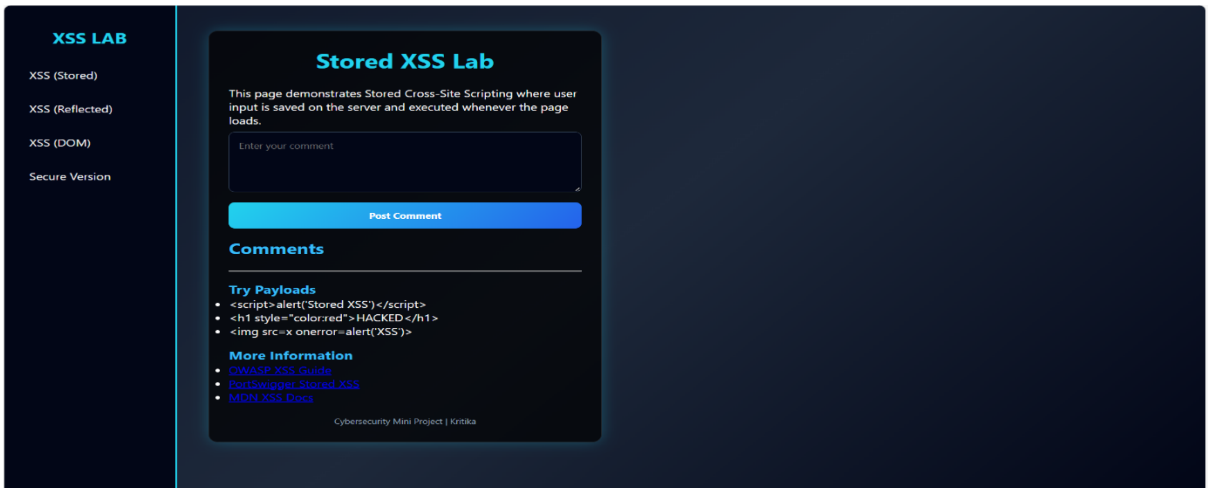
XSS Attack Lab

This document explains the implementation and demonstration of CrossSite Scripting (XSS) vulnerabilities using a Node.js and Express based lab environment. The project shows Stored XSS, Reflected XSS, DOM Based XSS and a Secure version to demonstrate prevention techniques.

Stored XSS Demonstration

Stored XSS occurs when user input is stored on the server and executed whenever the page loads. In this lab, comments are saved and rendered without sanitization, allowing scripts to execute.



Stored XSS Lab

This page demonstrates Stored Cross-Site Scripting where user input is saved on the server and executed whenever the page loads.

Comments

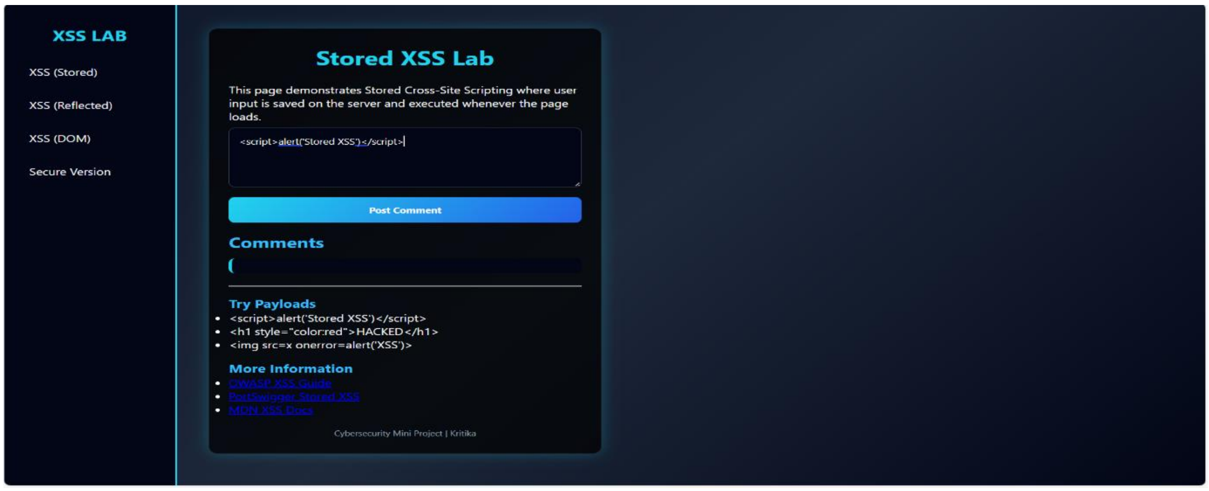
Try Payloads

- <script>alert('Stored XSS')</script>
- <h1 style="color:red">HACKED</h1>
- <img src=x onerror=alert('XSS')>

More Information

- OWASP XSS Guide
- PortSwigger Stored XSS
- MDN XSS Docs

Cybersecurity Mini Project | Kritika



Stored XSS Lab

This page demonstrates Stored Cross-Site Scripting where user input is saved on the server and executed whenever the page loads.

```
<script>alert('Stored XSS')</script>
```

