What Hacking Tools are used by hackers? Do you want to know:

- Can hacking skills be replaced with automated tools?
- Can facebook accounts be fired with just one click on HACK NOW button?

There are lot many questions related to this topic. So I thought, why not to cover this topic in a single blog post. If you are a true beginner, keep reading! This article gonna introduce you with multiple different concepts related to hacking tools.

IMPORTANCE OF TOOLS

Hacking Tools are the best companion of an Ethical Hacker. However, it is wrong to say that hacking is incomplete without those hacking tools. Please don't correlate my view with the automated scanning.

> *Hacking is all about finding the possibilities to exploit a target in order to achieve sensitive information or performing some unauthorized actions.*

So, if you don't have the knowledge, then no hacking tools can help you out. But, tools can definitely help you out to solve some of your problems. So, by using hacking tools, you can get maximum output in minimum duration.

Following are the different advantages of using hacking tools:

DECREASING WORKLOAD:

Tools are one of the best ways to automate the task. Suppose, you are exploring the target. so, in spite of manual approach, you can use various tools for the purpose such as for enumerating subdomains, grabbing the application versions and many other footprinting

steps.

Therefore, these hacking tools can be quite helpful for researchers who want to save their time and produce maximum output.

EASE THE PROCEDURE:

Hacking Tools are very much helpful if you want to verify small vulnerabilities in no time. I use a chrome extension to verify clickjacking vulnerability. It means, just within 10 seconds of opening a website I can report the vulnerability. This is just an example. I'll discuss some more tools in details.

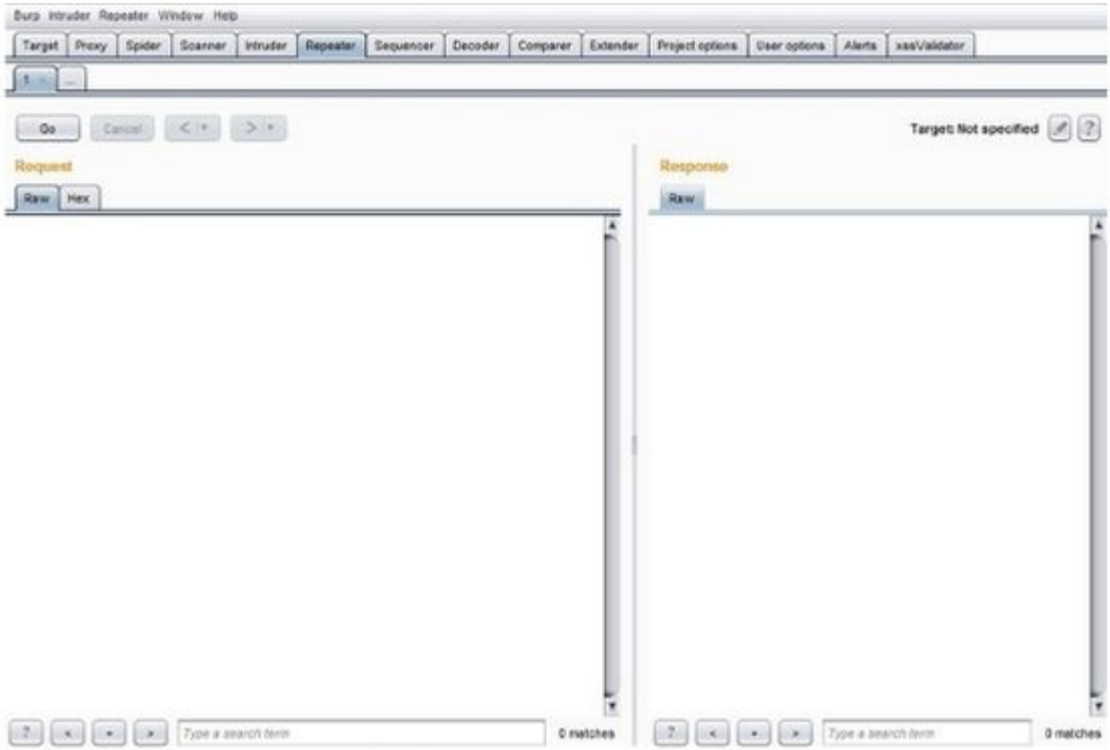
HACKER'S TOOLKIT

Hackers use a number of Hacking tools for different purposes. To be honest there is now an endless number of tools which can be used for recon purposes or for determining a vulnerability. In fact, it's not possible to share each and every tool with you guys.

However, I'll share some most important hacking tools without which you can't be good at Bug Bounty.

BURP SUITE: #1 hacking Tools

Burp Suite is one of the most wanted hacking tools in any Bug Bounty Hunter's toolkit. In simple terms, this acts as a mediator between your browser and the server. It'll help you to view and modify requests and responses.



Not only this much, but you can also bypass client-side security validations implemented by the developers. If you don’t have much idea about client-side and server-side validations, then don’t worry, let me explain you.

CLIENT SIDE VALIDATION VS SERVER SIDE VALIDATION:

In client-side validation, inputs are validated in the browser itself before reaching to the server. But in case of server-side validation, the request is sent to the server to verify the security guidelines and then only it validates.

Consider an example. suppose, a website uses a strong password mechanism, and you entered a simple password 1234. Now there will be 2 cases. If there is just client-side validation, It’ll instantly prompt you that password is weak. the browser won’t reload. But in case of server-side validation, the request will be validated by the server.

BURP SUITE CONTRIBUTION IN BUG BOUNTY:

Burp Suite i.e one of the best hacking tools, has a huge user base from around the world. Almost everyone who started with bug bounty uses this tool. Actually, this is a complete package with many integrated modules. Some of the most useful modules are:

- PROXY
- REPEATER
- INTRUDER
- COMPARER
- DECODER

In this blog post, I'll give you just an idea about these different modules so that you can at least start learning yourself.

Proxy is the primary and most useful part of the burp suite. Proxy is generally used for intercepting web traffic and modify it before sending to the webserver. Do you still remember I discussed bypassing client-side validation in the previous section?

Well, we can bypass client-side validation using the proxy module. Once we provided input and clicked on Enter button, the data will be first sent to the proxy, from there we can modify it.

Repeater module is basically used to check the intercepted request and do experiments by manipulating parameters and watch the response. The repeater module's window is divided into 2 parts request and response. We can modify the request and check the response for the same. This module is really helpful.

Intruder module is basically used for checking the Rate Limit issues. The rate limit is nothing but a brute force attack. Suppose if we are able to operate thousands of payloads within minutes successfully(200 OK) then it'll be considered as Rate Limit Issue. With the help of intruder, we can check this vulnerability.

Above 3 are the major and useful modules of Burp Suite. Master them. It'll help you very

much in your bug bounty journey. If you like to get detailed knowledge about the burp suite then check the below resources:

https://www.udemy.com/burp-suite/

WAPPALYZER

Wappalyer is another great tool. This is basically used for footprinting the target or finding details of the targeted web application. It'll unhide most of the technologies used by the web application.

This is a chrome extension. Once you installed it, you'll get information such as CMS used by a web application (if), Database information, Web Application versions (not every times) and much other information.

This will save your time to a great extent. You don't need any extra time to find all this information. Simply, click on the extension after opening the website. If you don't want to install, you can use the website too for the same purpose i.e. https://www.wappalyzer.com

VIRUSTOTAL

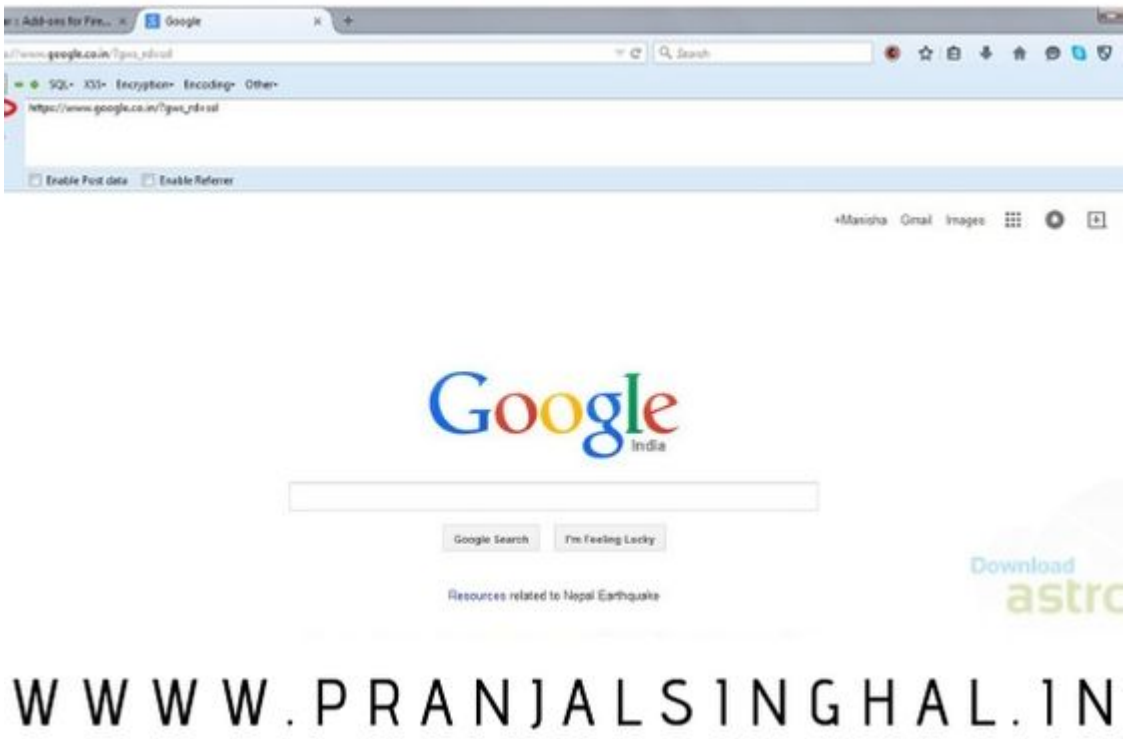
Virustotal is a google acquisition. From hacker's point of view, it is really helpful to find subdomains of a web application. Till date, I didn't find any other tool better than this. So you can blindly use this hacking tools to enumerate subdomains.

