VAATIXFODA

Vulnerability Assessment Applicativi FOnte Dati

Manuale Utente

	Funzione	Nome	firma
Emissione	Analista Programmatore	Gaetano Palumbo (TIX)	
Emissione	Specialista Tecnico	Matteo Andolfi (OSCAT)	
Emissione	Specialista Tecnico	Andrea Carpineti (OSCAT)	
Revisione	Capo Progetto Tecnico	Vincenzo Martiello (RT)	
Verifica	Specialista Tecnico		
Approvazione	Responsabile	Marco Vignoli	
Approvazione	Responsabile	Angelo Marcotulli	

LISTA DI DISTRIBUZIONE : po-progetti-ict@liste.regione.toscana.it ; responsabili tecnici di progetti ICT

AGGIORNAMENTI			
Versione	Data	Paragrafi Modificati	Motivo Modifica
1.0.0	13.11.2018		Prima stesura
1.0.1	16.11.2018		Revisione
1.0.3	08.02.2019		Aggiunta ulteriori filtraggi
1.0.4	12.03.2019		Distribuzione su po-progetti-ict
1.0.5	10.07.2019	4	Inserimento funzione per completare dati mancanti da parte del capoprogetto

Indice

1. INTRODUZIONE

Questo manuale rappresenta una guida delle funzionalità disponibili nell'ambito dell'applicazione vaatixfoda (il nome dell'applicativo e' una abbreviazione di **Vulnerability Assessment Applicativo Fonte Dati**).

L'applicazione **VaaTixFoda** è un repository descrittivo delle applicazioni, servizi web, dispiegati al Tix, dove è possibile monitorare per ognuno di esso i risultati dell'attività di cybersecurity: vulnerability assessment, e continuous integration.

VaaTixFoda è quindi la fonte dati per i processi TIX di Vulnerability Assessment di applicazioni web.

Tale applicazione è utilzzabile attraverso i piu' comuni browser: si consiglia l'uso del browser **Mozilla Firefox**, nelle sue ultime versioni stabili**.**

NOTA: Le immagini sono opportunamente modificate allo scopo di oscurare le informazioni relative alla raggiungibilità dei servizi. Gli utilizzatori della dashboard vedranno le URL complete.

2. ACRONIMI

ARPA	Accessi Ruoli Profili Applicazioni
CI	Continuous Integration
RT	Regione Toscana
VAA	Vulnerability Assessment Applicativi
VAI	Vulnerability Assessment Applicativi
TIX	Tuscany Internet eXchange

3. APPLICAZIONE VAATIXFODA

L'applicazione è raggiungibile tramite la url : https://resource.servizi.tix.it/vaatixfoda

L'uso di tale applicazione è riservato ai capi progetto responsabili delle singole applicazioni che oggetto di scansione si sicurezza applicativa.
Non è previsto l'accesso per fornitori.
Eventuali informazioni sono già presenti nei report VAA e CI inviati e possono essere utilizzati dai capi progetto per allineare i fornitori di riferimento.

Si ricorda che

- le scansioni CI sono eseguiti sul codice statico depositato sulla piattaforma OSCAT (riferimento oscat.rete.toscana.it per manualistica e riferimenti telefonici e telematici di supporto alla piattaforma)

- le scansioni VAA sono eseguite sul codice in esecuzione, **esclusivamente in ambiente di certificazione**

L'accesso all'applicativo è permesso esclusivamente con smartcard il cui certificato contenuto identifica l'utente capoprogetto o il Dirigente, attraverso le funzionalità di ARPA, come dipendente di Regione Toscana – Giunta Regionale. Nel dettaglio le specifiche sono le seguenti:

i **ruoli a**utorizzati ad accedere a tale servizio sono : •
Dipendente Giunta della Regione Toscana,
• Afferente Tix.

I **profili** associati ai ruoli sopra elencati sono :

- Responsabile di settore Regione Toscana, • Dipendente giunta della Regione Toscana,
- Operatore Tix.

3.1. Descrizione delle funzionalità riservate al Dirigente Responsabile di Settore, Dipendente Giunta Regione Toscana.

I profili applicativi Responsabile di settore Regione Toscana, e Dipendente giunta della Regione Toscana, possono svolgere le stesse funzioni applicative.
La differenziazione di tali ruoli avviene solo nella visualizzazione dei risultati delle funzioni associate ai profili.

Il profilo di Responsabile di settore di Regione Toscana, può visualizza il contenuto di tutto il personale di cui è Responsabile.

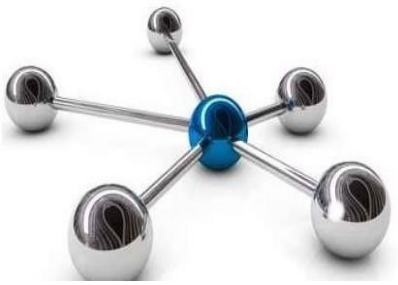
Il profilo Dipendente giunta della Regione può visualizzare il contenuto di cui è referente.

Di seguito è pubblicato il dettaglio delle funzioni.

3.2. Home Page

La home page è la pagina che si presenta subito dopo aver eseguito l'accesso tramite Arpa oppure Spid.

Tale pagina web è uguale per i due profili sopra elencati, si differenzia solo la dicitura associata al ruolo.



Se l'utente si è connesso al sistema ha il ruolo di **Dipendente Giunta della Regione Toscana** la dicitura associato al ruolo è :

Se la persona connessa al sistema ha il ruolo di Responsabile di settore di Regione Toscana la dicitura è

Entrambi i profili visualizzano nella Home Page il menù di navigazione:

3.3. Lista Applicazioni

Il concetto principale su cui si basa questa applicazione è quello di **WEB APPLICATION**, in quanto i test di scansione di sicurezza VAA oppure di CI si basano sulla singola web application; quindi la funzione lista applicazioni è importante perché permette di visualizzare l'elenco dei propri applicativi dispiegati su infrastrutture Tix.

