# LAB-5

NAME:S.BHAVYA SREE
REG.NO:19BCN7257

- ## How Securing coding is related to XSS:
    Firstly XSS has a vulnerability which gets fired due the poor checks and validation of user.every web developer uses Java Script and Html to build the website, but attacker can use some evil payloads of JS and inject them in the website (which may be at client level or at backend database level) mainly in the user input fields and he get some user cookies or redirecting user to another website or he can inject some own malicious script for his own benifits.So its a responsibility of Developer to check weather javascript code executing the attackers payload or not and should also sanatise or do escaping of some characters and should blacklist some common malicious words used in evil payloads.
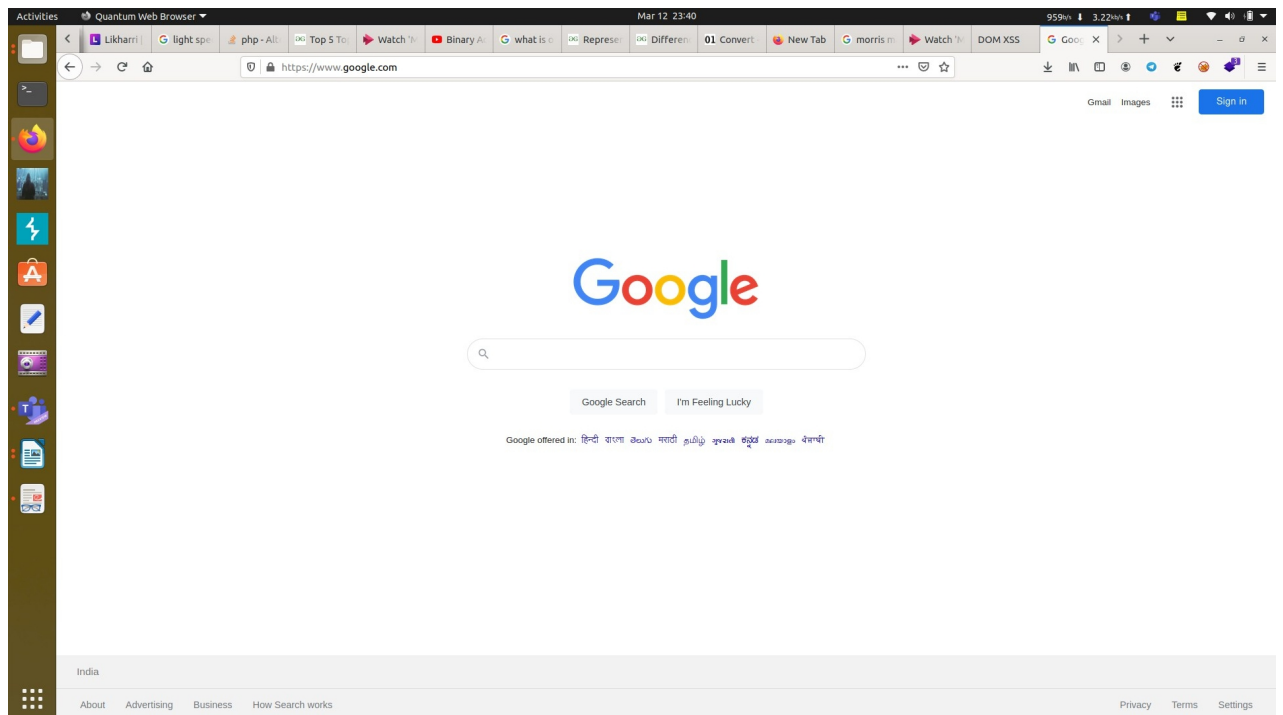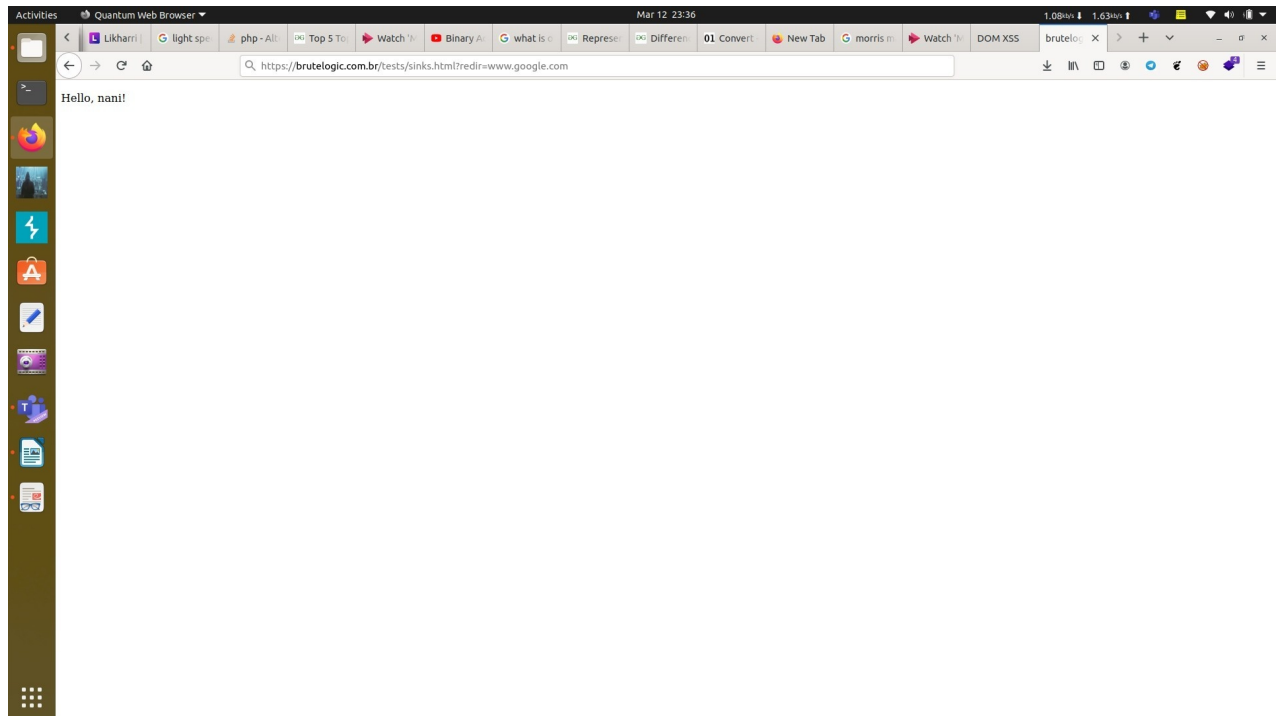
Reflected XSS:

Stored XSS:

DOM XSS:

Hello, nani!
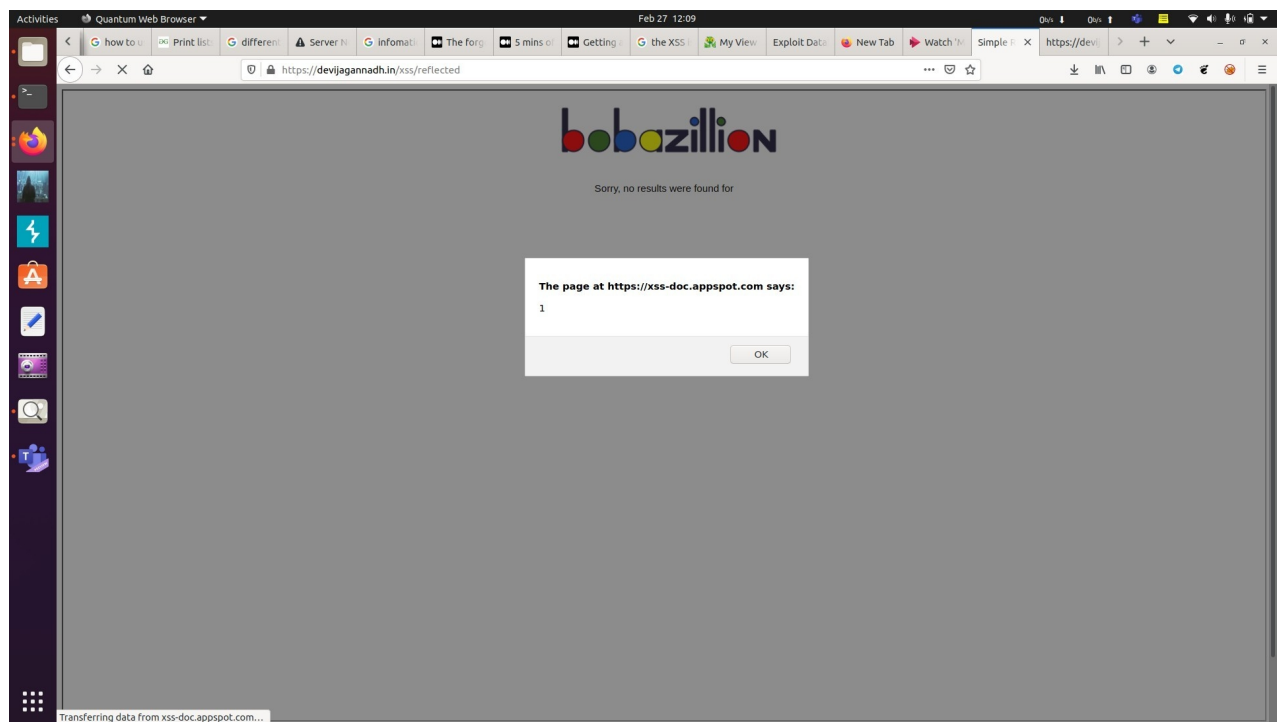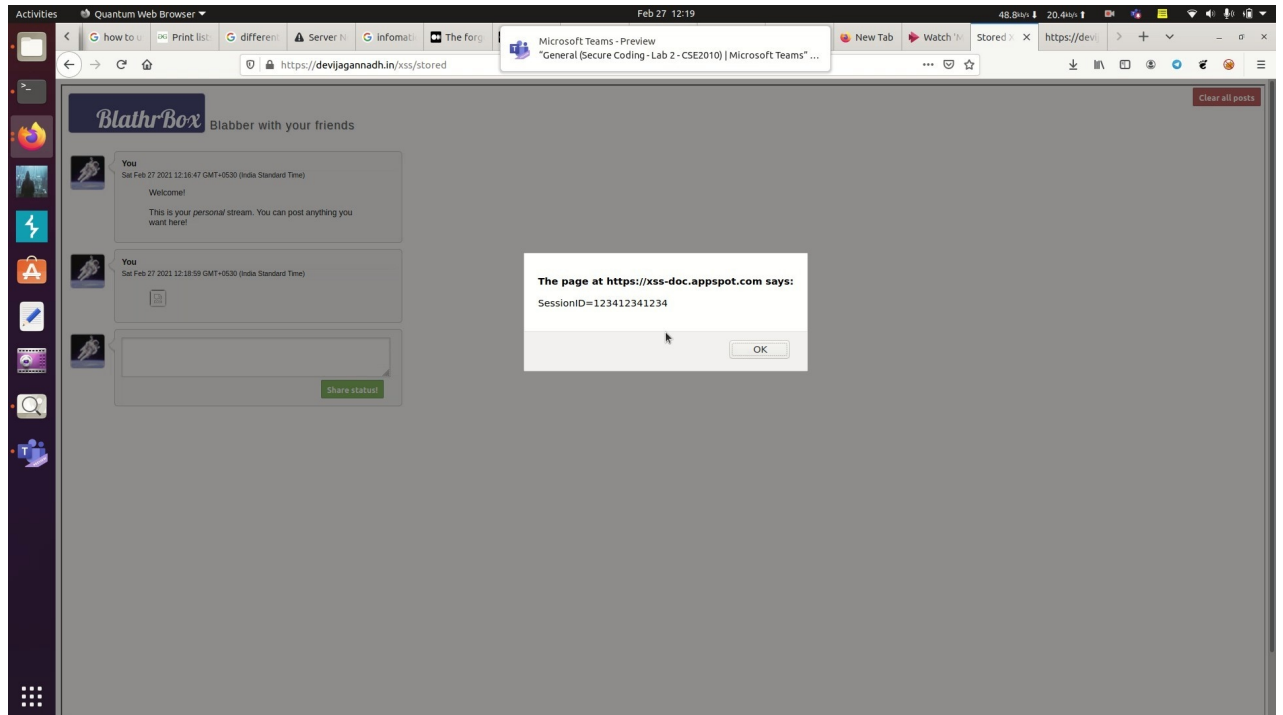
alf.nu:

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  return '<script>console.log("'+s+'");</script>';
}
```

Input 36

```
")</script><script>alert(1)</script>
```

Output Win!

```
<script>console.log("")</script><script>alert(1)</script>");</script>
```

Rate this level: ★★★★★

Warmup (36)
Adobe
JSON

User	Score	Browser