Comments

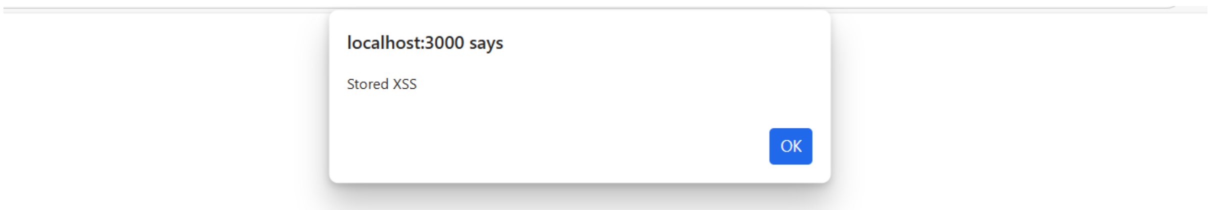
Try Payloads

- <script>alert('Stored XSS')</script>
- <h1 style="color:red">HACKED</h1>
- <img src=x onerror=alert('XSS')>

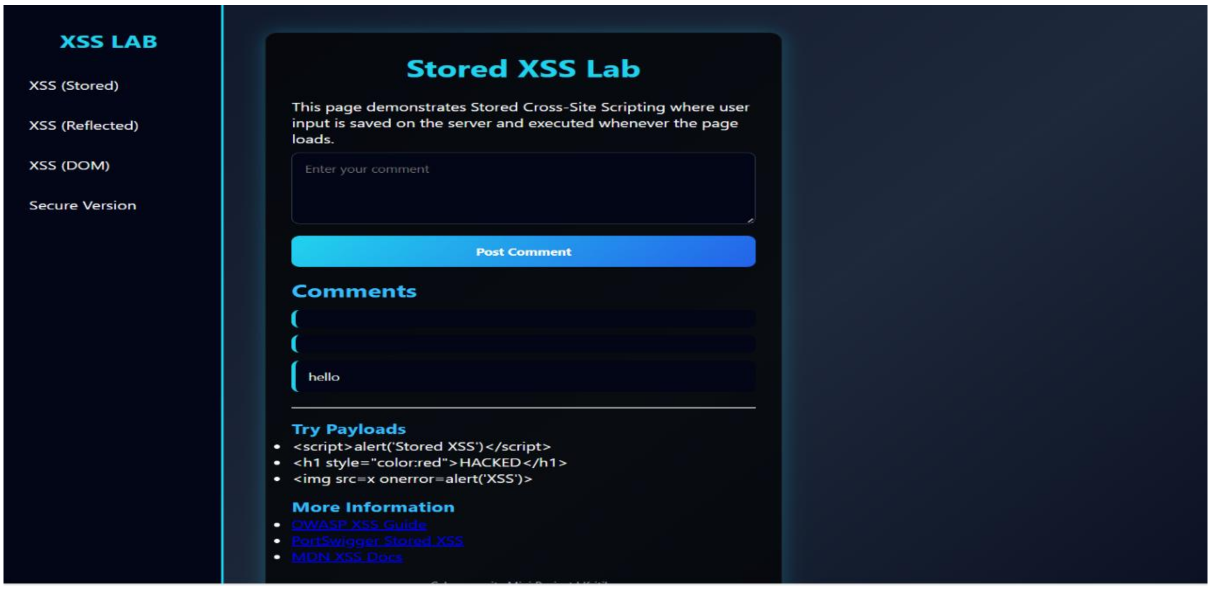
More Information

- OWASP XSS Guide
- PortSwigger Stored XSS
- MDN XSS Docs

Cybersecurity Mini Project | Kritika


localhost:3000 says

Stored XSS



Stored XSS Lab

This page demonstrates Stored Cross-Site Scripting where user input is saved on the server and executed whenever the page loads.

Comments

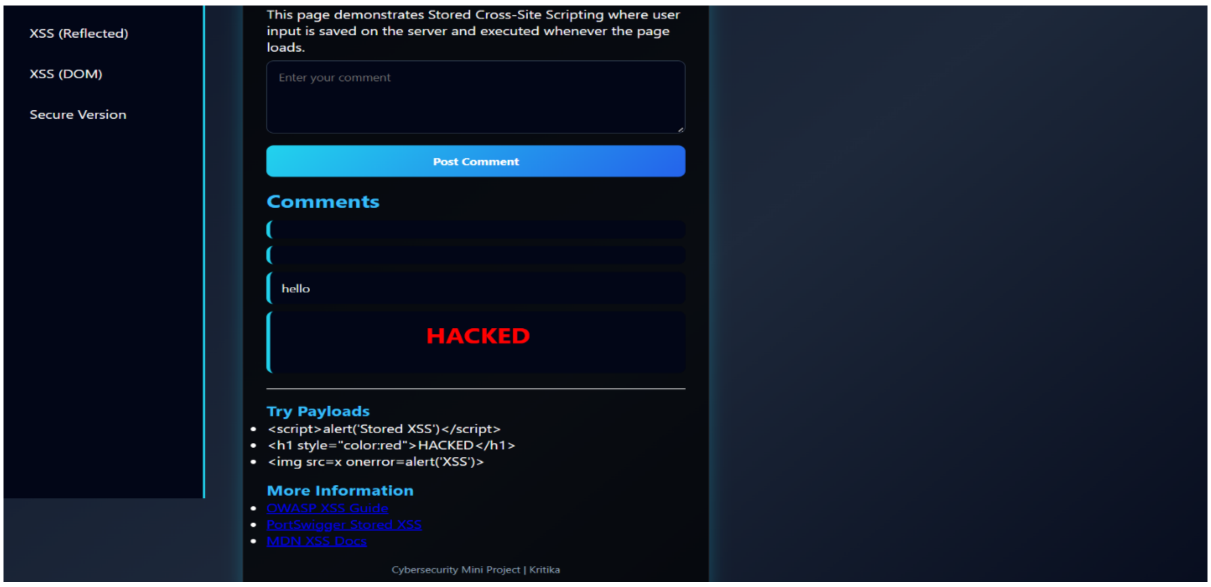
hello

Try Payloads

- <script>alert('Stored XSS')</script>
- <h1 style="color:red">HACKED</h1>
- <img src=x onerror=alert('XSS')>

More Information

- OWASP XSS Guide
- PortSwigger Stored XSS
- MDN XSS Docs



This page demonstrates Stored Cross-Site Scripting where user input is saved on the server and executed whenever the page loads.

