



Doing RECON the correct way

Hey guys, today we will discuss **Information gathering** aka **Recon** which is the foundation of every bug bounties or penetration tests which you will ever do. Many security researchers have found many CRITICAL and HIGH priority bugs just by doing proper information gathering which is the initial phase of a penetration test.

If I get 6 hours to chop a wood, I would spend the first 4 hours sharpening my ax.

This is exactly the case in this phase. Most of the researchers just start looking for vulnerabilities like **XSS**, **CSRF**, **IDOR** as soon as they get the target but with proper information gathering at the start people can know what the target is and the different technologies on which it is built and several other things. For now, we will keep this post general and simple and with time we will make sure to update it or write the 2nd part of it. So let's get started on what you should do in the initial phase of knowing your target.

1. Subdomain Enumeration:

We have already published a post on Subdomain Enumeration in which we discussed several tools and techniques by which you could do subdomain enumeration. You can find the post [here](#). In the time we last wrote that post, we came across some other cool tools which are much faster and bring better results when you

have a target like ***.target.com** and you need to enumerate all the subdomains.

Subfinder

One of these tools is **Subfinder**. You can get the tool from [here](#). It is faster than Subbrute or Sublist3r. It has been written in Go language so you will need to follow the instructions to install Go and setup this tool on your machine. Also, you will need to set up private API keys for some of the services like Virustotal to get results from them also. It has been mentioned in brief on that Github page. After installing the tool, there are several options which you can use. One of our favorites is:

```
./subfinder -d target.com
```

This will make sure to get subdomains from 22 passive data sources. But if you have a text file like this [all.txt](#) and you want to brute force the subdomains, then you can use the option below

```
./subfinder -d target.com -b -w all.txt
```

Subfinder is one of the fastest and mostly used subdomain enumeration tools out there recently. Make sure to use it to get juicy subdomains to gain more chances of getting a bug there.

Amass:

Amass is the second new tool which is there and we wanted to let you know in case you haven't used it yet. It has also been written in Go and is super fast. Installation instructions and everything else which you will need can be found [here](#).

After installation, you can simply run the command:

amass -d [target.com](#)

to get different subdomains for that target. There are many other different flags mentioned there which can help you in finding a quality number of good subdomains. Now if you are thinking, why we are talking about subdomain enumeration tool once again, and Subbrute or Sublist3r would suffice this purpose. Then we would like to add something, as of now Sublist3r has really become depreciated as a tool and you will find a great difference when you compare the results from Subfinder and Subbrute or Sublist3r. Make sure to try these 2 tools to have better chances of finding a different domain and ultimately getting a valid bug on that.

2. Censys:

Now, this is one tool which many researchers have been focussing on in recent years. And this is one of the coolest tools for information gathering. Censys actually scan the IP addresses and gathers information from a set of different ports. Creativity is a way while doing Censys search. A simple search like this, "[target.com](#)" **internal** might lead to unexpected results. There are many tutorials online available on how to get more than the normal information

usually shown and you should really check that out. You can access the tool from [here](#). Just enter any website's name in the Search Box and you will get a whole lot of results and many times subdomains data from there. Do take a look at it while doing information gathering.

3. Shodan:

Shodan is more or less the same as Censys except that it scans every IP addresses and generate a lot of data. The process is also almost the same and is really popular among bug bounty hunters. You can access the tool from [here](#). There are many books like [this](#) and online tutorial plus videos which goes into a deep study on different shodan techniques to get better results. Again creativity is the key here, so do gather some information on Shodan before gathering info on the target application. So do check this one out.

4. Github:

Github is the world's largest software development platform. It is one of the best places to look for various issues and knowledge about the technology stack the company is making it's products on.

While doing a Github Recon for a particular target, you could look for many things like:

Looking for secret keys labeled as **API_key** and **AWS_Secret**
Some internal credentials such as username, the password for Database or admin portals.

You could also get some different API endpoints and look for different domain patterns.

Not only this, there are many environments like dev, stage, and prod and you may find some interesting details or any interesting subdomain based on this.

Let's suppose the testing application is [target.com](#), then you could just make a search as

"target.com" "dev" or **"target.com" "prod"** to look for the above details.

For searching secrets like API_key, you can just make a search as **"target.com" API_key** and it might give you some unexpected results in many cases.

Similarly, if you want to refine your searches for passwords, you should make a search for **"target.com" password**

There are many tools available for Github Recon like **gitrob**, **git-all-secrets** etc, but the best way will be to do it manually so you don't miss anything important.

5. Amazon Web Services(AWS):

AWS s3 buckets are being used by a lot of companies to host their content nowadays. But many times unsecured methods leave them misconfigured which could then be an asset to a malicious hacker. In a CRITICAL scenario, this misconfigured s3 bucket may allow an attacker to read and write files on a bucket belonging to the company. Just as for finding any 'juicy' information on Github, it is

also possible to get a good amount of information while doing AWS recon.

Some of the ways can be like to use a Google Dork. Let's say the target is [abc.com](#) then a google search like

site:s3.amazonaws.com + [abc.com](#)

may provide you with some interesting results.

It is also possible to get s3 buckets on Github, so in this case, you may provide a search query in Github such as:

[“abc.com”](#) + [“s3”](#)

So this is all for this first post on Information Gathering. There are many other methods like dig command and archive.org which can be also helpful for getting various types of information. Information gathering is just what the name says. Gathering information from anywhere. Even though if you don't find any sensitive file during Recon, knowing the technology stack, subdomains will definitely give you an upper hand in the latter half of pentesting. In the upcoming months, we will make sure to make a part 2 for Information Gathering where we will talk about some of these topics in depth or add new updated tools and methodologies to help you in your penetration testing career.


Until then, keep practicing and Happy hacking. !!


A User can change the personal details
of any other user


Finding and exploiting Blind XSS


What do you think?


5 Responses


 Upvote

 Funny

 Love

 Surprised

 Angry

 Sad

0 Comments

ENCIPHERS

1 Login ▾

 Recommend

 Tweet

 Share

Sort by Best ▾



Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS 


Name

Be the first to comment.

ALSO ON ENCIPHERS

[Knoxss vs Burpsuite\(A practical Demonstration\)](#)


2 comments • 10 months ago

 **ENCIPHERS** — Thanks for putting your expert views on using KNOXSS and thanks for reading the blog post.

[Beginner's guide to Bug Bounty hunting](#)


[The Art Of Hacking \(Delhi Edition\) : Web Application Hacking – Basic Level](#)

1 comment • 10 months ago


 **kratos vlog** — hey any seminar in mumbai plz organize seminar in mumbai its our summer vaction we will join and learn

[By Hackers, for Hackers](#)

1 comment • 9 months ago

 **An-kit ĤHäKÙr** — Thanks you so much sir.
[Avatar](#)

3 comments • 5 months ago

 **iSec Doe** — Thanks, i hope you will do it soon, im so impatient to do it!! thanks a lot!!
[Avatar](#)

 [Subscribe](#)

 [Add Disqus to your site](#)

 [Disqus' Privacy Policy](#)

DISQUS



A team of passionate security professionals spending our each day learning, improving and contributing to a safer internet, one vulnerability as a time. We learn, practice, improvise and teach. Security is at the heart of ENCIPHERS.

QUICK LINKS

[About us](#)

[Services](#)

[Careers](#)

[Trainings](#)

[Contact us](#)

FOLLOW US



Twitter



Facebook



Youtube



Linkedin

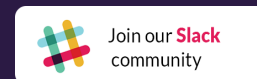
CONTACT US



+91.94508.28700



hello@enciphers.com



Design by Webchirpy