

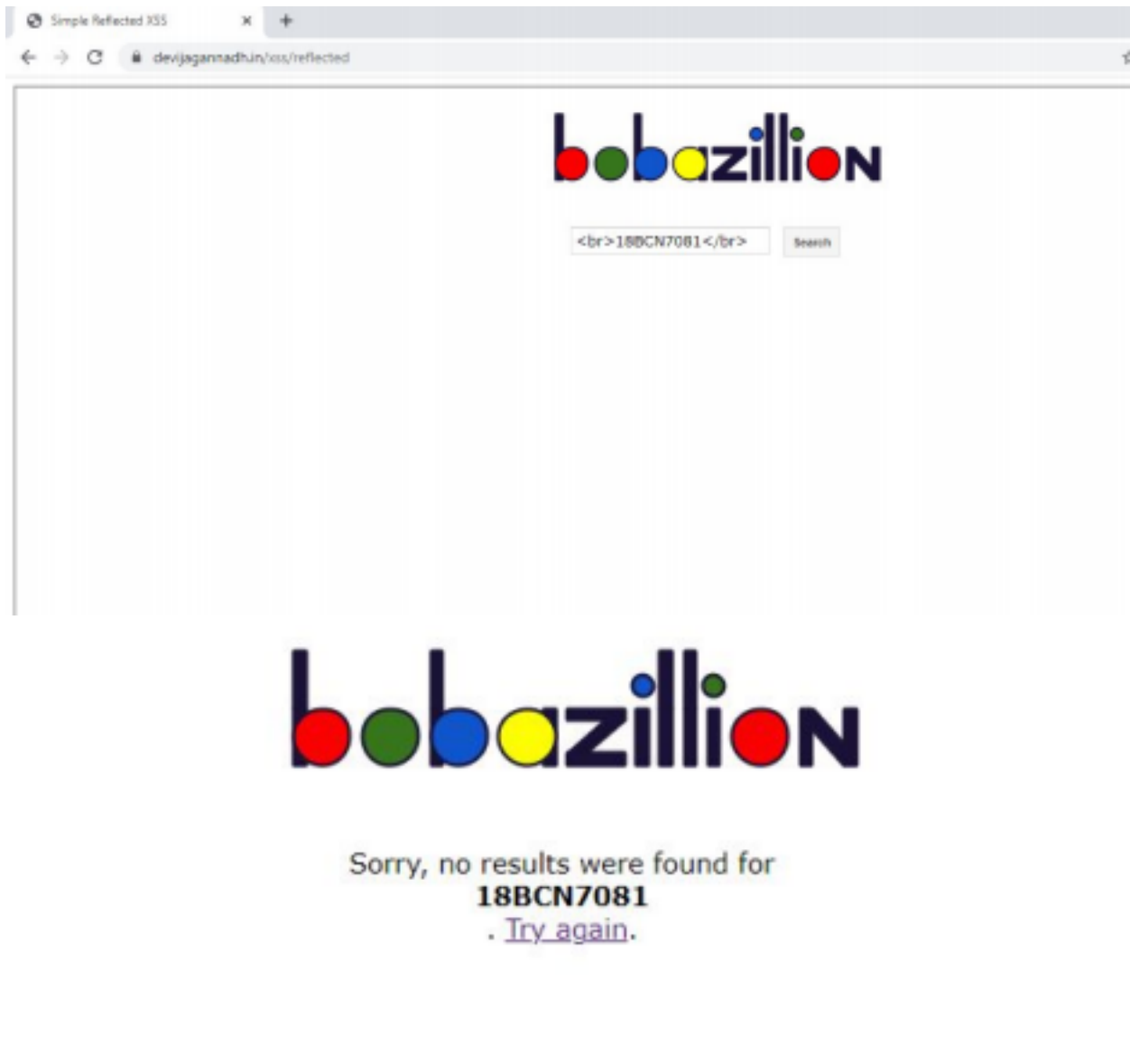
Secure Coding Lab-5

VENKATA SAI KARTHIK 18BCE7296

1.Reflected XSS

Commands and Outputs:

1) `
18BCN7081</br>`



2) `dattu`



`<a href="https://www.yo`

Search



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

I click on that, it will redirect into the page URL I have given.

