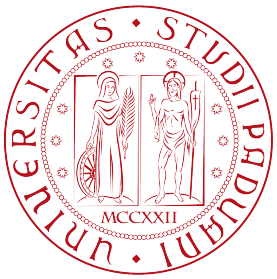
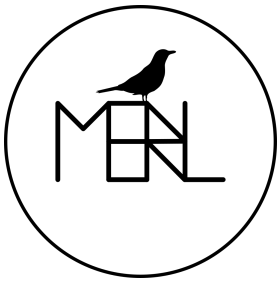


Università degli Studi di Padova
Laurea: Informatica
Corso: Ingegneria del Software
Anno Accademico: 2021/2022



Gruppo: MERL
Email: merlunipd@gmail.com

Manuale Utente

Informazioni sul documento

Versione	V2.0.0
Uso	Esterno
Data approvazione	08/06/2022
Distribuzione	Prof. *Vardanega Tullio* Prof. *Cardin Riccardo* *Zucchetti S.p.A.* Gruppo *MERL*

Registro delle Modifiche

Versione	Data	Autore	Verificatore	Modifica
v2.0.0	08/06/2022	Marco Mamprin	-	Approvazione
v1.0.2	27/05/2022	Mattia Zanellato	Riccardo Contin	Aggiornati capitoli ”Istruzioni all’uso” e ”Tutorial”
v1.0.1	23/05/2022	Marco Mazzucato	Lorenzo Onelia	Aggiunto capitolo ”Tutorial”
v1.0.0	29/04/2022	Mattia Zanellato	-	Approvazione
v0.0.2	28/04/2022	Marco Mazzucato	Emanuele Pase	Aggiunti capitoli ”Introduzione”, ”Requisiti minimi di sistema” e ”Installazione”
v0.0.1	28/04/2022	Lorenzo Onelia	Marco Mazzucato	Aggiunto capitolo ”Istruzioni all’uso”
v0.0.0	27/04/2022	Marco Mazzucato	Emanuele Pase	Creata prima struttura del documento

Indice

1 Introduzione **7**
- 1.1 Scopo del documento . . . 7
- 1.2 Scopo del Prodotto . . . 7
- 1.3 Glossario . . . 7

2 Requisiti Minimi di Sistema **8**
- 2.1 Requisiti Minimi . . . 8
- 2.2 Requisiti Consigliati . . . 8
- 2.3 Requisiti Hardware . . . 8
- 2.4 Browser . . . 8

3 Installazione **10**
- 3.1 Clonare il repository . . . 10
- 3.2 Avviare il server . . . 10
- 3.3 Avviare la web app . . . 11

4 Istruzioni all'uso **12**
- 4.1 Home . . . 12
  - 4.1.1 Carica dataset . . . 12
  - 4.1.2 Carica sessione . . . 14
- 4.2 Bottoni . . . 15
  - 4.2.1 Bottone Home . . . 15
  - 4.2.2 Nuovo Campionamento . . . 15
  - 4.2.3 Salva Sessione . . . 15
- 4.3 Filtri . . . 15
  - 4.3.1 Utente . . . 16
  - 4.3.2 Ip . . . 16
  - 4.3.3 Evento . . . 16
  - 4.3.4 Applicazione . . . 16
  - 4.3.5 Data . . . 16
- 4.4 Scatter Plot . . . 17
- 4.5 Parallel Coordinates . . . 17
- 4.6 Sankey Diagram . . . 18
- 4.7 Force-Directed Graph . . . 19

5 Tutorial **20**
5.1 Scatter Plot 1 20
5.2 Scatter Plot 2 21
5.3 Parallel Coordinates 22
5.4 Sankey Diagram 23
5.5 Force-Directed Graph 24

Elenco delle figure

3.1 Avvio dell'applicazione 11

4.1 Screenshot della Home 12
4.2 Screenshot della finestra di dialogo per il caricamento del dataset . . 13
4.3 Screenshot della lista dei grafici 13
4.4 Screenshot della finestra di dialogo per il caricamento della sessione . 14
4.5 Screenshot della sessione caricata 14
4.6 Screenshot che indica la posizione dei bottoni 15
4.7 Screenshot che indica la posizione dei filtri 16
4.8 Screenshot che mostra le informazioni di un punto 17
4.9 Screenshot che mostra le informazioni di una linea 18
4.10 Screenshot che mostra le informazioni di un nodo 18
4.11 Screenshot che mostra le informazioni di un utente 19
4.12 Screenshot che mostra la legenda 19

5.1 Informazioni Scatter Plot 1 20
5.2 Accessi sospetti Scatter Plot 1 21
5.3 Informazioni Scatter Plot 2 21
5.4 Utente sospetto Scatter Plot 2 22
5.5 Informazioni Parallel Coordinates 22
5.6 Tipo di applicazione dalla quale vengono effettuati tanti errori di accesso 23
5.7 Informazioni Sankey Diagram 23
5.8 Accessi dell'utente 21518 24
5.9 Informazioni Force-Directed Graph 24
5.10 Utenti sospetti 25

Elenco delle tabelle

2.1 Tabella dei requisiti consigliati 8
2.2 Tabella dei requisiti hardware 8
2.3 Tabella dei browser testati e supportati 9

1. Introduzione

1.1 Scopo del documento

Questo documento ha lo scopo di illustrare le istruzioni per l'utilizzo e le funzionalità fornite dall'applicazione. L'utente sarà quindi a conoscenza dei requisiti minimi necessari per il corretto funzionamento di *Login Warrior*, di come installarla in locale e di come farne un utilizzo consapevole.

1.2 Scopo del Prodotto

Al giorno d'oggi ogni servizio presente sul web richiede un'autenticazione$_G$ tramite login$_G$, fase fondamentale per la protezione dei dati di un individuo. Risulta ancora più importante se viene considerata la possibile presenza di malintenzionati con lo scopo di rubare ciò che dovrebbe essere privato. La presenza di attacchi informatici negli anni è andata aumentando e continua tuttora a crescere, per questo è necessario che questa pratica venga il più possibile riconosciuta e arginata.

