUOVO PROGETTO**

Cliente:

Nome:

Descrizione:

Data Inizio:

Note:

[INDIETRO](#)

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

### MODIFICA PROGETTO: SEGURO

Cliente:	<input type="text" value="Tacun Srls"/>
Nome:	<input type="text" value="Seguro"/>
Descrizione:	<input type="text" value="Test di sicurezza applicazione Web Seguro"/>
Data Inizio:	<input type="text" value="21"/> <input type="text" value="06"/> <input type="text" value="2022"/> <input type="text" value="oggi"/>
Data Fine:	<input type="text" value="--"/> <input type="text" value="--"/> <input type="text" value="--"/> <input type="text" value="oggi"/>
Note:	<input type="text"/>

[INDIETRO](#)

elimina

salva

### MODULI ASSOCIATI AL PROGETTO

il progetto non ha moduli associati

### UTENTI ASSOCIATI AL PROGETTO

non ci sono utenti associati al 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

### NUOVO MODULO

Progetto:	<input type="text" value="Seguro"/>
Nome:	<input type="text" value="Seguro!"/>
Versione:	<input type="text" value="3.2.20"/>
Referente:	<input type="text" value="Applicativo Referente (Esercizio)"/>
Resp.Sviluppo:	<input type="text" value="Sviluppo Responsabile (Sviluppo)"/>
Resp.Sicurezza:	<input type="text" value="Sicurezza Responsabile (Sicurezza)"/>
URI Test:	<input type="text" value="https://seguro.dev.tacun.it"/>
URI Esercizio:	<input type="text" value="https://seguro.tacun.it"/>
Descrizione:	<input type="text" value="Applicazione Web per la gestione dei test di sicurezza applica"/>

[INDIETRO](#)

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

**MODIFICA MODULO: SEGURO!**

Codice: M-TTQTTT6  
Stato: creazione  
Progetto: Seguro  
Nome: Seguro!  
Versione: 3.2.20  
Appguid: sicuro  
Referente: Applicativo Referente (Esercizio)  
Resp.Sviluppo: Sviluppo Responsabile (Sviluppo)  
Resp.Sicurezza: Sicurezza Responsabile (Sicurezza)  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applica

[INDIETRO](#)   [nota](#)   [allegato](#)   [messaggi](#)   [eventi](#)   [salva](#)   [elimina](#)   [rilascia](#)

**ELENCO PROFILI ASSOCIATI AL MODULO**

profilo	username	password	
utente anonimo	[anonimo]		<a href="#">dettagli</a>

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

### ELENCO PROFILI ASSOCIATI AL MODULO

profilo	username	password	
utente anonimo	[anonimo]		<a href="#">dettagli</a>

n. record: 1

[nuovo profilo](#)

### ATTRIBUTI ASSOCIATI AL MODULO

il modulo non ha attributi associati

Tipo: -- [associa](#)

### ELENCO UTENTI

utente	ruolo	inizio	fine	
Referente Applicativo	ref applicativo	21-06-2022 16:50	--	<a href="#">fine</a>
Responsabile Sicurezza	resp. sicurezza	21-06-2022 16:50	--	<a href="#">fine</a>
Responsabile Sviluppo	resp. sviluppo	21-06-2022 16:50	--	<a href="#">fine</a>

n. record: 3

Utente: -- Ruolo: -- [associa](#)

### ELENCO ALLEGATI

non ci sono allegati

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

### PROFILO

Modulo:	Seguro!
Profilo:	<input type="text" value="Amministratore"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="text" value="password"/>
Note:	<input type="text"/>
Creazione:	2022-06-21 16:50:10 (resp.collaudo)
Modifica:	2022-06-21 16:54:02 (resp.collaudo)

[INDIETRO](#)

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

The screenshot displays a web application interface for managing user profiles. At the top, there are tabs for 'Amministratore', 'admin', 'password', and 'dettagli'. Below this, a 'nuovo profilo' section is visible. The main heading is 'ATTRIBUTI ASSOCIATI AL MODULO', with a sub-message 'il modulo non ha attributi associati'. A dropdown menu is open, showing a list of attribute types such as 'DBMS -> DB2', 'DBMS -> MySQL', 'DBMS -> Oracle', 'DBMS -> SQL server', 'DBMS -> UDB', 'esposizione -> intranet', 'esposizione -> internet', 'esposizione -> intranet', 'infrastruttura -> gestore eventi', 'infrastruttura -> Oracle BI', 'infrastruttura -> PdD', 'infrastruttura -> profilazione', 'infrastruttura -> SOA', 'infrastruttura -> tracciatura', 'linguaggi -> .NET', 'linguaggi -> Ajax', 'linguaggi -> C++', 'linguaggi -> Java', 'linguaggi -> Javascript', 'linguaggi -> PHP', 'piattaforma -> BEA portal', 'piattaforma -> JBoss 4.x', and 'piattaforma -> JBoss 5.x'. Below the dropdown, there is a table with columns for 'utente', 'fine', and 'associa'. The table contains three rows of data. At the bottom, there is a form with a 'Utente:' field and an 'associa' button.

utente	fine	associa
Referente Applicati	16:50 --	fine
Responsabile Sicure	16:50 --	fine
Responsabile Svilu	16:50 --	fine

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

### ELENCO PROFILI ASSOCIATI AL MODULO

profilo	username	password	
Amministratore	admin	password	<a href="#">dettagli</a>

n. record: 1

[nuovo profilo](#)

### ATTRIBUTI ASSOCIATI AL MODULO

categoria	attributo	
DBMS	MySQL	<a href="#">elimina</a>
esposizione	intranet	<a href="#">elimina</a>
linguaggi	PHP	<a href="#">elimina</a>

n. record: 3

Tipo: -- [associa](#)

### ELENCO UTENTI

utente	ruolo	inizio	fine	
Referente Applicativo	ref applicativo	21-06-2022 16:50	--	<a href="#">fine</a>
Responsabile Sicurezza	resp.sicurezza	21-06-2022 16:50	--	<a href="#">fine</a>
Responsabile Sviluppo	resp.sviluppo	21-06-2022 16:50	--	<a href="#">fine</a>

n. record: 3

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

# Responsabile collaudo

## Rilascio del modulo

seguro.tacun.it says  
confermi rilascio del modulo?

Cancel OK

**MODIFICA MODULO: SEGURO!**

Codice: M-TTQTTT6  
Stato: creazione  
Progetto: Seguro  
Nome: Seguro!  
Versione: 3.2.20  
Appguid: seguro  
Referente: Applicativo Referente (Esercizio)  
Resp.Sviluppo: Sviluppo Responsabile (Sviluppo)  
Resp.Sicurezza: Sicurezza Responsabile (Sicurezza)  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applica

[INDIETRO](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [salva](#) [elimina](#) [rilascia](#)

**ELENCO PROFILI ASSOCIATI AL MODULO**

profilo	username	password	
Amministratore	admin	password	<a href="#">dettagli</a>

https://seguro.tacun.it/modulo/rilascia/M-TTQTTT6

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

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

---

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 destinatari di questo messaggio di verificare la correttezza dei dati inseriti, per quanto attenga alla propria competenza.

