Name: Kuldharan Sankalpa Rajendra

Ethical Hacking

Task 3:

Report on vulnerabilty finding in http://testasp.vulnweb.com/

TITLE: Cross Site Scripting
DOMAIN: vulnweb.com
SUBDOMAIN: testasp.vulnweb.com
Testing environment: Linux , Burpsuit , Wifi
Payload I used:<script>alert(1)<script

Steps to reproduce:

Step 1: Visit http://testasp.vulnweb.com/
Step 2: On the top menu you will find a search option.
Step 3: Click on it and you will be prompted with the Search box.
Step 4: You can intercept the request in Burp Suite
Step 5: Now you can find different payloads for XSS.
Step 6: Send the request to the intruder and paste all the payloads.
Step 7: Try to find a successful payload for XSS.
Step 8:Prepared a report for it.

Impact: Cross site Scripting can lead to stealing of your user data and it can be harmful for your website/company. User’s data is not safe due to XSS. With user interaction ,an attacker could execute arbitrary Javascript code in a victim’s browser.

Mitigation: If you want to prevent your website to be vulnerable of cross site scripting then you can just enable noscript on browser.

POC including screenshot/screen recording is including in the report which is attatched in ppts.