Il capitolato C5 ha proprio come obiettivo quello di trovare una soluzione a questo problema. L'idea è quella di riconoscere le attività lecite e quelle illecite attraverso la raccolta, l'analisi e la visualizzazione di dati sotto forma di grafici e modelli che permettano un riconoscimento immediato delle differenze nei tentativi di accesso.

Con questo scopo il gruppo *MERL* si impegnerà nella realizzazione di un'applicazione web$_G$ in grado di leggere grandi quantità di dati di login per poi mostrare tramite dei grafici la natura di questi, riuscendo nell'intento di riconoscere a primo impatto le attività sospette.

1.3 Glossario

Al fine di evitare incomprensioni relative alla terminologia usata all'interno del documento, viene fornito un Glossario nel file *Glossario V2.0.0* in grado di dare una definizione precisa per ogni vocabolo potenzialmente ambiguo. Tali termini verranno evidenziati all'interno del documento con una G in pedice.

2. Requisiti Minimi di Sistema

2.1 Requisiti Minimi

Per far funzionare l'applicazione non ci sono particolare richieste, trattandosi di una Single-page Application.

2.2 Requisiti Consigliati

Per avere un'esperienza completa nell'uso dell'applicazione si consiglia d'installare nella propria macchina i seguenti software:

Software	Versione	Riferimenti per il download
Node.js	16.14.2	https://nodejs.org/en/
Npm	8.x	Integrato nel download di Node.js

Tabella 2.1: Tabella dei requisiti consigliati

2.3 Requisiti Hardware

Al fine di garantire prestazioni accettabili si consiglia di soddisfare i seguenti requisiti hardware:

Componente	Versione
Processore	Quad-Core
RAM	8GB

Tabella 2.2: Tabella dei requisiti hardware

2.4 Browser

I browser testati e resi compatibili con l'applicazione sono:

Browser	Versione
Chrome	99
Edge	99
Firefox	98
Opera	83
Safari	15.2

Tabella 2.3: Tabella dei browser testati e supportati

3. Installazione

Per utilizzare l'applicazione web è necessario:

- Clonare il repository$_G$;
- Avviare il server;
- Avviare la web app.

3.1 Clonare il repository

- Scaricare il codice come file .zip direttamente dal repository *login-warrior*:

  https://github.com/merlunipd/login-warrior

  oppure, avendo *Git*$_G$ installato in locale, è possibile clonare il repository con il comando:

  ```
  git clone https://github.com/merlunipd/login-warrior
  ```

- Localizzare da terminale la cartella in cui è stato estratto/clonato il prodotto:

  ```
  cd percorso\LoginWarrior
  ```

3.2 Avviare il server

- Entrare nella cartella `login_warrior` con i seguenti comandi:

  ```
  cd src
  cd login_warrior
  ```

- In caso di primo avvio, per crea la cartella `node_modules` dove vengono installate tutte le dipendenza necessarie digitare:

  ```
  npm install
  ```

- Per listare gli script impostati digitare (**Opzionale**):

  ```
  npm run
  ```

- Per eseguire un server locale che permette l'accesso all'applicazione digitare:

  ```
  npm run server
  ```

3.3 Avviare la web app

Dopo aver avviato il server come spiegato nel passo precedente, l'applicazione sarà disponibile aprendo l'indirizzo fornito dal terminale:

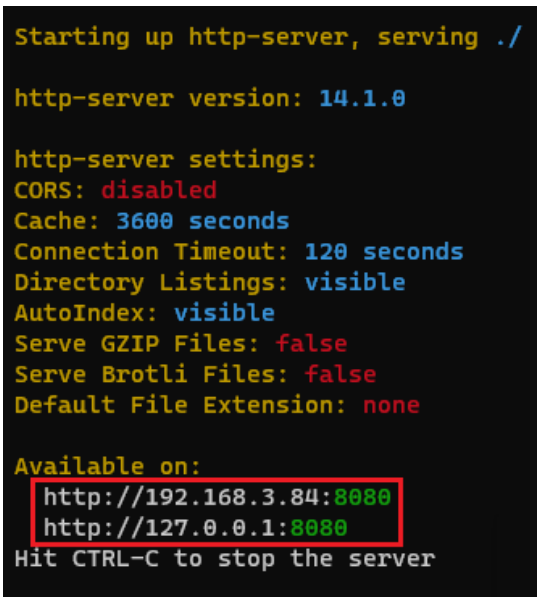


Figura 3.1: Avvio dell'applicazione

4. Istruzioni all'uso

Il seguente capitolo fornirà tutte le spiegazioni per il corretto utilizzo del prodotto.

4.1 Home

Questa è la prima schermata disponibile dell'applicazione. Qui è possibile caricare i dati sotto forma di dataset o di sessione salvata in precedenza.