Comments

hello

HACKED

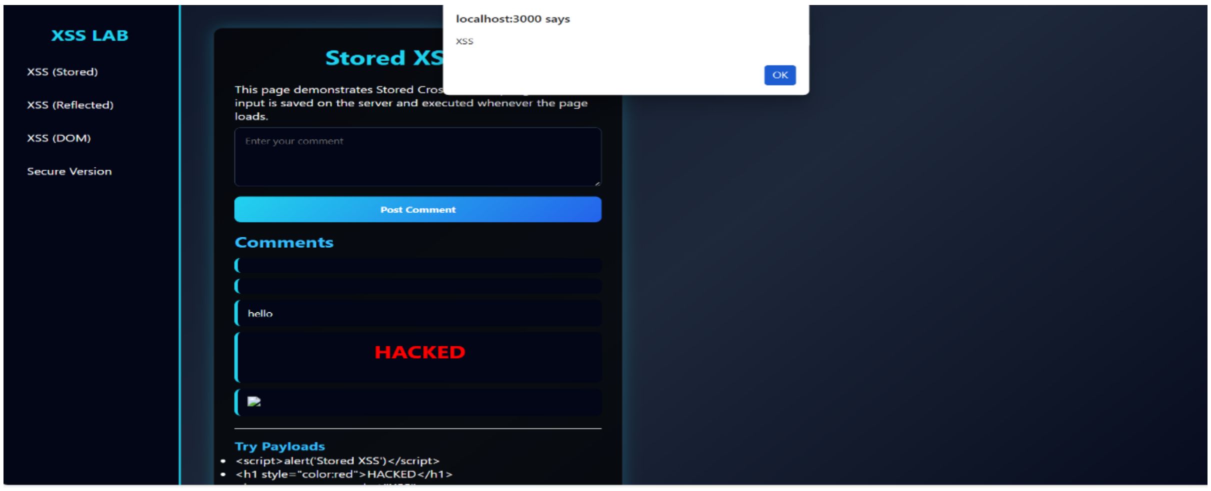
Try Payloads

- <script>alert('Stored XSS')</script>
- <h1 style="color:red">HACKED</h1>
- <img src=x onerror=alert('XSS')>

More Information

- OWASP XSS Guide
- PortSwigger Stored XSS
- MDN XSS Docs

Cybersecurity Mini Project | Kritika



localhost:3000 says

xss

This page demonstrates Stored Cros
input is saved on the server and executed whenever the page
loads.

hello

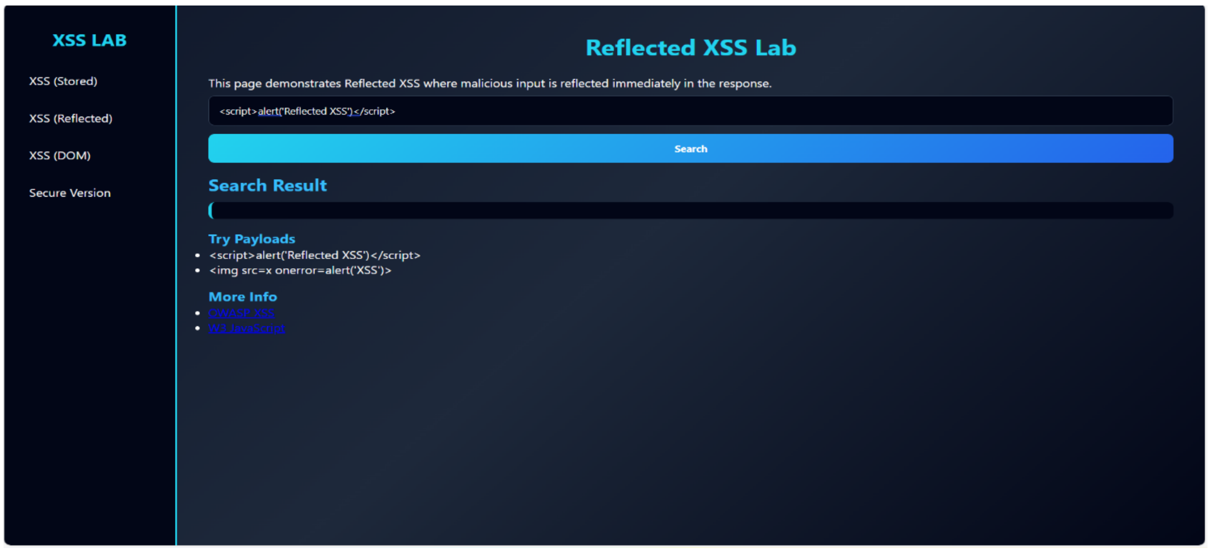
HACKED

Try Payloads

- <script>alert('Stored XSS')</script>
- <h1 style="color:red">HACKED</h1>

Reflected XSS Demonstration

Reflected XSS happens when user input is immediately returned in the response. The attack runs instantly when a crafted input is submitted



Reflected XSS Lab

This page demonstrates Reflected XSS where malicious input is reflected immediately in the response.

