



CyberChef

Information Security Inc.

Contents

- About CyberChef
- Live demo
- Browser support
- Testing Environment
- Required packages
- Installing CyberChef
- Using CyberChef
- References

About CyberChef

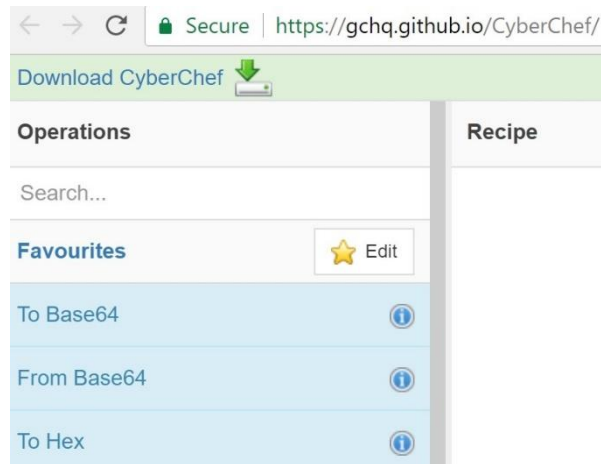
- CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser

I HATE BEING SEXY BUT
I'M A CHEF SO CAN'T HELP IT!
#CYBERCHEFSAYS



Live demo

- Have fun!
<https://gchq.github.io/CyberChef/>



Browser support

- Google Chrome 40+
- Mozilla Firefox 35+
- Microsoft Edge 14+

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Required packages

- Git, npm, Grunt `npm install -g grunt-cli`
- Installing node and npm
(<http://www.free4net.com/2014/06/installing-nodejs-and-npm-in-kali-linux.html>)

```
apt-get install python g++ make checkinstall fakeroot
src=$(mktemp -d) && cd $src
wget -N http://nodejs.org/dist/node-latest.tar.gz
tar xzvf node-latest.tar.gz && cd node-v*
./configure
fakeroot checkinstall -y --install=no --pkgversion $(echo $(pwd) | sed -n -re's/.*node-v(.+)$/\1/p') make -j$((nproc)+1) install
dpkg -i node *
```

Installing CyberChef

- Download GitHub and install CyberChef repository

```
git clone https://github.com/gchq/CyberChef.git
cd CyberChef/
npm install
```