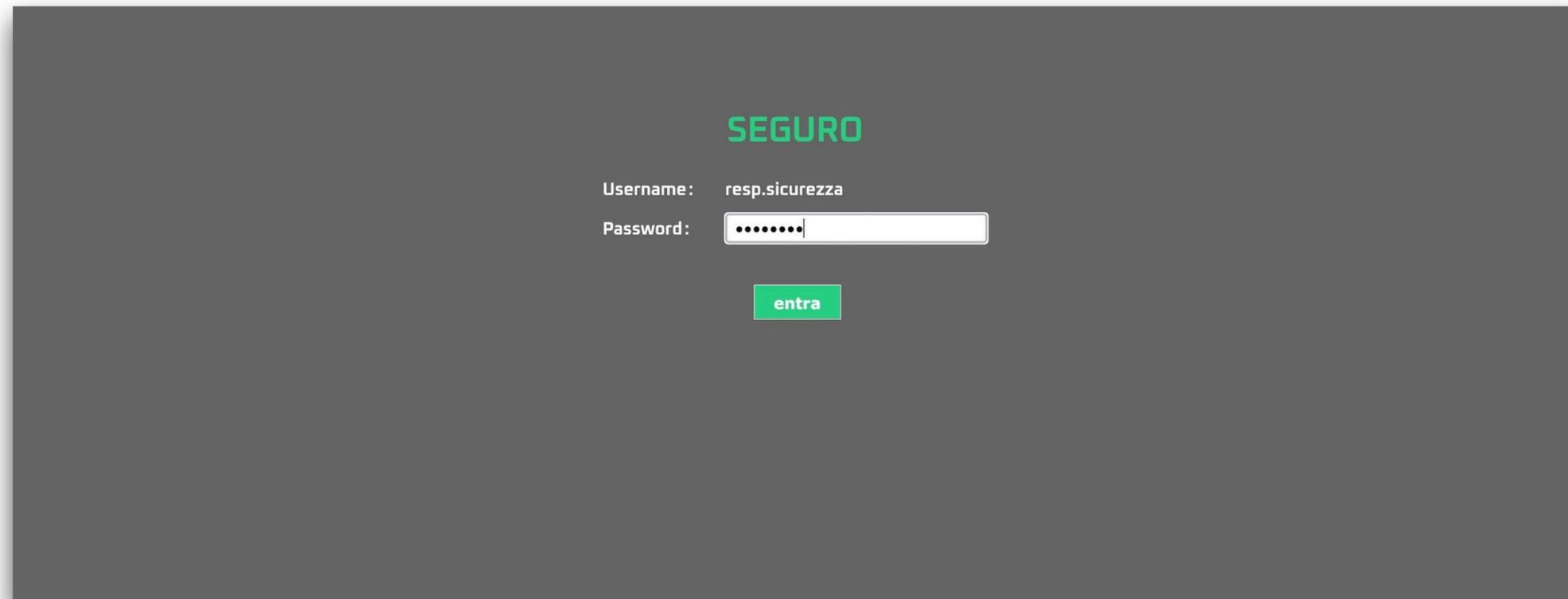
**ATTENZIONE:** data la natura invasiva delle prove cui sarà sottoposta l'applicazione in oggetto, è indispensabile che, prima dell'avvio dei test, il gruppo di sviluppo generi una copia di tutte le basi-dati utilizzate dal sistema per poterle ripristinare in caso venissero alterate nel corso dei controlli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

Ulteriori informazioni sono disponibili sul sistema di gestione dei 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



SEGURO

Username: resp.sicurezza

Password:

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

# Responsabile sicurezza

## Home page

**HOME-PAGE UTENTE**

**RIEPILOGO ATTIVITÀ**

	settimana	mese	anno	totali
collaudi effettuati	0	0	0	0
applicazioni verificate	0	0	0	0
URI esaminate	0	0	0	0
attacchi completati	0	0	0	0
attacchi corretti:	0	0	0	0

**ULTIMI MESSAGGI**

non ci sono messaggi non letti

**ELENCO MODULI ASSOCIATI ALL'UTENTE**

codice	nome	progetto	referente	resp.sviluppo	stato	data test	
M-TTQTTT6	Seguro!	Seguro	Referente Applicativo	Responsabile Sviluppo	rilascio		<a href="#">dettagli</a>

n. record: 1

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

### DATI MODULO: SEGURO!

**Codice:** M-TTQTTT6  
**Progetto:** Seguro  
**Nome:** Seguro!  
**Stato:** rilascio  
**Versione:** 3.2.20  
**Rilasciato:** 21-06-2022  
**Appguid:** seguro  
**Referente:** Referente Applicativo  
**Resp.Sviluppo:** Responsabile Sviluppo  
**Resp.Sicurezza:** Responsabile Sicurezza  
**URI Test:** https://seguro.dev.tacun.it  
**URI Esercizio:** https://seguro.tacun.it  
**Descrizione:** Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#)

[scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [nuovo test](#)

### ATTACCHI ASSOCIATI AL MODULO

il modulo non ha attacchi associati

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

### URI ASSOCIATE AL MODULO

il modulo non ha URI associate

### ELENCO PROFILI ASSOCIATI AL MODULO

profilo	username	password	
Amministratore	admin	password	<a href="#">dettagli</a>

n. record: 1

[nuovo profilo](#)

### ATTRIBUTI ASSOCIATI AL MODULO

categoria	attributo	
DBMS	MySQL	<a href="#">elimina</a>
esposizione	intranet	<a href="#">elimina</a>
linguaggi	PHP	<a href="#">elimina</a>

n. record: 3

Tipo: -- [associa](#)

### ELENCO UTENTI

utente	ruolo	inizio	fine
Referente Applicativo	ref.applicativo	21-06-2022 16:50	--
Responsabile Sicurezza	resp.sicurezza	21-06-2022 16:50	--
Responsabile Sviluppo	resp.sviluppo	21-06-2022 16:50	--

n. record: 3

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

seguro.tacun.it says  
confermi apertura di nuova sessione di test sul modulo?

Cancel OK

Codice: Seguro  
Progetto: Seguro  
Nome: Seguro!  
Stato: rilascio  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#) [scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [nuovo test](#)

