Bug Bounting

Basic Terminologies:

1. Injection point.
(username, password, sign in, singnup, comment, forms, search)
2. Vulnerability.
is a flaw or weakness of system.
3. payload <script> alert(1) </script>
is a script or code that is used to identify vulnerability.
4. Exploitation
Taking advantage of that vulnerability to gain system acess.

Information Gathering:

1. choose a website.
Sub domain | daily visitors | fraction.
eg: amazon.in | 16530000 | 82.22%.
2. Find subdomaens - Google it, find subdomins
more subdomins - more bugs.
3. you have to rank the subdomains by unpopularity less traffic domin

Subdomins information gathering.

https://www.wolframalpha.com/

https://dnsdumpster.com/.

https://searchdns.netcraft.com.

https://pentest-tools.com/home

Burpsuite pro.

Xss (cross site scripting bug):

Identification of cross site scripting bug using burp suite:

Cause and effects:

The xss bug could cause the threats and damage to the website by allowing the hacker or hunter to take advantage over the bug and to perform the actions such as.

1.) Phishing attack.

it means the exact copy of the website is made and could let the native users to use and hacker could gain data.

2.) URL reDirection:

The link of the site may lead to open the another website much dangerous act.

Process of Finding xss Bug:

2 ways of Exploiting the xss Bug:

↳ Manual hunting.

↳ Burpsuite.

Burp Suite:

→ Open Burp suite pro (∵ it will be supported by minjava & jak file should be pre installed in the host machine).

→ click on Dash Board turn off unnecessary radio buttons.

→ click on proxy. configure proxy settings manualy in the fire fox browser by adjusting the network settings in Fire fox

Again Download and install CA certificate of Burpsuite and install it in the Fire Fox using click on the privacy option in Fire Fox.

Browse the path and now the proxy is configured successfully.

→ open Burp suite and ensure the manual proxy connection.

→ Turn on intercept load the webpage in proxy connected web browsers.

→ Now the respective content of the host is displayed in the proxy option and ensure that correct host is displayed if not reload and turn off and turn on the intercept.

→ Now we need to scan that host site for finding the parameters.
To do that right click on the proxy Activity and then scan.

NOTE:* Turn off the intercept.
Now click on the dashboard to see how the scan is being performed.

* click on the Target that shows the parameters double click on the parame option to find the vulnerable parameters

attack.

* Select the parameter which could have a bug. Send it to the repeater.

Now, Select the only read colour text and try to modify and search the same text in the search field if the fields are matched there may be a chance of expose of bug. Now coming to the crazy part attack to find the bug.

* Click on it send to intruder. based on the repeating texts then select the mode of attack.
    * Sniper - single match.
    * Battering ram - 2 match found.
    * Cluster Bomb - 20 matches and more injection points.
    * Pitch for - more than 2 matches.
* Click on the payload option in the same tab of intruder.
* load all the xss payloads.
    * paste, edit payloads as per convinence and start attack.

* All the possible links would be displayed of consisting xss bug now click on it show response in browser,

Copy & paste the link in browser.

once you paste in browser a pop up Menu would appear consisting of the xss bug.

Now in the payload field of the link, just simply enter the document.URL and copy the link.

Now we sucessfully found the xss bug, we can report it to the client and can get bounty or accredition by reporting the respective website - mostly hackerone.com.

Note:

~ Read the hactivity more than once to find which kind of bugs they accept.

/* sucessfully found and reported this xss bug */

Types of vulnerabilities:

* XSS.
* CSRF
* open Redirect vulnerability.
* html injection
* Sensitive Data Expose.
* Dependency bug;
* etc...
* parameter Tampering.

→ parameter Tampering: —

change / modify the contents in the website depending on the bug and making the further proceedings using burpsuite.

eg: Generally in any ecommerce we can find a bug of kind and buy the product to the least of least amount.

Steps:

→ open the website and add to cart or buy option
→ Turn on the intercept
→ In Raw search for price eg: 4200
→ Match is found.
⇒ change the price to 1 rupee.
⇒ Forward and intercept off

→ Now place the order

parameter tampering | data Data tampering.

which is performed to manuplate the website creds.

SENSITIVE DATA EXPOSE BUG :

Sensitive Data Expose vulnerabilities can occur when a web application doesnt adequately protect sensitive information such as credit card information, Such as credit card data, medical history, session tokens

It is used to exploit the data and dump data.

It is often said that most common flaw is failing to encrypt data. One example of this vulnerability is to clear text submission of password

Burp Scanner

Steps :

* First ensure burp configured with your browser. In the Burp proxy intercept tab ensure intercept is off.
* Visit the web application you are testing in your browser acess the log in page of the web app

Return to Burp.

- In the proxy intercept tab, ensure intercept is on.
- Enter login details if mentioned from hactivity login from the submit request. in this example by clicking login.

Return to Burp.

- The raw request details should now be displayed in the proxy intercept tab.

Right click on the Request to bring up the context menu and click "Do an active scan".

- Results are displayed in target
  - In this example the scanner via has detected that the application has an issue clear text submission of password.

By clicking on the individual issue you can view a description of vul and suggest remedition in advisory tab.

Burp Scanner checks for a variety of types of data exposure, including SSH keys, credit card numbers. and email addresses etc..

Cross site request Forgery bug:

//Account takeover.

- intercept and get login page raw only then Engagement tools copy html.
  save in note pad.
  open the file in default browser.

This bug is identified in username, password field and also delete account page

How to report

→ when generating the CSRF poc. , Right click save item as name.de.

Broken Link Hijacking:

- download the broken link checker github
  npm install broken-link-checker -g.

To run cmd - blc https://google.com -ro.

↳ it checks all the home page

or use website:

www.deadlinkcheckers.com

check manually all the links