**DAY 39**

The endpoints where you can try out XSS payloads procedure to identify XSS vulnerability.

1. Select a target.

2. Search for the user input fields (search bar, login, registration page, comment, review, write your story page).

3. Give a basic text as input and submit it.

4. Check for the reflection of the text you submitted in the following:

1. Title of the page

2. Same input field

3. Anywhere in the webpage

4. In the URL

Automation to find XSS vulnerability using burpsuite:

Intruder tool:

-Intruder is used to automate the vulnerability testing using custom payload

->Action->send to intruder->turn off intercept

Go to intruder:

->Positions

->clear $

->double click input field (ex. search)

->Add $

->click payloads

Payloads can be downloaded from github

Ex. github.com/payloadbox/xss-payload-list

->click load and select file

->start attack

Intruder by default will only provide us with first http response.

So, we should configure burpsuite intruder to follow all the http redirections.

For each and every usage of the intruder we need to configure this settings:

In burpsuite

->click options

->scroll to bottom

->under redirections, select always