Il profilo di **Dipendente giunta della Regione Toscana**, visualizza tutte le applicazioni, servizi (Front-end) dispiegati al Tix, di cui è referente. (vedi fig. 1)

(fig. 1) Preview della lista applicativa di un referente di RT di cui è stato volontariamente eliminata la colonna referente ente.

Il profilo di **Responsabile di Settore**, visualizza tutte le applicazioni , servizi (Front-end) dispiegati al Tix, assegnati al personale sottoposto.(fig.1.A)

(fig.1.A) Preview della lista applicativa di un Responsabile di settore di RT di cui è stato volontariamente eliminata la colonna referente ente.

Da ora sia le funzioni che i dati saranno uguali per i due profili.

I campi della preview

- VAA Effettuato
- CI effettuato

Indicano per ogni applicazione i test eseguiti di sicurezza (VAA), o continuous integration (CI) (Fig.2).

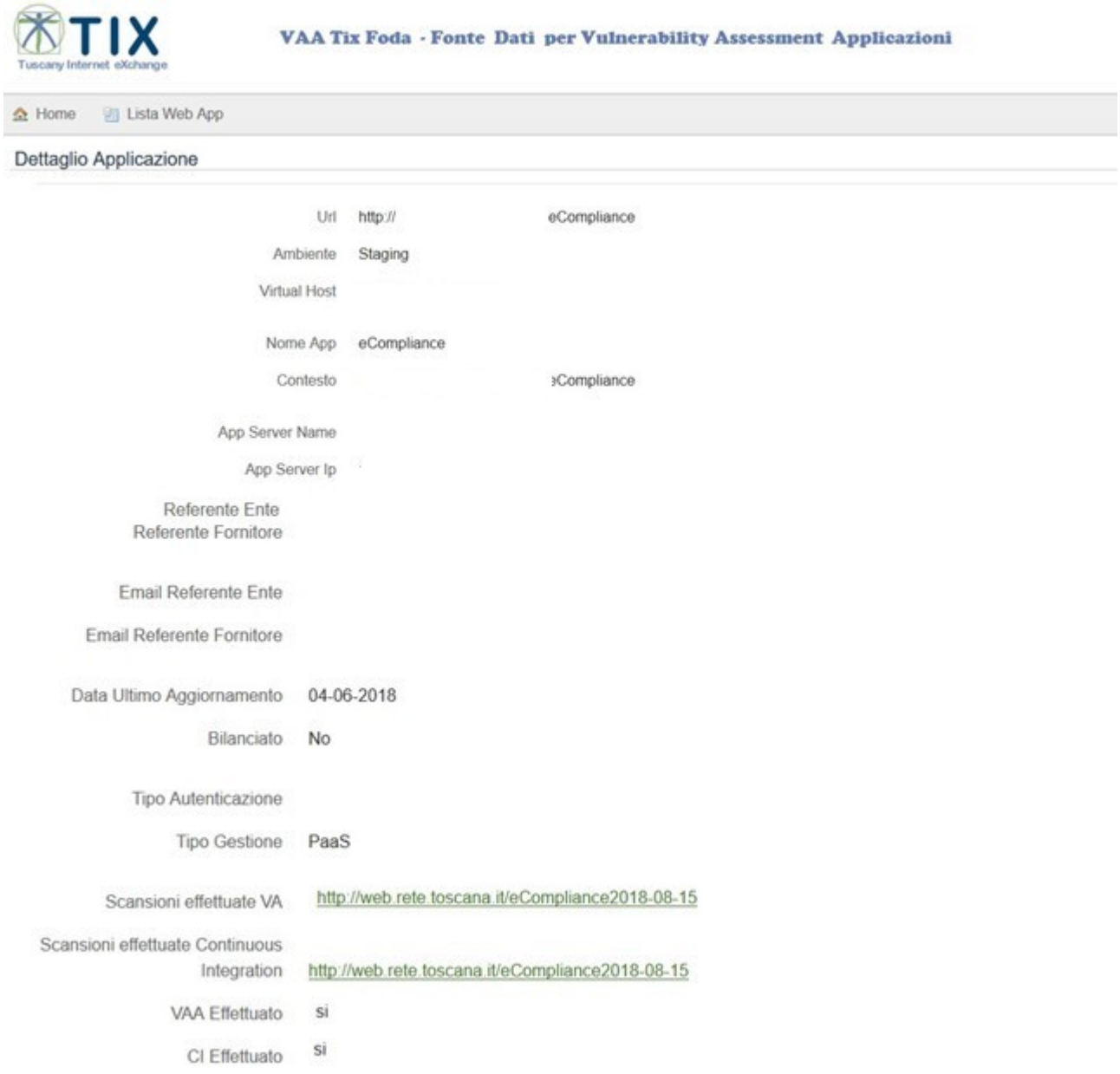
VAA Effettuato	CI Effettuato
✓	✗
✗	✗
✓	✗
✗	✗
✗	✗
✗	✗
✓	✗
✗	✗

(fig.2)

Come si evince dalla (fig 1), oppure (fig.1.a) la colonna **Nome App** è di colore verde e **linkabile.**

Nome App	Tipo Autenticazione	Contesto	Referente Ente	VAA Effettuato	CI Effettuato
ITT_user_attribute*		http://wsitest.e.toscana.it/ITT_user_attribute*		✓	✗

Questo significa che cliccando sul nome della singola applicazione si aprirà la pagina di dettaglio della singola applicazione dove sono definiti tutti i dati che la rappresentano (vedi fig.3) .



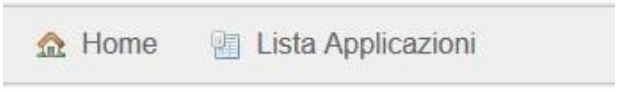
(fig.3) Elenco dati relativi alla singola applicazione web.