### ATTACCHI ASSOCIATI AL MODULO

il modulo non ha attacchi associati

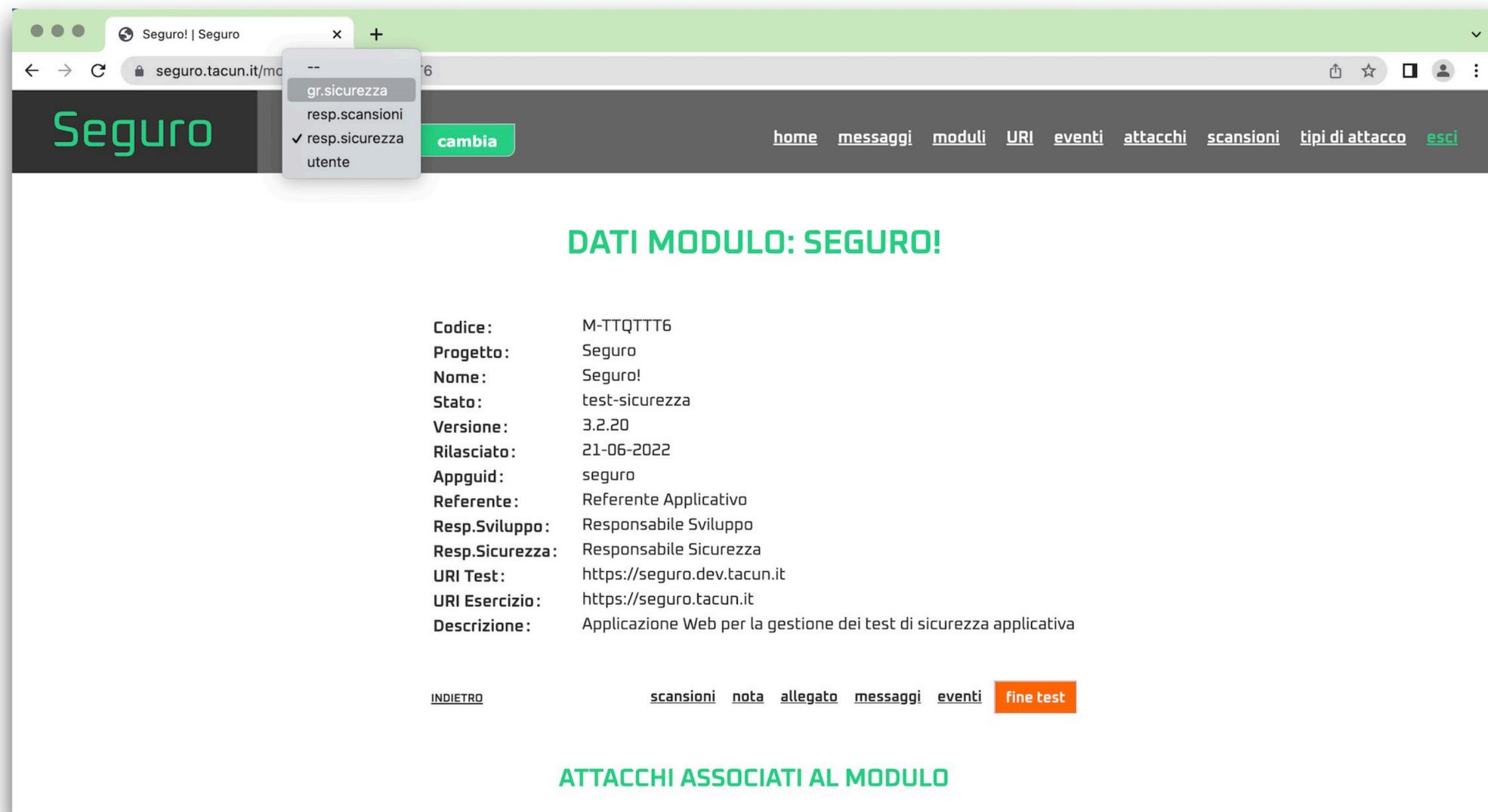
Facendo click sul bottone **nuovo test**, nella barra sotto ai dati anagrafici del modulo, si avvia una nuova sessione di test.

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



The screenshot shows a web browser window with the URL `seguro.tacun.it/modulo`. The page title is "Seguro! | Seguro". A dropdown menu is open, showing the current role "gr.sicurezza" and the target role "resp.sicurezza" which is selected with a checkmark. A green "cambia" button is visible next to the dropdown. The main content area displays "DATI MODULO: SEGURO!" followed by a list of module details:

Codice:	M-TTQTTT6
Progetto:	Seguro
Nome:	Seguro!
Stato:	test-sicurezza
Versione:	3.2.20
Rilasciato:	21-06-2022
Appguid:	seguro
Referente:	Referente Applicativo
Resp.Sviluppo:	Responsabile Sviluppo
Resp.Sicurezza:	Responsabile Sicurezza
URI Test:	https://seguro.dev.tacun.it
URI Esercizio:	https://seguro.tacun.it
Descrizione:	Applicazione Web per la gestione dei test di sicurezza applicativa

At the bottom of the details section, there are navigation links: "INDIETRO", "scansioni", "nota", "allegato", "messaggi", "eventi", and a highlighted "fine test" button. Below this, the heading "ATTACCHI ASSOCIATI AL MODULO" is visible.

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

**ATTRIBUTI ASSOCIATI AL MODULO**

categoria	attributo	
DBMS	MySQL	elimina
esposizione	intranet	elimina
linguaggi	PHP	elimina

n. record: 3

Tipo: --

**ELENCO UTENTI**

utente	ruolo	inizio	fine
Referente Applicativo	ref applicativo	21-06-2022 16:50	--
Responsabile Sicurezza	resp.sicurezza	21-06-2022 16:50	--
Responsabile Sviluppo	resp.sviluppo	21-06-2022 16:50	--

n. record: 3

Utente: --  Ruolo: gr.sicurezza

**ALLEGATI**

non ci sono allegati

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

categoria	attributo	
DBMS	MySQL	<b>elimina</b>
esposizione	intranet	<b>elimina</b>
linguaggi	PHP	<b>elimina</b>

n. record: 3

Tipo: -- **associa**

### 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	--	<b>fine</b>
Responsabile Sviluppo	resp.sviluppo	21-06-2022 16:50	--	

n. record: 4

Utente: -- Ruolo: -- **associa**

### ELENCO ALLEGATI

non ci sono allegati

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!

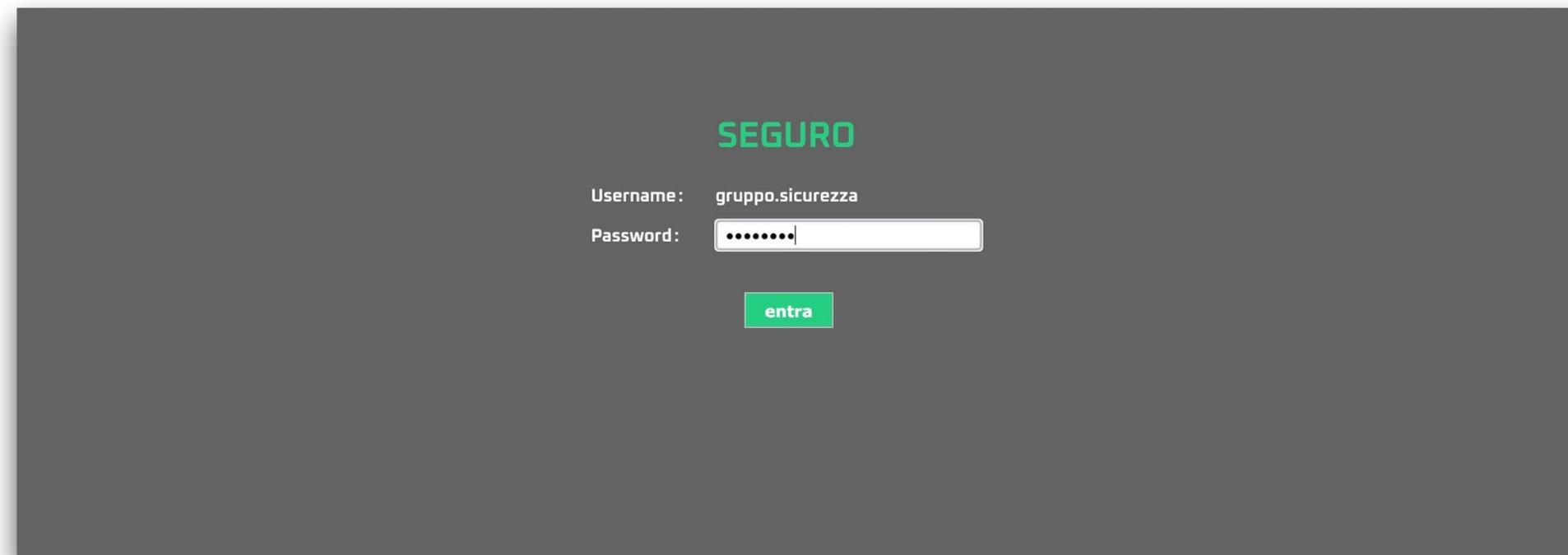
con il ruolo di: gr.sicurezza

Ulteriori informazioni sono disponibili sul sistema di gestione dei 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



