**Corso di Programmazione Web e Mobile**

**A.A. 2021-2022**

**XSSDetector**

º Eros, Capobianco, ------- »

# Introduzione

XSS Detector è una piattaforma Web che si propone come strumento di Cyber Difesa ed essere quindi utilizzata dagli operatori per scovare falle di tipo XSS DOM Based.

L’applicazione si propone attraverso una Homepage molto minimale con lo scopo di trasferire all’utente chiarezza sulle proprie funzionalità tramite delle brevi spiegazioni dei concetti chiave sui quali essa è fondata.

La pagina XSS Detector propone invece lo strumento offerto all’utente, il quale tramite un semplice form potrà inserire la pagina web che sarà target dell’analisi, una volta terminata, verrà proposto all’utente un report PDF nel quale saranno indicate le vulnerabilità trovate.

Gli utenti inoltre potranno visualizzare un elenco rappresentante le ultime scansioni effettuate in modo da rendere trasparente la ricerca delle vulnerabilità.

## Breve analisi dei requisiti

### Destinatari

**Capacità e possibilità tecniche**.

L’applicazione web XSS Detector è stata concepita con lo scopo di permettere agli operatori di sicurezza di individuare velocemente le possibili vulnerabilità XSS DOM Based di un sito web, perciò è verosimile pensare che venga usato soltanto da operatori nel campo della sicurezza informatica, tuttavia essendo semplice da utilizzare siccome composta principalmente da due form, potrebbe essere utilizzata anche da programmatori o appassionati del web.

L’applicazione può essere inoltre utilizzata tramite diversi comuni device come: computer, smartphone e tablet.

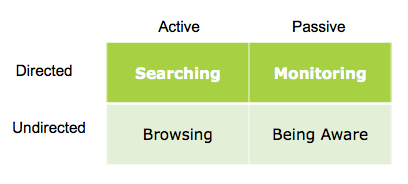
**Linguaggio.**

XSS Detector è utilizzato per compiere analisi di codici sorgenti, per questo motivo è presumibile una conoscenza dei linguaggi del web (HTML, CSS, Javascript, ecc…) da parte dell’utilizzatore della piattaforma.

Inoltre si può ritenere fondamentale una conoscenza della lingua inglese per comprendere il codice segnalato ed eventualmente in seguito compiere le opportune modifiche per correggere le vulnerabilità segnalate.

**Motivazione**

**L’utente che utilizzerà l’applicazione web sarà principalmente mosso da motivazioni di natura lavorativa. Un operatore addetto alle analisi di sicurezza di una piattaforma\sito web potrebbe visitare XSS Detector per facilitare e velocizzare i tempi di esecuzione delle proprie analisi di sicurezza. Possiamo affermare che XSS Detector è predisposta ad una ricerca diretta siccome i visitatori troveranno la piattaforma ricercando strumenti di analisi vulnerabilità che rientrano in una categoria di software utilizzati da pochi operatori con lo scopo di analizzare le vulnerabilità. Tuttavia la pagina “Recent Scan” può fornire informazioni passive ad un utente che visita la piattaforma per curiosità.**



### Modello di valore

Il valore di “XSS Detector” è facilmente identificabile in quanto esistono pochissimi strumenti di questo tipo, i quali richiedono abbonamenti e pagamenti per poter essere utilizzati.

I servizi offerti dalla nostra applicazione invece sono resi disponibili a qualsiasi utente, il che presuppone una maggiore visibilità della piattaforma rispetto ad altre possibili soluzioni online.

Le possibilità di guadagno rispetto ad un possibile investimento possono essere identificate nel posizionamento di banner pubblicitari ed allo sviluppo di una versione “Premium” che permetta l’utilizzo di funzioni avanzate.

### Flusso dei dati

### ****Reperimento dei contenuti****

**I contenuti dell’applicativo principalmente sono il report pdf delle vulnerabilità scoperte durante la fase di analisi e la lista di scansioni recenti tratta dalla sintesi delle precedenti scansioni, lo stile di presentazione dei contenuti sopracitati è spartano e formale, tipico stile utilizzato nei software di questa tipologia in quanto semplifica la ricezione dei contenuti da parte di un operatore.**

**L’analisi del codice sorgente dei target è ottenuta tramite l’utilizzo di due liste di parole chiave utili nell’identificazione delle vulnerabilità XSS DOM Based, il codice una volta filtrato da queste liste produce delle variabili che verranno utilizzate a loro volta nella produzione del report pdf tramite la libreria pdfkit che presenterà all’utente finale le vulnerabilità scoperte.**

**La tabella presente nella pagina delle scansioni precedenti invece recupera i dati da presentare tramite una chiamata XMLHTTP request ad una API REST che espone i dati della lista di scansioni presenti nel database.**

### Aspetti tecnologici

XSS Detector è stata pensata principalmente per essere utilizzata da computer, vi sono presenti però delle media query nel foglio di stile css che permettono di ottenere un’interfaccia presentabile anche su altri tipi di device.

