It's time to stop being a LEECHER

Cracking FOR DUMMIES®

1st Edition

Start contributing to the forum today

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Dr. Cisco Ramon

DISCLAIMER

This eBook is for educational purpose only. The author cannot be held responsible for any misuse of this eBook. Here, the term “Cracking” is a general term for the process of using something in a way, of which one doesn’t have an ownership. The tutorial doesn’t condone nor promote cracking in any form of Brute force or credential stuffing. This eBook is a product of long-term research using several sources from the internet.

By reading forward, you **agree** to the disclaimer above and will be solely responsible for the action you bring upon yourself. On a lighter note, you can enjoy reading the book even for the sake of learning something new.

Happy reading!

~ Cisco Ramon

INTRODUCTION

There are no prerequisites for cracking/checking but it is expected that you are aware of what you are trying to do. This eBook will intend to formalise you with how crackers get hold of accounts of various services across the world such as NordVPN, Hulu etc and use it to their advantage by selling or just using in general.

The book will also include short explanations about the things required for the cracking process in the next part.

Cracking is a term which roughly reflects the usage of a product for which you don't have the ownership. Cracked games and softwares are examples of that. In this tutorial, cracking refers to the act of getting access to a stranger's account in order to benefit from the premium services he/she has bought. It's an old practice and the companies have been trying to minimize this as much as possible by frequently changing APIs and introducing captchas in their login process.

In cracking, you are basically trying to illegally get access to the account by trying a list of available login combinations. This is called credential stuffing.

THE TUTORIAL DOES NOT PROMOTE CRACKING.

These combinations can reach the crackers through several sources such as Data Breach and bad password habits. Many users are known to use the same email and password combination for several of the services they are registered on. The crackers try to use the same combination on their target site trying to gain access.

NOTE: Credential stuffing is an illegal process and this book doesn't promote it in any form.

COMMON REQUIREMENTS

There are basically two common ingredients required before you start cracking using any of the methods mentioned. They are Combos and Proxies.

COMBOS

Combos or Combolists or Wordlist (new lingo also refer to them as Wombos) are simple combinations Email and Password separated by delimiter such as colon ':'. These combinations are counted by the lines and can be found in sizes as small as 1000 lines to 1 billion or more. Obtaining these lists are another process called Dumping and will require another tutorial. The combos can be found in various types depending on the purpose you need them for. The prominent ones are Email:Password, Username:Password or User:User.

The different types of combos are used depending on the service you are trying to break into. A service which requires the user to login using Email and Password will require the same type of combo. The main purpose of the combo is that a cracker tries the combination on the login page of a website/service and attempts to gain access to that service. This was mentioned earlier as credential stuffing. It's basically like trying to get into a locked room with several keys in hand and trying every key available to get the access to the room. Once a key unlocks the lock and in the case of cracking, a combination manages to get access to the site, we term that successful trial as a **HIT**. The only difference with cracking is that a cracker tries to get access to more of these combinations so that he can sell them or store them for future use.

PROXIES

Let’s take another real-life example. Imagine a Guard is protecting the said room and doesn’t allow the same person to keep attempting to open the door suspecting that the person is up to no good. Same is the scenario in the case of cracking, every login is identified by an IP or a proxy address and if the website you are trying to access suspects something strange, it bans the IP/Proxy address. Therefore, Proxies are used as a disguise to show as a different user every time the cracker attempts to login into the website. Depending on the security of a service, proxies may or may not be needed. Moreover, proxies help in protecting your own identity to the victim site.

Proxies are of three types: HTTP, SOCKS4 and SOCKS5. Certain websites work with specific type of proxies which can be understood with time and experience.

Further, proxies can also be categorised on their source such as datacenter and residential. Additionally, proxies can also be based on geolocation such USA, UK proxies. Lastly, there are rotating proxies which means that certain number of proxies are rotated for use through channels/ports.

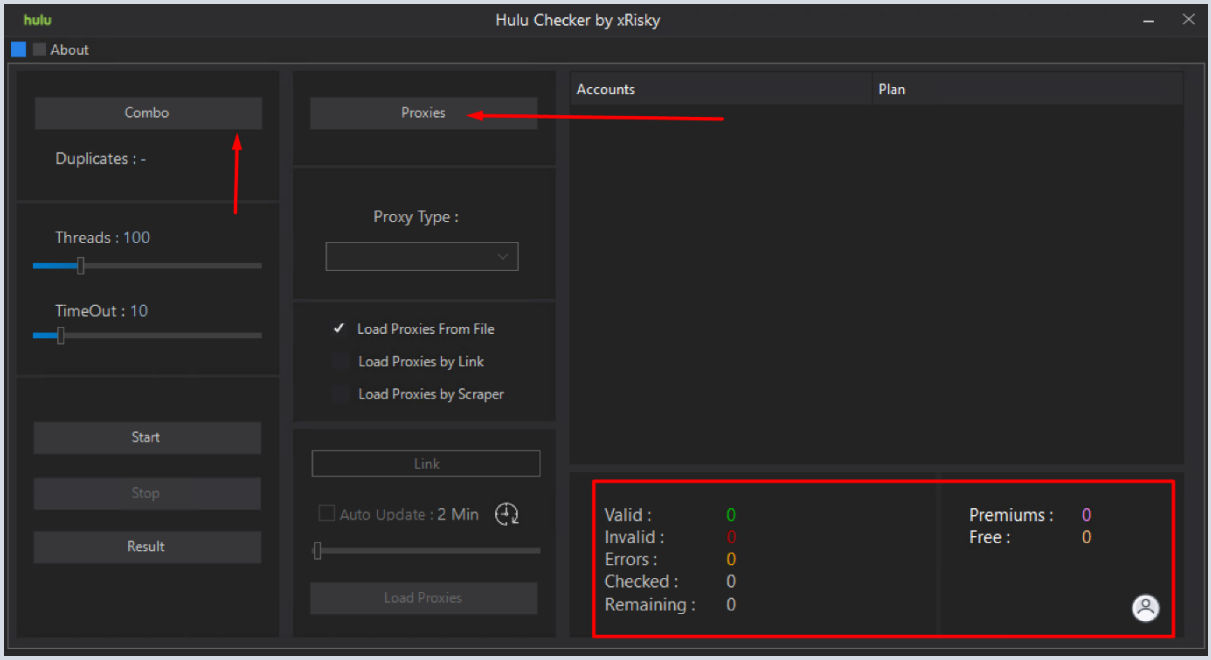
Proxyscrape is a popular free proxy source.

TOOLS

There are several tools on the cracking forums which are operating worldwide. Some are specifically coded to crack accounts for a site and others are universal tools which just need a reconfiguration to carry out the needed action.

The tutorial will try to explain how you can combine the ingredients mentioned earlier and the tools to get a meaningful result.

1. **Using specialised checkers**
   There are several coders who utilize their knowledge to make a tool which can ease the whole process. They get hold of the login APIs from the targeted site and run the combolists against the login link.



Screenshot from a specialised checker for Hulu

There are the specified locations to feed the combo and proxies to the checker. Once they are imported, the user will have to set the number of threads depending on the specs of the computer and the proxy type depending on the ones you have. With all the said things set, the checker is started, the stats will be displayed in the space highlighted by the red rectangle.

Valid: refers to those combinations which were successful in logging into the account and are also called as HITS.

Invalid: counts the number of combinations which did not work for the said site.
Errors: As mentioned earlier when the website starts detecting suspicious logins, it starts to ban the IPs which lead to errors in the checker.

Checked: Sum of both Valid and Invalid combinations.

Remaining: The combinations which are yet to be tried by the checker.

Premiums: The sole reason these accounts are cracked. They show the number of accounts which have premium benefits in the accounts.

Free: They are the accounts which do not have an active premium subscription.

There is also a box just above the stats which show the premium combinations. Depending on the creator of a tool, this space may or may not be available.