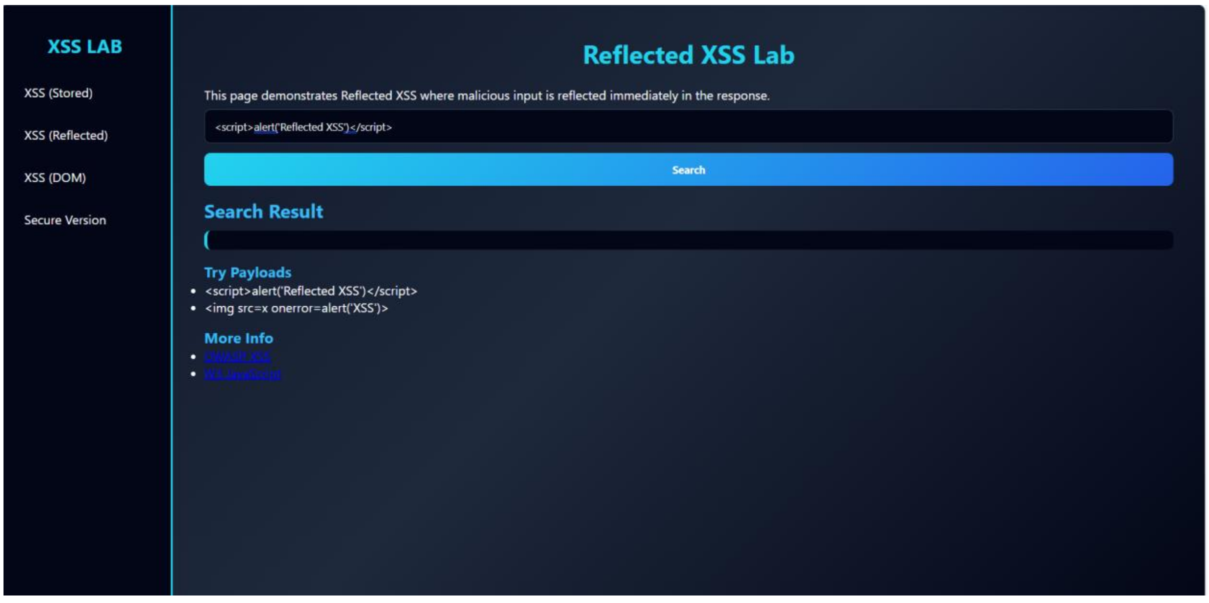
```
<script>alert('Reflected XSS')</script>
```

Try Payloads

- <script>alert('Reflected XSS')</script>
- <img src=x onerror=alert('XSS')>

More Info

- OWASP XSS
- W3 JavaScript



Reflected XSS Lab

This page demonstrates Reflected XSS where malicious input is reflected immediately in the response.

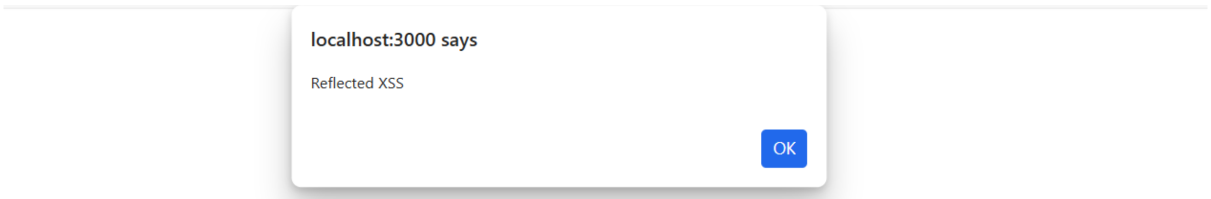
```
<script>alert('Reflected XSS')</script>
```

Try Payloads

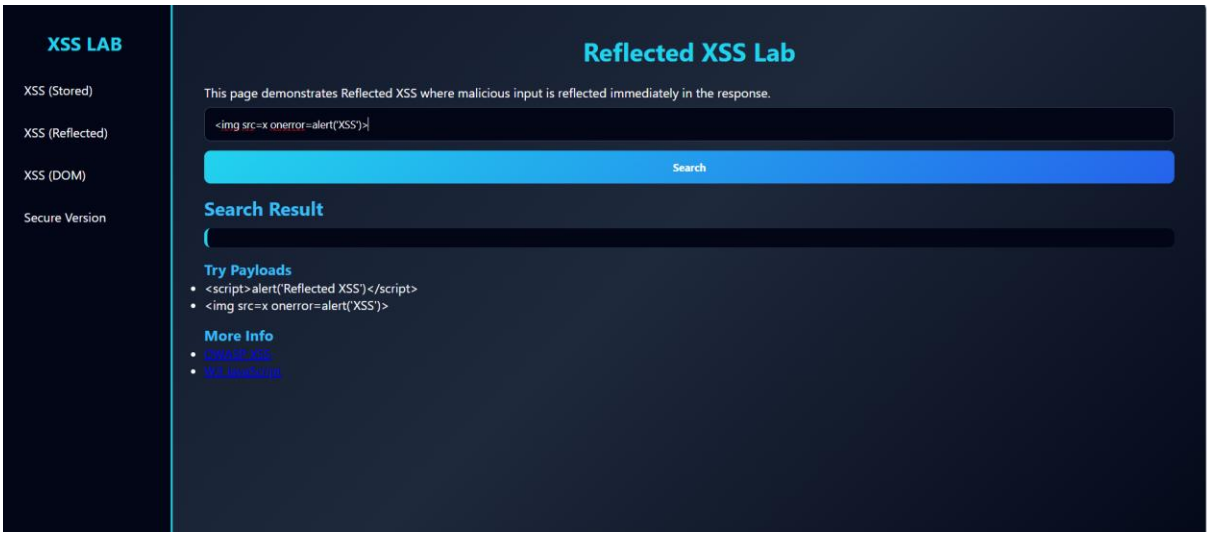
- <script>alert('Reflected XSS')</script>
- <img src=x onerror=alert('XSS')>