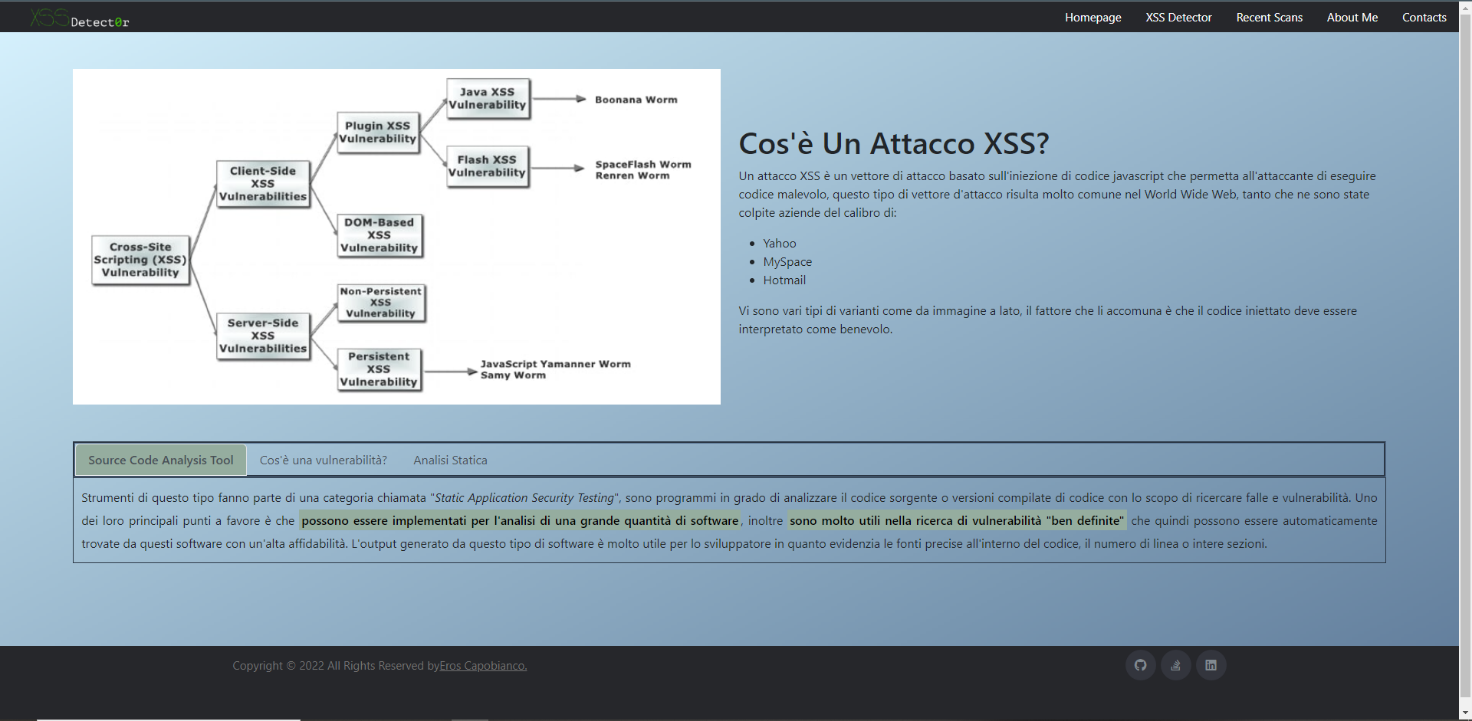
Per la costruzione dell’applicativo si è utilizzato il modello MVC, in particolare i modelli implementati sono contacts e xssdetector che permettono di definire la struttura del database, i controller sono stati implementati in modo da permettere una corretta gestione delle pagine xss detector e contatti, mentre vi sono molteplici view scritte attraverso il template engine PUG in HTML5.

Le tecnologie utilizzate per lo sviluppo sono:

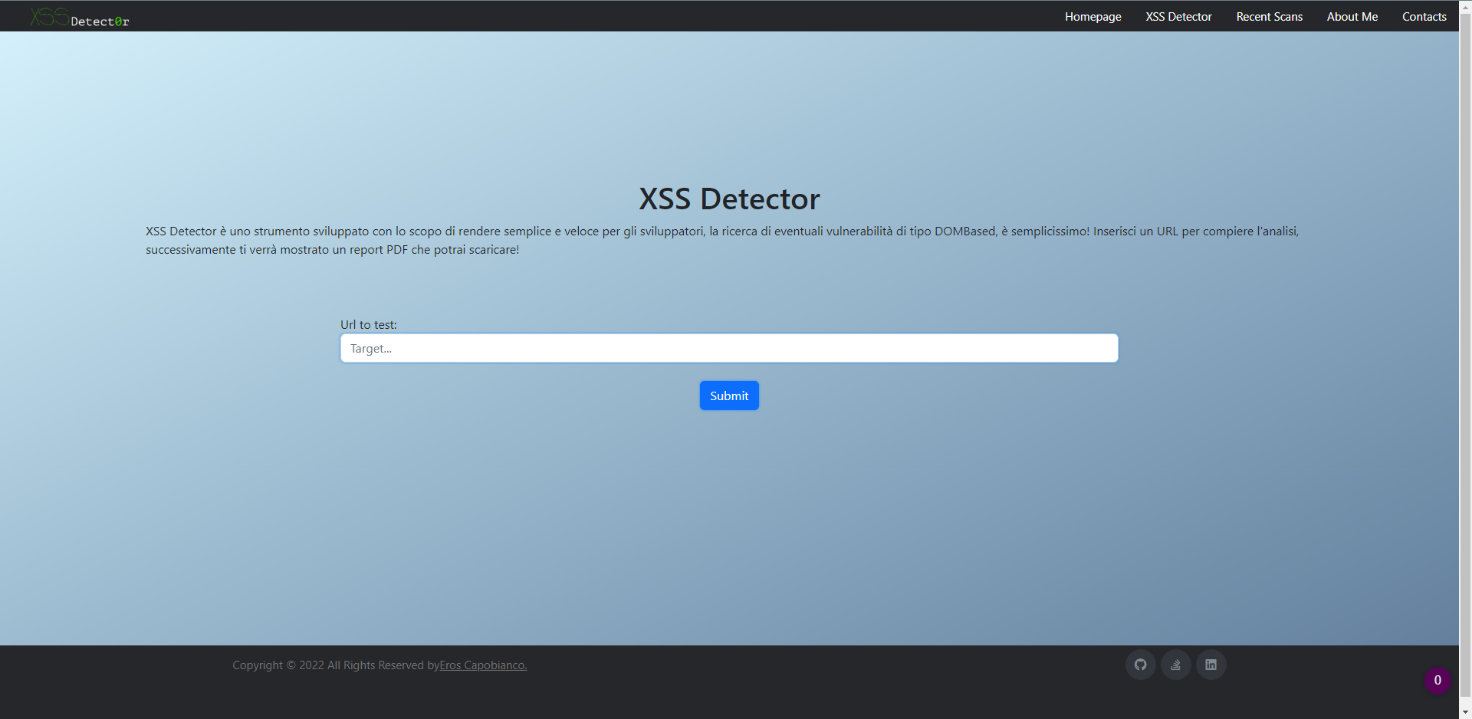
* NodeJs: Utilizzato per gestire l’applicativo (Richiesta)
* express: Libreria node utilizzata per gestire le chiamate http
* PUG: Utilizzato come template engine nella costruzione delle view
* pdfkit: Libreria utilizzata per la costruzione del report in formato PDF
* Mongoose: Strumento utilizzato per la gestione del database MongoDB
* Nodemailer: Libreria utilizzata per l’invio di mail ad una particolare casella di ricezione dei contatti.
* Nodemon: Libreria utilizzata per la interpretazione automatica del codice.
* Puppeteer: Libreria utilizzata per la gestione del browser chromium

# Interfacce

1. Homepage



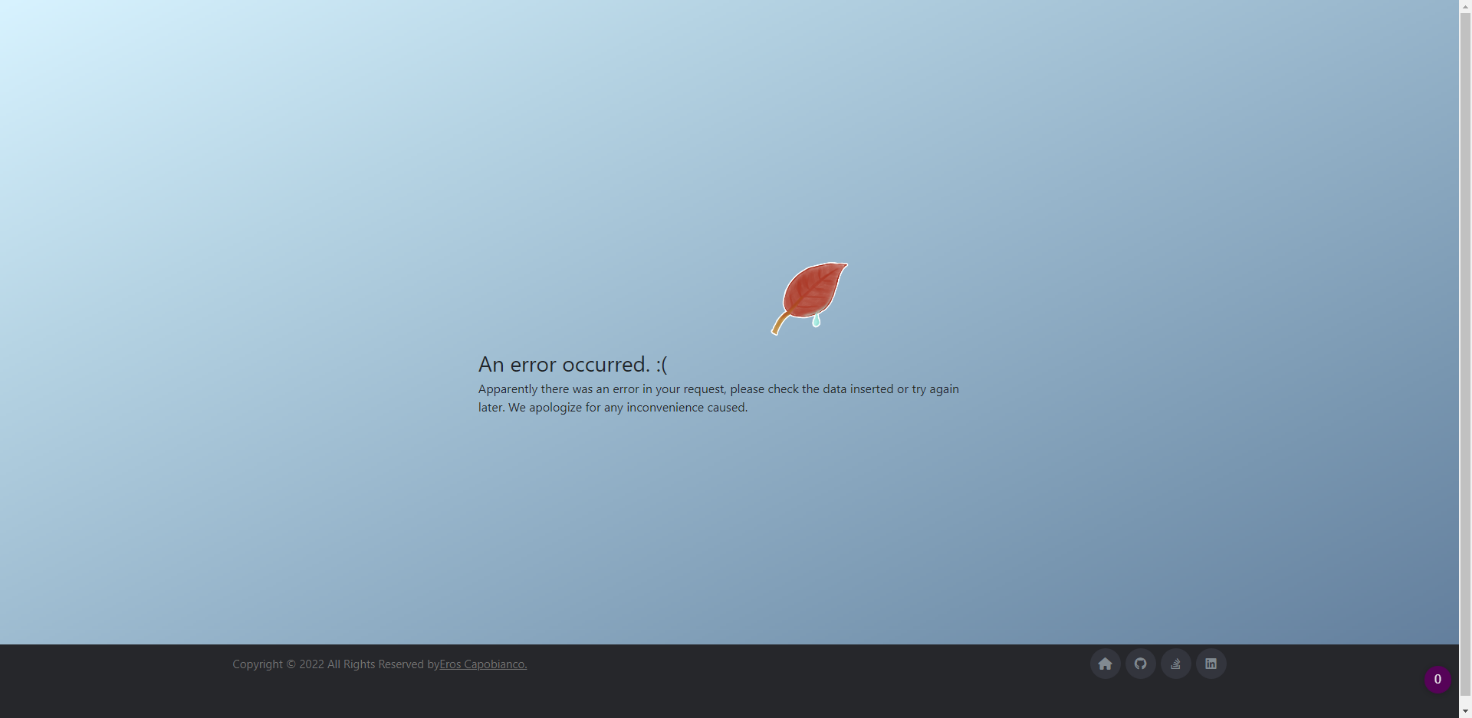
La schermata homepage sarà la prima pagina in cui capiterà l’utente, perciò in questa pagina vengono brevemente spiegati alcuni concetti fondamentali per comprendere XSS Detector.



Schermata che rappresenta lo strumento, è composta da un form da compilare inserendo l’URL di una pagina web da analizzare.



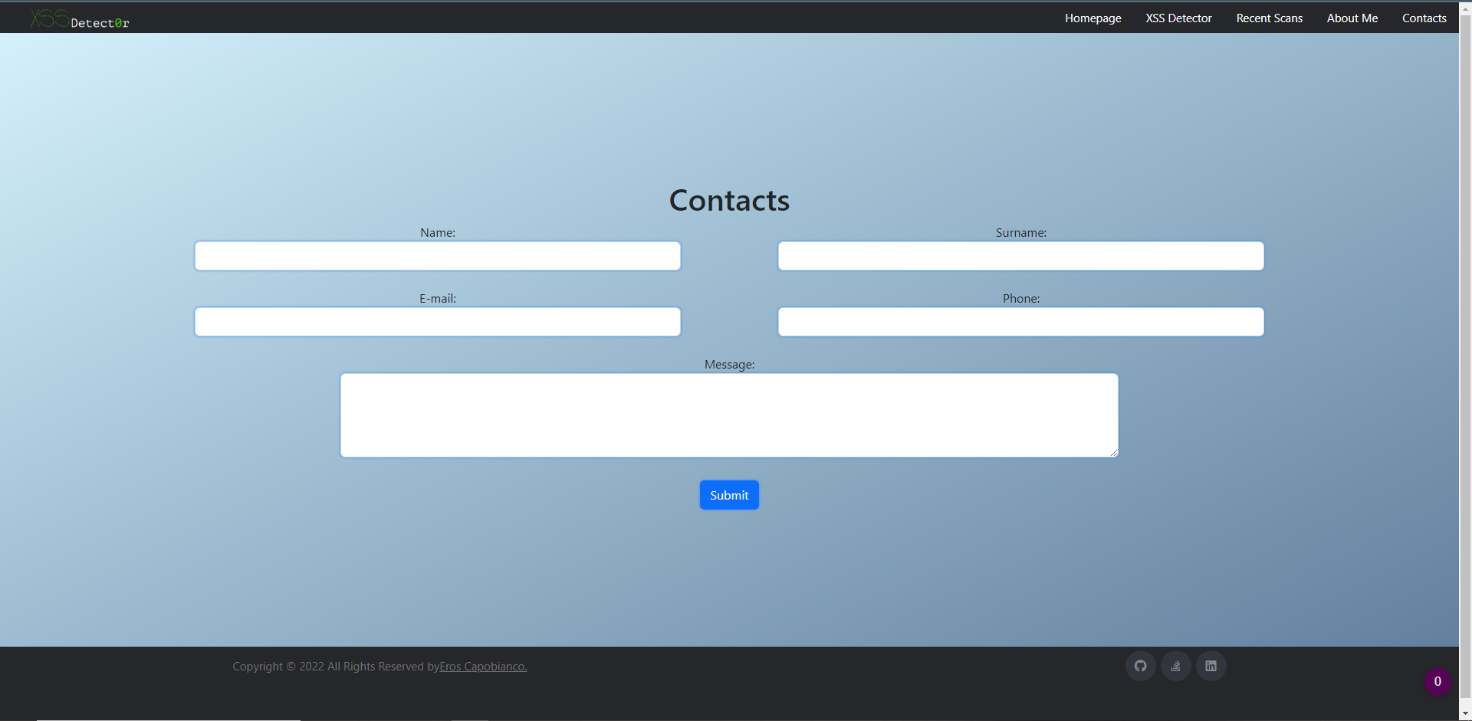
Possiamo vedere un esempio di report presentato all’utente dalla schermata precedente, è stata scelta la presentazione tramite PDF in quanto viene resa agevole la stampa ed il download attraverso le icone presenti nel file.



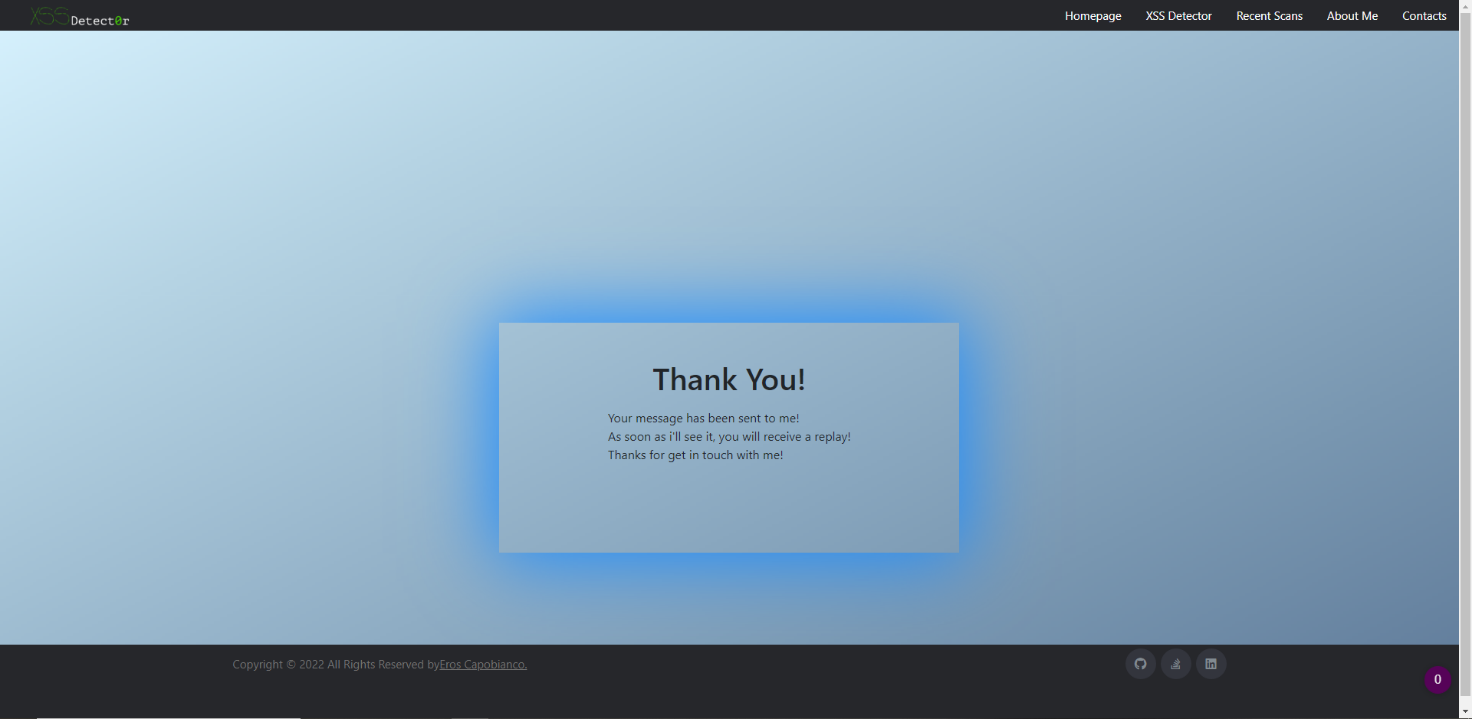
La schermata precedente mostra la pagina di errore che verrà visualizzata nel caso in cui non venga inserito un URL nel form xss detector o non sarà stato possibile ricevere tale URL.