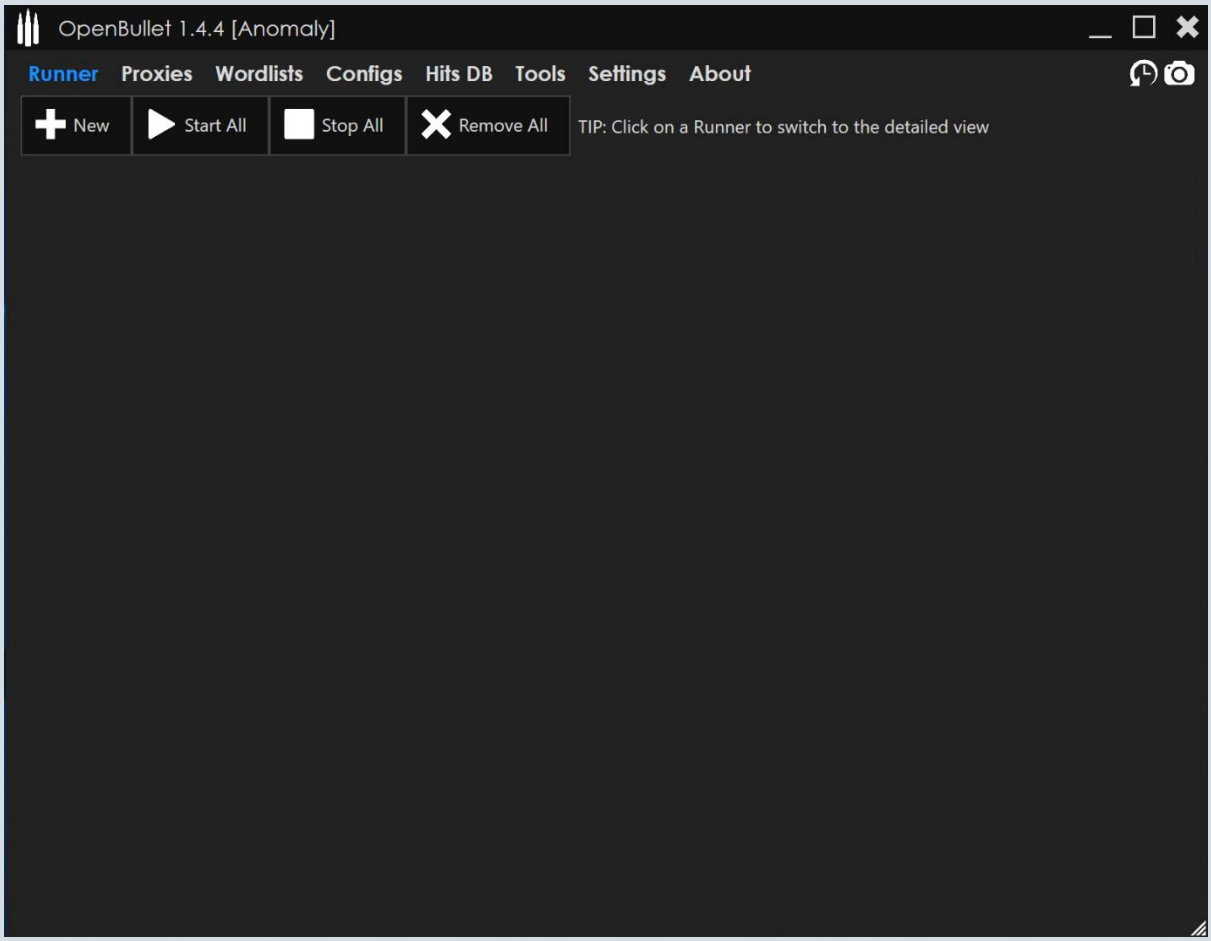
In this case there is a missing stat called CPM which can be referred to as Checks Per Minute or Combo Per Minute (Too many full forms for this, not sure which is the correct one). CPM is basically how many lines of the combo list is checked by the checker in one minute.

2. **Using universal penetration testing tools**

There are several penetration testing tools available such as Open Bullet, Storm etc. Here, we will use the example of Openbullet. A very common tool among the crackers and very readily available on the internet as this is not the intended purpose of the tool.

To use this tool, you will also need configs for the desired site apart from the combos, proxies and the tool itself.
After getting the config, you can place the configs in the configs folder of the tool using the Windows Explorer. The tutorial will use a modded version of the same tool.

Upon launching the program, a user is presented with the following window.