More Info

- OWASP XSS
- W3 JavaScript


localhost:3000 says

Reflected XSS



Reflected XSS Lab

This page demonstrates Reflected XSS where malicious input is reflected immediately in the response.

```
<img src=x onerror=alert('XSS')>
```

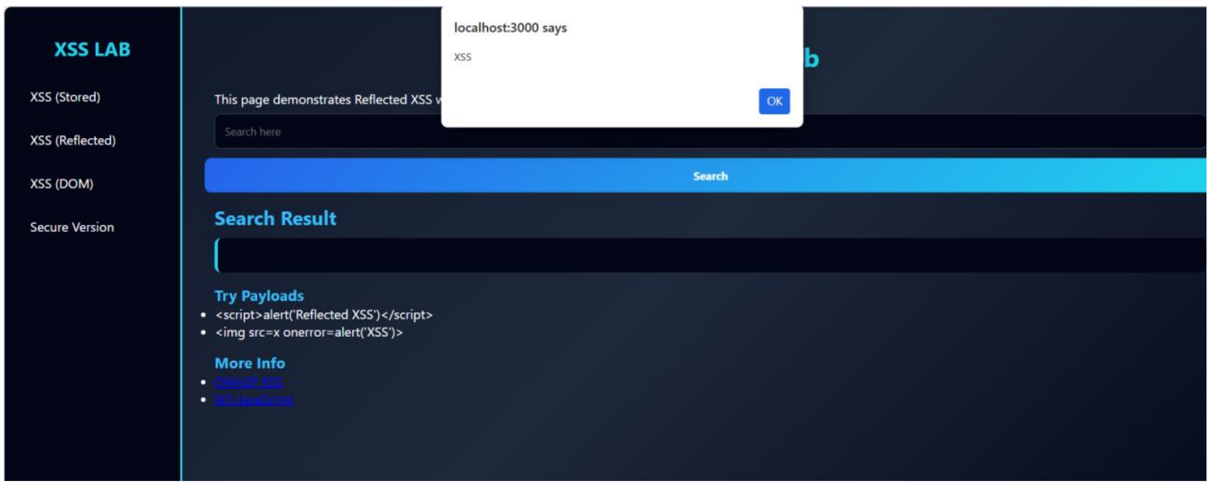
Search Result

Try Payloads

- <script>alert('Reflected XSS')</script>
- <img src=x onerror=alert('XSS')>

More Info

- OWASP XSS
- W3 JavaScript



localhost:3000 says

XSS

This page demonstrates Reflected XSS v

Search Result

Try Payloads

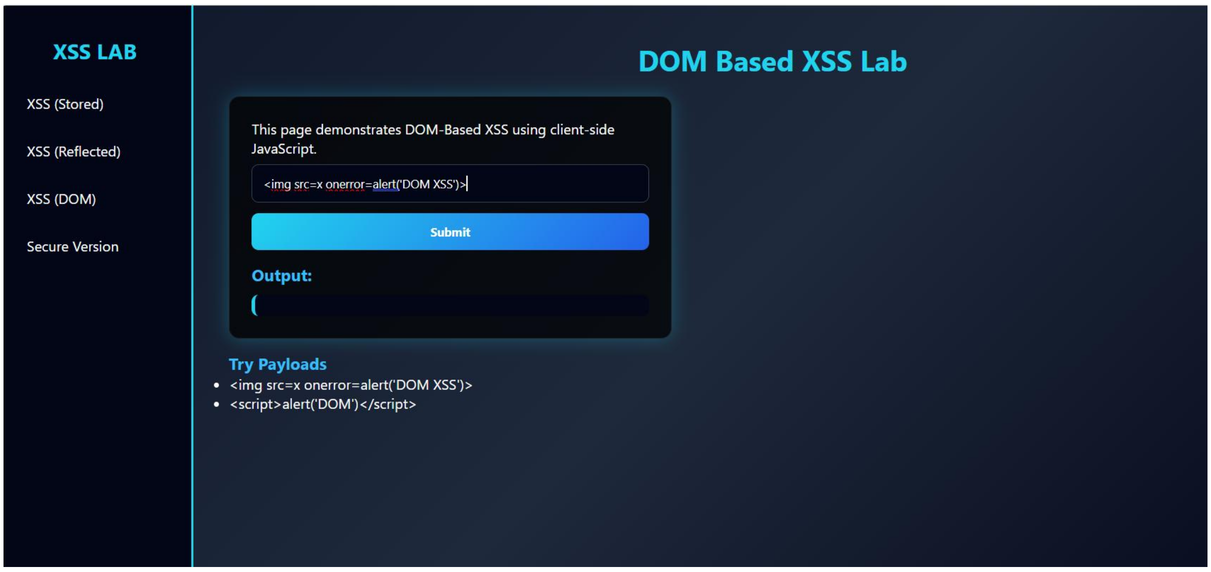
- <script>alert('Reflected XSS')</script>
- <img src=x onerror=alert('XSS')>