**SEGURO**

Username: gruppo.sicurezza

Password:

**entra**

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

# Gruppo Sicurezza

## Home-page

### HOME-PAGE UTENTE

#### ULTIMI MESSAGGI

modulo	da	oggetto	data	
Seguro!	sistema	notifica dell'associazione al modulo: Seguro!	23-06-2022 17:29:16	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	23-06-2022 18:01:12	<a href="#">dettagli</a>
				n. record: 2

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	test-sicurezza	23-06-2022	<a href="#">dettagli</a>
							n. record: 1

#### ELENCO URI ASSEGNATE

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

### DATI MODULO: SEGURO!

Codice:	M-TTQTTT6
Progetto:	Seguro
Nome:	Seguro!
Stato:	test-sicurezza
Versione:	3.2.20
Rilasciato:	21-06-2022
Appguid:	seguro
Referente:	Referente Applicativo
Resp.Sviluppo:	Responsabile Sviluppo
Resp.Sicurezza:	Responsabile Sicurezza
URI Test:	https://seguro.dev.tacun.it
URI Esercizio:	https://seguro.tacun.it
Descrizione:	Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#)

[scansioni](#) [nuova URI](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#)

### ATTACCHI ASSOCIATI AL MODULO

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	<a href="#">dettagli</a>

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

**NUOVA URI**

Modulo:	Seguro->Seguro!
URI:	<input "="" type="text" value="https://seguro.tacun.it/entra?p_dest="/>
Path Menu:	<input type="text" value="Maschera di login"/>
Azione:	<input type="text" value="login"/>
Piattaforma:	<input type="text" value="PHP"/>

[INDIETRO](#)

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

URI correttamente inserita

### MODIFICA URI

Codice: U-TT6TTTE  
Modulo: Seguro!  
URI:   
Apri La URI: https://seguro.tacun.it/entra?p\_dest=  
Azione:   
Path Menu:   
Piattaforma:

[INDIETRO](#)      [nuovo attacco](#)   [elimina](#)   [salva](#)

### ATTACCHI ASSOCIATI ALLA URI

la URI non ha attacchi associati

### EVENTI ASSOCIATI ALLA URI

data	utente	tipo	classe	esito
24-06-2022 09:57:38	Gruppo Sicurezza	creazione	uri	OK

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

# Gruppo Sicurezza

## Nuovo attacco

### NUOVO ATTACCO

URI: U-TT6TTTE

Profilo:

Tipo:

Parametro:

[INDIETRO](#)

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

### MODIFICA ATTACCO

Codice:	A-ZZ6ZZZ
URI:	https://seguro.tacun.it/entra?p_dest=
Profilo:	<input type="text" value="gruppo.sicurezza"/>
Tipo:	<input type="text" value="Cross Site Scripting (XSS)"/>
Parametro:	<input type="text" value="p_dest"/>
Descrizione:	<input "1"="1" or="" type="text" value="Aggiunta al valore del campo la stringa: "/>
Effetto:	<p>ATTENZIONE: mentre il campo <b>descrizione</b> è visibile solo al gruppo di lavoro, il campo <b>effetto</b> compare nei documenti e non deve contenere informazioni che permettano di replicare l'attacco</p> <p>Una eccezione non gestita mostra dei dettagli sull'architettura di sistema:</p> <pre>UIException Object (   [error:protected] =&gt; accesso negato   [title:protected] =&gt; errore utente   [message:protected] =&gt; utente inesistente o password errata   [string:Exception:private] =&gt;   [code:protected] =&gt; 0   [file:protected] =&gt; /usr/local/src/seguro/www/utente.login.php   [line:protected] =&gt; 78   [trace:Exception:private] =&gt; Array )</pre>
Esito:	<input type="text" value="riuscito"/>
Livello:	<input type="text" value="basso"/>

[INDIETRO](#)      [nuovo allegato](#)    [elimina](#)    [salva](#)

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

### MODIFICA ATTACCO

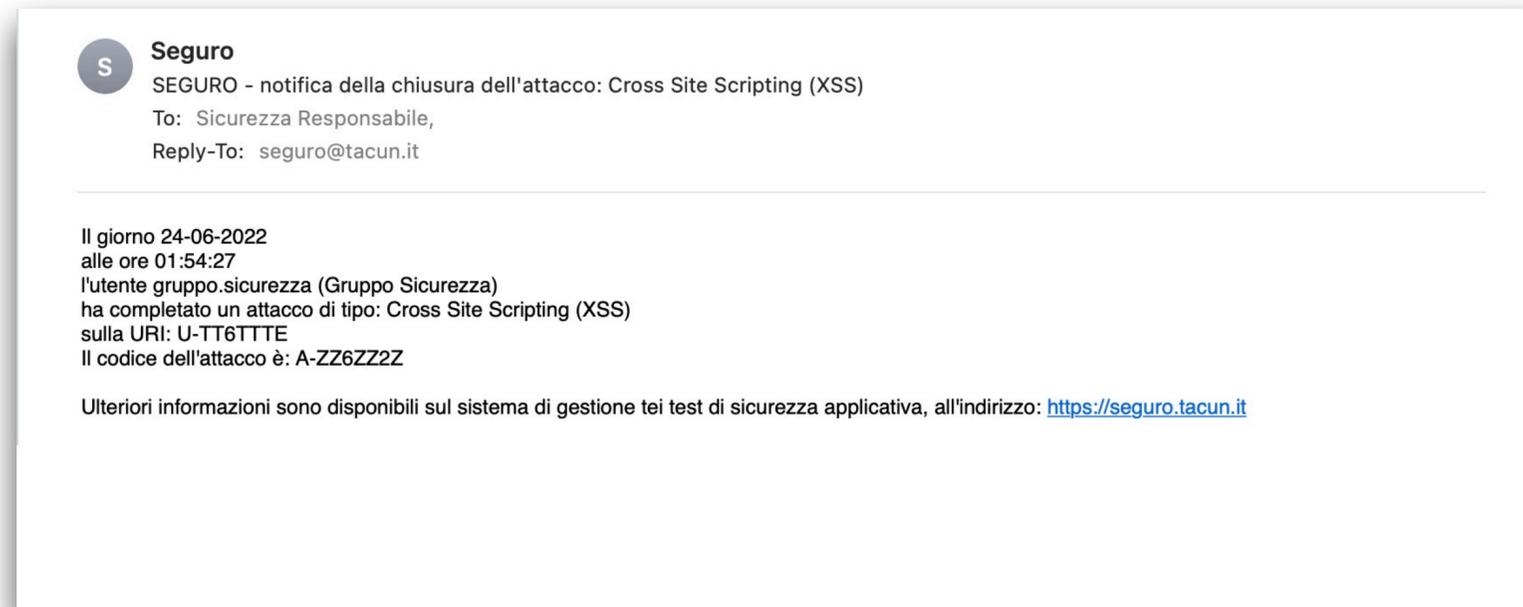
Codice:	A-ZZ6ZZZZ
URI:	https://seguero.tacun.it/entra?p_dest=
Profilo:	gruppo.sicurezza
Tipo:	Cross Site Scripting (XSS)
Parametro:	p_dest
Descrizione:	Aggiunta al valore del campo la stringa: " OR "1"="1 <small>ATTENZIONE: mentre il campo <b>descrizione</b> è visibile solo al gruppo di lavoro, il campo <b>effetto</b> compare nei documenti e non deve contenere informazioni che permettano di replicare l'attacco</small>
Effetto:	Una eccezione non gestita mostra dei dettagli sull'architettura di sistema: <pre>UIException Object (   [error:protected] =&gt; accesso negato   [title:protected] =&gt; errore utente   [message:protected] =&gt; utente inesistente o password errata   [string:Exception:private] =&gt;   [code:protected] =&gt; 0   [file:protected] =&gt; /usr/local/src/seguero/www/utente.login.php   [line:protected] =&gt; 78</pre>
Esito:	riuscito
Livello:	basso

