

**NAME:k.jayanth**

**REG NO:** 19bci7021

Lab-5

### **Types of XSS**

1. Reflected XSS: Inputs gets reflected
- 



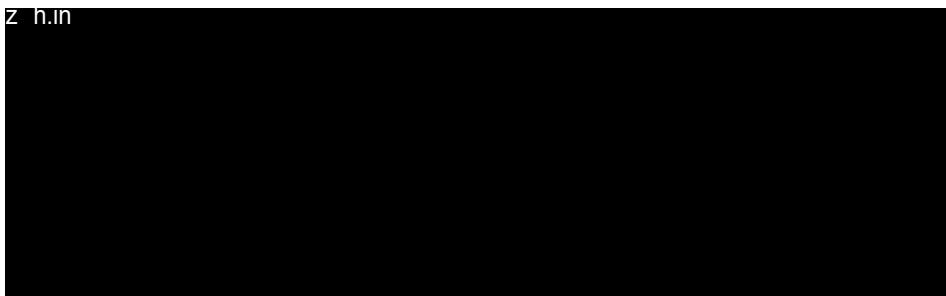
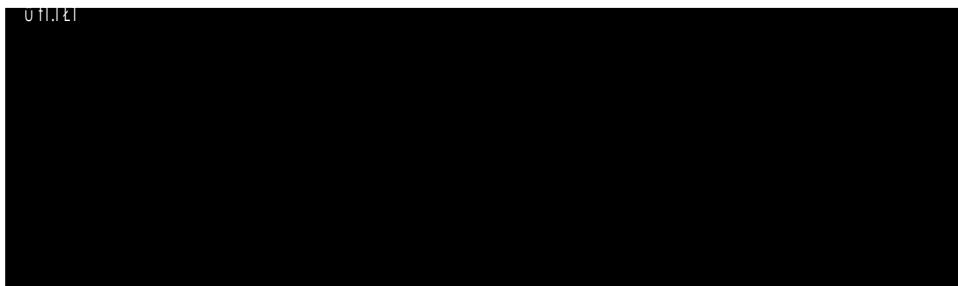
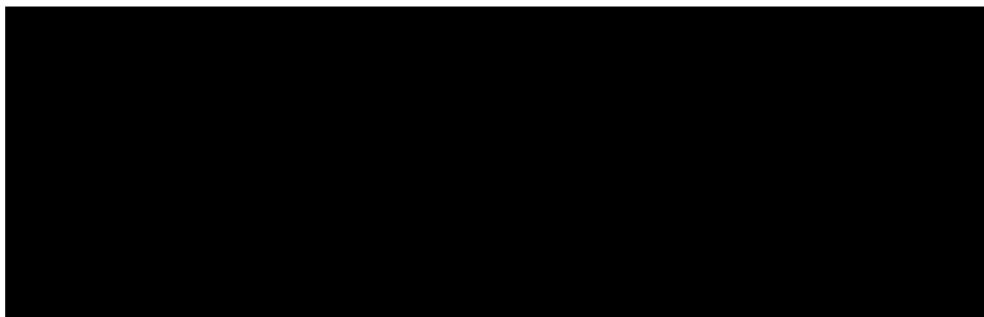
Sorry, no results were found for **amazon**. [Try again.](#)



Sorry, no results were found for **amazon**. [Try again.](#)

# b«kaz1iixn

Sorry, no results were found for  
amazon  
. Tory aeain.

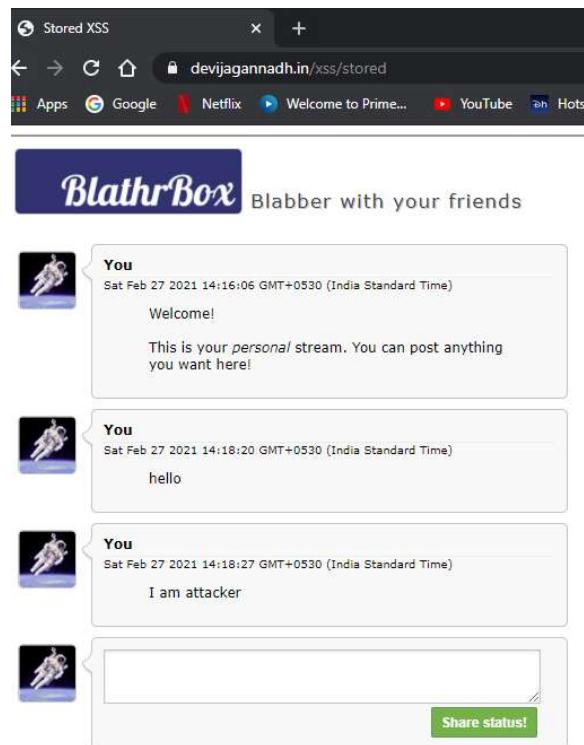


And in TripAdvisor website:

The image contains three screenshots of a web browser showing reflected XSS attacks on the TripAdvisor website.

- Screenshot 1:** A screenshot of a local file (c.html) in a browser. The page displays a "This page says" alert box containing the text "1". Below it is the TripAdvisor search bar with the placeholder "Search Tripadvisor".
- Screenshot 2:** A screenshot of the TripAdvisor website at tripadvisor.in/Search?q="reflectedxss"><img%20src%3Dx%20onerror%3Dalert(1)>&search... The page displays a "www.tripadvisor.in says" alert box containing the text "1". Below it is the TripAdvisor search bar with the query " "reflectedxss"><img src=x onerror=alert(1)>" highlighted.
- Screenshot 3:** A screenshot of the TripAdvisor website at https://www.tripadvisor.in. The page displays a "www.tripadvisor.in says" alert box containing the text "1". Below it is the TripAdvisor search bar with the query " "reflectedxss"><img src=x onerror=alert(1)>" highlighted. The browser's developer tools are open, showing the reflected payload in the network tab.