More Info

- OWASP XSS
- W3 JavaScript

DOM XSS Demonstration

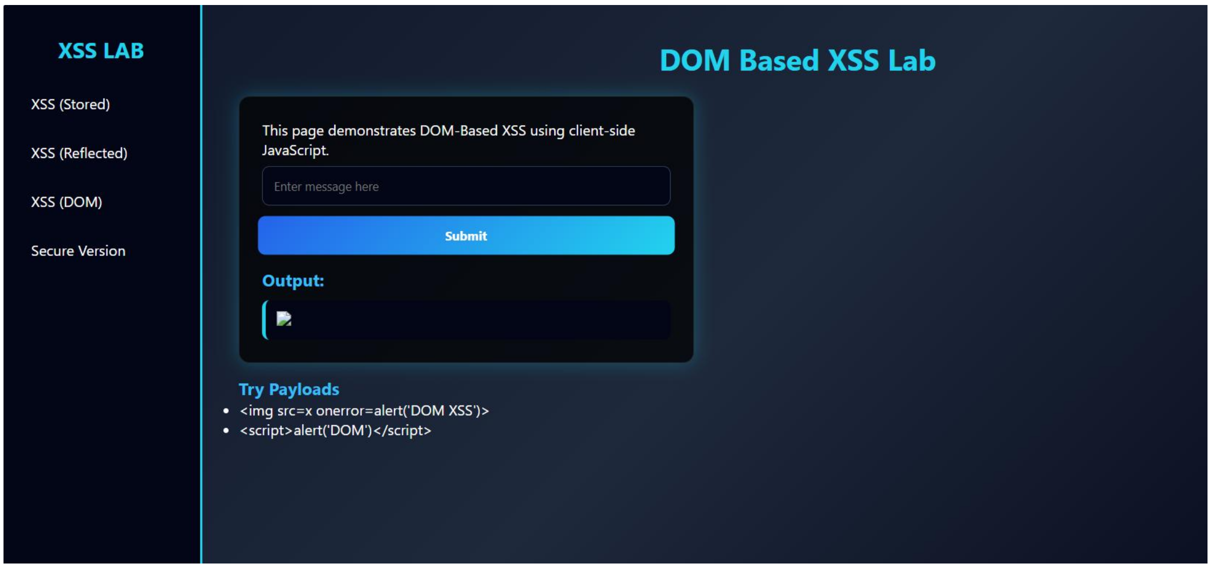
DOM Based XSS occurs entirely on the client side when JavaScript dynamically modifies page content using unsafe user input



This page demonstrates DOM-Based XSS using client-side JavaScript.

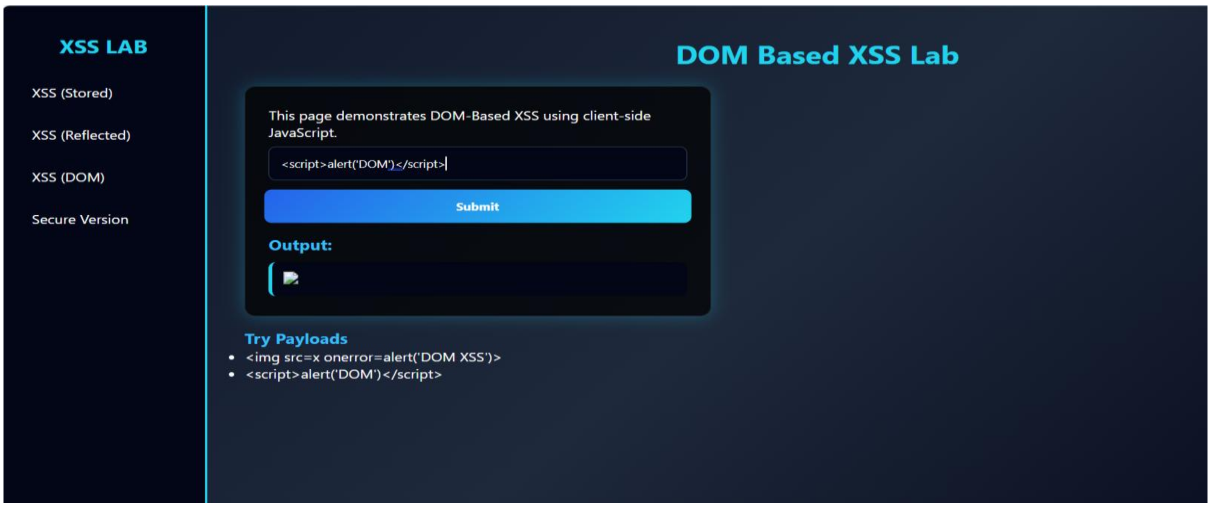
```
<img src=x onerror=alert('DOM XSS')>
```

- <img src=x onerror=alert('DOM XSS')>
- <script>alert('DOM')</script>



This page demonstrates DOM-Based XSS using client-side JavaScript.