[INDIETRO](#)      [nuovo allegato](#)   [elimina](#)   [completato](#)   [salva](#)

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



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

### DATI MODULO: SEGURO!

Codice: M-TTQTTT6  
Progetto: Seguro  
Nome: Seguro!  
Stato: test-sicurezza  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#)

[scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [fine test](#)

### ATTACCHI ASSOCIATI AL MODULO

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	visibile	mostra	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	no	no	<a href="#">mostra</a>	<a href="#">dettagli</a>

n. record: 1

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

### MODIFICA ATTACCO

Codice:	A-ZZ6ZZZZ
URI:	https://seguero.tacun.it/entra?p_dest=
Profilo:	<input type="text" value="gruppo.sicurezza"/>
Tipo:	<input type="text" value="Cross Site Scripting (XSS)"/>
Parametro:	<input type="text" value="p_dest"/>
Descrizione:	<input "1"="1" or="" type="text" value="Aggiunta al valore del campo la stringa: "/>
	<small>ATTENZIONE: mentre il campo <b>descrizione</b> è visibile solo al gruppo di lavoro, il campo <b>effetto</b> compare nei documenti e non deve contenere informazioni che permettano di replicare l'attacco</small>
Effetto:	<input type="text" value="Una eccezione non gestita mostra dei dettagli sull'architettura di sistema:&lt;br/&gt;&lt;br/&gt;UIException Object&lt;br/&gt;(&lt;br/&gt;  [error:protected] =&gt; accesso negato&lt;br/&gt;  [title:protected] =&gt; errore utente&lt;br/&gt;  [message:protected] =&gt; utente inesistente o password errata&lt;br/&gt;  [string:Exception:private] =&gt;&lt;br/&gt;  [code:protected] =&gt; 0"/>
Esito:	<input type="text" value="riuscito"/>
Livello:	<input type="text" value="basso"/>

[INDIETRO](#)      [nuovo allegato](#)   [elimina](#)   [salva](#)

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

l'attacco è stato reso visibile al gruppo di sviluppo

### DATI MODULO: SEGURO!

Codice: M-TTQTTT6  
Progetto: Seguro  
Nome: Seguro!  
Stato: test-sicurezza  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#) [scansioni](#) [nota](#) [allegato](#) [messaggi](#) [eventi](#) [fine test](#)

### ATTACCHI ASSOCIATI AL MODULO

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	visibile	mostra

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



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

**ESITO TEST PER MODULO: SEGURO!**

Codice:	M-TTQTTT6
Progetto:	Seguro
Nome:	Seguro!
Referente:	Referente Applicativo
Resp.Sviluppo:	Responsabile Sviluppo
Esito Test:	<input type="text" value="sicurezza-ko"/>
Note:	<input type="text" value="La vulnerabilità va corretta."/>

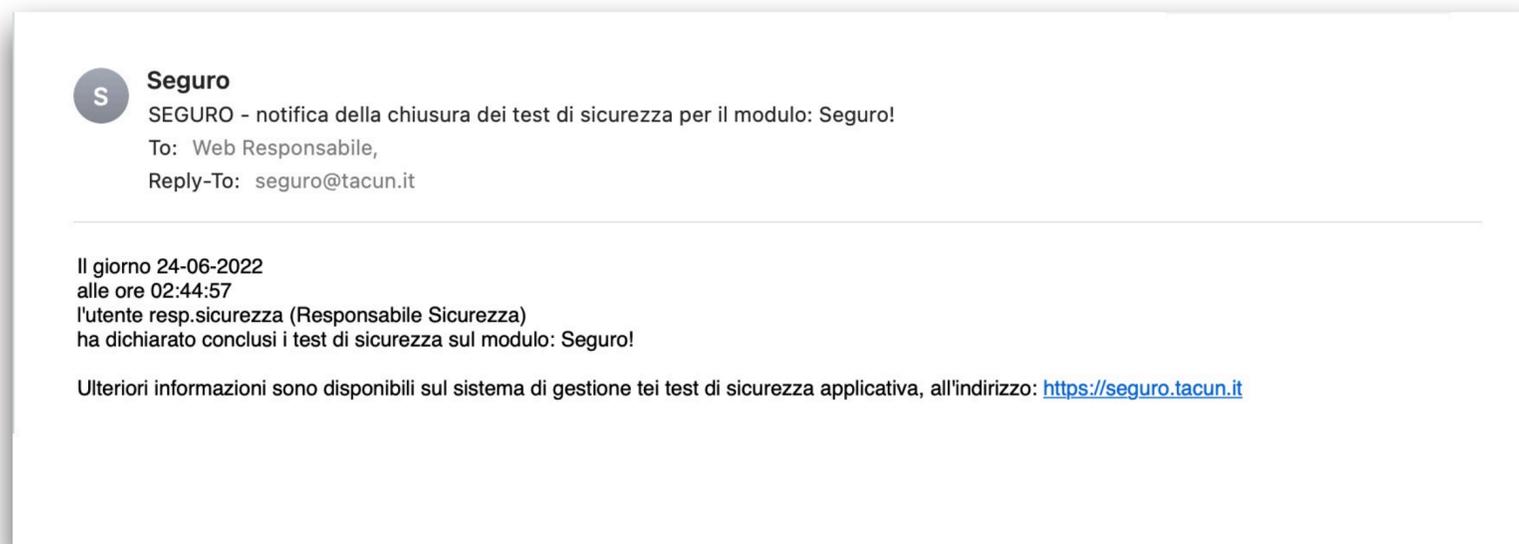
[INDIETRO](#)