## 2. Stored XSS: Input gets stored in server



The screenshot shows a web browser window with the title "Stored XSS". The address bar displays "devijagannadh.in/xss/stored". Below the address bar, there are several icons for various websites like Apps, Google, Netflix, Prime, YouTube, and Hots.

The main content area shows a social media-like interface for "BlathrBox". It has a dark blue header with the text "BlathrBox" and "Blabber with your friends". The interface consists of a list of posts from a user named "You".

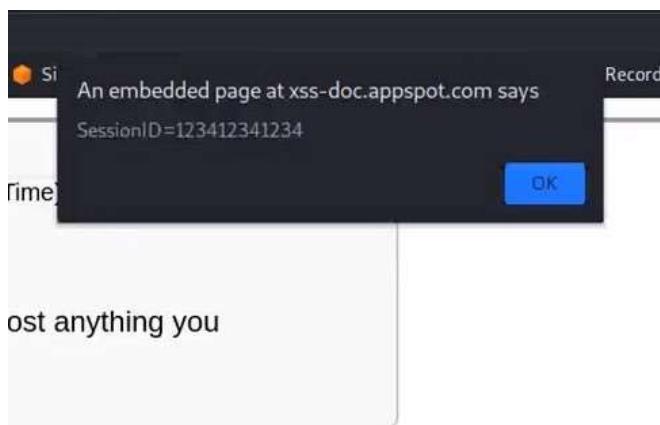
- You**  
Sat Feb 27 2021 14:16:06 GMT+0530 (India Standard Time)  
Welcome!  
This is your *personal stream*. You can post anything you want here!
- You**  
Sat Feb 27 2021 14:18:20 GMT+0530 (India Standard Time)  
hello
- You**  
Sat Feb 27 2021 14:18:27 GMT+0530 (India Standard Time)  
I am attacker
- You**  
  
**Share status!**

The screenshot shows a web browser with two tabs open, both titled "Stored XSS". The active tab's address bar shows "devijagannadh.in/xss/stored". The page content is from a site called "BlathrBox" with the tagline "Blabber with your friends". The interface consists of a list of messages from a user named "You". Each message includes a timestamp, a profile icon of a person on a rocket, and the message text. The messages are:

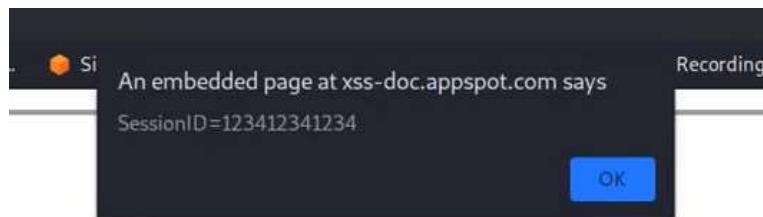
- Sat Feb 27 2021 14:16:06 GMT+0530 (India Standard Time)  
Welcome!  
This is your *personal* stream. You can post anything you want here!
- Sat Feb 27 2021 14:18:20 GMT+0530 (India Standard Time)  
hello
- Sat Feb 27 2021 14:18:27 GMT+0530 (India Standard Time)  
I am attacker
- Sat Feb 27 2021 14:19:26 GMT+0530 (India Standard Time)  
Hello, I am victim

At the bottom, there is a text input field with a placeholder "Post anything you want here!" and a green "Share status!" button.

At attacker side after applying payload:

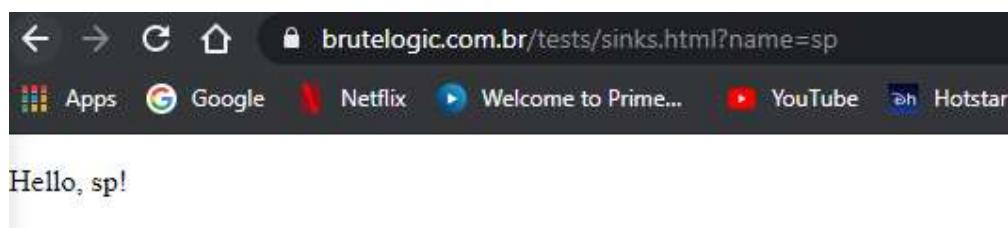


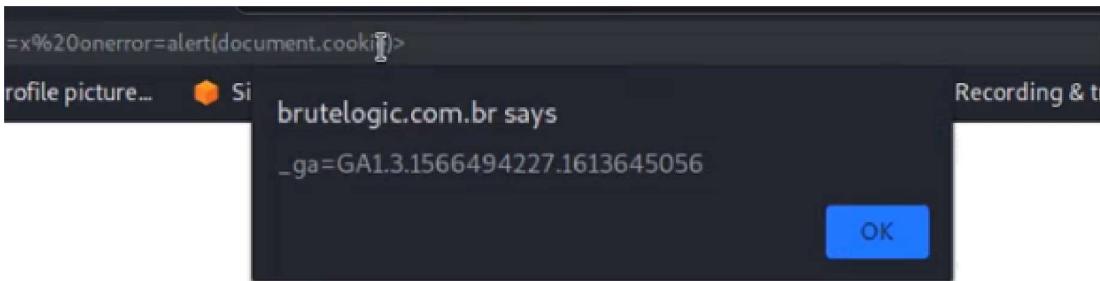
At receiver side:



your friends

### 3.Dom XSS: Input gets stored in Dom





brutelogic.com.br

**Placements shine on our U<sup>S</sup> Graduating Batch**

#### **OUR RECRUITERS**

**“I ÖY ž Öé ēl žia aā 1 ÖE E ži =° Tz E i c i g”**