When

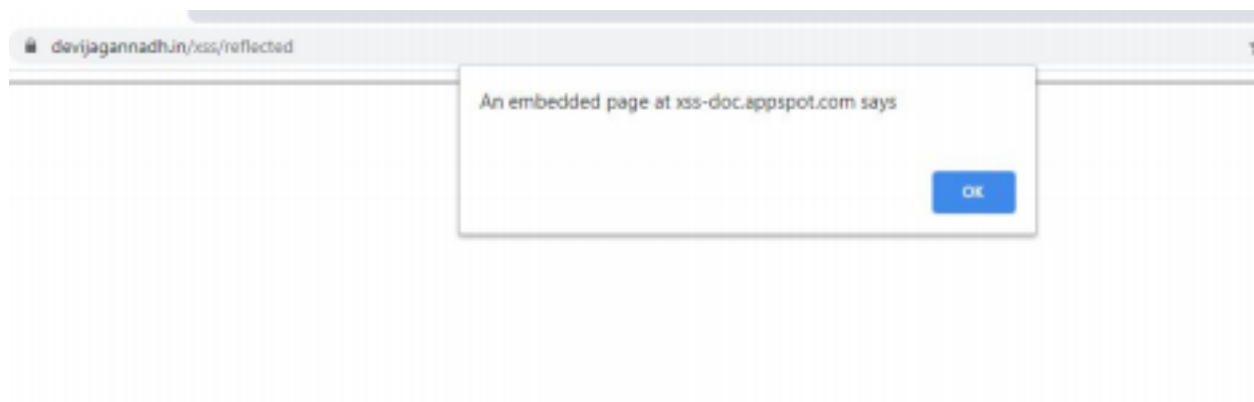


www.youtube.com refused to connect.

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

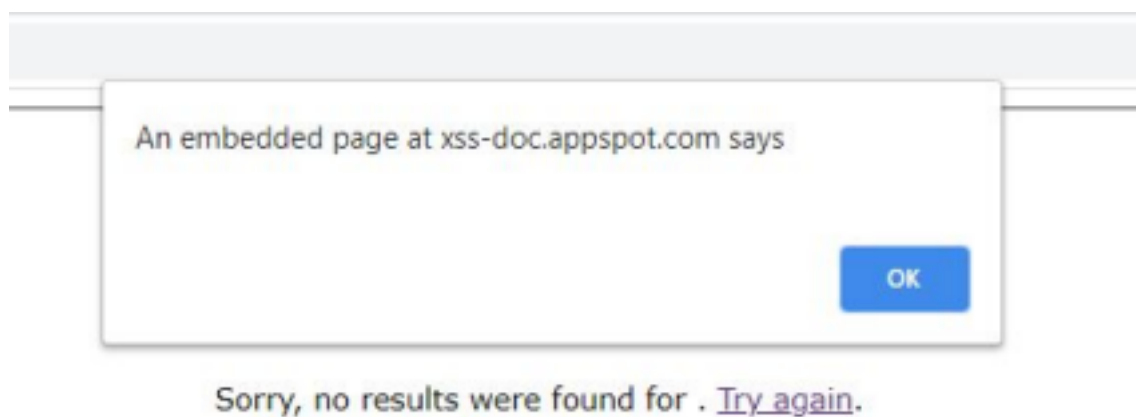


The Payload we entered should give a reply with the Session Cookie.



4) ``

The Payload we entered should give a reply with the Session Cookie.