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

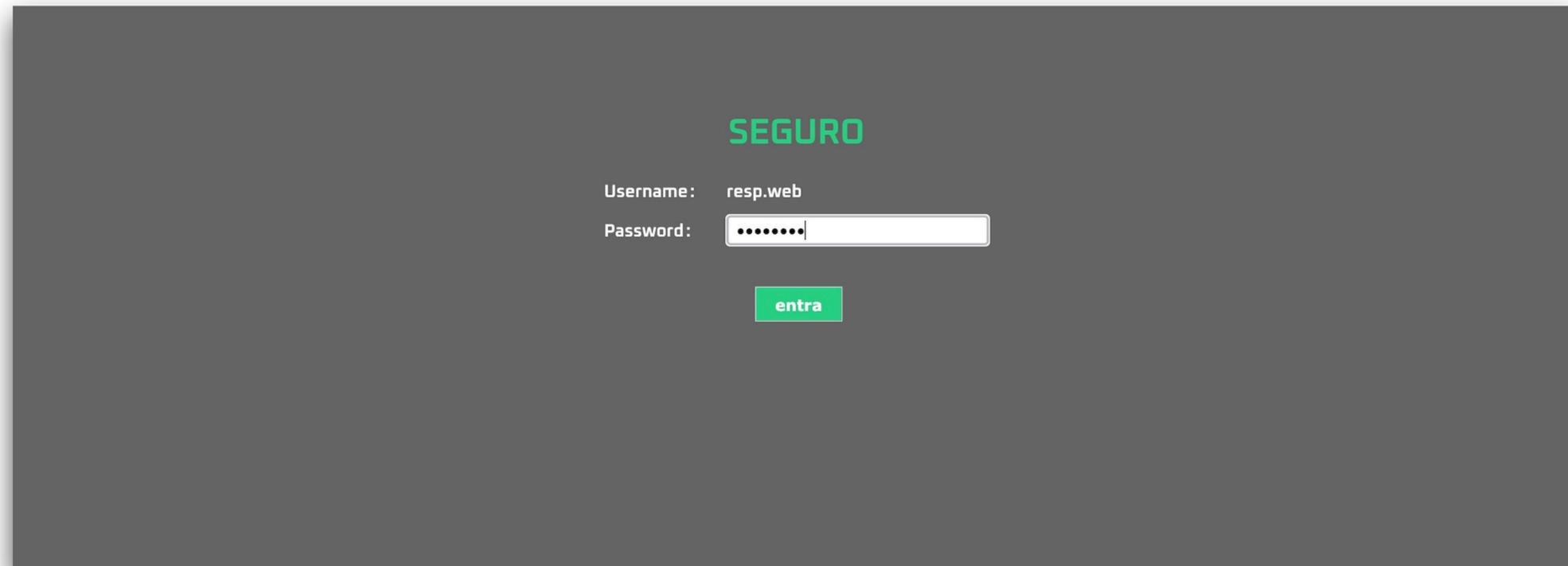
## Verifica esito test



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



A screenshot of a login interface on a dark grey background. At the top center, the word "SEGURO" is displayed in green. Below it, the text "Username: resp.web" is shown. Underneath, the text "Password:" is followed by a white input field containing seven black dots. At the bottom center, there is a green button with the white text "entra".

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

# Responsabile Web

## Home page

### HOME-PAGE UTENTE

#### RIEPILOGO ATTIVITÀ

	settimana	mese	anno	totali
collaudi effettuati	0	1	1	1
applicazioni verificate	0	1	1	1
URI esaminate	0	1	1	1
attacchi completati	0	1	1	1
attacchi corretti:	0	0	0	0

#### 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	<a href="#">dettagli</a>
Seguro!	sistema	notifica della pubblicazione dell'attacco: A-ZZ6ZZZZ	24-06-2022 12:39:31	<a href="#">dettagli</a>
Seguro!	sistema	notifica della chiusura dei test di sicurezza per il modulo: Seguro!	24-06-2022 12:44:57	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	24-06-2022 12:47:50	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	27-06-2022 13:45:44	<a href="#">dettagli</a>

n. record: 5

i messaggi con il fondo grigio scuro non sono stati letti

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



The screenshot displays a web interface titled "ELENCO MODULI". At the top, there is a search bar with four filters: "Referente: --", "Progetto: --", "Stato: --", and "Cerca:" followed by a search icon. Below the search bar, a note states "la ricerca per chiave avviene all'interno del nome del modulo". The main content is a table with the following columns: "codice", "nome", "versione", "progetto", "referente", "resp.sviluppo", and "stato". A single row is visible, with the cell containing the "dettagli" button highlighted in red. The table footer indicates "n. record: 1".

codice	nome	versione	progetto	referente	resp.sviluppo	stato	
M-TTQTTT6	Seguro!	3.2.20	Seguro	Referente Applicativo	Responsabile Sviluppo	sicurezza-ko	<a href="#">dettagli</a>

n. record: 1

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

The screenshot shows the 'Seguro' web application interface. At the top left, the logo 'Seguro' is displayed. A navigation bar contains 'resp.web' and a green 'cambia' button. A modal dialog box is open, displaying the text 'seguro.tacun.it says' and 'confermi invio in correzione del modulo?' with 'Cancel' and 'OK' buttons. Below the dialog, the heading 'DATI MODULO: SEGURO!' is shown in green. The main content area lists the following details:

- Codice: M-TTQTTT6
- Progetto: Seguro
- Nome: Seguro!
- Stato: sicurezza-ko
- Versione: 3.2.20
- Rilasciato: 21-06-2022
- Appguid: sicuro
- Referente: Referente Applicativo
- Resp.Sviluppo: Responsabile Sviluppo
- Resp.Sicurezza: Responsabile Sicurezza
- URI Test: https://seguro.dev.tacun.it
- URI Esercizio: https://seguro.tacun.it
- Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

At the bottom of the details section, there are navigation links: 'INDIETRO', 'nota', 'allegato', 'messaggi', 'eventi', and a highlighted orange 'in correzione' button. Below this is the heading 'ATTACCHI ASSOCIATI AL MODULO' in green. A table lists associated attacks:

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	no	dettagli

At the bottom right of the table, it says 'n. record: 1'. The browser address bar at the bottom left shows 'https://seguro.tacun.it/modulo/correzione/new/M-TTQTTT6'.

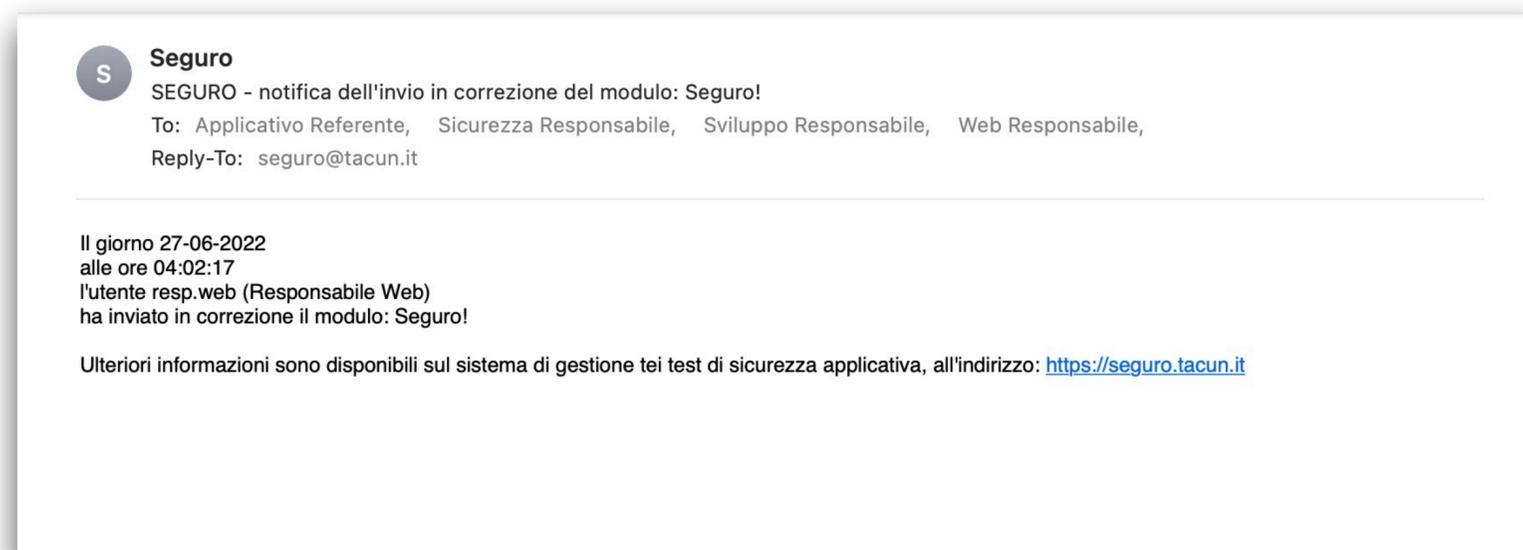
Il responsabile Web può vedere i dettagli di tutte le entità legate al modulo, ma non le può modificare.

