Presentation for Review-I

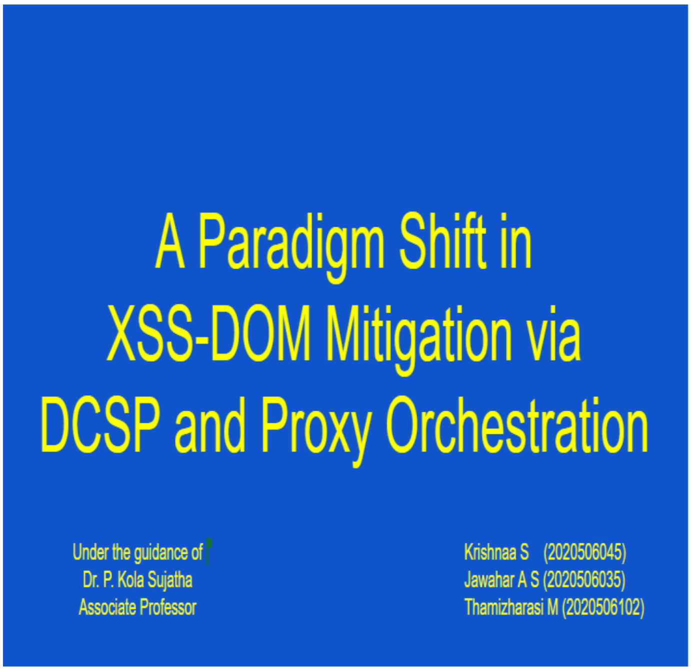
Under the guidance of Dr. P. Kola Sujatha, Associate Professor

Team Members:

Krishnaa S (2020506045)

Jawahar A S (2020506035)

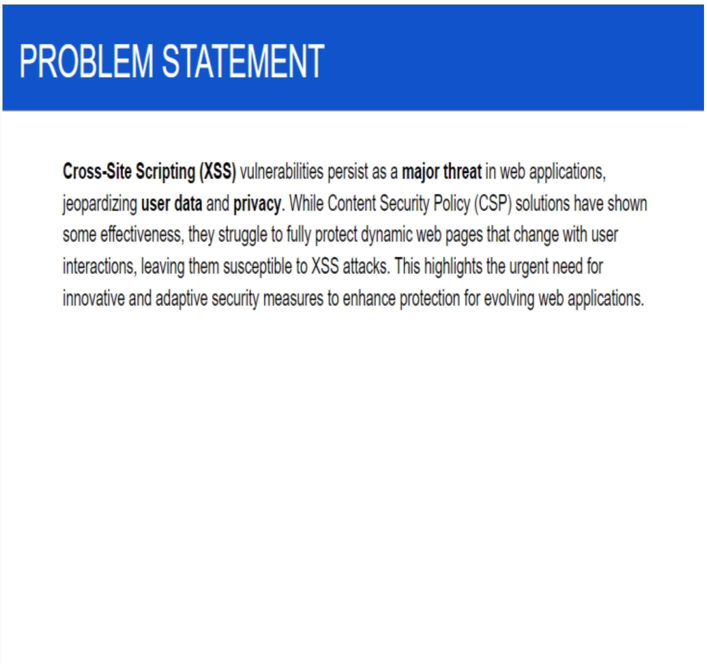
Thamizharasi M (2020506102)



# A Paradigm Shift in XSS-DOM Mitigation via DCSP and Proxy Orchestration

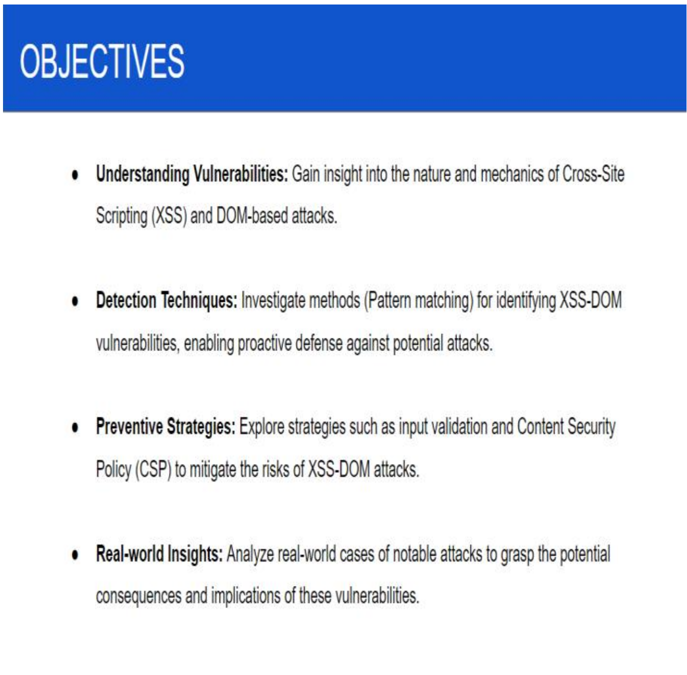
Under the guidance of
Dr. P. Kola Sujatha
Associate Professor

Krishnaa S (2020506045)
Jawahar A S (2020506035)
Thamizharasi M (2020506102)



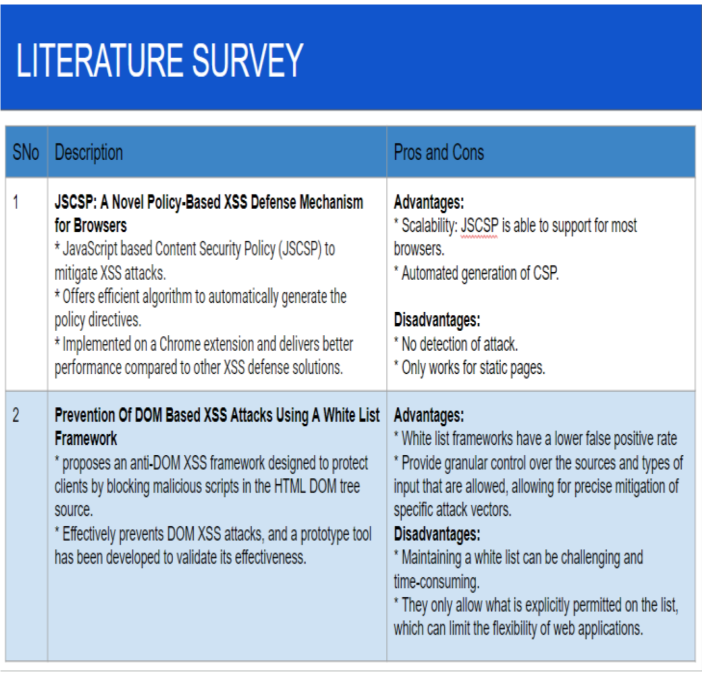
## PROBLEM STATEMENT

**Cross-Site Scripting (XSS)** vulnerabilities persist as a **major threat** in web applications, jeopardizing **user data** and **privacy**. While Content Security Policy (CSP) solutions have shown some effectiveness, they struggle to fully protect dynamic web pages that change with user interactions, leaving them susceptible to XSS attacks. This highlights the urgent need for innovative and adaptive security measures to enhance protection for evolving web applications.



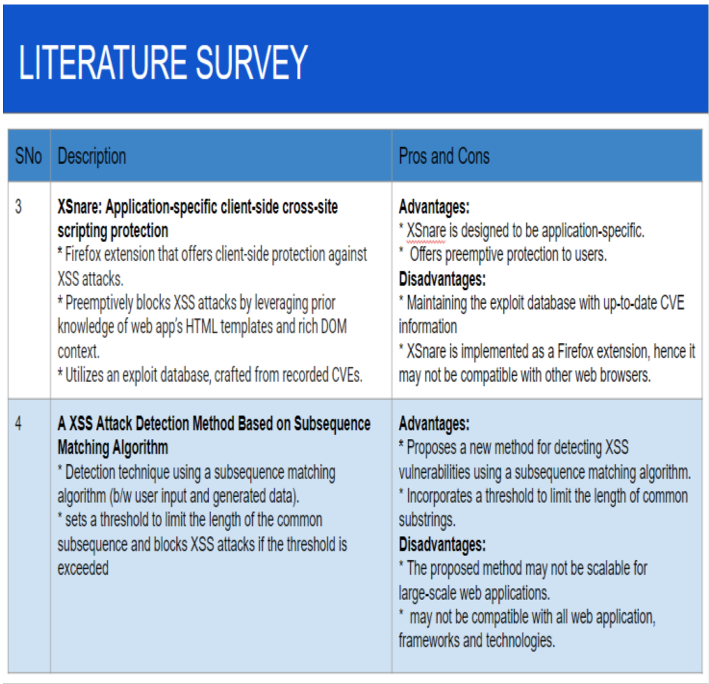
## OBJECTIVES

- **Understanding Vulnerabilities:** Gain insight into the nature and mechanics of Cross-Site Scripting (XSS) and DOM-based attacks.
- **Detection Techniques:** Investigate methods (Pattern matching) for identifying XSS-DOM vulnerabilities, enabling proactive defense against potential attacks.
- **Preventive Strategies:** Explore strategies such as input validation and Content Security Policy (CSP) to mitigate the risks of XSS-DOM attacks.
- **Real-world Insights:** Analyze real-world cases of notable attacks to grasp the potential consequences and implications of these vulnerabilities.