3.4. I dati :

Rappresentano l'elenco storico dei test eseguiti sulla singola applicazione con la data di esecuzione, e sono linkabili.

Cliccando sul link si apre la pagina di Dettaglio del singolo test dove vi sono i dati che sono il risultato del test (VAA e CI), che vedremo di seguito.

Nella barra del menu in alto alla pagina vi sono i tasti :



- Home permette di ritornare alla Pagina iniziale
- Lista Applicazioni permette di ritornare alla pagina della lista applicazioni.

3.5. Lista VAA

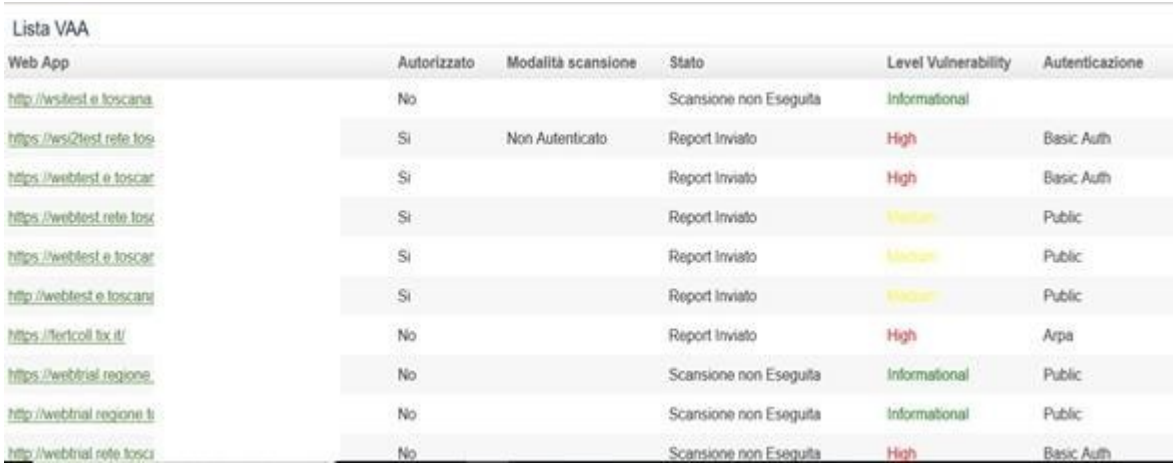
Nella Home Page un'altra funzione importate è la Lista VAA, questa funzione restituisce una lista di risultati dei test di sicurezza Vulnerability Assessment Applicativi, delle applicazioni a cui sono stati eseguiti.

Quindi ricordando che :

- il profilo di **Dipendente giunta della Regione Toscana**, visualizza i risultati dei test di sicurezza vulnerability assessment, eseguiti, relativi alle applicazioni per cui è referente .

- il profilo di **Responsabile di Settore**, visualizza i risultati dei test di sicurezza vulenrability assessment, eseguiti, per le applicazioni assegnate al personale sottoposto.

La funzione Lista VAA permette di visualizzare la preview dei test di vulenrability assessment eseguiti. (fig.4)



Lista VAA

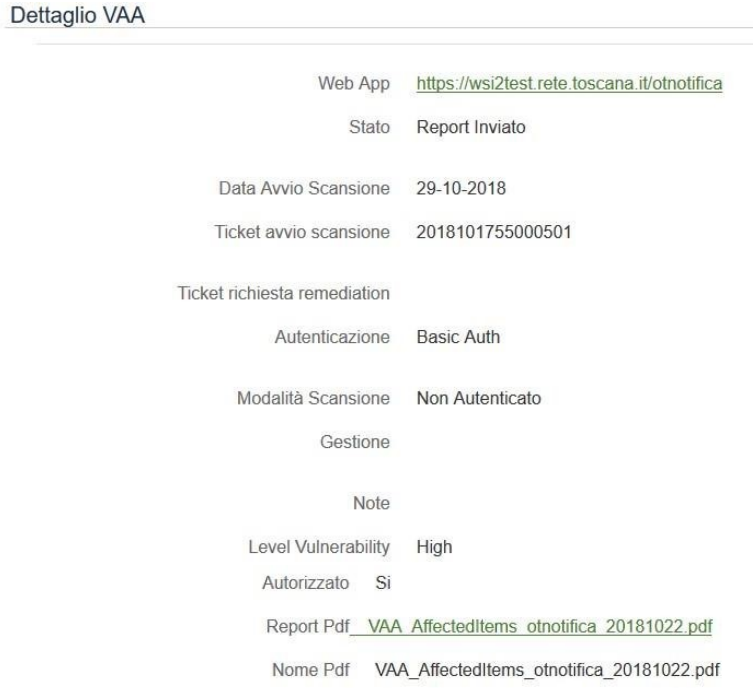
Web App	Autorizzato	Modalità scansione	Stato	Level Vulnerability	Autenticazione
http://wsitest.e.toscana	No		Scansione non Eseguita	Informational	
https://wsi2test.rete.tos	Si	Non Autenticato	Report Inviato	High	Basic Auth
https://webtest.e.toscar	Si		Report Inviato	High	Basic Auth
https://webtest.rete.tosc	Si		Report Inviato		Public
https://webtest.e.toscar	Si		Report Inviato		Public
http://webtest.e.toscan	Si		Report Inviato		Public
https://fertcoll.fix.it/	No		Report Inviato	High	Arpa
https://webtrial.regione	No		Scansione non Eseguita	Informational	Public
http://webtrial.regione.t	No		Scansione non Eseguita	Informational	Public
http://webtrial.rete.tosc	No		Scansione non Eseguita	High	Basic Auth

(fig.4) lista dei VAA eseguiti con il relativo livello di vulnerabilità colorato in base al grado di vulnerabilità (i colori utilizzati sono della medesima gradazione di quelli contenuti nei report Executive Summary, Vulnerability Details, Remediation Plan, che vi vengono inviati).