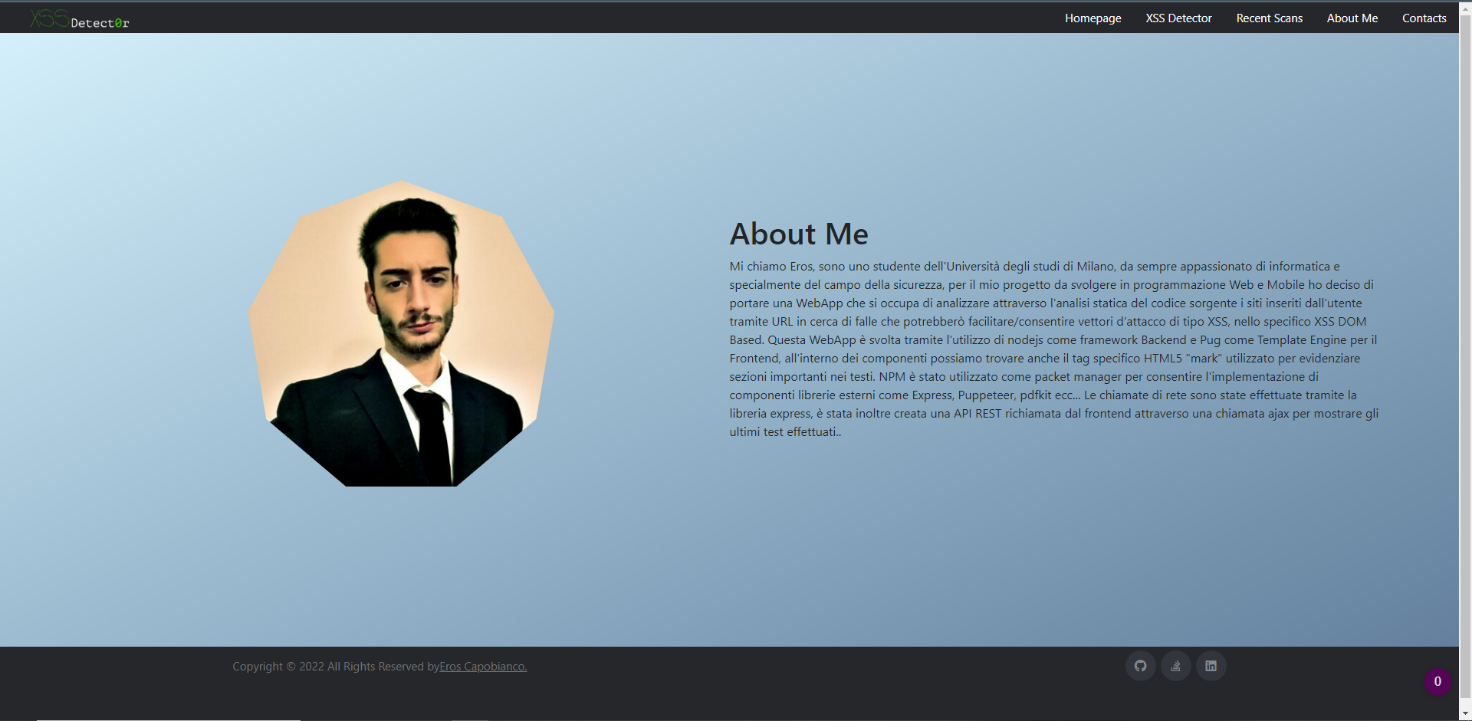
La rappresentazione delle precedenti scansioni è identificata dalla tabella generata dinamicamente in base ai dati ricevuti tramite la richiesta xmlhttp, in rosso possiamo notare le pagine possibilmente vulnerabili, mentre in verde sono colorate le righe in cui vi sono pagine non vulnerabili.



La pagina di contatto è composta da un semplice form che recupererà i dati dell’utente ed invierà una mail alla mia casella di posta elettronica contenente il messaggio inserito.



Una volta che il form di contatto è stato inviato una semplice pagina “Thank you” ringrazierà l’utente per la comunicazione inviata.



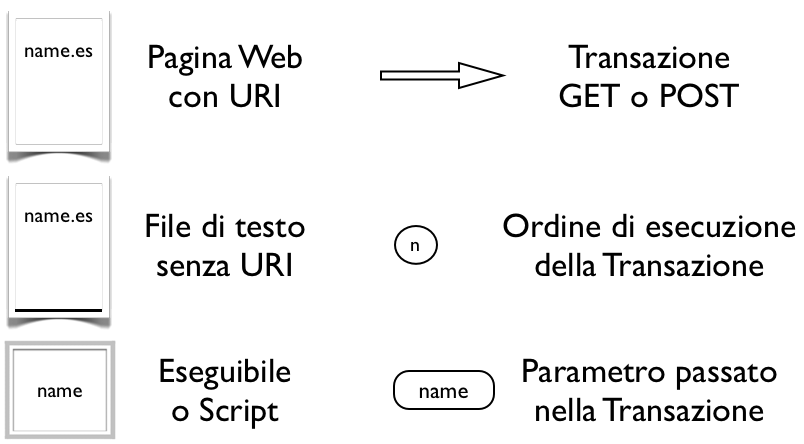
Si è voluto inserire inoltre una pagina contenente una breve presentazione dell’autore della piattaforma composta da un’immagine ed una breve descrizione a lato.

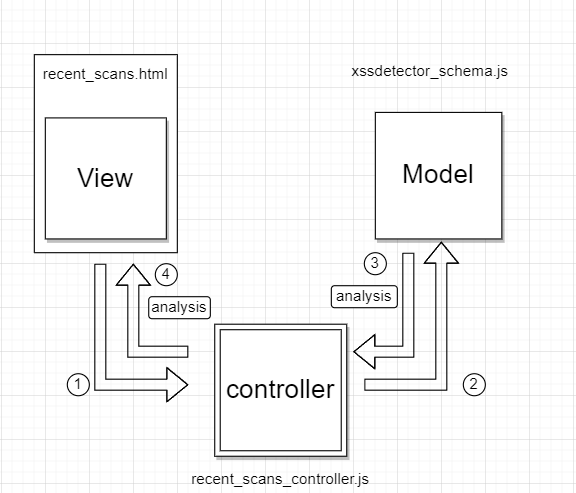
# Architettura

## Diagramma dell'ordine gerarchico delle risorse

## 

## Descrizione delle risorse

Figura 2: Legenda della notazione utilizzata



Nell’immagine precedente possiamo vedere un esempio di implementazione del modello MVC.

Figura 3: Esempio MVC pagina recent\_scans.html

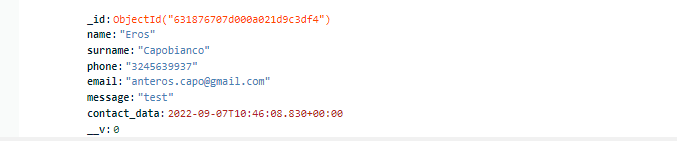
## Altri diagrammi

Di seguito il diagramma del Database:

1. Modello della collezione xssdetector



1. Modello della collezione contacts

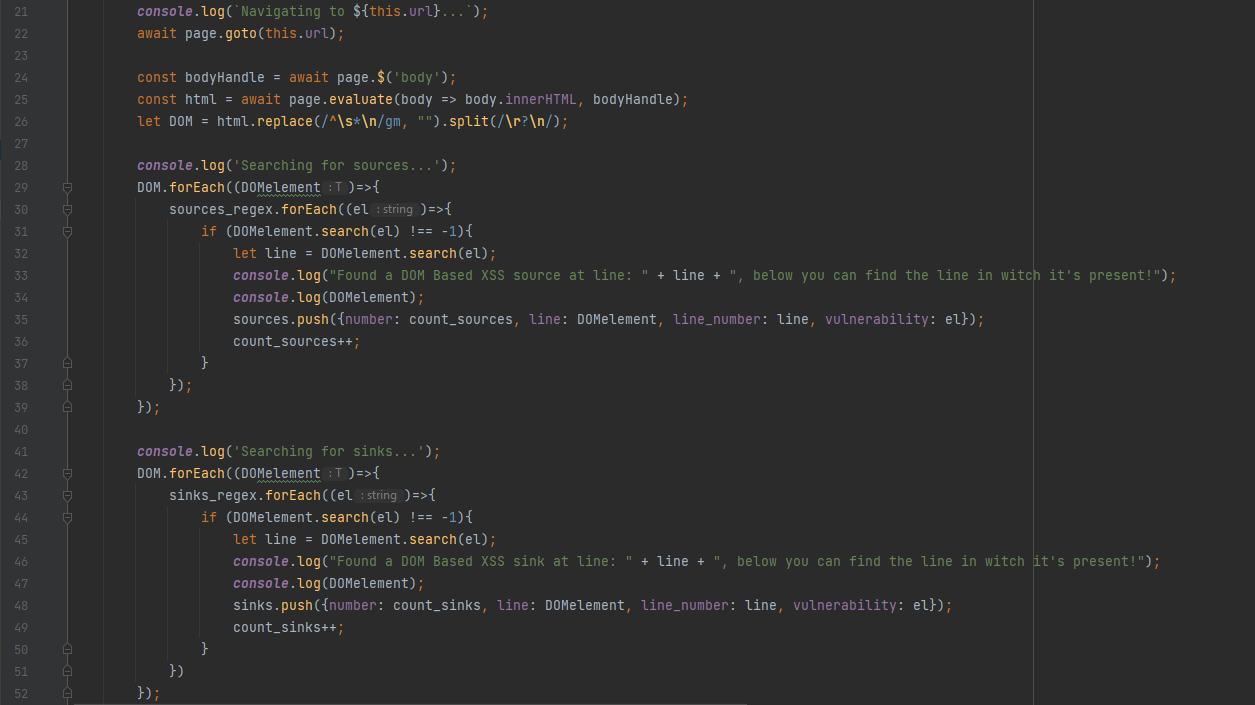


# Codice

*Frammenti del codice più significativo*

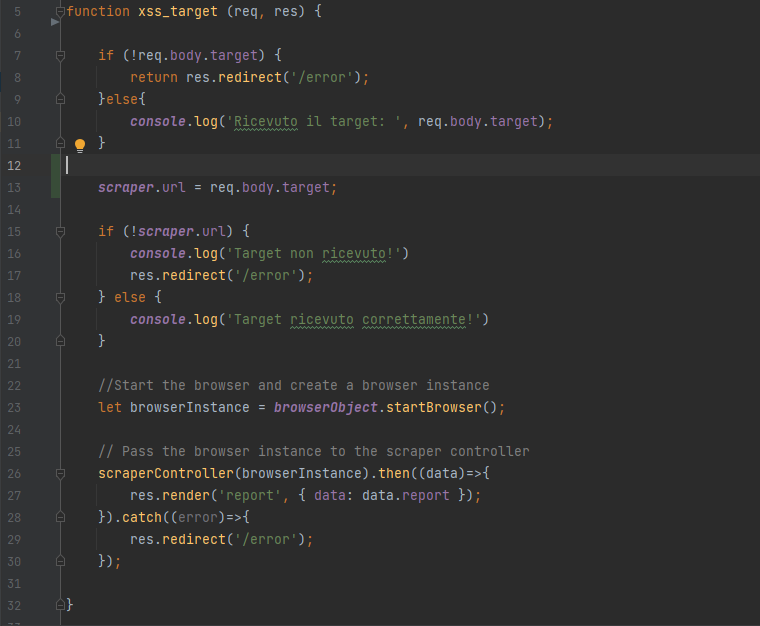
1. Di seguito un frammento di codice incaricato di compiere l’analisi del codice recuperato tramite scraping della pagina web inserita dall’utente.

Come primo step viene recuperato il codice dalla URL ricevuta, successivamente come secondo step viene ripulito il codice dalle linee vuote e viene suddiviso in un array di linee tramite gli indicatori di nuova linea. A questo punto il terzo step sarà composto da due cicli for each che scorrendo tutte le linee cercheranno un match con la lista di keywords suscettibili alle vulnerabilità, se trovate salveranno i dati relativi a tale vulnerabilità in un array di oggetti.

**

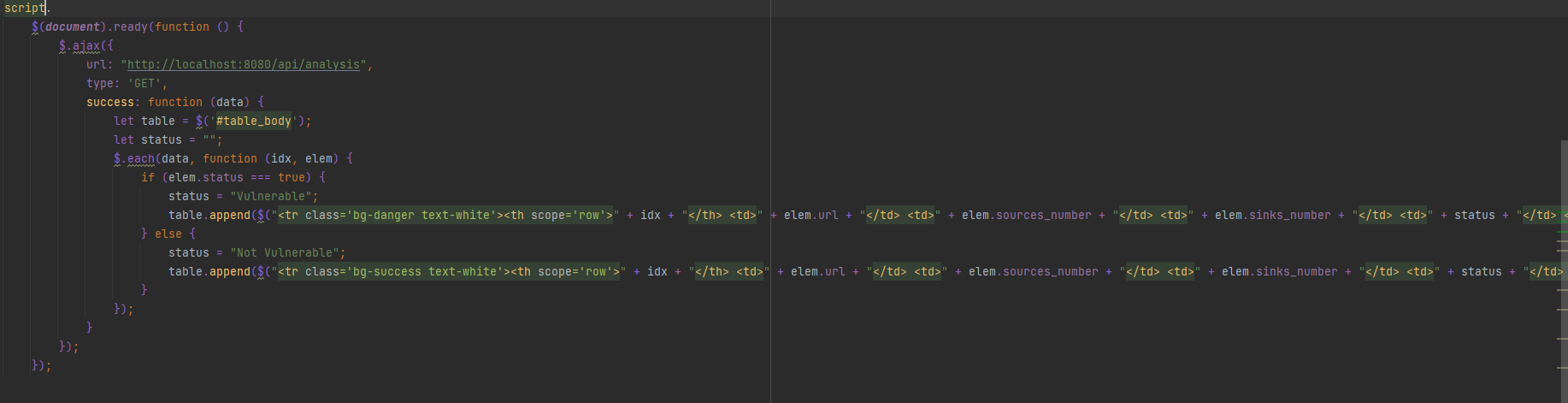
1. Di seguito la funzione che riceverà la URL inserita.

Questa funzione si occuperà di reindirizzare l’utente alla pagina di errore se non viene ricevuta la URL. In caso positivo invece verrà avviato il browser chromium headless e verrà passata l’istanza del browser allo scraper controller che si occuperà come visto in precedenza di recuperare il codice e compiere le analisi.

**

1. Di seguito un frammento di codice raffigurante una chiamata ajax alle API REST rese disponibili dal server.

La chiamata ajax se avrà successo riempirà il corpo della tabella nella pagina recent scan con le righe personalizzate in base ai dati ricevuti dalle api.

**

# Conclusioni

XSS Detector è un sito web che offre ai propri utenti uno strumento difficilmente ritrovabile gratuitamente. Questo strumento di analisi delle vulnerabilità XSS DOM Based rappresenta un punto di riferimento per un operatore nel campo della sicurezza informatica, lo strumento di test incorporato risulta per l’utente molto semplice da utilizzare, il che velocizza tutte le operazioni di analisi del codice sorgente che altrimenti sarebbero svolte manualmente dall’operatore impiegando grandi quantità di tempo.

# Nota bibliografica e sitografica

1. <https://owasp.org/www-community/attacks/DOM_Based_XSS>
2. <http://www.webappsec.org/projects/articles/071105.shtml>
3. <https://brightsec.com/blog/dom-based-xss/>
4. <https://pugjs.org/api/getting-started.html>
5. <https://pdfkit.org/index.html>
6. <https://www.mongodb.com/docs/>