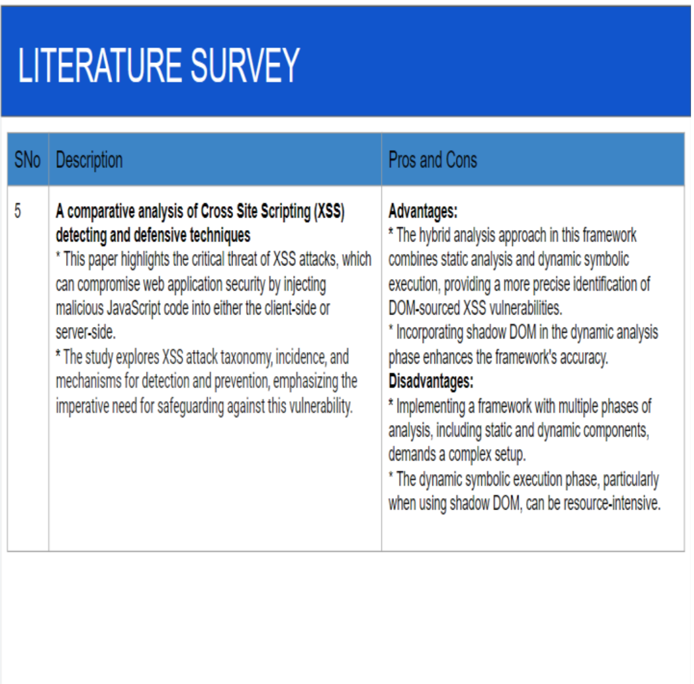
## LITERATURE SURVEY

| SNo | Description | Pros and Cons |
|---|---|---|
| 1 | **JSCSP: A Novel Policy-Based XSS Defense Mechanism for Browsers**<br>* JavaScript based Content Security Policy (JSCSP) to mitigate XSS attacks.<br>* Offers efficient algorithm to automatically generate the policy directives.<br>* Implemented on a Chrome extension and delivers better performance compared to other XSS defense solutions. | **Advantages:**<br>* Scalability: JSCSP is able to support for most browsers.<br>* Automated generation of CSP.<br>**Disadvantages:**<br>* No detection of attack.<br>* Only works for static pages. |
| 2 | **Prevention Of DOM Based XSS Attacks Using A White List Framework**<br>* proposes an anti-DOM XSS framework designed to protect clients by blocking malicious scripts in the HTML DOM tree source.<br>* Effectively prevents DOM XSS attacks, and a prototype tool has been developed to validate its effectiveness. | **Advantages:**<br>* White list frameworks have a lower false positive rate<br>* Provide granular control over the sources and types of input that are allowed, allowing for precise mitigation of specific attack vectors.<br>**Disadvantages:**<br>* Maintaining a white list can be challenging and time-consuming.<br>* They only allow what is explicitly permitted on the list, which can limit the flexibility of web applications. |