- <img src=x onerror=alert('DOM XSS')>
- <script>alert('DOM')</script>



DOM Based XSS Lab

This page demonstrates DOM-Based XSS using client-side JavaScript.

```
<script>alert('DOM')</script>
```

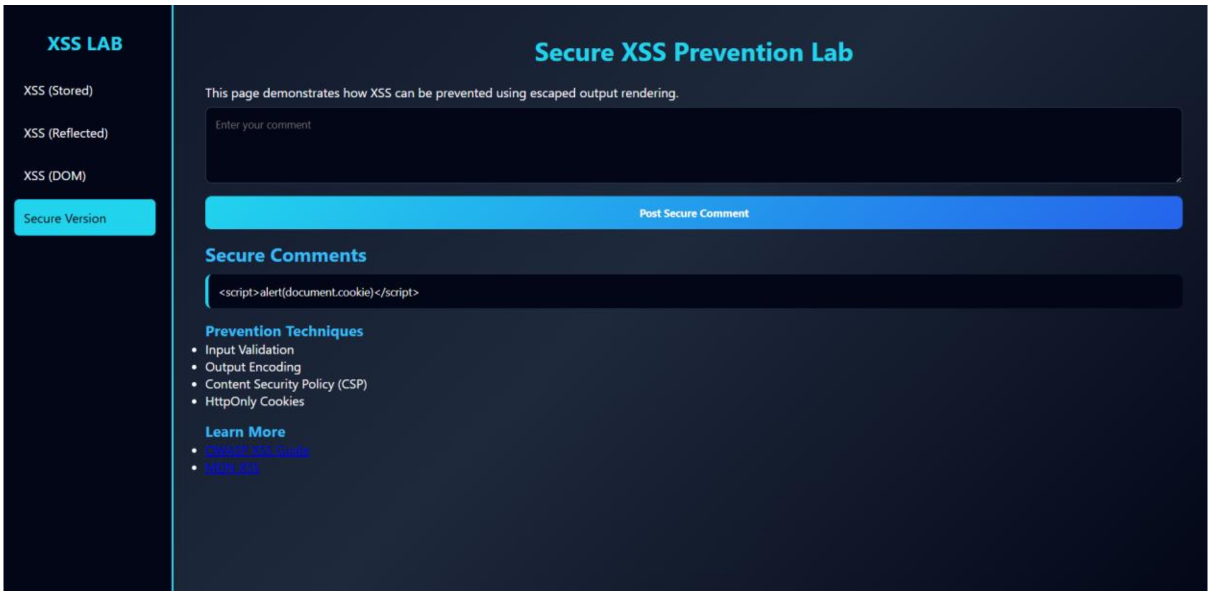
Output:

Try Payloads

- `<img src=x onerror=alert('DOM XSS')>`
- `<script>alert('DOM')</script>`

Secure Version Demonstration

The secure page shows how output encoding and safe rendering prevent script execution



Secure XSS Prevention Lab

This page demonstrates how XSS can be prevented using escaped output rendering.

Secure Comments

```
<script>alert(document.cookie)</script>
```

Prevention Techniques

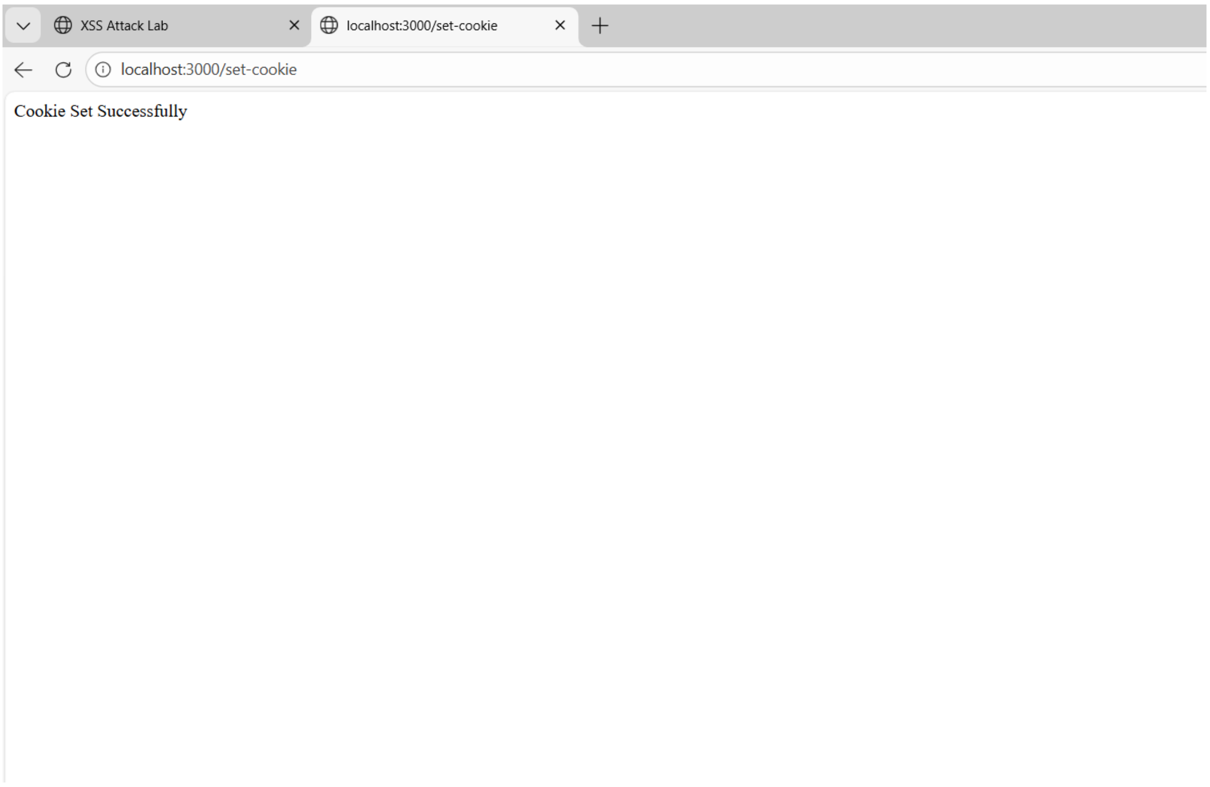
- Input Validation
- Output Encoding
- Content Security Policy (CSP)
- HttpOnly Cookies