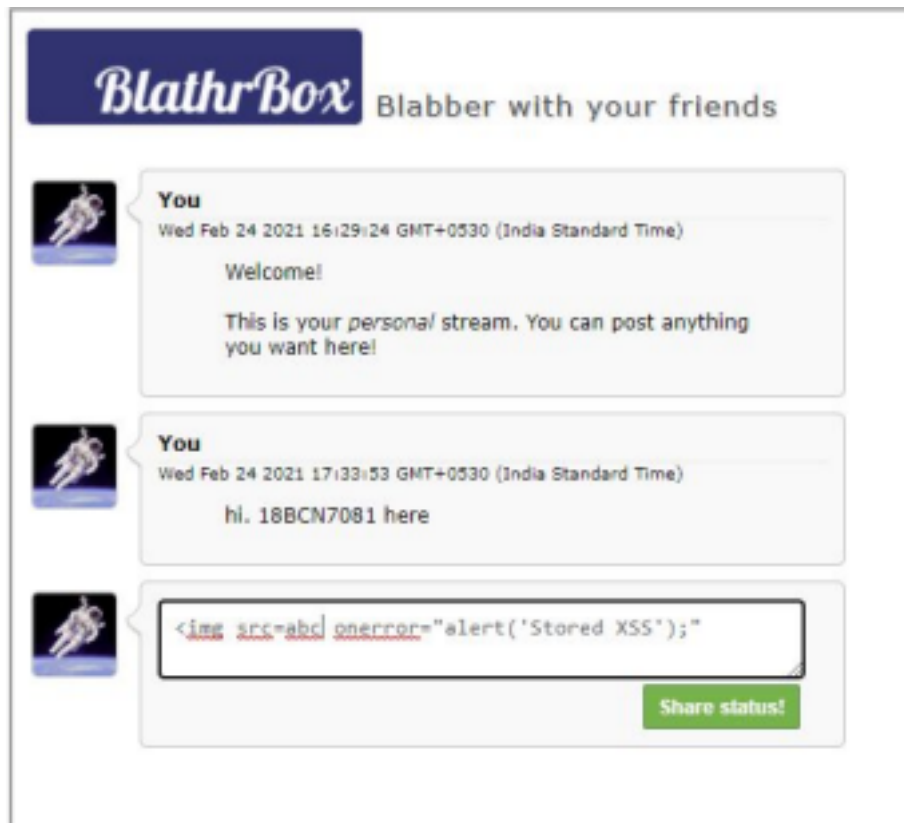


With
Advanced Cross Site Scripting, This RXSS can transfer the Victim's cookie to the
Attacker.

2. Stored XSS

Commands and Outputs You can see the malicious code and output below

1)



2)

BlathrBox

Blabber with your friends



You

Wed Feb 24 2021 16:29:24 GMT+0530 (India Standard Time)

Welcome!

This is your *personal* stream. You can post anything you want here!



You

Wed Feb 24 2021 17:33:53 GMT+0530 (India Standard Time)

hi. 18BCN7081 here



You

Wed Feb 24 2021 17:38:44 GMT+0530 (India Standard Time)

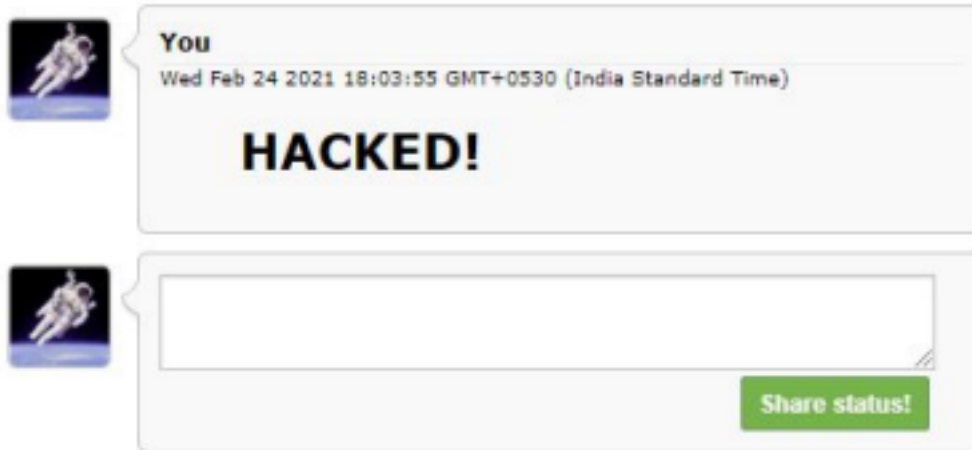


```
<img src=x onerror="alert(document.cookie);"
```

Share status!