La preview Lista VAA indica la singola applicazione oggetto di test VA con la URL di colore verde e linkabile.

https://wsi2test.rete.toscana.it/otnotifica	Si	Non Autenticato	Report Inviato	High	Basic Auth

Cliccando sul link si apre la pagina di dettaglio del test di VA dove vi sono tutti i risultati relativi al test. (fig.5)



Dettaglio VAA

Web App	https://wsi2test.rete.toscana.it/otnotifica
Stato	Report Inviato
Data Avvio Scansione	29-10-2018
Ticket avvio scansione	2018101755000501
Ticket richiesta remediation	
Autenticazione	Basic Auth
Modalità Scansione	Non Autenticato
Gestione	
Note	
Level Vulnerability	High
Autorizzato	Si
Report Pdf	VAA_AffectedItems_otnotifica_20181022.pdf
Nome Pdf	VAA_AffectedItems_otnotifica_20181022.pdf

(fig.5) elenco dati VAA

Come si vede in figura l'oggetto principale è sempre la web app ed è linkabile (conduce alla proprietà dell'applicazione) , i dati riportati sotto sono il risultato del test eseguito sulla web app.

Funzione molto comoda è quella del download o visualizzazione del report completo al seguente link della pagina Dettaglio VAA:

La barra del menu al top della pagina ha i tasti

- Home ritorna alla home page
- Lista VAA ritorna alla lista dei VA eseguiti.

3.6. Lista CI

Ultima funzione presente nella home page è la lista Continuous Integration.

La funzione **Lista CI** permette :

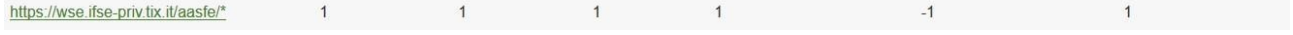
- Per il profilo di **Dipendente giunta della Regione Toscana**, di visualizzare i risultati dei test di sicurezza continuous integration, eseguiti relativi alle applicazioni per cui è referente.

- Per il profilo di **Responsabile di Settore**, di visualizzare i risultati dei test di sicurezza continuous integration eseguiti, per le applicazioni assegnate al personale sottoposto.

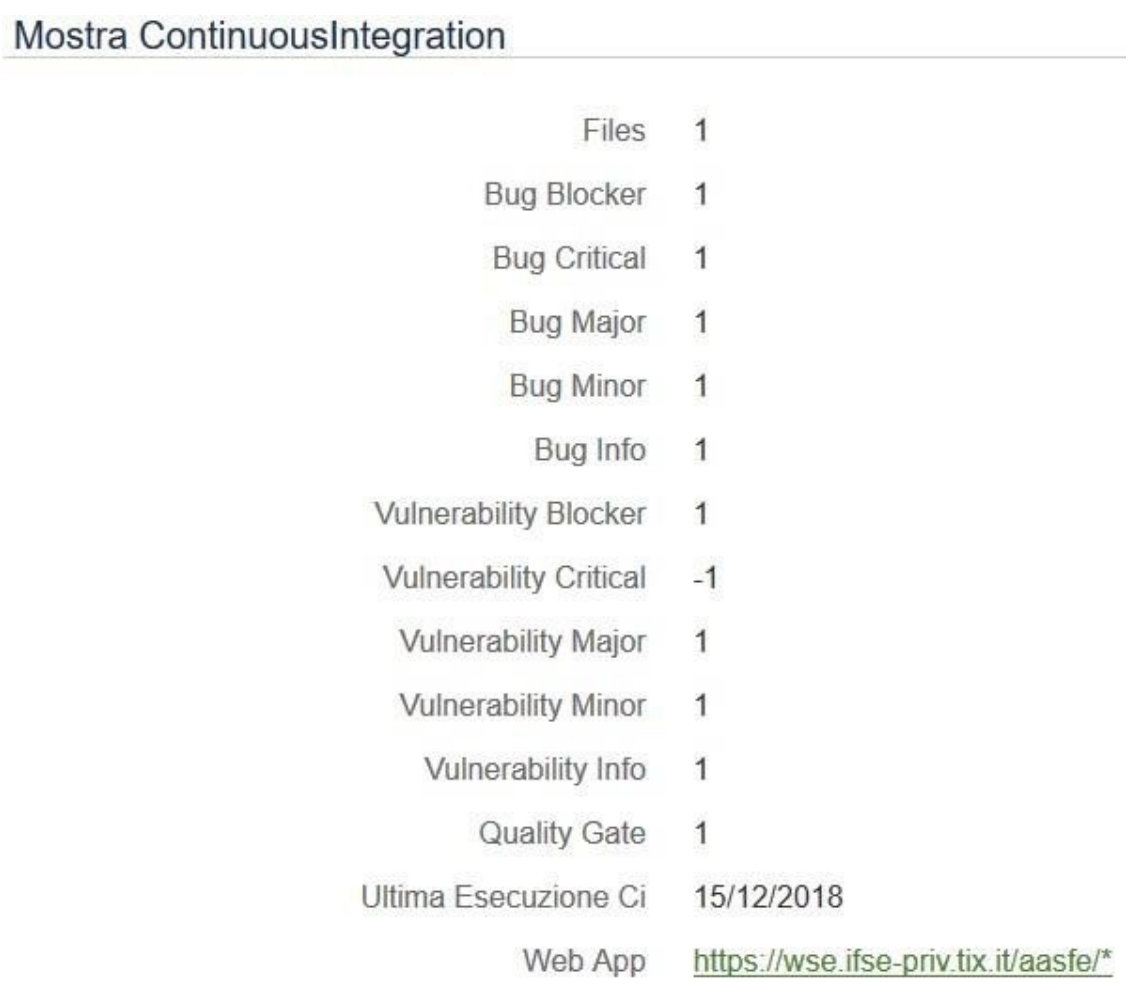
La funzione Lista CI permette di visualizzare la preview dei test di continuous integration eseguiti.
(fig.6) Preview risultati test

.(fig.6) Preview risultati test continuous integration

La preview Lista CI indica la singola applicazione oggetto di test CI con la URL di colore verde e linkabile.