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

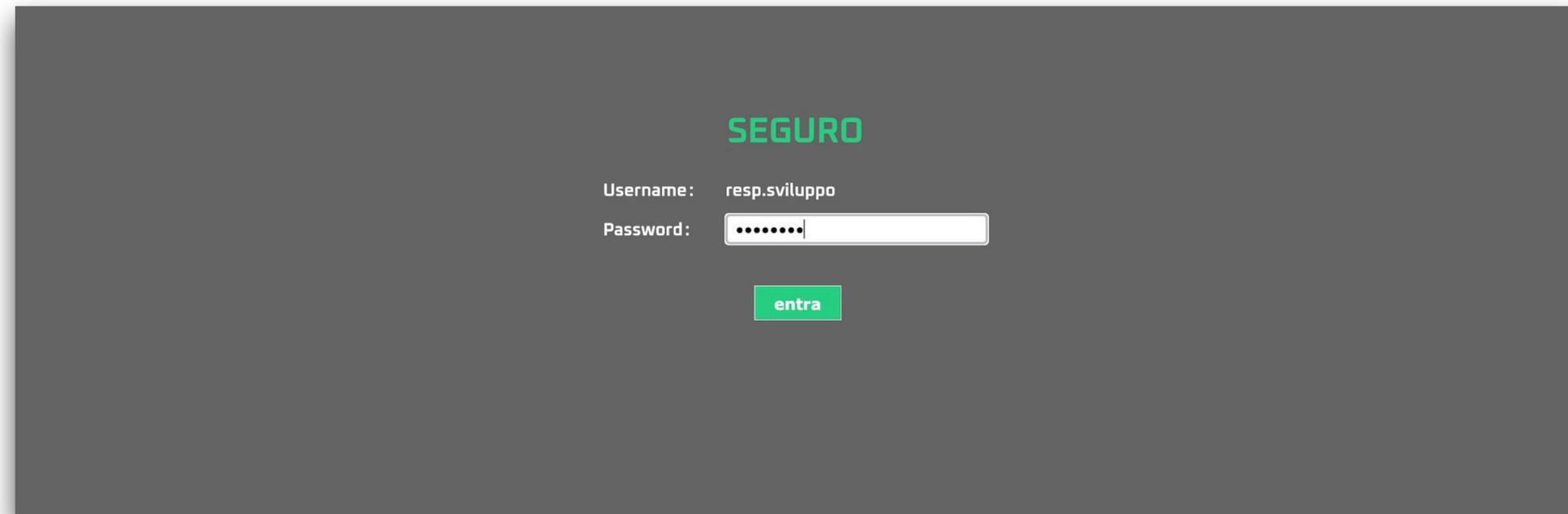


Quando un modulo è inviato in correzione, il sistema invia a tutti i responsabili un messaggio di notifica.

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

# Responsabile gruppo di Sviluppo

## Login



SEGURO

Username: resp.sviluppo

Password:

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	<a href="#">dettagli</a>
Seguro!	sistema	notifica della pubblicazione dell'attacco: A-ZZ6ZZZZ	24-06-2022 12:39:31	<a href="#">dettagli</a>
Seguro!	sistema	notifica dell'invio in correzione del modulo: Seguro!	27-06-2022 14:02:17	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	27-06-2022 14:39:08	<a href="#">dettagli</a>

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	<a href="#">dettagli</a>

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

### DATI MODULO: SEGURO!

Codice: M-TTQTTT6  
Progetto: Seguro  
Nome: Seguro!  
Stato: correzione  
Versione: 3.2.20  
Rilasciato: 21-06-2022  
Appguid: seguro  
Referente: Referente Applicativo  
Resp.Sviluppo: Responsabile Sviluppo  
Resp.Sicurezza: Responsabile Sicurezza  
URI Test: https://seguro.dev.tacun.it  
URI Esercizio: https://seguro.tacun.it  
Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

[INDIETRO](#)

[nota](#) [allegato](#) [messaggi](#) [eventi](#) [corretto](#)

### ATTACCHI ASSOCIATI AL MODULO

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	no	<a href="#">dettagli</a>

n. record: 1

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

**Seguro** gr.sviluppo **cambia** [home](#) [messaggi](#) [moduli](#) [URI](#) [tipi di attacco](#) [esci](#)

### MODIFICA ATTACCO

**Codice:** A-ZZ6ZZZZ  
**URI:** [https://seguro.tacun.it/entra?p\\_dest=](https://seguro.tacun.it/entra?p_dest=)  
**Profilo:** gruppo.sicurezza  
**Tipo:** Cross Site Scripting (XSS)  
**Parametro:** p\_dest  
**Esito:** riuscito  
**Livello:** alto  
**Effetto:** Una eccezione non gestita mostra dei dettagli sull'architettura di sistema:  
UIException Object  
(  
[error:protected] => accesso negato  
[title:protected] => errore utente  
[message:protected] => utente inesistente o password errata  
[string:Exception:private] =>  
[code:protected] => 0  
[file:protected] => /usr/local/src/seguro/www/utente.login.php  
[line:protected] => 78  
[trace:Exception:private] => Array  
(  
)

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	<a href="#">dettagli</a>
Seguro!	sistema	notifica della pubblicazione dell'attacco: A-ZZ6ZZZZ	24-06-2022 12:39:31	<a href="#">dettagli</a>
Seguro!	sistema	notifica dell'invio in correzione del modulo: Seguro!	27-06-2022 14:02:17	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	27-06-2022 14:39:08	<a href="#">dettagli</a>

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	<a href="#">dettagli</a>

n. record: 1

#### ELENCO URI ASSEGNATE

codice	URI	modulo	stato	
U-TT6TTTE	<a href="https://seguro.tacun.it/entra?p_dest=">https://seguro.tacun.it/entra?p_dest=</a>	Seguro!	correzione	<a href="#">dettagli</a>

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

```
[code:protected] => 0
[file:protected] => /usr/local/src/seguro/www/utente.login.php
[line:protected] => 78
[trace:Exception:private] => Array
(
)

[previous:Exception:private] =>
)
```

Corretto:  sì  no

Note:

La vulnerabilità era determinata dal parametro di configurazione `__DEBUG` che causa la visualizzazione delle informazioni relative alla sessione:

```
if(__DEBUG) {
    print_f($_SESSION);
    print_f($e);
    die;
}
```

Chiuso: 24-06-2022 11:54:27  
Confermato: 24-06-2022 12:39:31

[INDIETRO](#) [scarica PDF rapporto](#) [salva](#)