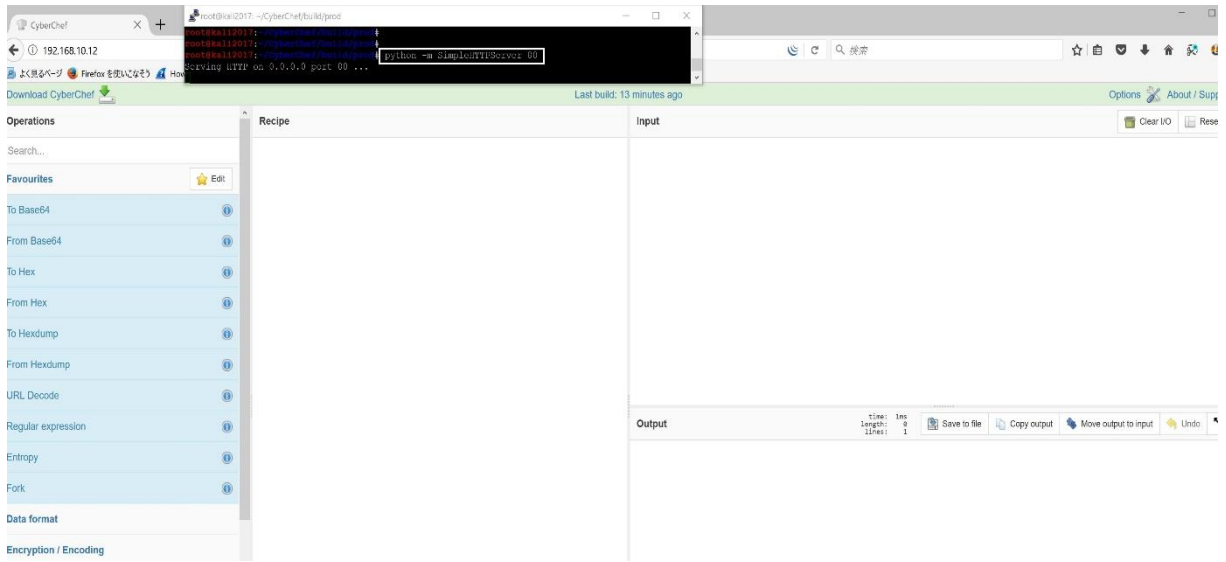

Installing CyberChef

- Compiling CyberChef => the following command It will lint, test, compile and compress all the source files and create a production-ready build in build/prod. It will also create the inline version of CyberChef at the same location, called cyberchef.htm

```
root@kali2017:~/CyberChef# grunt prod  
Running "eslint:configs" (eslint) task  
  
Running "eslint:core" (eslint) task
```

Using CyberChef

- Running a python webserver and start using CyberChef



Using CyberChef

- Disassemble x86

The screenshot shows the CyberChef web interface. On the left is a sidebar with various recipes, including 'Disassemble x86'. The main area displays the configuration for the 'Disassemble x86' recipe, which is highlighted with a green background. The configuration includes:

- Bit mode: 64
- Compatibility: Full x86 architecture
- Code Segment (CS): 16
- Offset (IP): 0
- Checkboxes: Show instruction hex (checked), Show instruction position (checked)

The 'Input' field contains the hex string: 9090908820ae. The 'Output' field shows the disassembled instructions:

Hex	Instruction
0000000000000000 90	NOP
0000000000000001 90	NOP
0000000000000002 90	NOP
0000000000000003 8820	MOV BYTE PTR [RAX],AH
0000000000000005 AE	SCAS AL, BYTE PTR [RDI]

Performance metrics for the output: time: 2ms, length: 307, lines: 6. A 'Save to file' button is also visible.

Using CyberChef

- On Apache webserver for production purposes

```
root@kali2017:~/var/www/html/prod# pwd
/var/www/html/prod
root@kali2017:~/var/www/html/prod# service apache2 start
root@kali2017:~/var/www/html/prod# ls -alh
total 15M
drwxr-xr-x 3 root root 4.0K Oct 24 06:45 .
drwxr-xr-x 3 root root 4.0K Oct 24 06:45 ..
-rwxr-xr-x 1 root root 889K Oct 24 06:45 CharEnc.js
-rwxr-xr-x 1 root root 510K Oct 24 06:45 Ciphers.js
-rwxr-xr-x 1 root root 1.2M Oct 24 06:45 Code.js
-rwxr-xr-x 1 root root 564K Oct 24 06:45 Compression.js
-rwxr-xr-x 1 root root 4.9M Oct 24 06:45 cyberchef.htm
-rwxr-xr-x 1 root root 503K Oct 24 06:45 Diff.js
-rwxr-xr-x 1 root root 3.9K Oct 24 06:45 Encodings.js
-rwxr-xr-x 1 root root 609K Oct 24 06:45 Hashing.js
-rwxr-xr-x 1 root root 1.1M Oct 24 06:45 HTTP.js
-rwxr-xr-x 1 root root 516K Oct 24 06:45 Image.js
drwxr-xr-x 2 root root 4.0K Oct 24 06:45 images
-rwxr-xr-x 1 root root 26K Oct 24 06:45 index.html
-rwxr-xr-x 1 root root 530K Oct 24 06:45 JSBN.js
-rwxr-xr-x 1 root root 2.0M Oct 24 06:45 main.js
-rwxr-xr-x 1 root root 734K Oct 24 06:45 PublicKey.js
-rwxr-xr-x 1 root root 120K Oct 24 06:45 Shellcode.js
-rwxr-xr-x 1 root root 130K Oct 24 06:45 styles.css
-rwxr-xr-x 1 root root 497K Oct 24 06:45 URL.js
```


References

- Kitploit

http://www.kitploit.com/2017/08/cyberchef-cyber-swiss-army-knife-web_5.html

- Kali Linux

<https://www.kali.org/downloads/>

- Npm

<http://www.free4net.com/2014/06/installing-nodejs-and-npm-in-kali-linux.html>