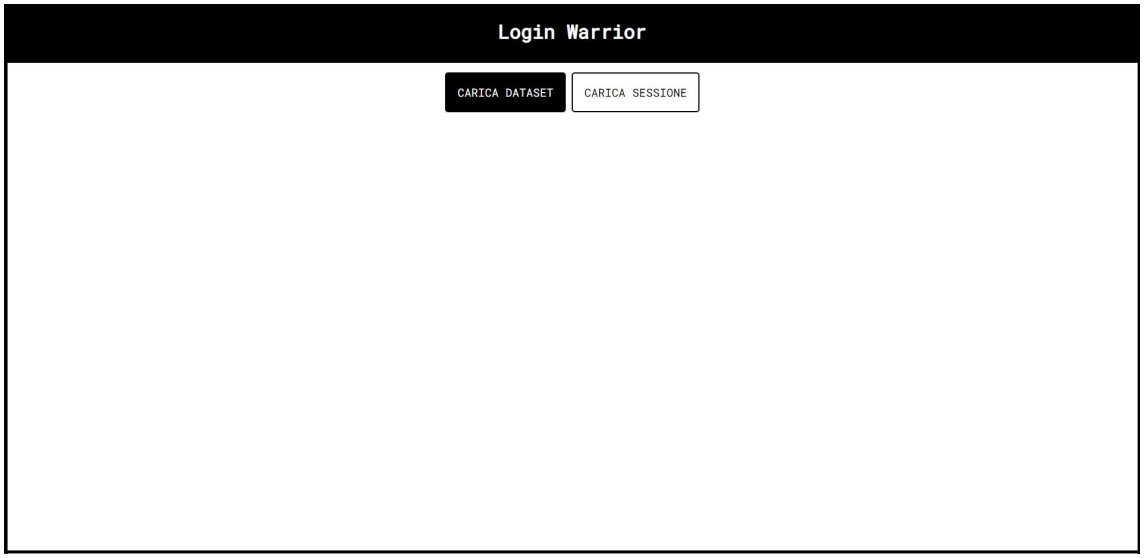


Figura 4.1: Screenshot della Home

4.1.1 Carica dataset

Cliccando su "Carica dataset" comparirà una finestra di dialogo che ci permetterà di caricare il dataset. Seleziona quindi il file in formato .csv desiderato e poi clicca su "Apri" per caricare il file.

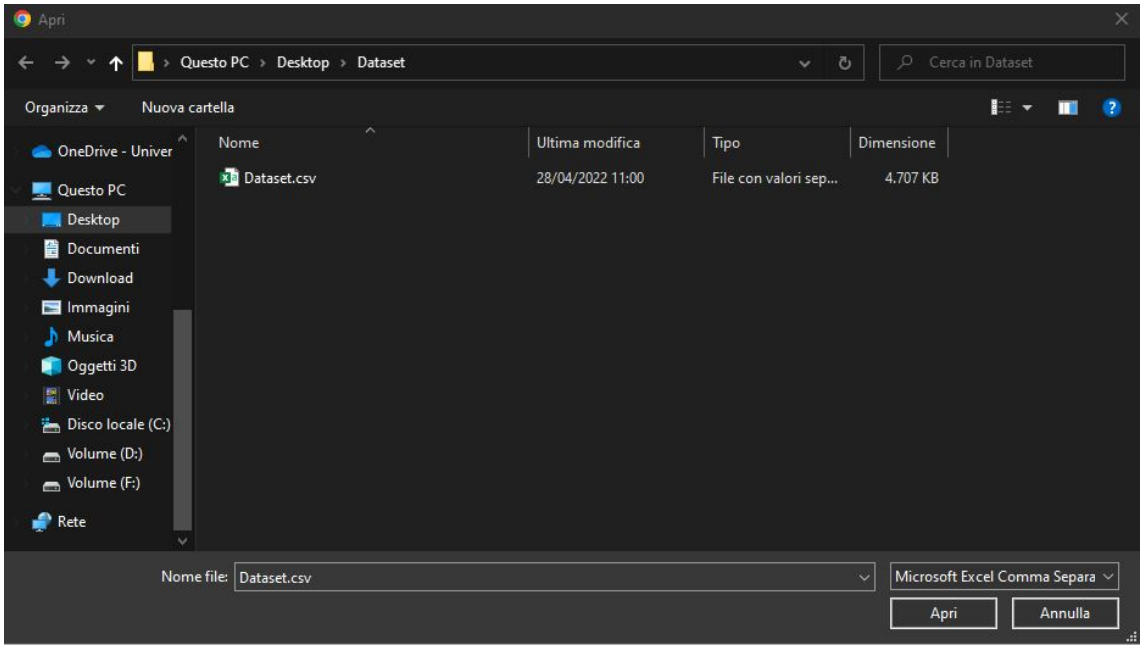


Figura 4.2: Screenshot della finestra di dialogo per il caricamento del dataset

Dopo aver caricato il dataset comparirà una lista dei grafici disponibili. Si potrà scegliere tra vari tipi di:

- *Scatter Plot*;
- *Parallel Coordinates*;
- *Sankey Diagram.*

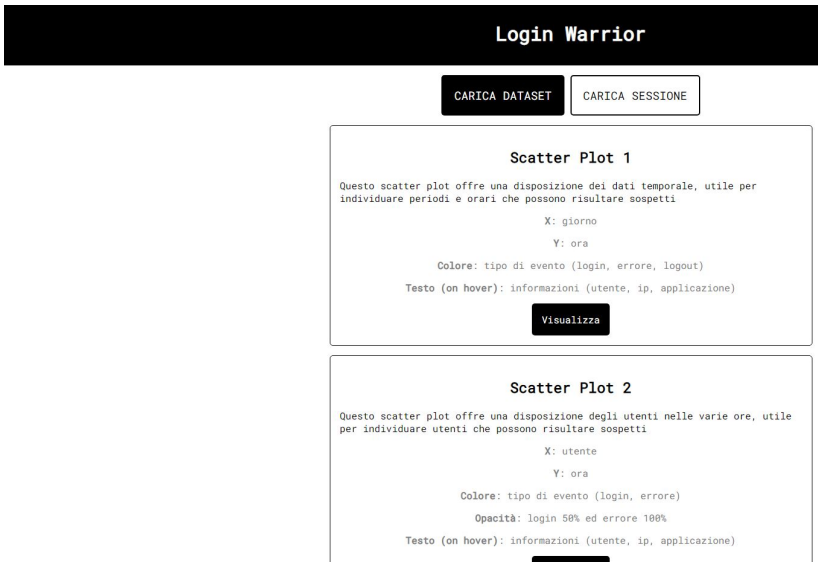


Figura 4.3: Screenshot della lista dei grafici

Successivamente per visionare il grafico desiderato basterà premere il relativo bottone "Visualizza".