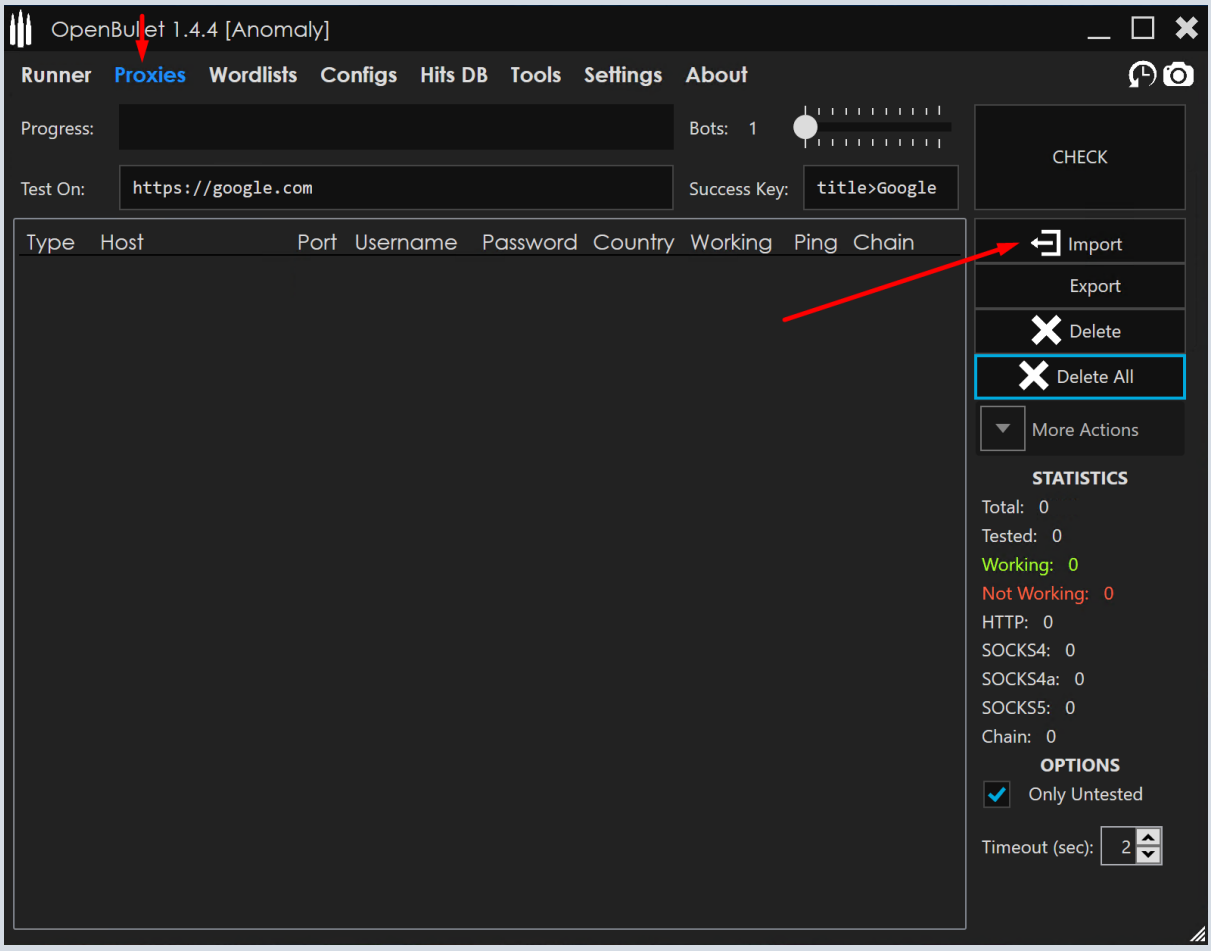


- Runner are the modules which run your specified config to check accounts.

- Proxies tab is used to store the proxies which you import to the tool.
- Wordlists contains the combos you want to test using the tool. Using this function is optional.
- Configs tab shows all the configs that you have placed in the main config folder. If the user chooses to use a new config while the tool is running, he/she can simply place the config in the config folder of OpenBullet and then use the rescan option in the Configs tab.

How to use:

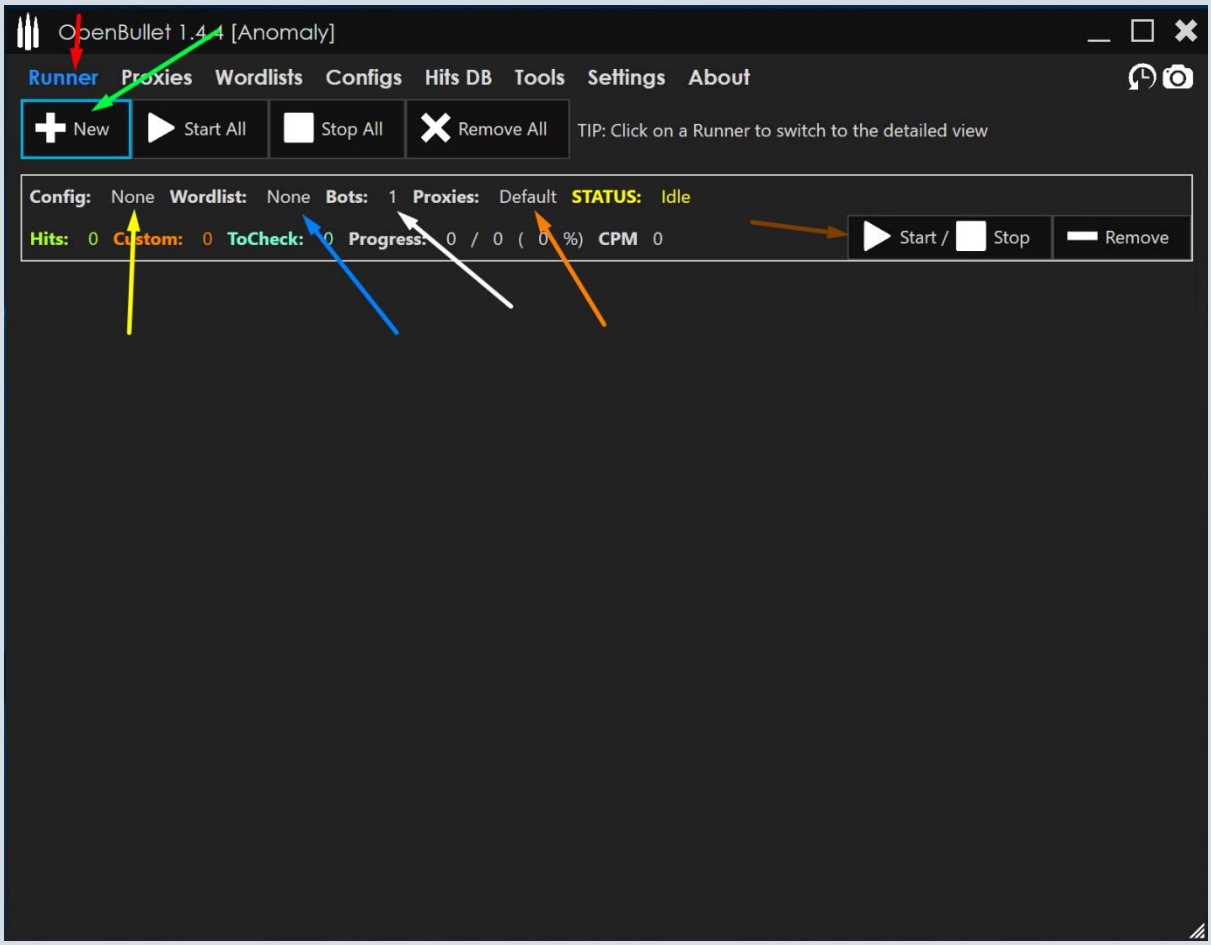
Importing the proxies. You will be presented with the following screen.



The user can simply click on the import button and import the proxies through file, paste or API.

To start cracking/checking~

Click on the Runner Tab and click on the new button indicated by the green arrow.



A runner will be created as shown. The coloured arrows will be used for easier navigation.

Yellow: Clicking on the shown area will open the dialogue box to choose the desired config.

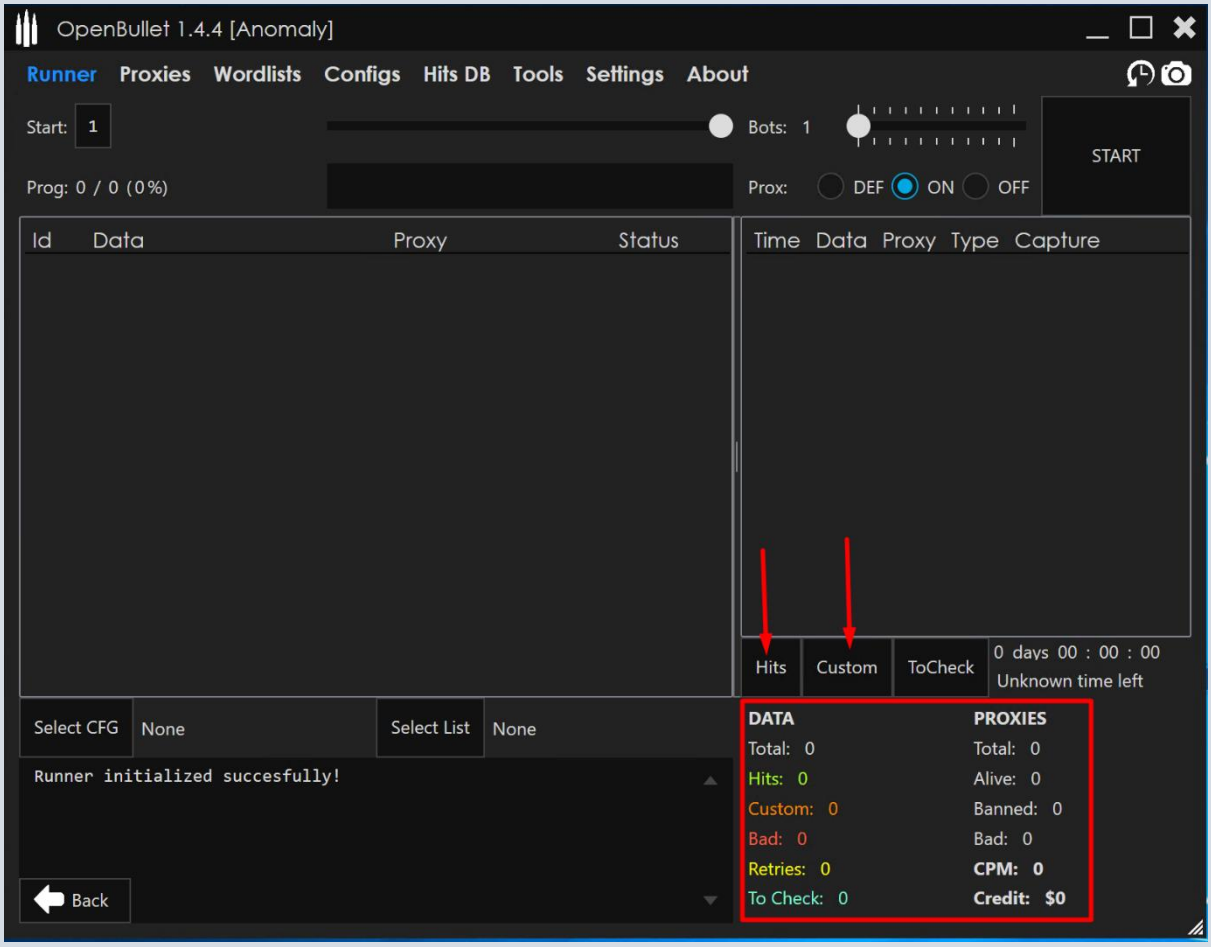
Blue: Here, you will be asked to choose the combo. You can either choose from the already loaded combo or choose a completely new one using the browse option.

White: This refers to how many threads/bots that can be put to work for faster working of the tool. Depending on the specs of the computer, this can be reduced or increased.

Orange: That opens up the option to choose whether you want to use the proxies or not. As mentioned earlier, some configs may or may not require proxies.

Brown: After executing all the steps above, the start button can be clicked to start the process.

Understanding the progress~



Hits tab will show the premium accounts with Capture depending on the config.

Custom tab will show the free accounts.

In the stats box, retries are equivalent to errors as explained in the specialised checker. Additionally, the proxies stat show how many proxies are successfully working for that login.

After the checking is completed, the hits can be saved by coping from the hits tab or saving through the Hits DB. As per recent developments, configs can now automatically the hits in txt files.

CONCLUSION

The tutorial which you hopefully read in full was curated using the little knowledge which the author possesses about cracking. There are new developments every day so there are possibilities that some points may have gone unnoticed. In case of any discrepancy please feel free to drop a feedback on the thread where it is posted.

To bring to notice again that this tutorial was only for education purpose and does not intend to promote cracking of any kind. Users using this shall do it on their own responsibility. Thank you.