

Red Blood



Contents

Contents.....	1
Introduction:	1
Installations:.....	2
Overview:	2
Download &upload:	4
Profile:.....	6
Custom modules:	7
Modules Key words:.....	7
Random string:.....	10
Files:	11
Block connections:	11

Introduction:

Red blood is a Command-and-Control framework which will help you for red team operations.

Installations:

Requirement:

- 1- [Node.js](#)
- 2- Install npm packages

Setup:

```
$ git clone https://github.com/kira2040k/RedbloodC2/  
$ cd RedbloodC2  
$ npm install
```

Check:

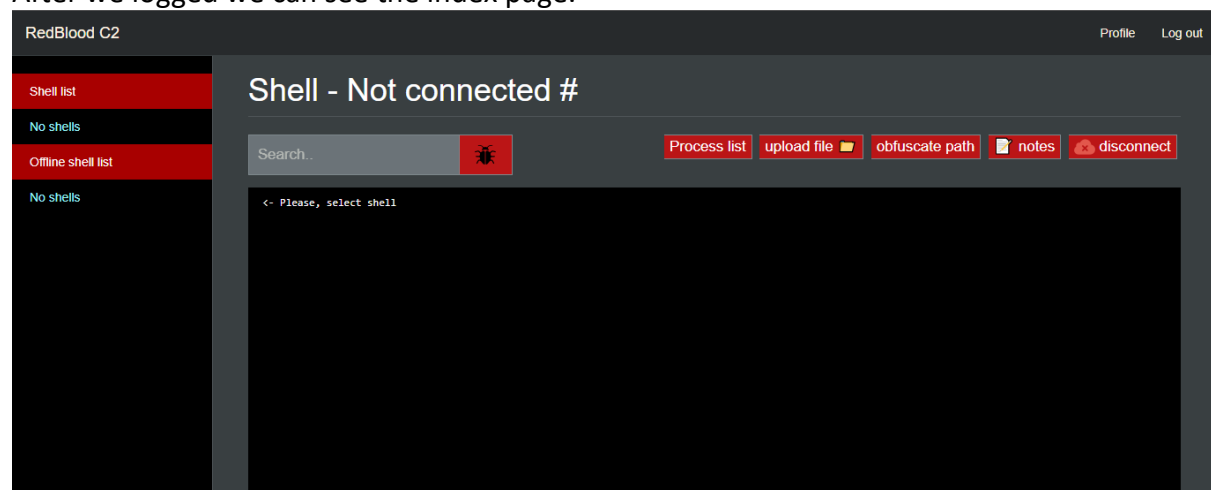
```
$ node server.js
```

Output:

```
app listening on port 80!  
http://localhost:80  
  
username:admin  
password:admin
```

Overview:

After we logged we can see the index page.



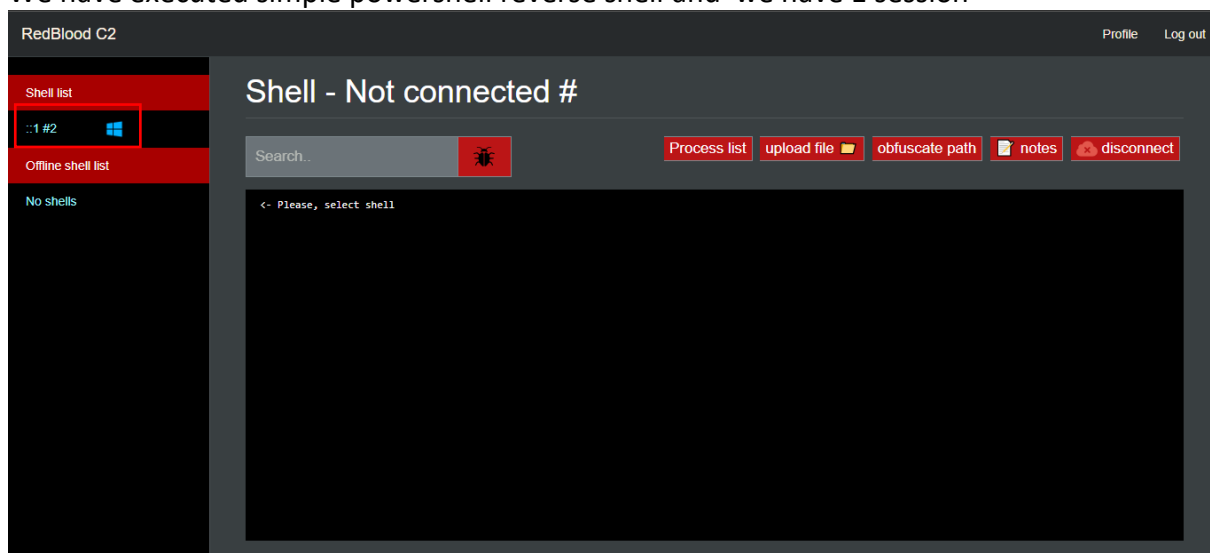
In config.js file we can control and customize the C2.

```
const settings = {
  block_tor:false,
  block_proxy:false,
  block_anonymous:false,
  port:80,
  token_expire:'1800s', // 30M
  offline_shells:true,
  listeners_ports:[443,1337],
  http_reverse_listeners:8080,
  colors:{
    shell_list_background_color:"black",
    index_background:"#333333",
    terminal_color:"white",
    terminal_background_color:"black",
  }
};
```

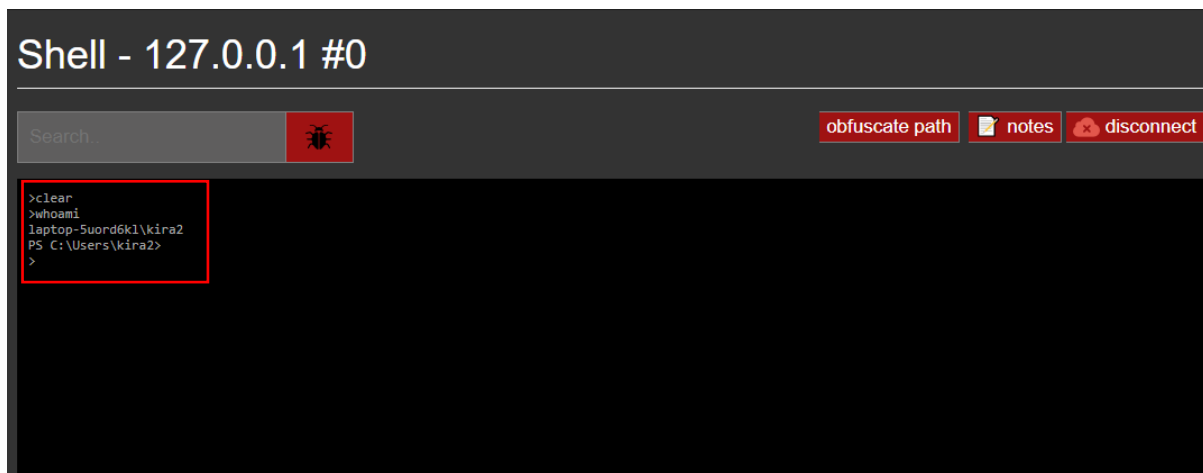
The C2 will be listen on two ports by default 443 and 1337 for tcp and 8080 for http

Simple reverse shell:

We have executed simple powershell reverse shell and we have 1 session



If we navigate to It and execute 'whoami' command



We can see our result let's execute module

Download &upload:

We have 2 sessions tcp and http. http has more features like download and upload files but tcp sessions does not have it.

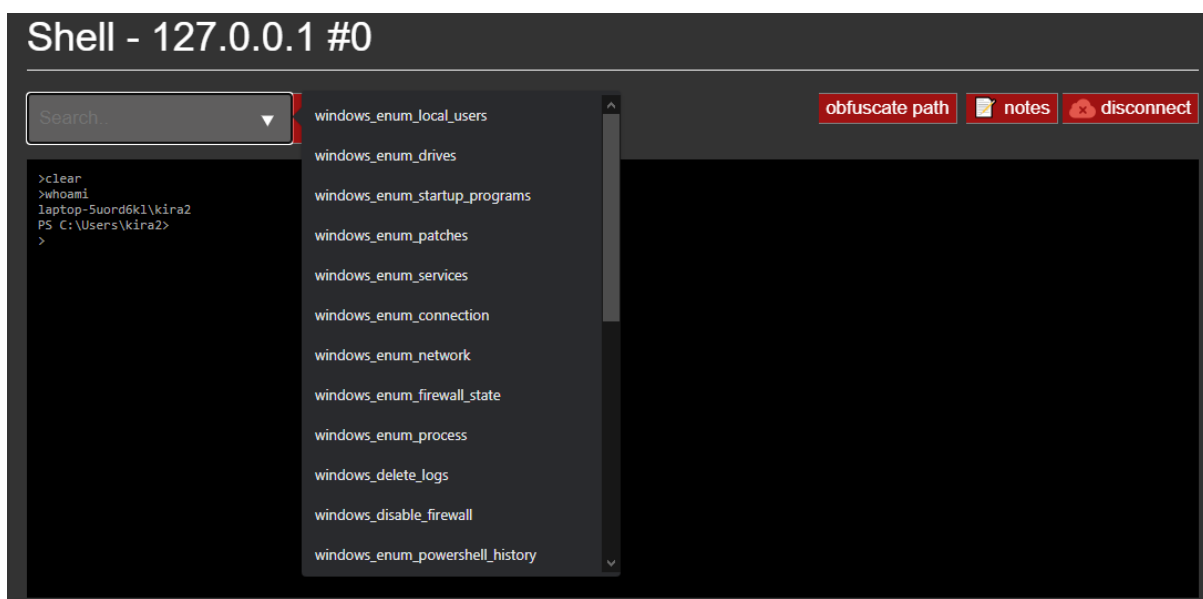
To download file from target use :

```
!download <path to download>
```

And for upload you can click upload file in the index page or upload from terminal using


```
!upload
```

Modules:



Here all modules we have now. I will select windows_enum_process module

windows_enum_process



Description:
list all processing

Copy command

As you can see we can see the description and copy command also if we click on the bug the module will be execute.

```
PS C:\Users\kira2>
Image Name PID Session Name Session# Mem Usage
=====
System Idle Process 0 Services 0 8 K
System 4 Services 0 5,448 K
Registry 124 Services 0 120,200 K
smss.exe 540 Services 0 1,096 K
csrss.exe 852 Services 0 5,880 K
wininit.exe 952 Services 0 6,316 K
csrss.exe 960 Console 1 6,632 K
services.exe 84 Services 0 9,928 K
lsass.exe 772 Services 0 28,244 K
svchost.exe 1060 Services 0 35,728 K
WUDFHost.exe 1080 Services 0 8,952 K
fontdrvhost.exe 1108 Services 0 3,136 K
winlogon.exe 1204 Console 1 12,844 K
fontdrvhost.exe 1252 Console 1 10,612 K
svchost.exe 1308 Services 0 18,088 K
svchost.exe 1360 Services 0 10,340 K
dwm.exe 1444 Console 1 151,712 K
svchost.exe 1512 Services 0 8,464 K
svchost.exe 1532 Services 0 10,968 K
svchost.exe 1584 Services 0 7,016 K
svchost.exe 1592 Services 0 6,116 K
svchost.exe 1708 Services 0 9,528 K
```

Also we can execute it using the terminal with “run” keyword

```
> run windows_enum_process
```

this will execute the same thing.

Notes:



Note for every session we have. We can store creds there.

obfuscate path:

it's way for obfuscate paths for hide and only work on powershell
if we try to obfuscate this path .

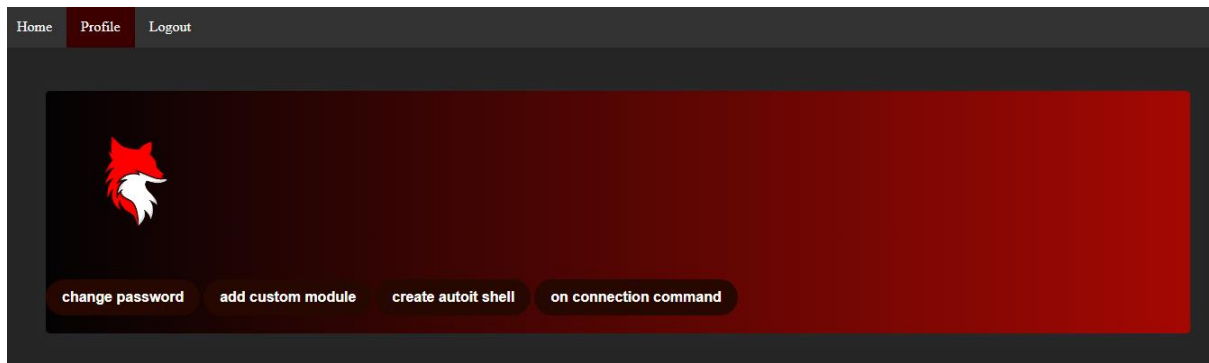


We will get.

```
$En?:Hom???ve\users\`TEST` \?.??C`M
```

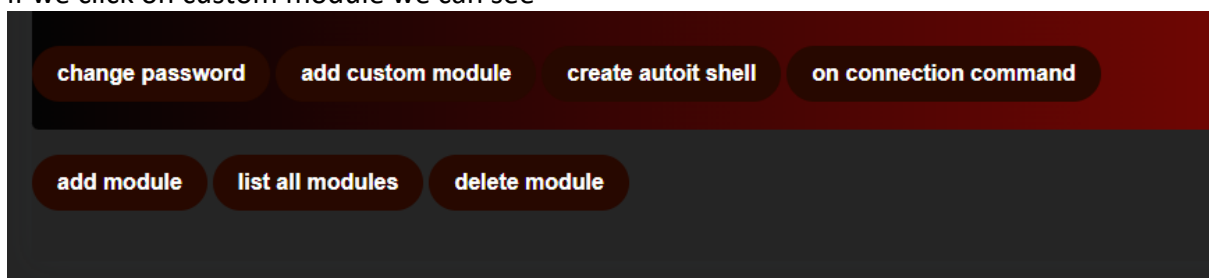
Profile:

From profile page we can control and make custom modules



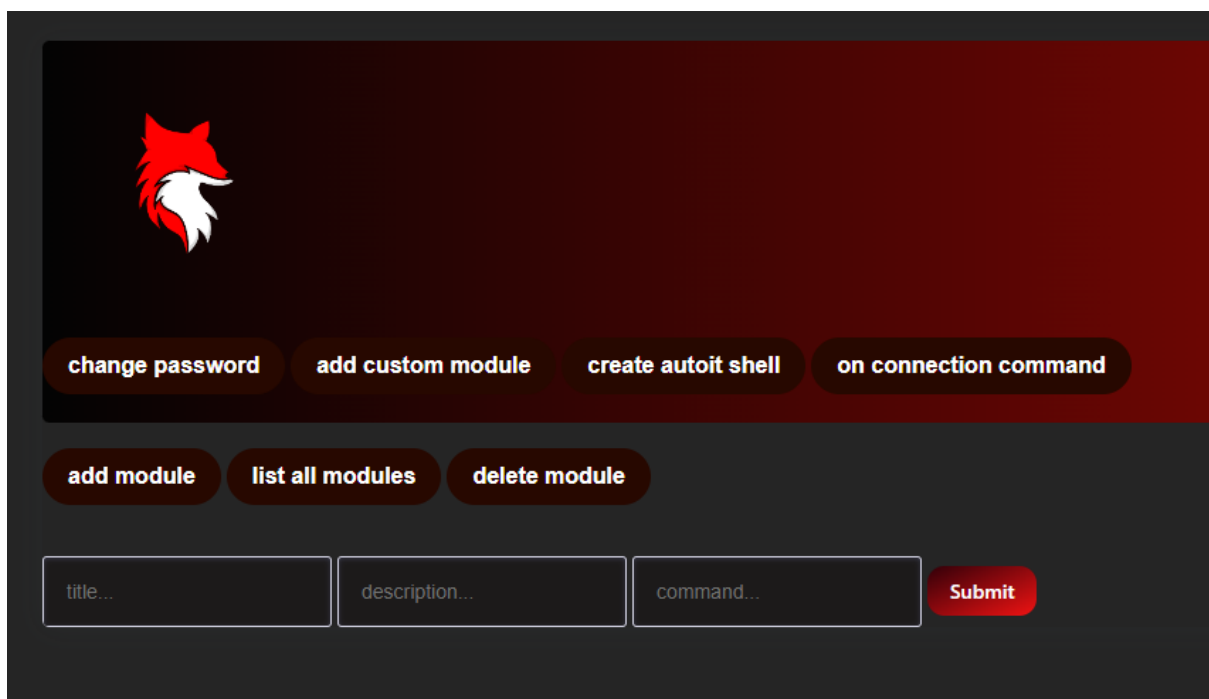
Custom modules:

if we click on custom module we can see



Add module - list modules – delete module

It's easy to understand but I will explain add module. Because there is good thing there.



Modules Key words:

In modules we have keywords to extend modules functionality

Argument:

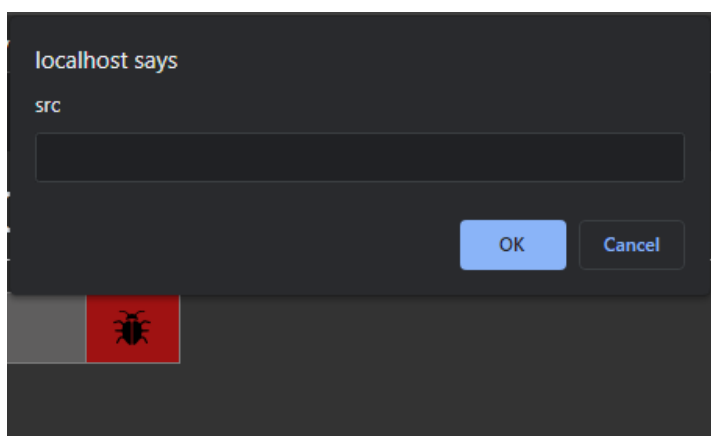
Put the title and description but when put the command we have extra option there. **We can use arguments.**

For example I want to make module for copy file and it will have 2 arguments source file and destination file.

I can put this on command input.

```
copy kiraC1_src_kiraC1 kiraC2_dst_kiraC2
```

Now let's execute this new module



It will ask you for argument from website

If we want to execute it from terminal we can use it like this.

```
>run windows_copy srcfilehere dstfilehere
```

If we have 3 arguments just put C3 and C4....

Random number:

For create random number in the module to make the module more randomize you can enter

```
kiraRandomint
```

but you have to put number in the end to be:

```
kiraRandomint1
```

so that's mean replace all kiraRandomint with random number the length of the number and the number it self is a random the number on the end is important to **change all numbers and make it same or different**

example:

```
$number2 = 1
```

```
$number2 = 2
```

Here we have 2 numbers and we want to make it random every time so let's use kiraRandomint keyword

```
$number2 = kiraRandomint1
```

```
$number2 = kiraRandomint1
```

When we run the module in the victim the new payload will be for example


```
$number2 = 221132
$number2 = 221132
```

And if we run the module again we will get different number. If I want to make 1 random number and 2 randoms number but linked tighter I can do it just change the end on the keyword

Let's see this code :

```
$number1 = kiraRandomint1
$number1 = kiraRandomint1
$number2 = kiraRandomint2
$number3 = kiraRandomint3
```