4.1.2 Carica sessione

Cliccando su "Carica sessione" comparirà una finestra di dialogo che ci permetterà di caricare i dati di una sessione salvata in precedenza. Seleziona quindi il file in formato .json desiderato e poi clicca su "Apri" per caricare il file.

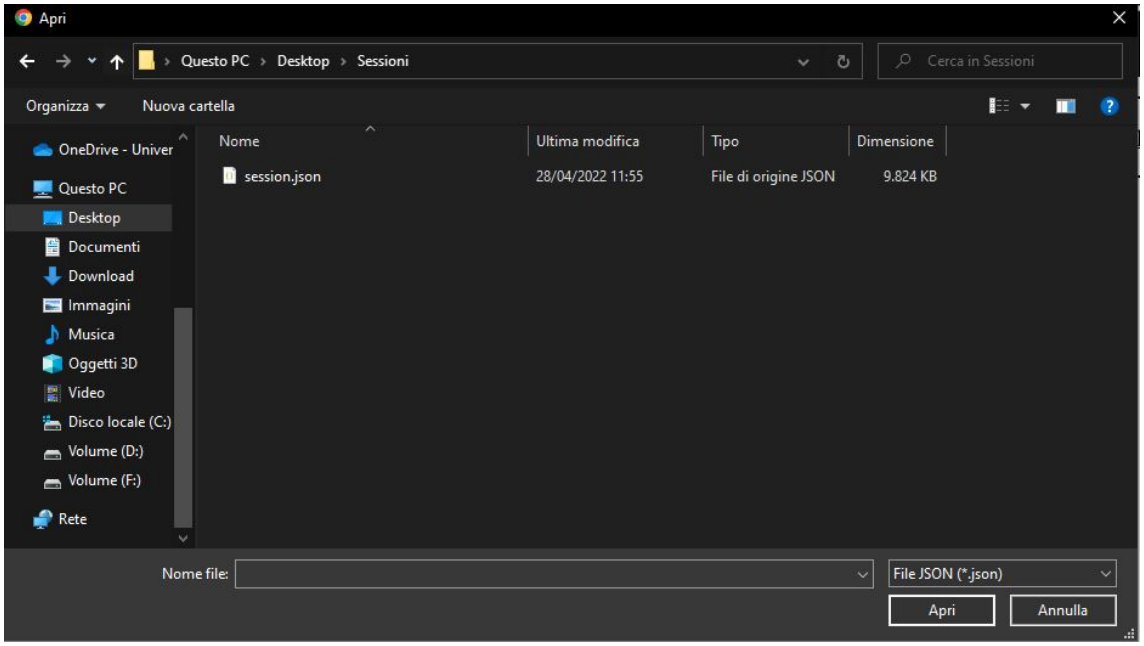


Figura 4.4: Screenshot della finestra di dialogo per il caricamento della sessione

Dopo aver caricato la sessione nel sistema si potrà proseguire il lavoro da dove era stato salvato.

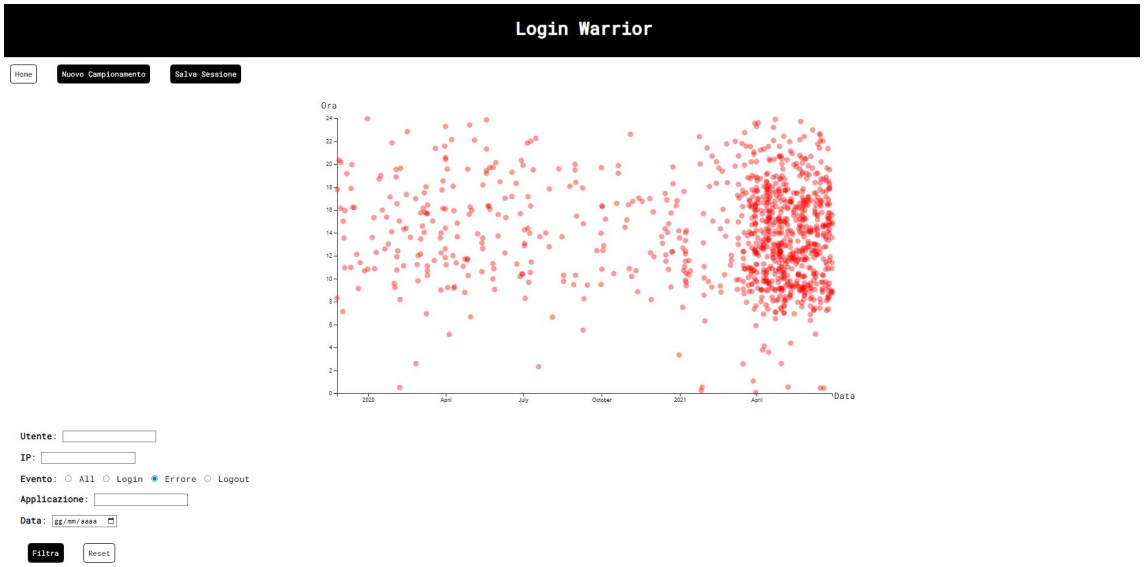


Figura 4.5: Screenshot della sessione caricata

4.2 Bottoni

Nella pagina di visualizzazione del grafico, sono disponibili tre bottoni. Questi si trovano nell'estremo superiore sinistro della pagina.