Subdomains are the hidden tressure. It'll be a foolish act if we directly start testing the main domain. You should first target the subdomain. Virustotal will give you all the available subdomains of a particular website.

HACKBAR

Hackbar is a great extension of firefox for manipulating the URL in an easy way. It has payloads for MySQL XSS etc. Sometimes URL looks soo messy. with hack bar, you can easily

make it look simple and readable by dividing each parameter line by line.



Actually, you'll understand it once you'll start using it. Apart from payloads. It'll make your testing a bit easier by decoding the complicated URLs.

Apart from that, the address bar used to change the URL each time, which will irritate you for sure. So, you can utilize the hack bar here.

EDITTHISCOOKIE:

EditThisCookie is a facebook extension which is used to import and export session cookies. In case you don't know what cookie is, the cookie is a small piece of information stored in the browser which enables fast access to the webserver.

A cookie contains session related information. So, to exploit session and authentication-related issues, we can use this tool for easy import, export, and edit the cookies. Though there are many extensions available for the same purpose, but this is truly better.

HACK FACEBOOK ACCOUNT WITH ONE CLICK – REALLY?

This is one of the most common questions. Can facebook accounts really be hacked with some tools available online? When I searched on google, I found multiple tools online claiming that they can hack facebook accounts in minutes. Guys, before I proceed, note it down

> *No tool can hack facebook account in minutes. Not even with Bruteforce attack.*

But, it doesn't mean facebook accounts can't be hacked. Facebook account can be hacked with the following techniques:

Phishing
Keylogging

You can search for those methods on google. There are plenty of resources available. However, these both methods are obsolete now and most of the people knew these techniques.

Though techniques got old but not the ideas. How about chaining this with some open redirect vulnerability of any trusted website. The conversion chances will be pretty higher. Since I got multiple queries regarding this so I thought of creating this section.

The conclusion is that hacking is based on playing with the mindset of the victim by using technology. If you never heard the word of Social Engineering then search it out on google .

FINAL WORDS

There is ‘n’ number of tools in Bug Bounty Industry. And obviously, it’s not possible to explain about each of them here in this article. However, I have tried my best to cover at least some basic and important tools which you must know in order to start with Bug Bounty.

If you’ll master the hacking tools I mentioned then you’ll cover almost 50-70% of Bug Bounty and you can start testing any live target. Burp suite itself is enough because of various modules. I have provided you 2 best resources to learn about Burp Suite. Learn from there because they are the best.

Here, I didn’t discuss Kali Linux. The reason is that I assume you guys are new in the field and it’ll be difficult for you to switch from GUI to the command-line interface. But this is 100% true hacking is incomplete without Kali Linux.

In the future, I’ll make a separate post on hacking tools you can use with Kali Linux. Some tools such as DirBuster, Sublister, etc are extremely useful. But it’s not like that you can’t start your Bug Bounty journey without them. They will simply work as an addon. Part 2 will come for sure.

Guys, it took a lot of time to wite approx 2k words article. Please leave your honest reviews either on my

Facebook Page
Facebook Group
Twitter Account

If you aren’t connected with me, then join me now. We’ll discuss the confusions there

I hope you guys will do the best! Keep rocking and Happy Hacking

Pranjal Singhal

I am a freelancer Cybersecurity researcher and a digital marketer. I have already helped Top IT Giants to secure their web applications and maintain a safe environment for their users. Sharing and Caring is my motive. I love to guide beginners about making a successful career in the cybersecurity industry.