
```
$ reGeorgSocksProxy.py [-h] [-l] [-p] [-r] -u [-v]
```

Socks server for reGeorg HTTP(s) tunneller

optional arguments:

-h, --help	show this help message and exit
-l, --listen-on	The default listening address
-p, --listen-port	The default listening port
-r, --read-buff	Local read buffer, max data to be sent per POST
-u, --url	The url containing the tunnel script
-v, --verbose	Verbose output[INFO DEBUG]

- **Step 1.** Upload tunnel.(aspx|ashx|jsp|php) to a webserver (How you do that is up to you)
- **Step 2.** Configure you tools to use a socks proxy, use the ip address and port you specified when you started the reGeorgSocksProxy.py

** Note, if you tools, such as NMap doesn't support socks proxies, use [proxychains](#) (see wiki)

Step 3. Hack the planet :)

Example

```
$ python reGeorgSocksProxy.py -p 8080 -u  
http://upload.sensepost.net:8080/tunnel/tunnel.jsp
```

License

MIT