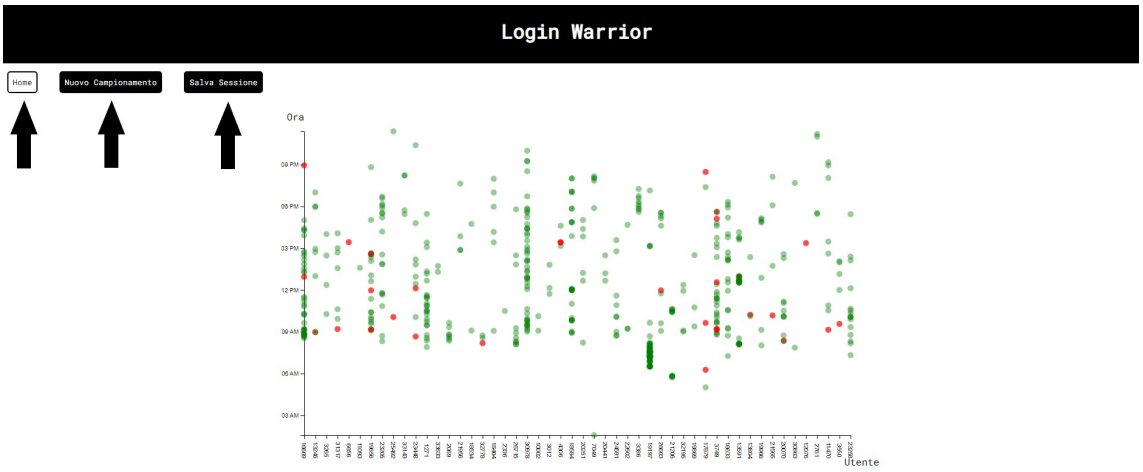


Figura 4.6: Screenshot che indica la posizione dei bottoni

4.2.1 Bottone Home

Questo bottone permette di ritornare alla Home in qualsiasi momento mantenendo comunque in memoria il dataset caricato, permettendo di scegliere un altra tipologia di grafico o di caricare un nuovo file.

4.2.2 Nuovo Campionamento

Ogni grafico attua un appropriato algoritmo di campionamento dei dati per permettere all'utilizzatore di avere una buona visualizzazione delle informazioni (il numero di dati potrebbe essere estremamente grande, quindi non gestibile). Questo bottone permette di estrapolare ogni volta dei dati nuovi attraverso l'algoritmo di campionamento. Se il numero di dati del dataset è inferiore al numero massimo di dati che il grafico può visualizzare questo bottone non provoca cambiamenti.

4.2.3 Salva Sessione

Questo bottone permette di salvare la sessione corrente in tutti i suoi aspetti, compresi i filtri e dataset intero. Basterà premerlo per scaricare la sessione nel formato .json.

4.3 Filtri

In ogni grafico è possibile impostare dei filtri. Questi sono impostabili dall'estremo inferiore sinistro della pagina. Una volta inseriti i filtri desiderati occorre premere

il bottone "Filtra" per applicarli. Per resettare i filtri invece occorre premere il bottone "Reset".

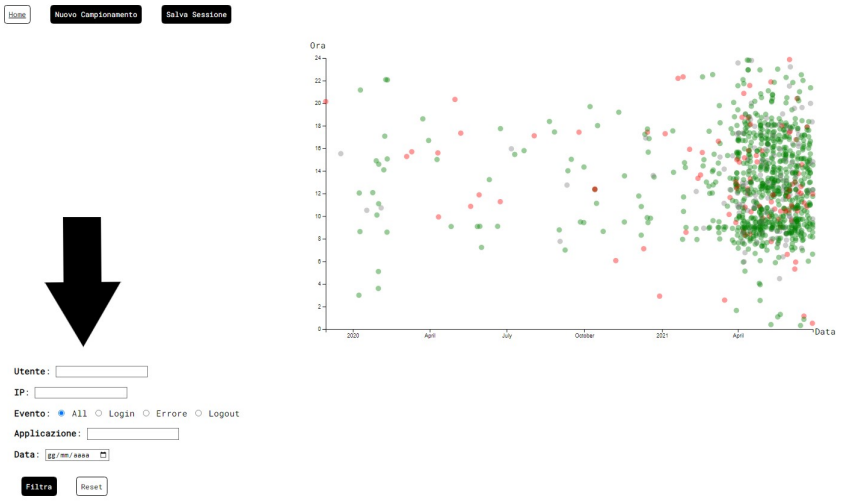


Figura 4.7: Screenshot che indica la posizione dei filtri

4.3.1 Utente

In questo campo è possibile inserire il numero di un utente se si vuole visualizzare il grafico contenente solo i suoi accessi.

4.3.2 Ip

In questo campo è possibile inserire un indirizzo IP se si vuole visualizzare il grafico contenente solo i suoi accessi.

4.3.3 Evento

Questo filtro permette di filtrare i dati secondo i vari tipi di evento, ovvero:

- Login;
- Errore;
- Logout.

4.3.4 Applicazione

In questo campo è possibile inserire il nome di un'applicazione se si vuole visualizzare il grafico contenente solo gli accesi effettuati tramite essa.

4.3.5 Data

Qui viene fornito un calendario dal quale è possibile scegliere una data che permette di visualizzare gli accessi avvenuti in quella determinata giornata.

4.4 Scatter Plot

Il grafico *Scatter Plot* permette di visualizzare ogni azione degli utenti sotto forma di punti all'interno del piano cartesiano. Ogni evento ha un colore differente per avere una più facile visualizzazione. Il verde indica un login effettuato con successo, il rosso un errore e il grigio un logout. Per visualizzare le informazioni di ogni evento si dovrà posizionare il cursore al di sopra del pallino scelto. Le informazioni disponibili sono:

- Ip;
- Numero Utente;
- Tipologia di evento;
- Data;
- Applicazione da dove è stata compiuta l'azione.