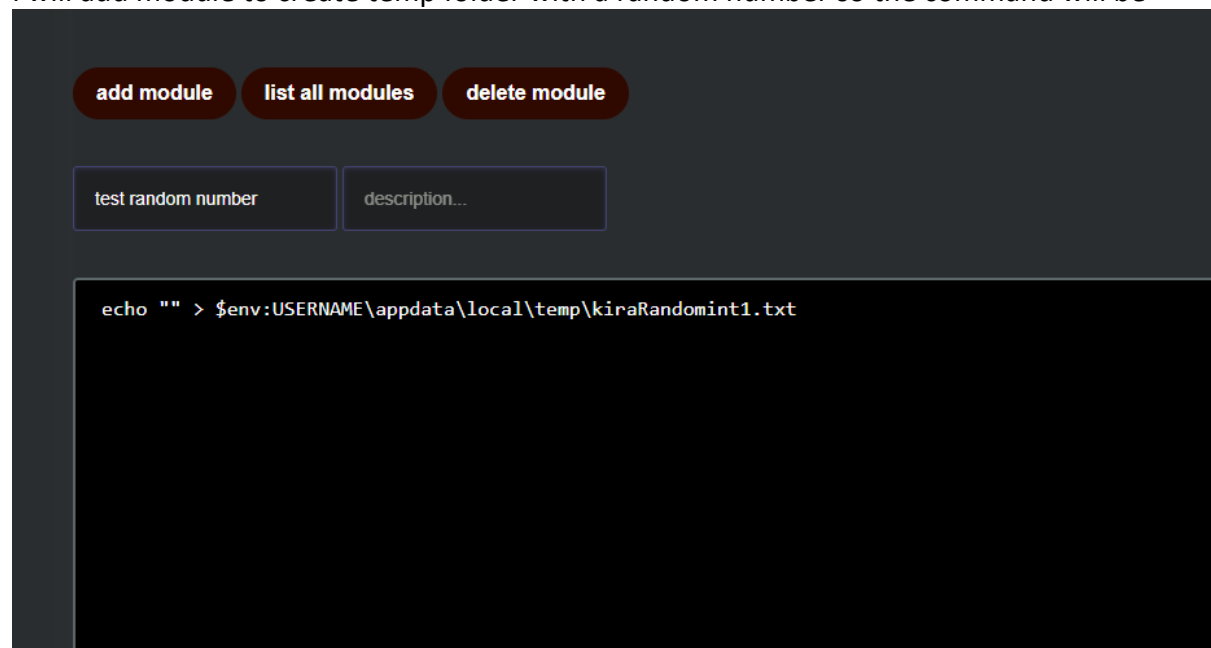
When we want to run the module, the executed module will be like this

```
$number1 = 12122
$number1 = 12122
$number2 = 2321
$number3 = 32434
```

The first two numbers are the same because in the end of the keyword is 1.

Real example:

I will add module to create temp folder with a random number so the command will be



The screenshot shows a dark-themed interface for managing modules. At the top, there are three buttons: "add module", "list all modules", and "delete module". Below these buttons are two input fields: "test random number" and "description...". At the bottom, there is a large text area containing the command: `echo "" > $env:USERNAME\appdata\local\temp\kiraRandomint1.txt`.

This is the command in the module now let's save it and run it on the target machine. If we run the module we will get

```
echo "" > $env:USERNAME\appdata\local\temp\5547123525605.txt
```

Random string:

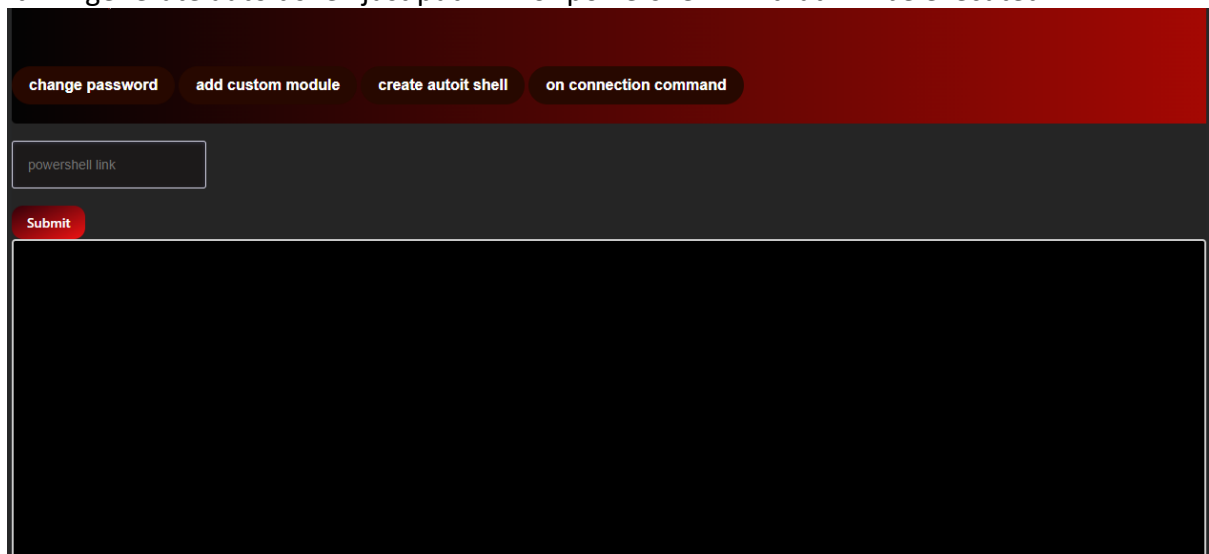
It's the same thing but with

```
kiraRandomstr
```

keyword you can combine them to make it more randomize

Autoit:

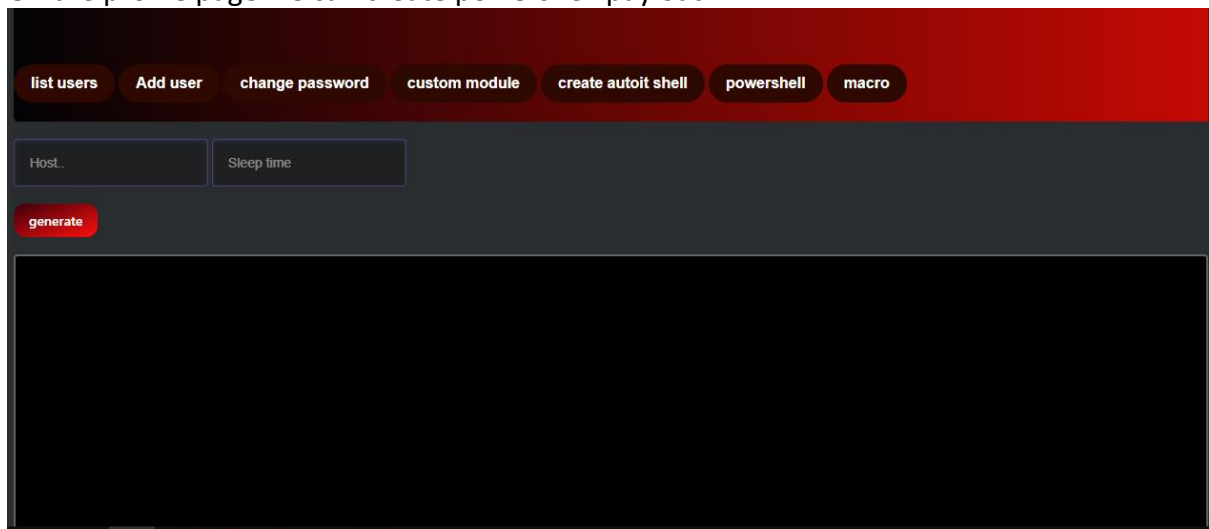
It will generate autoit shell just put link for powershell link that will be executed.



The screenshot shows a web interface for generating an Autoit shell. At the top, there is a red header bar with four buttons: "change password", "add custom module", "create autoit shell", and "on connection command". Below the header, there is a text input field labeled "powershell link". Below the input field, there is a red button labeled "Submit". The main area of the interface is a large black rectangle, likely for displaying the generated code or output.

Powershell:

On the profile page we can create powershell payload



The screenshot shows a web interface for generating a Powershell payload. At the top, there is a red header bar with six buttons: "list users", "Add user", "change password", "custom module", "create autoit shell", "powershell", and "macro". Below the header, there are two text input fields: "Host" and "Sleep time". Below the input fields, there is a red button labeled "generate". The main area of the interface is a large black rectangle, likely for displaying the generated payload or output.

Because the payload is http reverse shell you have to put the sleep time carefully

And the host will be the domain with port from config.js file

Files:

Config.js file:

In config.js file you will find a lot of setting that you can customize your C2 with. Like terminal color or sessions

.env:

There is two values you can changes them

You have to change TOKEN_SECRET value to unique value you can do it with node .

```
crypto.randomBytes(64).toString('hex');
```

Also there are ipdata api key value change it to your key

Block connections:

Because malware analysis use vpns for test malwares we create this feature. After you put your ipdata key change config.js values

```
block_tor:false,  
  block_proxy:false,  
  block_anonymous:false,
```

as you can see we have 3 options block tor,vpns,proxy just change any one of them to true and will block it using [ipdata](#).