Cliccando sul link si apre la pagina di dettaglio del test di CI dove vi sono tutti i risultati relativi al test. (fig.6)



Come si vede in figura l'oggetto principale è sempre la web app ed è linkabile (conduce alla proprietà dell'applicazione), i dati riportati sopra sono il risultato del test eseguito sulla web app. La barra del menu al top della pagina ha i tasti

- Home ritorna alla home page
- Lista VAA ritorna alla lista dei VA eseguiti.

4. INSERIMENTO DATI MANCANTI VAATIXFODA

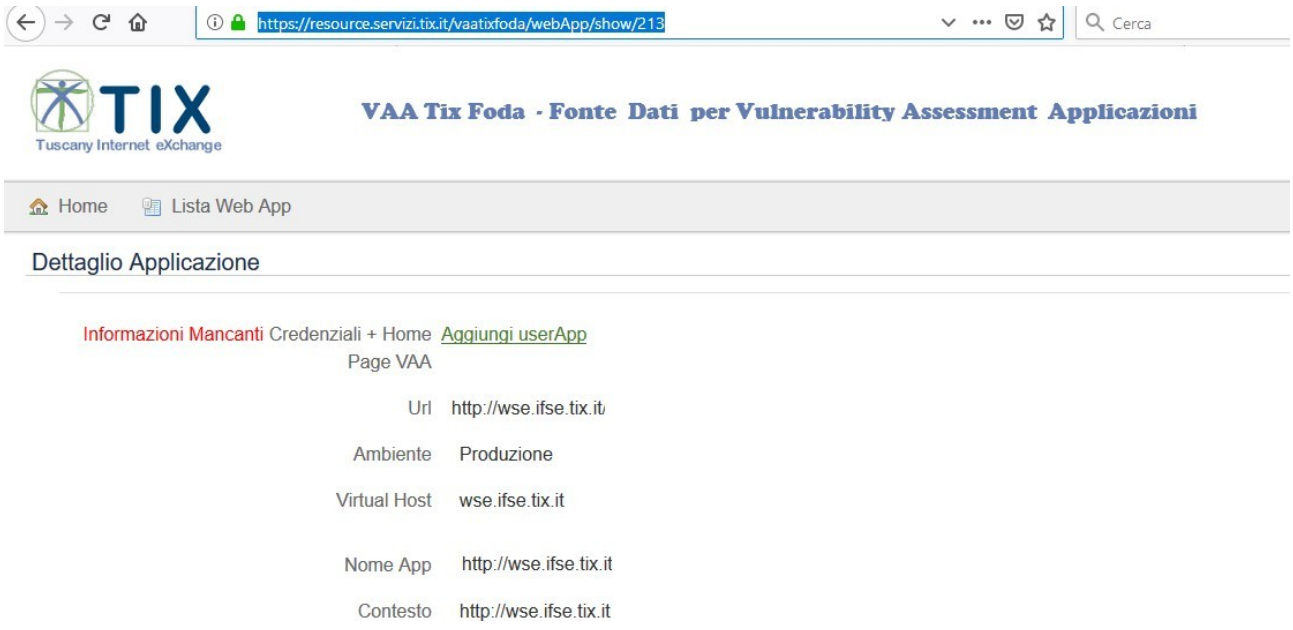
Questo capitolo serve a descrivere i processi relativi all'inserimento dei dati all'interno dell'applicazione VaaTixFoda che risultano necessari all'attività di sicurezza Vulnerability Assesstment.

4.1. Inserimento dati tramite link

Il primo metodo per inserire i dati mancanti all'interno dell'applicazione VaaTixFoda è tramite tramite LINK.

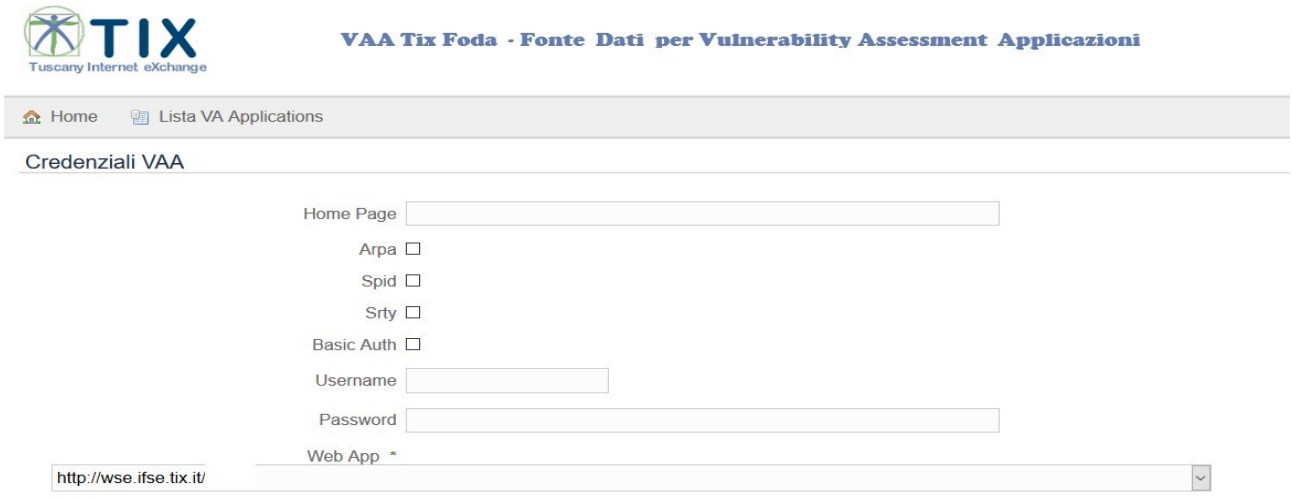
Ad i referenti applicativi della Regione Toscana, verrà comunicato tramite email un link (come foto che segue), di collegamento alla scheda applicativa di cui sono referenti, che contiene tutti i dati relativi all'applicazione. Esempio https://resource.servizi.tix.it/vaatixfoda/webApp/show/213