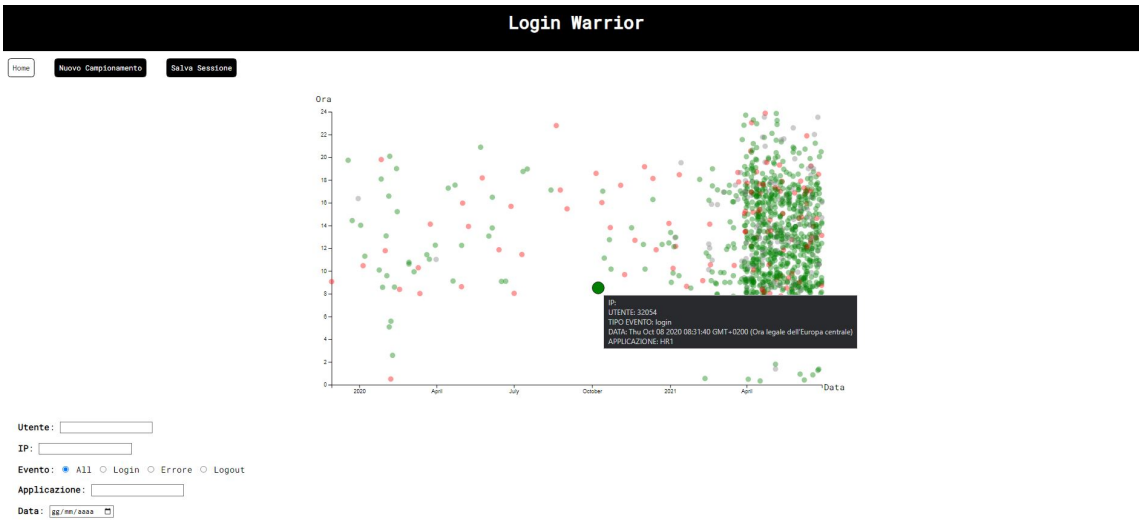


Figura 4.8: Screenshot che mostra le informazioni di un punto

4.5 Parallel Coordinates

Il grafico *Parallel Coordinates* permette di visualizzare ogni accesso sotto forma di linea. Per visualizzare le informazioni di un particolare evento si dovrà posizionare il cursore al di sopra della linea scelta. Le informazioni disponibili sono:

- Ip;
- Numero Utente;
- Tipologia di evento;
- Data;

- Applicazione da dove è stata compiuta l'azione.

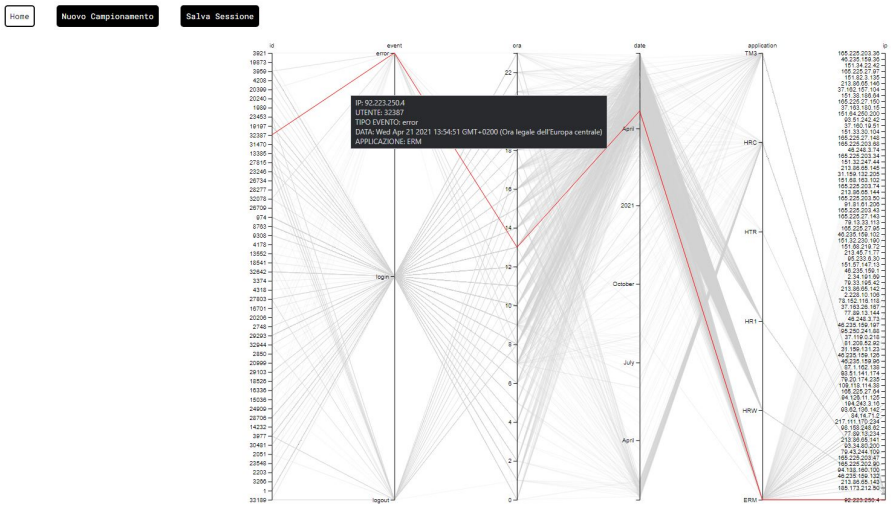


Figura 4.9: Screenshot che mostra le informazioni di una linea

4.6 Sankey Diagram

Il grafico *Sankey Diagram* permette di visualizzare gli eventi raggruppati in nodi. È per esempio possibile visualizzare quanti login ci sono stati nel mese di Aprile nell'orario d'ufficio. Per visualizzare il numero di dati che ogni nodo contiene basterà posizionare il cursore al di sopra del rettangolo colorato che indica i dati che ci interessano.

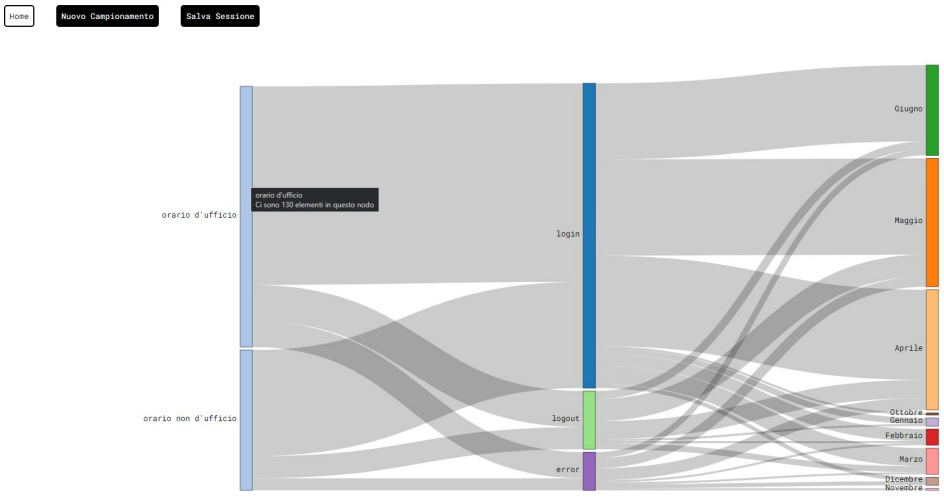


Figura 4.10: Screenshot che mostra le informazioni di un nodo

4.7 Force-Directed Graph

Il grafico *Force-Directed Graph* permette di visualizzare i vari utenti con il loro rapporto Login/Errori. Come indicato dalla legenda i nodi colorati di nero indicano i vari range di rapporto Login/Errori mentre i nodi con i vari colori indicano in che range l'utente si trova. Posizionando il cursore sui nodi neri viene visualizzato il range a cui ci si riferisce, mentre posizionandolo su un nodo colorato vengono mostrate le informazioni rilevanti di quel determinato utente:

- id;
- numero di login corretti;
- numero di login errati;
- percentuale relativa al rapporto Login/Errori.