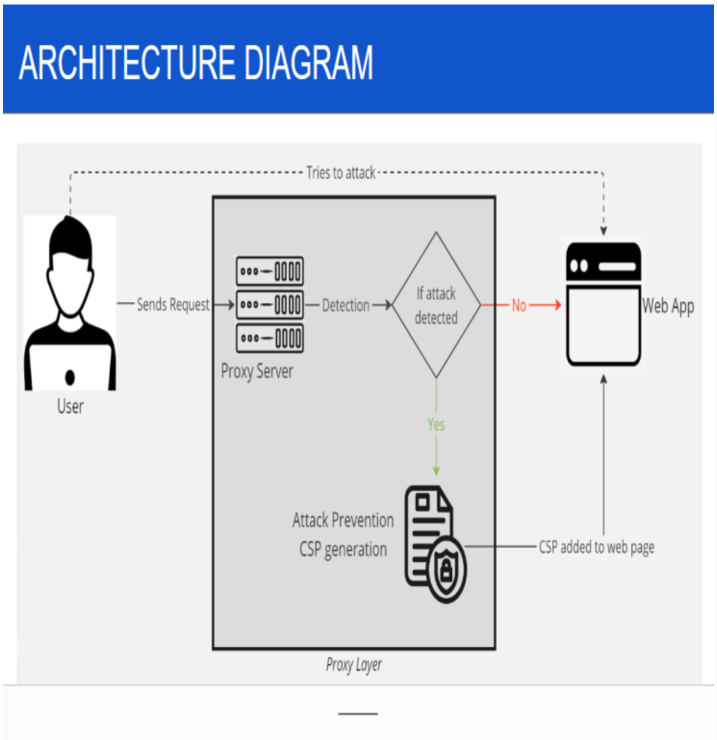
# LITERATURE SURVEY

| SNo | Description | Pros and Cons |
|---|---|---|
| 3 | **XSnare: Application-specific client-side cross-site scripting protection**<br>* Firefox extension that offers client-side protection against XSS attacks.<br>* Preemptively blocks XSS attacks by leveraging prior knowledge of web app's HTML templates and rich DOM context.<br>* Utilizes an exploit database, crafted from recorded CVEs. | **Advantages:**<br>* XSnare is designed to be application-specific.<br>* Offers preemptive protection to users.<br>**Disadvantages:**<br>* Maintaining the exploit database with up-to-date CVE information<br>* XSnare is implemented as a Firefox extension, hence it may not be compatible with other web browsers. |
| 4 | **A XSS Attack Detection Method Based on Subsequence Matching Algorithm**<br>* Detection technique using a subsequence matching algorithm (b/w user input and generated data).<br>* sets a threshold to limit the length of the common subsequence and blocks XSS attacks if the threshold is exceeded | **Advantages:**<br>* Proposes a new method for detecting XSS vulnerabilities using a subsequence matching algorithm.<br>* Incorporates a threshold to limit the length of common substrings.<br>**Disadvantages:**<br>* The proposed method may not be scalable for large-scale web applications.<br>* may not be compatible with all web application, frameworks and technologies. |

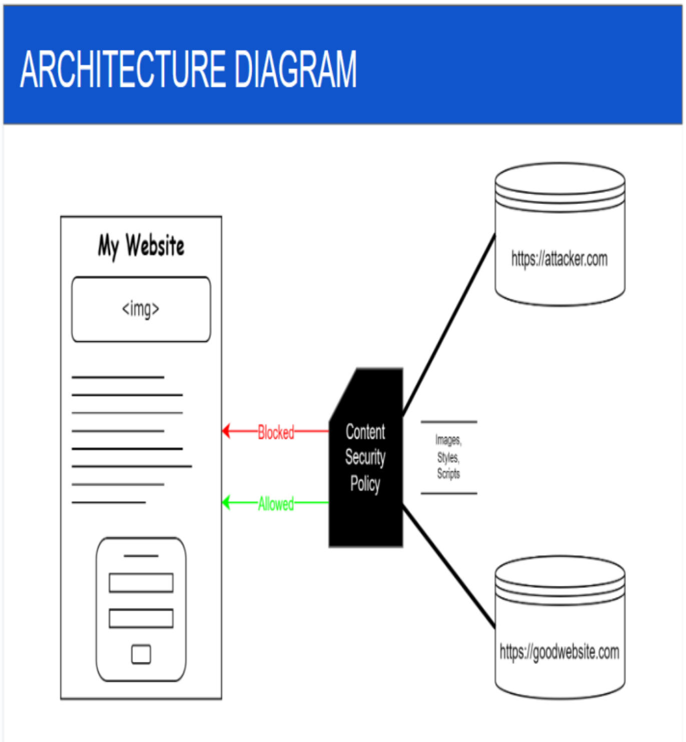


# LITERATURE SURVEY

| SNo | Description | Pros and Cons |
|---|---|---|
| 5 | **A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques**<br>* This paper highlights the critical threat of XSS attacks, which can compromise web application security by injecting malicious JavaScript code into either the client-side or server-side.<br>* The study explores XSS attack taxonomy, incidence, and mechanisms for detection and prevention, emphasizing the imperative need for safeguarding against this vulnerability. | **Advantages:**<br>* The hybrid analysis approach in this framework combines static analysis and dynamic symbolic execution, providing a more precise identification of DOM-sourced XSS vulnerabilities.<br>* Incorporating shadow DOM in the dynamic analysis phase enhances the framework's accuracy.<br>**Disadvantages:**<br>* Implementing a framework with multiple phases of analysis, including static and dynamic components, demands a complex setup.<br>* The dynamic symbolic execution phase, particularly when using shadow DOM, can be resource-intensive. |