Learn More

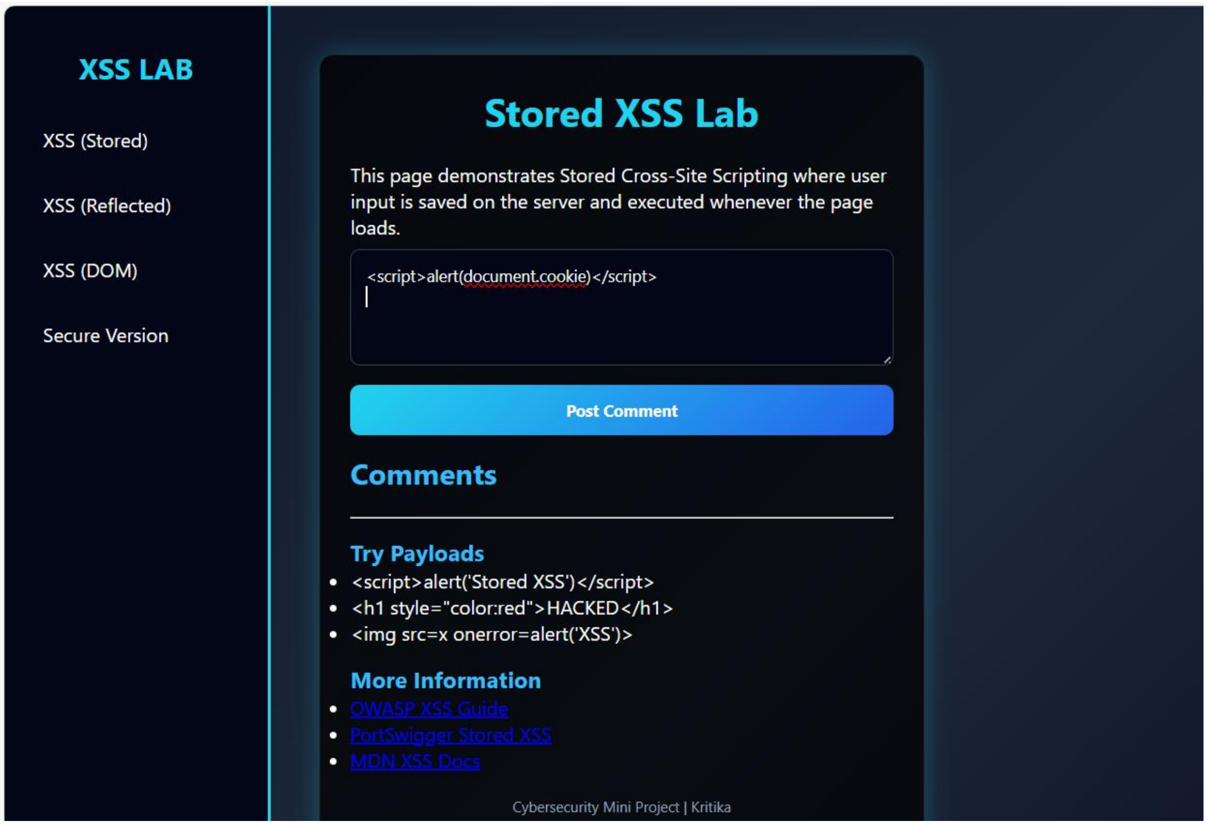
- OWASP XSS Guide
- MDN XSS

Cookie / Session Exposure Demonstration

This section demonstrates how XSS can expose cookies using document.cookie. A demo cookie is set and then accessed via JavaScript payload.



Cookie Set Successfully



Stored XSS Lab

This page demonstrates Stored Cross-Site Scripting where user input is saved on the server and executed whenever the page loads.

```
<script>alert(document.cookie)</script>
```

Comments

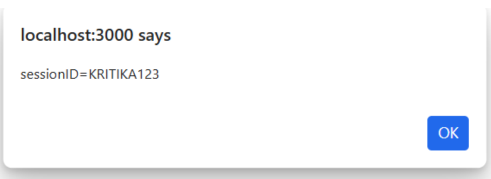
Try Payloads

- `<script>alert('Stored XSS')</script>`
- `<h1 style="color:red">HACKED</h1>`
- `<img src=x onerror=alert('XSS')>`

More Information

- OWASP XSS Guide
- PortSwigger Stored XSS
- MDN XSS Docs

Cybersecurity Mini Project | Kritika



```
localhost:3000 says

sessionID=KRITIKA123
```