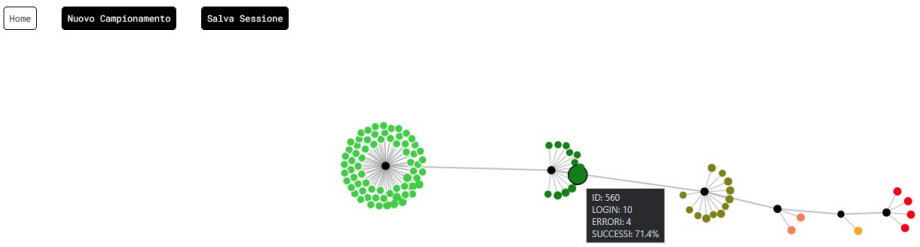


Figura 4.11: Screenshot che mostra le informazioni di un utente

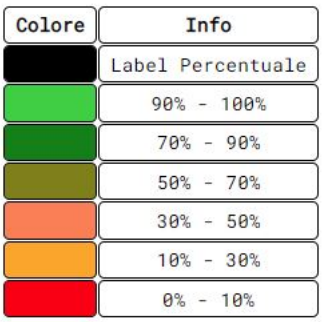


Figura 4.12: Screenshot che mostra la legenda

5. Tutorial

L'applicazione permette di visualizzare i dati mediante diverse tipologie di grafici, di seguito viene spiegata l'utilità di ognuno di questi e il modo con cui usare correttamente l'applicazione *LoginWarrior*.

5.1 Scatter Plot 1

Figura 5.1: Informazioni Scatter Plot 1

Questa prima tipologia di *Scatter Plot* permette di individuare degli accessi sbagliati eseguiti in orari sospetti, quindi per esempio durante l'orario non di ufficio. Eseguendo un nuovo campionamento si può notare se queste anomalie persistono oppure se era un errore dovuto a quello specifico campionamento. In caso quella anomalia dovesse persistere si può posizionarsi sopra con il mouse e nelle informazioni vedere l'utente o gli utenti sospetti.

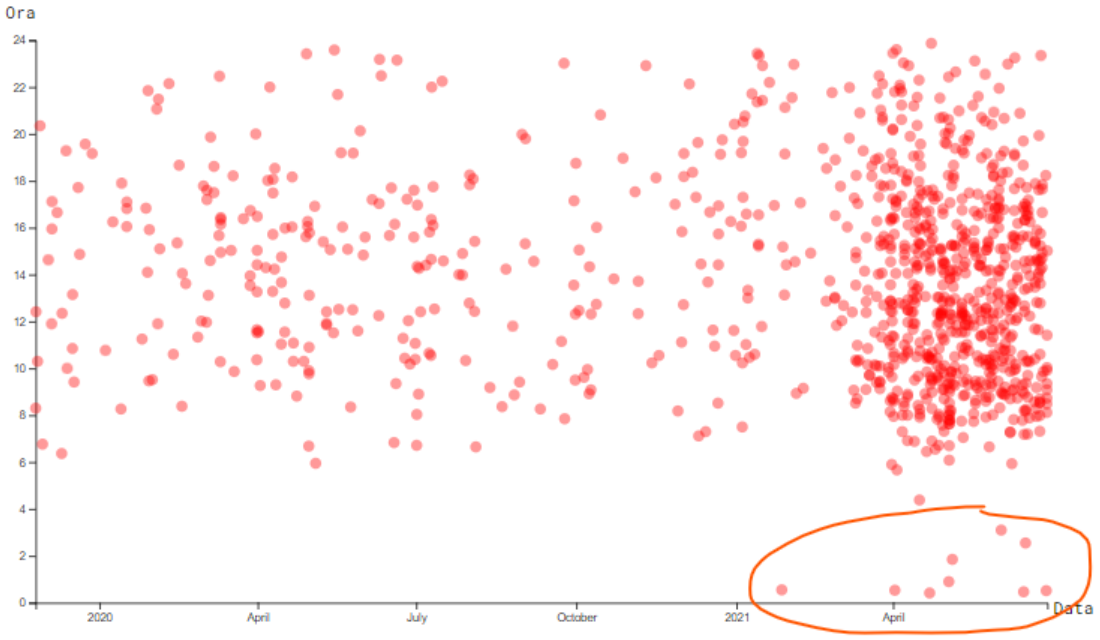


Figura 5.2: Accessi sospetti Scatter Plot 1

5.2 Scatter Plot 2

Figura 5.3: Informazioni Scatter Plot 2

Questa seconda tipologia di *Scatter Plot* permette di individuare un utente che ha una percentuale di accessi sbagliati più alta di quelli andati a buon fine, basta guardare le varie linee verticali che si riferiscono ad un singolo utente. Anche in questo grafico gli accessi sbagliati più sospetti sono quelli effettuati durante l'orario non di ufficio, indicato sull'asse y.

Figura 5.4: Utente sospetto Scatter Plot 2

5.3 Parallel Coordinates

Figura 5.5: Informazioni Parallel Coordinates

Questa tipologia di grafico offre una visione su tutte le dimensioni, infatti ogni asse verticale ne rappresenta una. È un grafico molto utile se si filtra per tipo di evento, in particolare login errato, perchè così facendo possiamo vedere il periodo in cui ne

sono stati effettuati maggiormente e anche il tipo di applicazione dalla quale sono stati fatti.