# ARCHITECTURE DIAGRAM

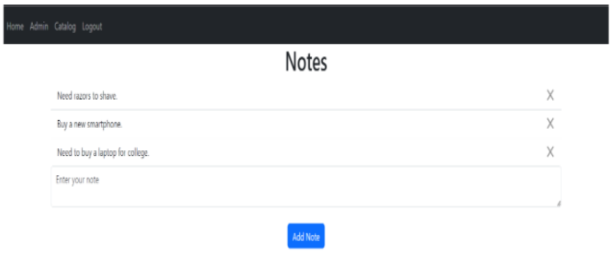


# ARCHITECTURE DIAGRAM

# IMPLEMENTATION

Created a E-Commerce Website to test XSS-DOM Web attack

- In this page we can add notes like shopping list in Amazon



Notes

Need razors to shave.

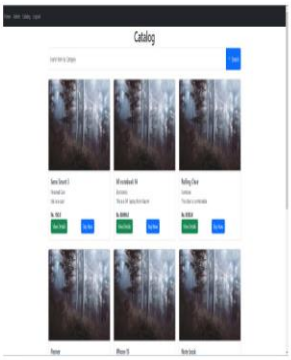
Buy a new smartphone.

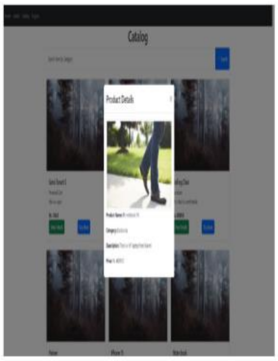
Need to buy a laptop for college.

Enter your note

# IMPLEMENTATION

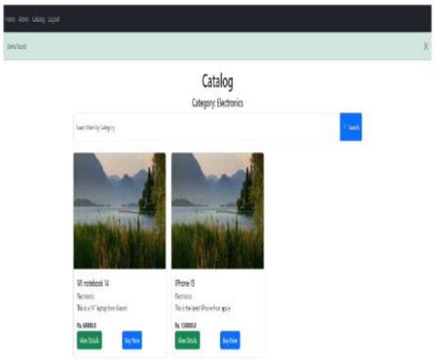
- And we created few more pages with feed option where we can inject the script code to attack the page.





# IMPLEMENTATION

- Search by category page



Items found

Catalog

Category: Electronics

Search Item by Category

MI notebook 14

Electronics

This is a 14" laptop from Xiaomi

Rs. 60000.0

IPhone 15

Electronics

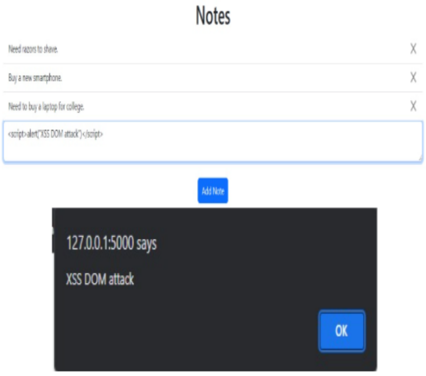
This is the latest IPhone from apple

Rs. 130000.0

# IMPLEMENTATION

Detection of XSS – DOM attack

- In notes page, by feeding the script through the input bar.



Notes

Need razors to shave.

Buy a new smartphone.

Need to buy a laptop for college.

```
<script>alert("XSS DOM attack")</script>
```

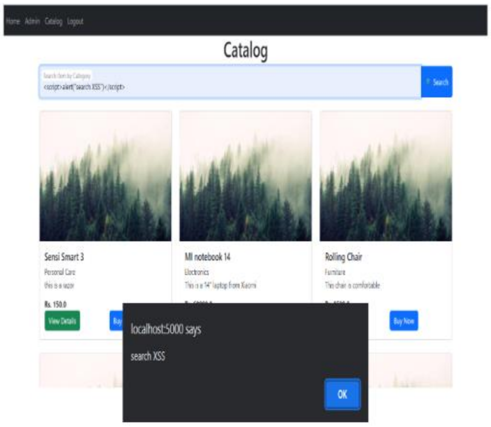
127.0.0.1:5000 says

XSS DOM attack

## IMPLEMENTATION

Detection of XSS – DOM attack

- In User page , by feeding the script through the category search bar. So that will lead to the missing information in the result page.



