Web pentesting/Bug Bounty hunting guide v2

By: Aayan

Introduction:

As I have described some prerequisites for pentesting/ethical hacking, I hope you are back here after completing that prerequisites guide. This guide will be only about bug bounty hunting, hacking ethically. Bug bounty hunting is easy for those who are not easy to give up in finding something new and for those who loves to try new things and learn new things.

You should be highly interested in it to hunt medium to high and high to critical bugs in websites, and always remember the good researchers are those who describe impact, solution , and markdown the report perfectly because developers are not always free to spends hours on your report to read it understand the impact, basically they'll reject it and look at other reports from researchers.

There are many researchers not just you are the one testing the particular website. There can be 100 to 500 and 500 to 1500 researchers on single target, you should always go for serious weakness go for subdomains first and do not stop when you have found low-medium weakness bug. Keep thinking out of the box.

Networking (TCP/IP, HTTP):

I hope you must have done network plus N10-007 as it is the foundational networking course, and now after that learn and dig deeper little more about TCP/IP and HTTP web protocol, you should know how web communication works how server and client exchange data, transfer and receive the data, always understand the system how it works to perfectly find flaws and break.

Focus perfecly on HTTP how GET,POST,DELETE,PUT requests work and what are response headers status codes mean, as they are the reponse status codes from server.

TCP/IP: https://youtu.be/F_pAs9OSFFo

HTTP: https://developer.mozilla.org/en-US/docs/Web/HTTP

Web Technologies (html,js,php,Sql):

After learning how client and server communication works, you must know the languages take place to make web exactly a web and web technologies concepts already described in developer.mozilla.org invest your time on learning and understanding those concepts my mate, I repeat try to understand how these all things work together and to make web a web.

I have included urls about these where you can learn these web technologies, below in this page.

HTML: https://www.w3schools.com/html/default.asp
JS: https://youtu.be/hKB-YGF14SY
PHP: https://www.w3schools.com/php/default.asp
SQL: https://www.w3schools.com/sql/default.asp

web technologies concepts
essential : https://developer.mozilla.org/en-US/docs/Web
do not spend all time in this but atleast read it.

Web Security and hands on testing:

First of all it is gonna be little theoratical but I believe you'll enjoy learning and understanding about web security concepts as because you have learned fundamentals, you know how web works and it's basic technologies. Try to understand where the developer always makes mistake because his/her mistake causes a flaw/weakness in website which you find it as Security researcher and report it.

After that my favourite book about web security testing is OWASP web testing guide, you should follow it after learning basic web languages , web technologies and security concepts as security concepts are described in this book but MDN is doing great I mean developer.mozilla.org concepts are best and friendly do not spend all time in it just read and understand basics then give your quality time to OWASP book.

As you'll be going through information gathering, web server fingerprinting from OWASP book have research on live website along with it, keep doing practical and also when the chapter comes about hacking/exploiting like XSS go to the portswigger website there will be same concept labs and all free I have inluded url for these all.

I have also included urls for 2 proxy tools used for web pentesting as these tools are the tools every web pentester/H4ck3r uses.

WEB SECURITY: https://developer.mozilla.org/en-US/docs/Web/Security

OWASP testing guide:
https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

portswigger academy labs: https://portswigger.net/web-security

Burpsuite tutorials: https://www.youtube.com/playlist?list=PLoX0sUafNGbH9bmbIANk3D50FNUmuJIF3

Zap tutorial: https://youtu.be/41OlmzEODgU

After all this go to bugcrowd website sign up as researcher and look for public programs exploit and report, let me give you a tutorial about how to make good and understandable report as every web owner wants.

Report tutorial: https://www.bugcrowd.com/resources/webinars/how-to-make-a-good-submission/