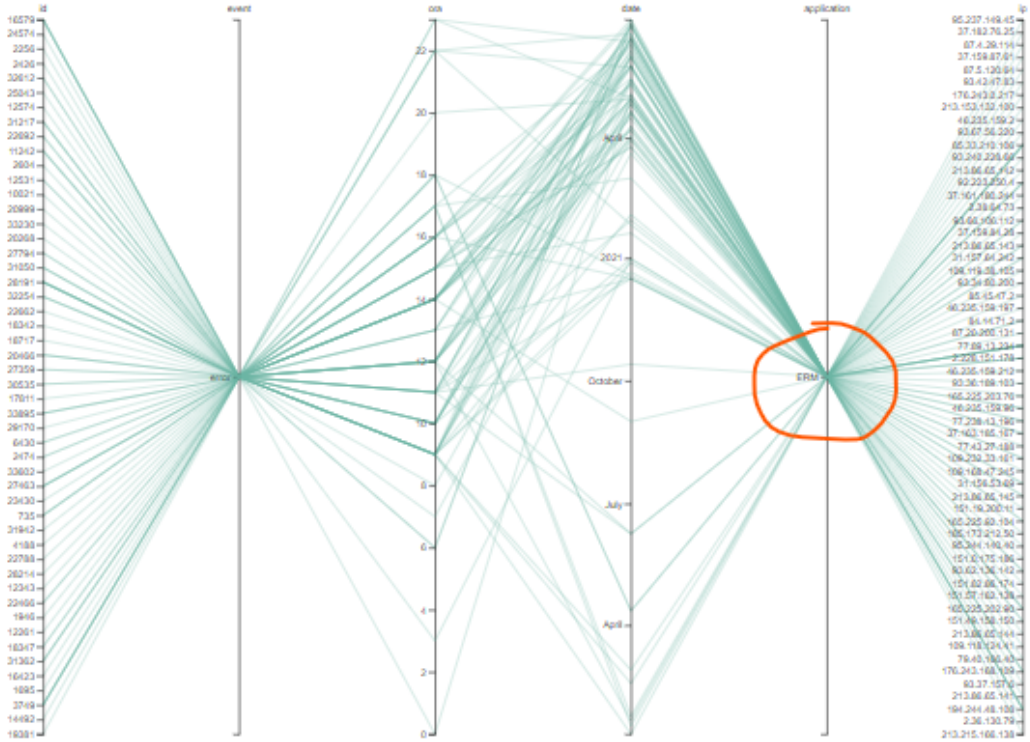


Figura 5.6: Tipo di applicazione dalla quale vengono effettuati tanti errori di accesso

5.4 Sankey Diagram

Figura 5.7: Informazioni Sankey Diagram

Questa tipologia di grafico è formata da barre dalle quali escono dei fasci. Si può notare nell'orario di ufficio e in quelo non di ufficio tramite la grandezza dei fasci uscenti la distribuzione di login, logout ed errori. È un grafico utile se si filtra per utente perchè permette di avere un quadro generale del suo comportamento e la distribuzione degli accessi.

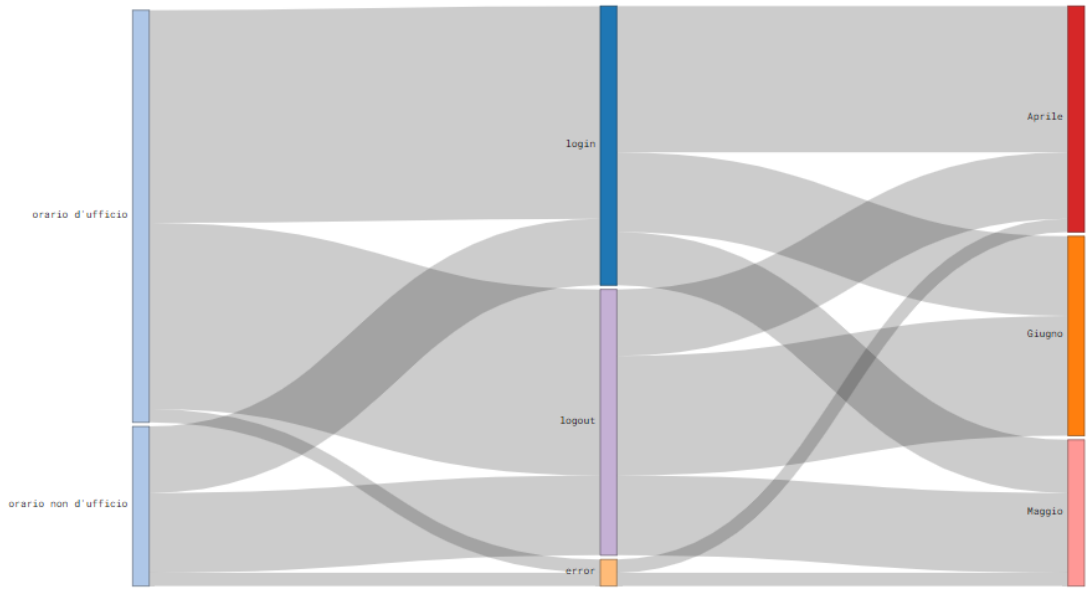


Figura 5.8: Accessi dell'utente 21518

5.5 Force-Directed Graph

Figura 5.9: Informazioni Force-Directed Graph

Questa tipologia di grafico mostra quali utenti sono più sospetti nelle loro azioni. Risulta molto utile ad identificare gli utenti con un rapporto Login/Errori basso, individuati dai colori tendenti al rosso, che indica un elevato numero di login errati rispetto ai login corretti. Grazie a questo grafico possiamo individuare in modo

immediato gli utenti sospetti e questo ci permette poi di andare a controllare negli altri grafici più nel dettaglio le azioni di questi utenti.

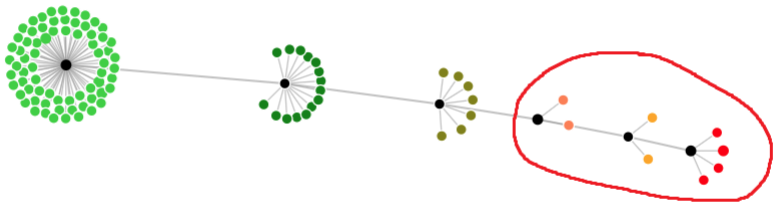


Figura 5.10: Utenti sospetti