Nell'email di comunicazione da parte del Tix sarà presente il seguente link, che collegherà tramite arpa l'accesso alla scheda applicativa :

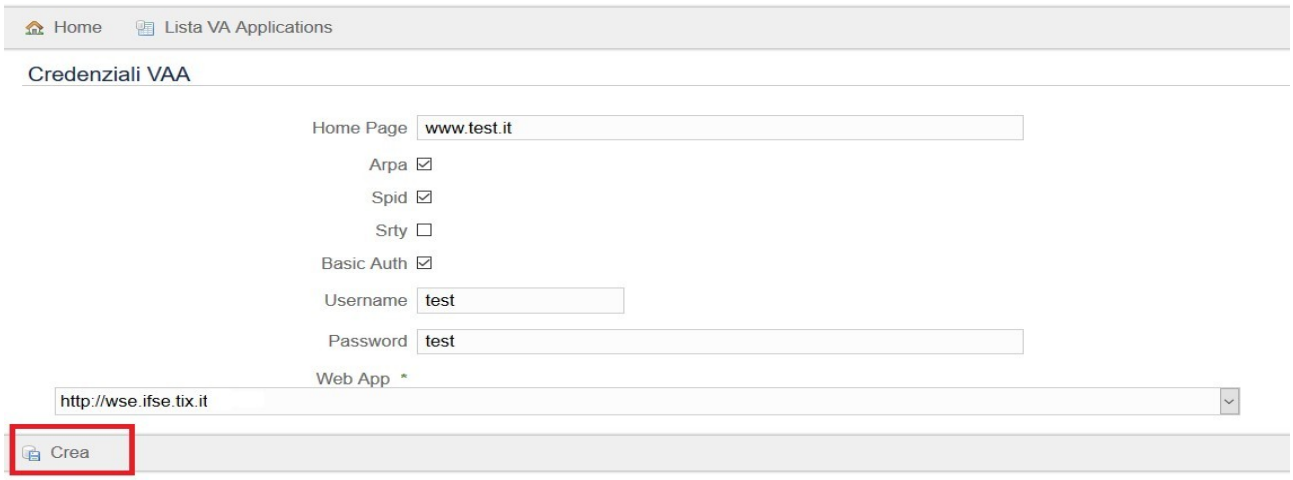


Come si vede dall'immagine vi sono Informazioni mancanti quindi cliccando sul tasto verde (link) Aggiungi userApp si possono aggiungere:

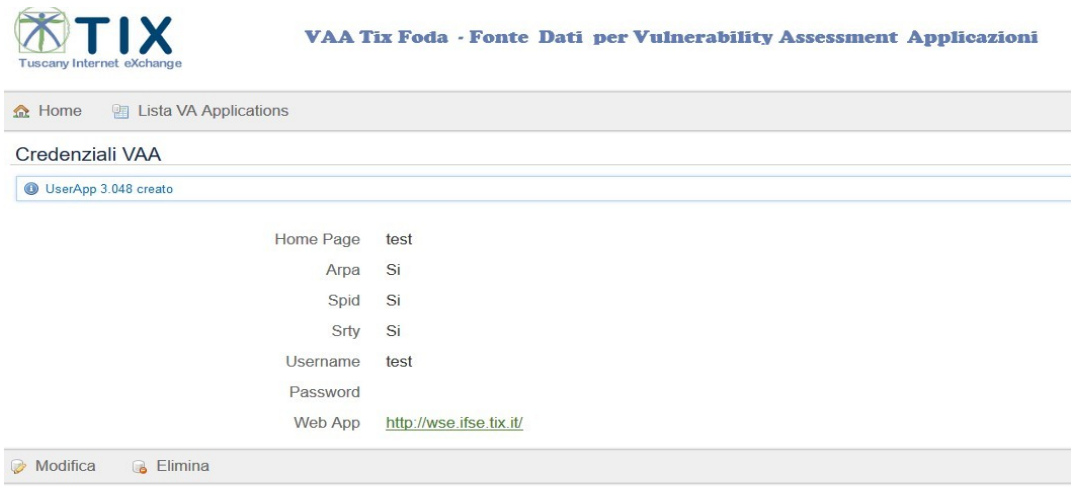
Cliccando su Aggiungi UserApp si ha l'opportunità di aggiungere le seguenti informazioni :



In basso vi è l'applicazione oggetto di informazioni mancanti, sopra vi sono le informazioni da aggiungere.



Valorizzate le informazione mancanti cliccare sul pulsante CREA.



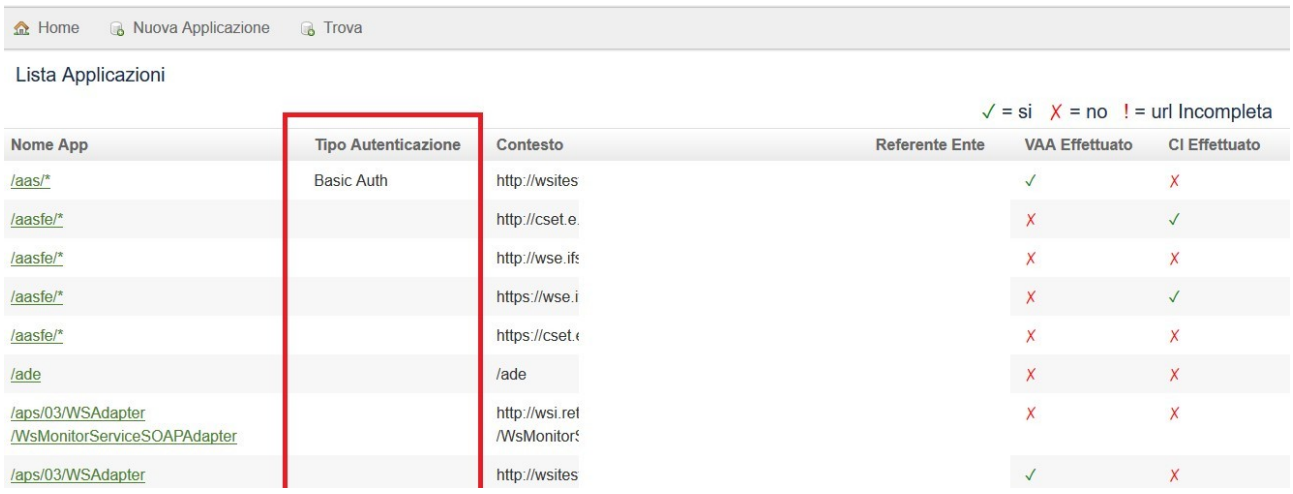
Come si vede dall'immagine la password è assente perché visibile solo all'operatore che prenderà in gestione tale attività.

4.2. Inserimento dati da Lista Applicazioni

Un altro metodo per inserire i dati necessari per l'attività di sicurezza, è quello dalla funzione lista applicazioni, descritto come segue.

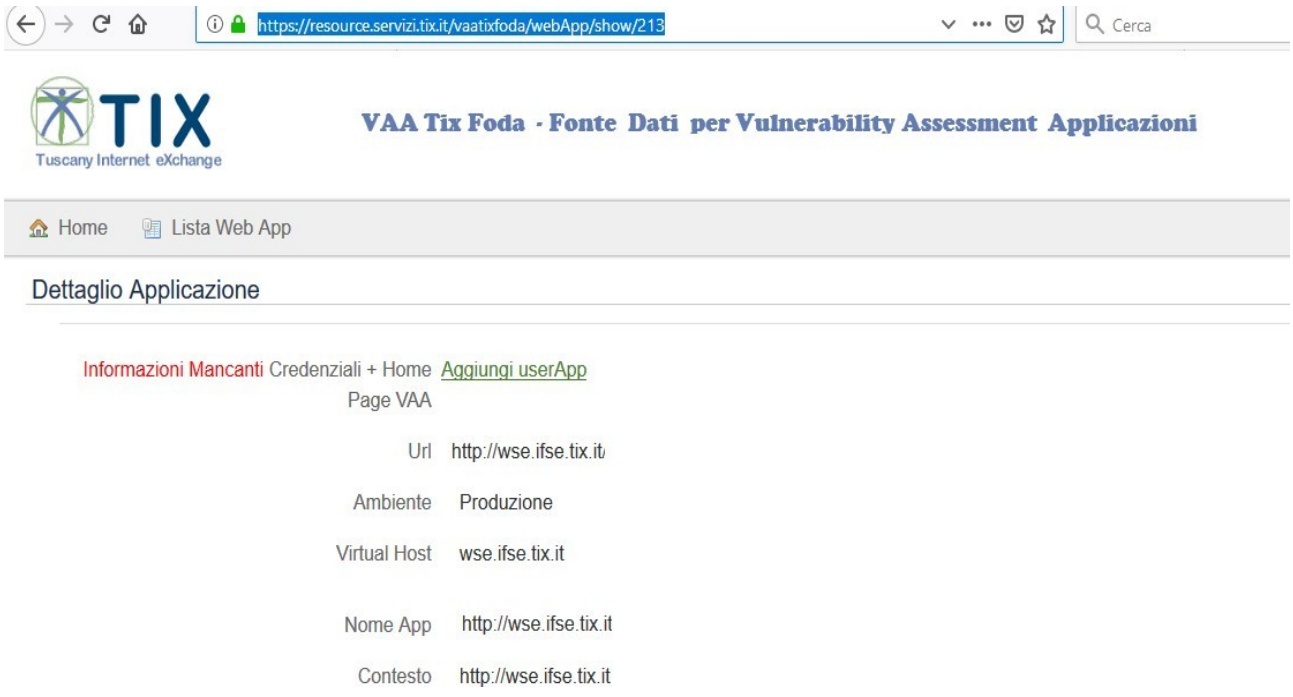
Accedere all'applicazione VaaTixFoda, cliccare su Lista Applicazioni :

In questo modo per i referenti di Regione Toscana, si accede alla lista applicazioni di cui si è responsabili.



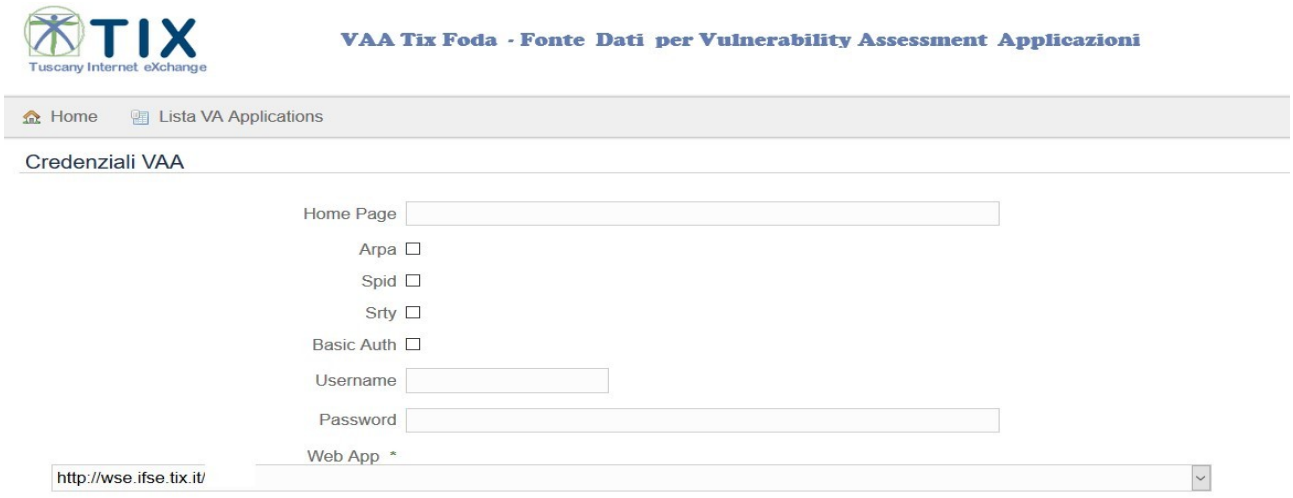
Nell'immagine sopra è raffigurata la lista di applicazioni di cui si è responsabili.

Per tutte le applicazioni che non hanno valorizzato il campo Tipo Autenticazione, se si clicca sul link (a sinistra in verde) si visualizza la scheda applicativa come segue :

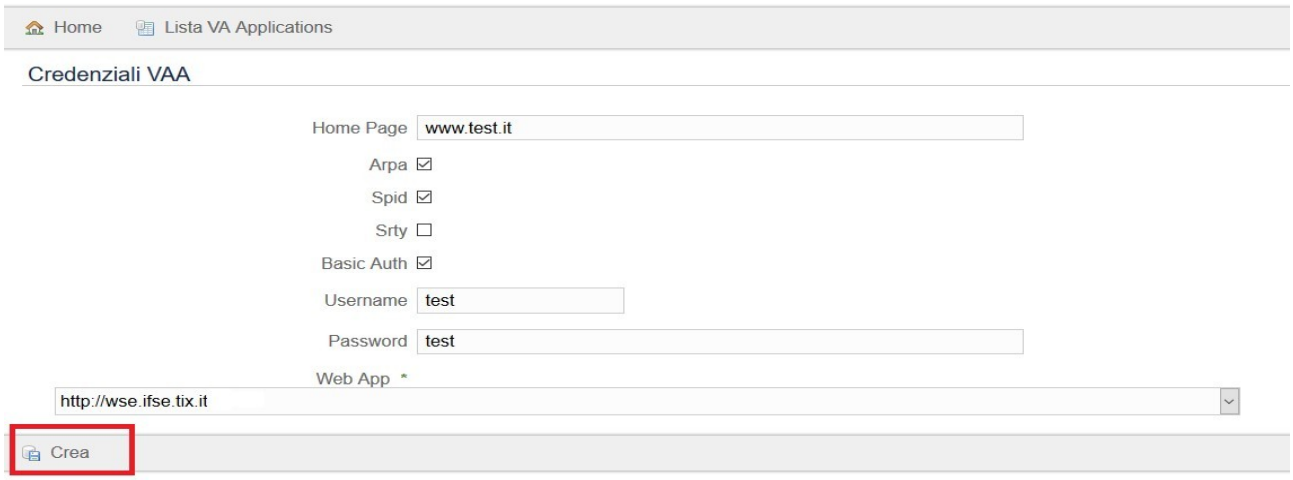


Come si vede dall'immagine vi sono Informazioni mancanti quindi cliccando sul tasto verde (link) Aggiungi userApp si possono aggiungere:

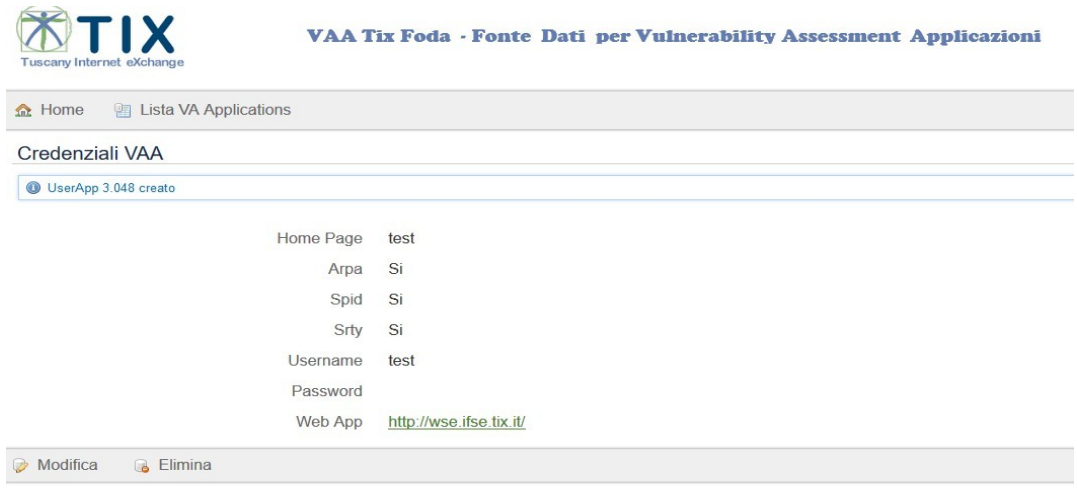
Cliccando su Aggiungi UserApp si ha l'opportunità di aggiungere le seguenti informazioni :



In basso vi è l'applicazione oggetto di informazioni mancanti, sopra vi sono le informazioni da aggiungere.



Valorizzate le informazioni mancanti cliccare sul pulsante CREA.



Come si vede dall'immagine dopo il salvataggio, la password è assente perché visibile solo all'operatore che prenderà in gestione tale attività.