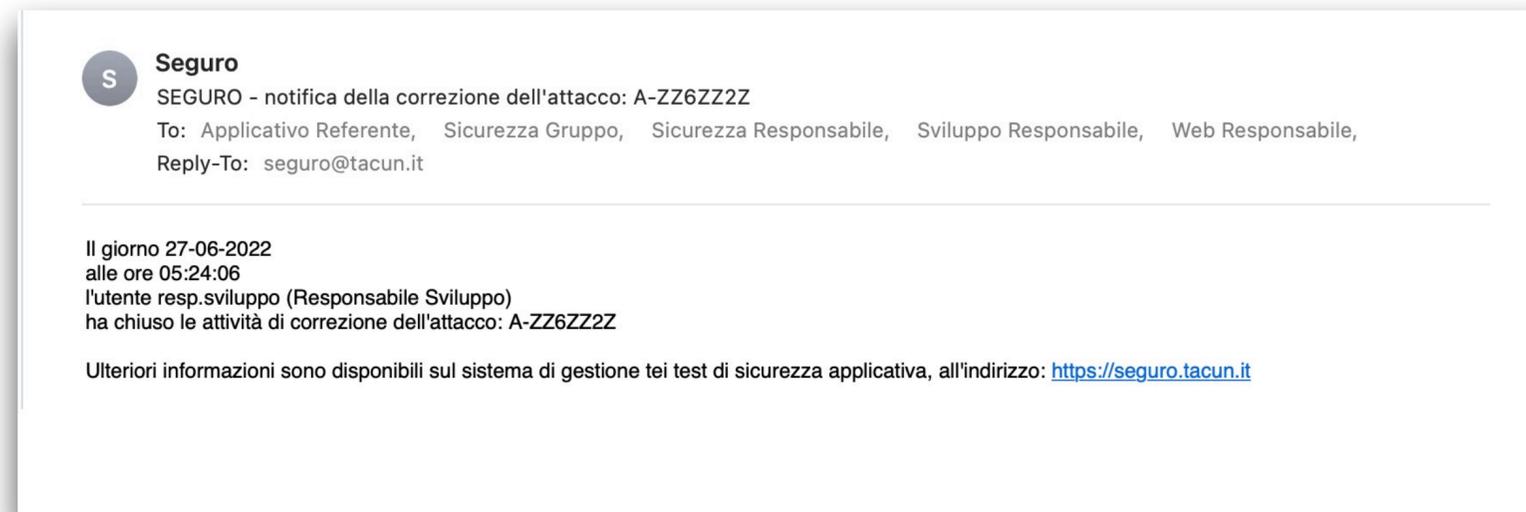
**ELENCO ALLEGATI**  
non ci sono allegati

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



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	<a href="#">dettagli</a>
Seguro!	sistema	notifica della pubblicazione dell'attacco: A-ZZ6ZZZZ	24-06-2022 12:39:31	<a href="#">dettagli</a>
Seguro!	sistema	notifica dell'invio in correzione del modulo: Seguro!	27-06-2022 14:02:17	<a href="#">dettagli</a>
sistema	sistema	notifica dell'assegnazione di un certificato digitale	27-06-2022 14:39:08	<a href="#">dettagli</a>
Seguro!	sistema	notifica della correzione dell'attacco: A-ZZ6ZZZZ	27-06-2022 15:24:06	<a href="#">dettagli</a>

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	<a href="#">dettagli</a>

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

The screenshot shows a web application interface. At the top left, the logo "Seguro" is visible. The user is logged in as "resp.sviluppo" with a "cambia" button next to it. A confirmation dialog box is open, asking "seguro.tacun.it says confermi completamento delle attività di correzione del modulo?" with "Cancel" and "OK" buttons. Below the dialog, the page title "DATI MODULO: SEGURO!" is partially visible. The main content area displays the following details:

- Codice: M-TTQTTT6
- Progetto: Seguro
- Nome: Seguro!
- Stato: correzione
- Versione: 3.2.20
- Rilasciato: 21-06-2022
- Appguid: seguro
- Referente: Referente Applicativo
- Resp.Sviluppo: Responsabile Sviluppo
- Resp.Sicurezza: Responsabile Sicurezza
- URI Test: https://seguro.dev.tacun.it
- URI Esercizio: https://seguro.tacun.it
- Descrizione: Applicazione Web per la gestione dei test di sicurezza applicativa

At the bottom of the details, there are navigation links: "INDIETRO", "nota", "allegato", "messaggi", "eventi", and a highlighted "corretto" button.

Below the details, the section "ATTACCHI ASSOCIATI AL MODULO" contains a table:

codice	URI	profilo	tipo	parametro	aperto	esito	corretto	
A-ZZ6ZZZZ	U-TT6TTTE	gruppo.sicurezza	Cross Site Scripting (XSS)	p_dest	24-06-2022	riuscito	sì	dettagli

The footer shows the URL "https://seguro.tacun.it/modulo/correzione/end/M-TTQTTT6" and "n. record: 1".

L'utente accede alla maschera di modifica dati modulo.

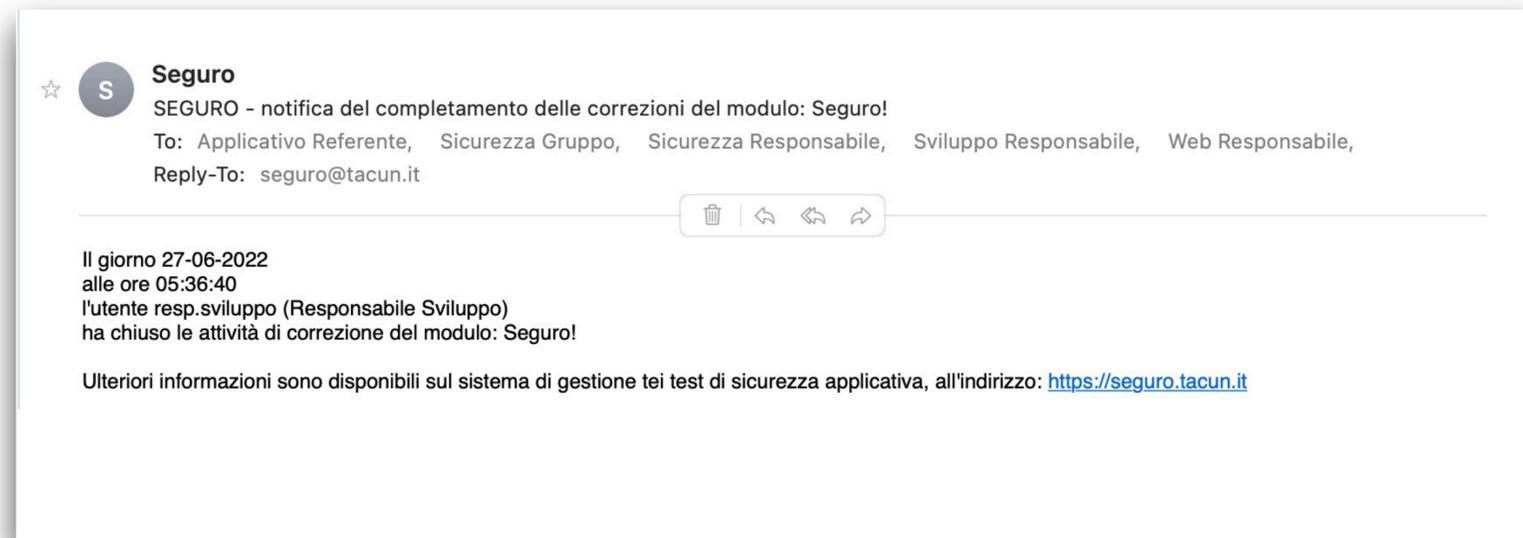
Tutte le URL e tutti gli attacchi hanno sfondo verde perché corretti.

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



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>