`<script>alert("search XSS")</script>`

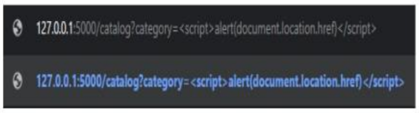
localhost:5000 says

search XSS

## IMPLEMENTATION

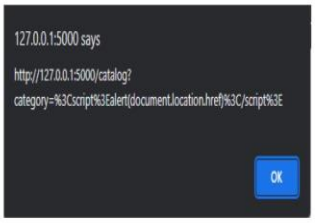
Detection of XSS – DOM attack

- By feeding through the URL.



127.0.0.1:5000/catalog?category=<script>alert(document.location.href)</script>

127.0.0.1:5000/catalog?category=<script>alert(document.location.href)</script>

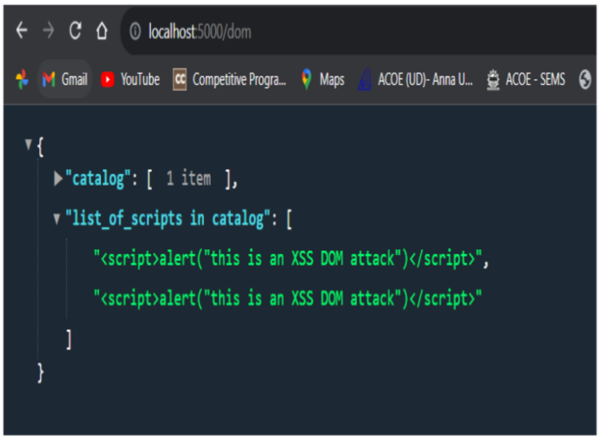


127.0.0.1:5000 says

http://127.0.0.1:5000/catalog?category=%3Cscript%3Ealert(document.location.href)%3C/script%3E

## IMPLEMENTATION

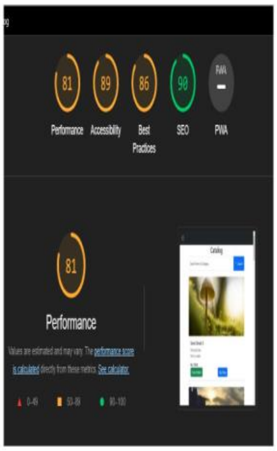
- Detection of XSS – DOM attack using Regular expression and pattern matching



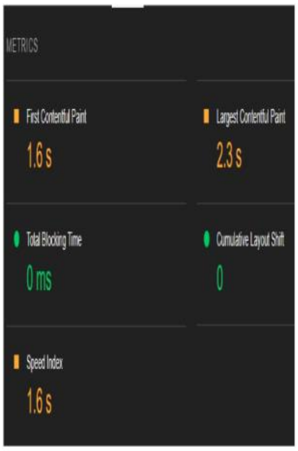
```
▼{
  ▶"catalog": [ 1 item ],
  ▼"list_of_scripts in catalog": [
      "<script>alert("this is an XSS DOM attack")</script>",
      "<script>alert("this is an XSS DOM attack")</script>"
    ]
}
```

## EVALUATION METRICS

- Evaluated our website using Google Lighthouse



81
Performance
89
Accessibility
86
Best Practices
90
SEO
PWA
81
Performance
Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.
0–49
50–89
90–100
Catalog



METRICS

First Contentful Paint 1.6 s

Largest Contentful Paint 2.3 s

Total Blocking Time 0 ms

Cumulative Layout Shift 0

Speed Index 1.6 s

## BENEFITS

- **Uncompromised User Confidence:** Mitigating XSS-DOM vulnerabilities fosters user trust in application's security and reliability.

- **Preserved Data Integrity:** By neutralizing these threats, you maintain the integrity of user data, preventing unauthorized access and tampering.

- **Enhanced Brand Reputation:** A secure application reflects positively on a brand, positioning the owner as a responsible and security-conscious provider.

- **Reduced Legal and Financial Risk:** Preventing attacks helps you avoid potential legal liabilities and financial losses that can arise from data breaches or compromised user information.

## CONTRIBUTION

| | |
|---|---|
| Krishnaa S | • Developed admin and catalog pages<br>• Configured SQLite database<br>• Implemented backend logic with Flask<br>• Integrated attack detection using regex |
| Jawahar A S | • Designed front-end of Notes page |
| Thamizharasi M | • Designed front-end of Login and Sign-up page |

# THANK YOU