An embedded page at xss-doc.appspot.com says

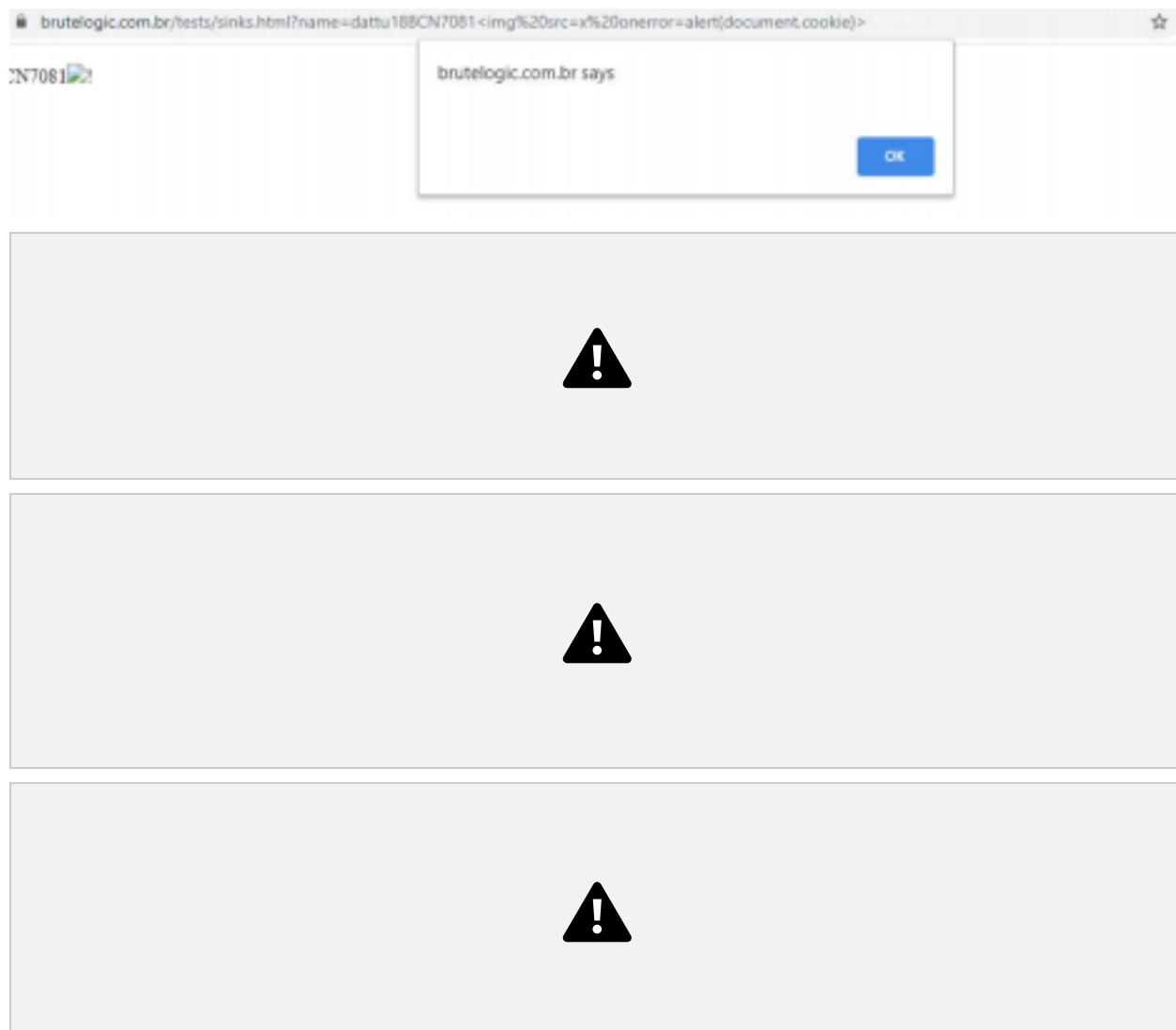
OK



3.Dom XSS

Commands and Outputs:





How Secure Coding is related to XSS?

Secure Coding plays a huge role in preventing these XSS attacks. These cross site scripting attacks can only be used in such websites where scripts can be executed even though they are not meant to. Such websites are vulnerable to XSS. These XSS attacks can be prevented by limiting the few characters usable in the fields, such that no malicious payloads/ scripts can be executed in our websites. Nowadays there are numerous websites which are vulnerable to XSS. By implementing some several restrictions like Character limitation etc, our websites can be secured and will be invulnerable to XSS.

Challenge:

