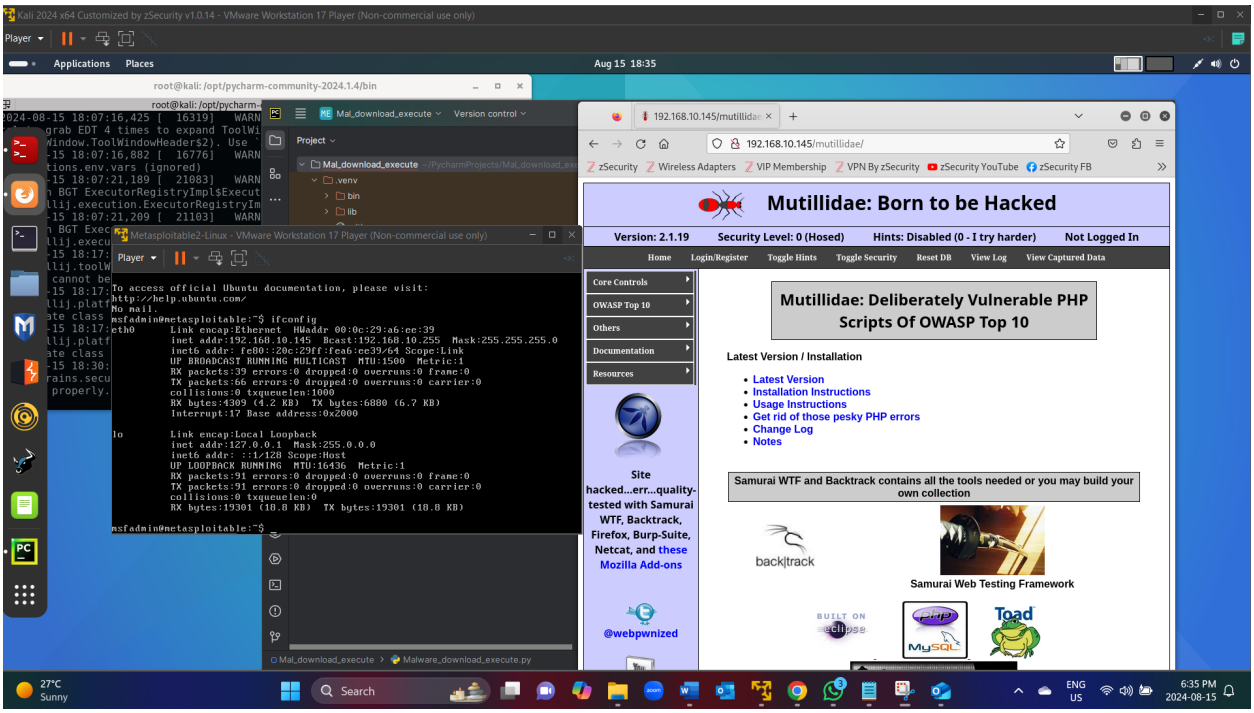
WEBSITE/ WEB APPLICATION HACKING:

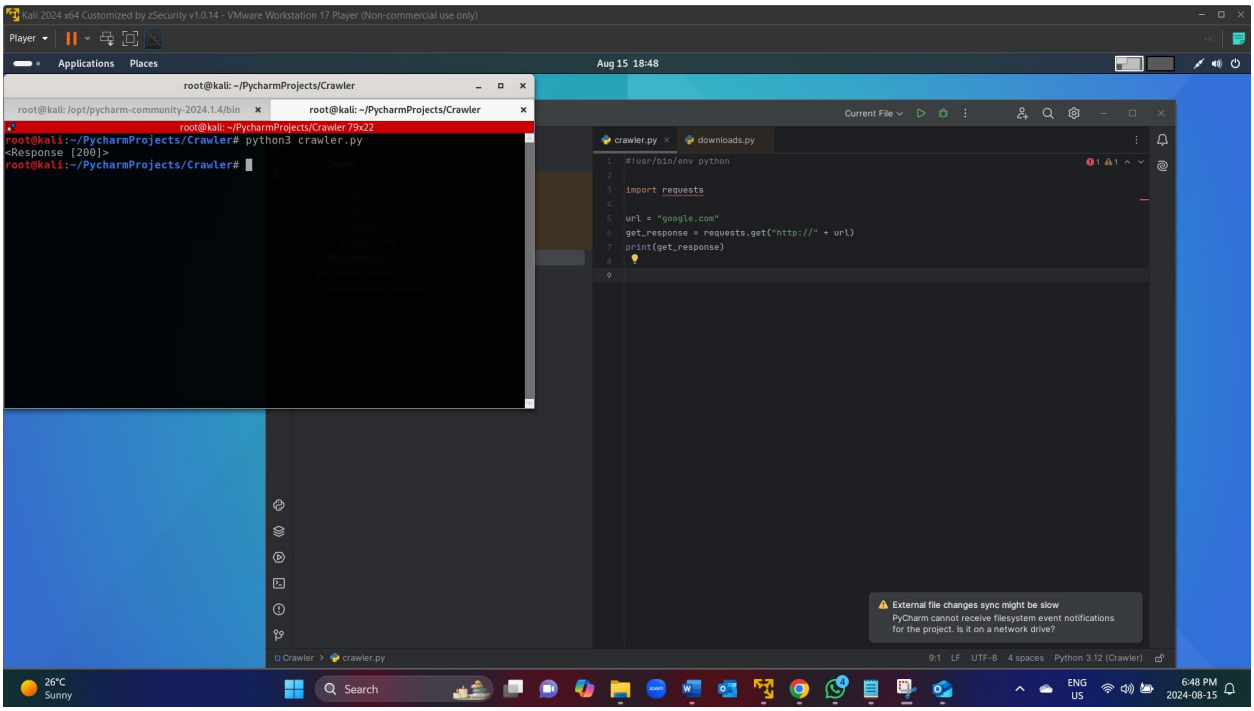
Download Metasploitable:

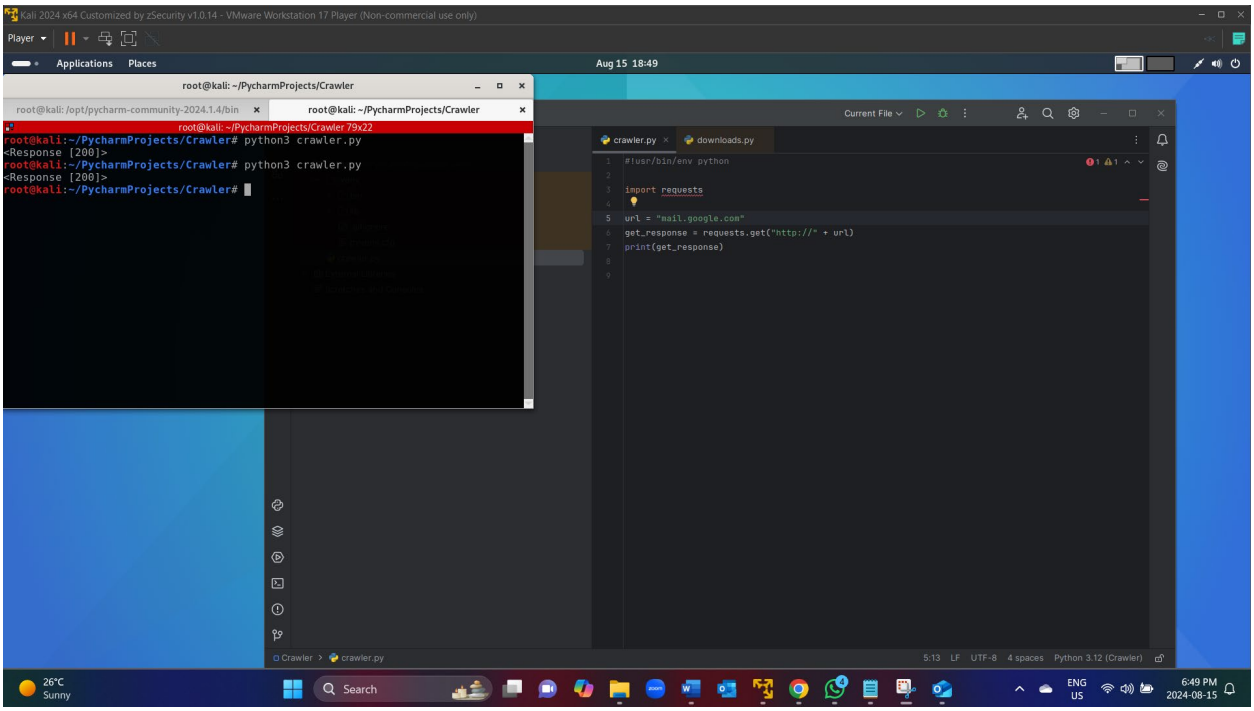


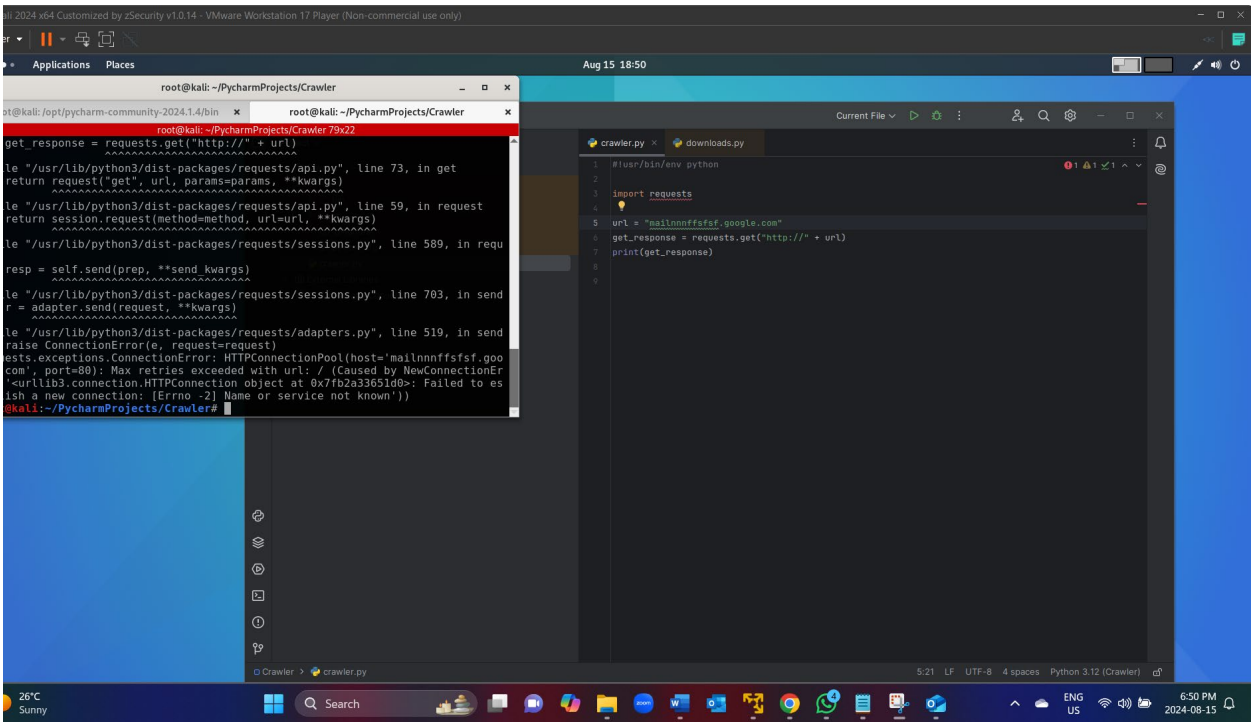
Website Hacking – Writing a Crawler:

Sending GET Requests To Web Servers:

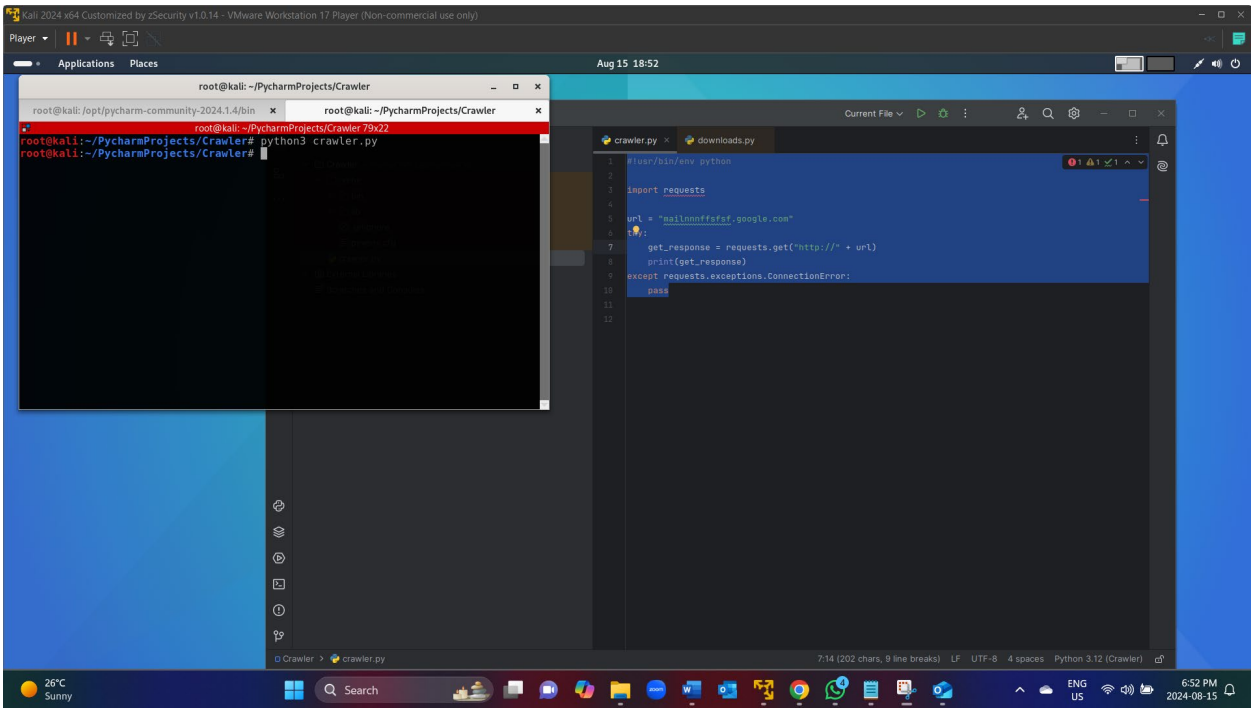
```
#!usr/bin/env python

import requests

url = "google.com"
get_response = requests.get("http://" + url)
print(get_response)
```



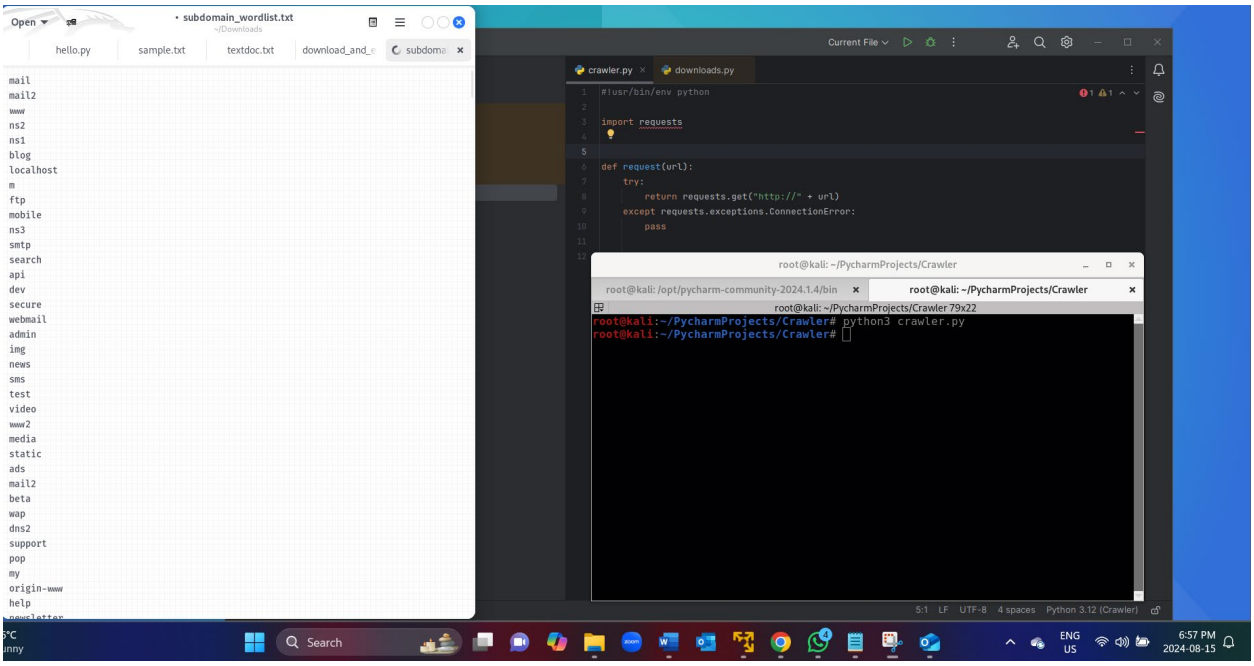

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 15 18:49
root@kali: ~/PycharmProjects/Crawler
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/Crawler
root@kali: ~/PycharmProjects/Crawler 79x22
root@kali:~/PycharmProjects/Crawler# python3 crawler.py
<Response [200]>
root@kali:~/PycharmProjects/Crawler# python3 crawler.py
<Response [200]>
root@kali:~/PycharmProjects/Crawler#
Current File
crawler.py
downloads.py
#!usr/bin/env python
import requests
url = "mail.google.com"
get_response = requests.get("http://" + url)
print(get_response)
Crawler
crawler.py
5:13 LF UTF-8 4 spaces Python 3.12 (Crawler)
26°C
Sunny
Search
ENG
US
6:49 PM
2024-08-15


Applications
Places
Aug 15 18:50
root@kali: ~/PycharmProjects/Crawler
root@kali: ~/PycharmProjects/Crawler 79x22
get_response = requests.get("http://" + url)
le "/usr/lib/python3/dist-packages/requests/api.py", line 73, in get
return request("get", url, params=params, **kwargs)
le "/usr/lib/python3/dist-packages/requests/api.py", line 59, in request
return session.request(method=method, url=url, **kwargs)
le "/usr/lib/python3/dist-packages/requests/sessions.py", line 589, in requ
resp = self.send(prep, **send_kwargs)
le "/usr/lib/python3/dist-packages/requests/sessions.py", line 703, in send
r = adapter.send(request, **kwargs)
le "/usr/lib/python3/dist-packages/requests/adapters.py", line 519, in send
raise ConnectionError(e, request=request)
ests.exceptions.ConnectionError: HTTPConnectionPool(host='mailnnnffsfsf.goo
com', port=80): Max retries exceeded with url: / (Caused by NewConnectionEr
'<urllib3.connection.HTTPConnection object at 0x7fb2a33651d0>: Failed to es
ish a new connection: [Errno -2] Name or service not known'))
@kali:~/PycharmProjects/Crawler#
Current File
crawler.py
downloads.py
#!usr/bin/env python
import requests
url = "mailnnnffsfsf.google.com"
get_response = requests.get("http://" + url)
print(get_response)
Crawler
crawler.py
5:21 LF UTF-8 4 spaces Python 3.12 (Crawler)
26°C
Sunny
Search
ENG
US
6:50 PM
2024-08-15

```
#!usr/bin/env python


import requests


url = "mailnnnffsfsf.google.com"
try:
    get_response = requests.get("http://" + url)
    print(get_response)
except requests.exceptions.ConnectionError:
    pass
```

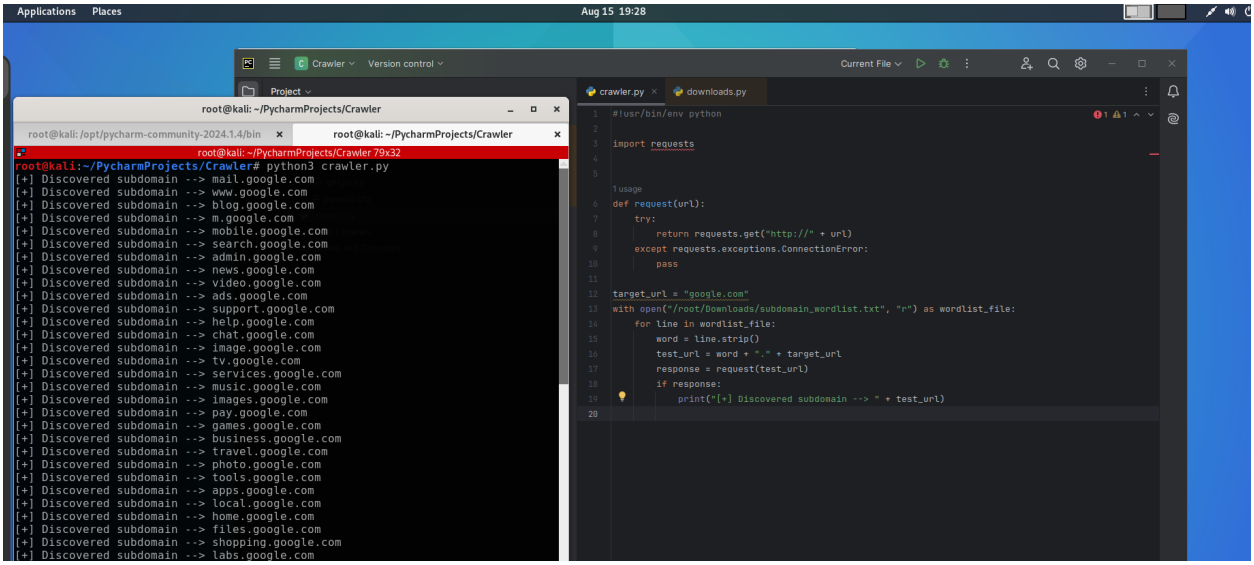


Discovering Website Subdomains Using Python

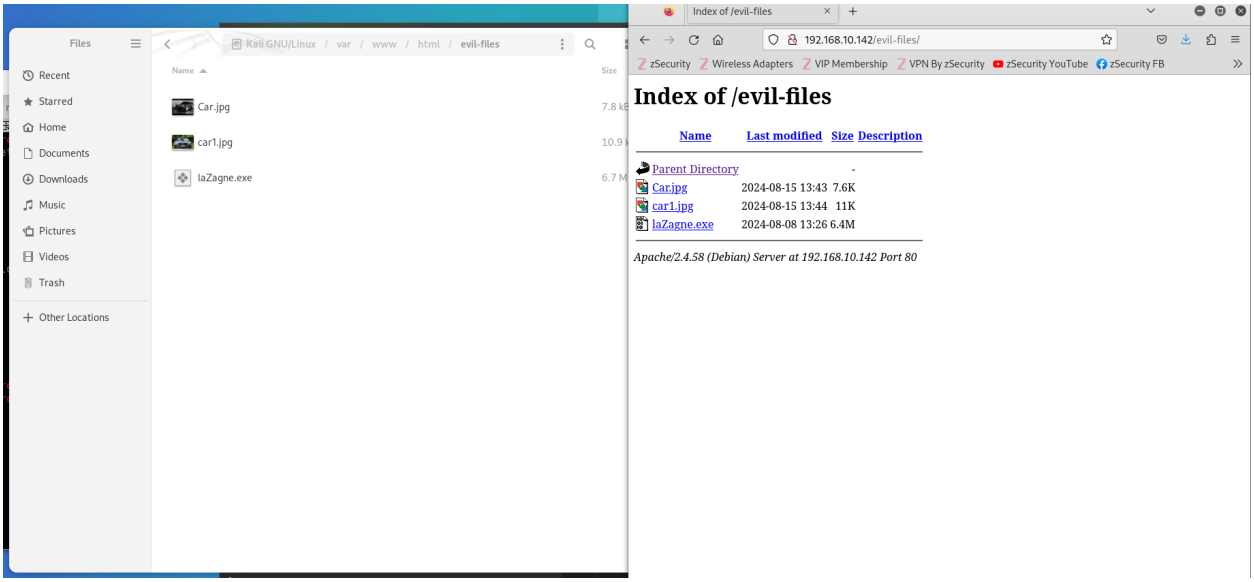


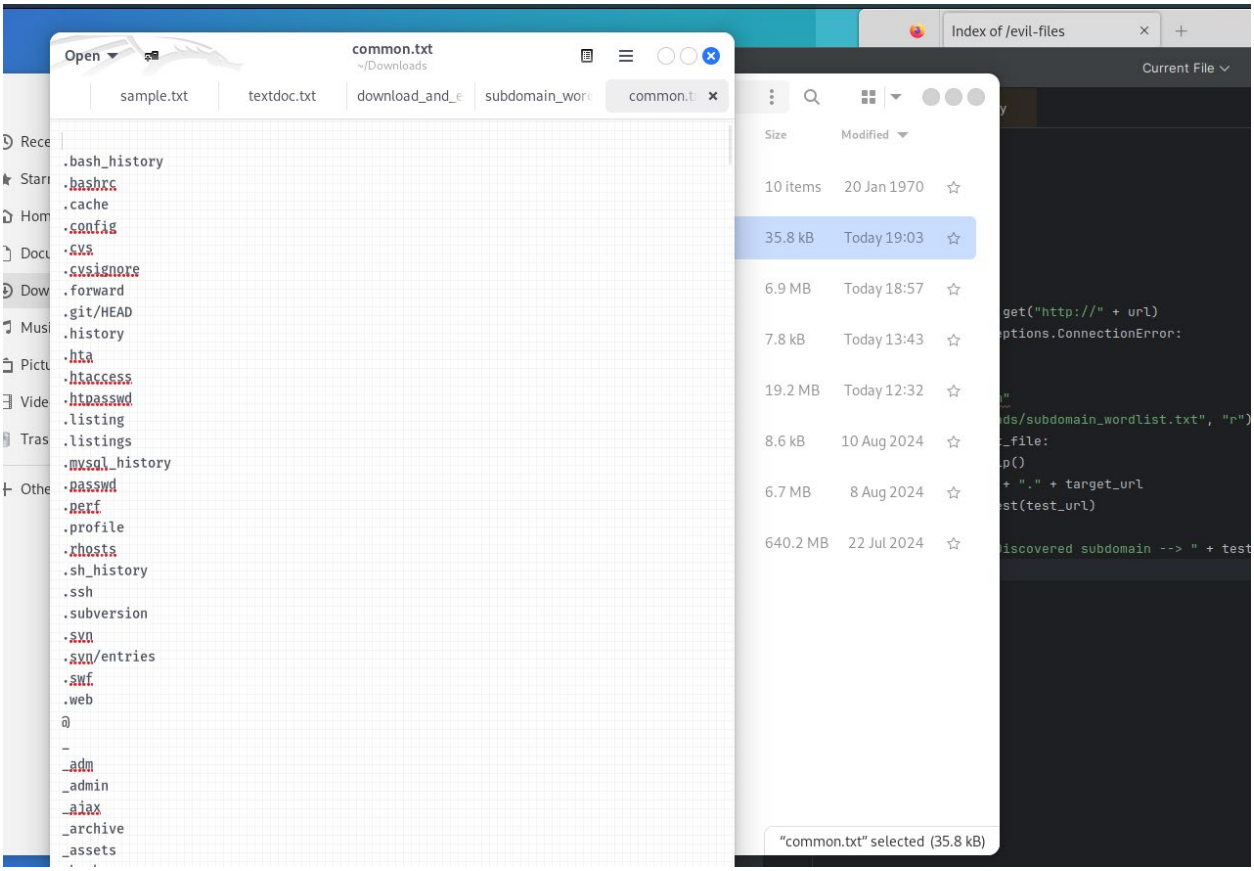

```
#!usr/bin/env python


import requests


def request(url):
    try:
        return requests.get("http://" + url)
    except requests.exceptions.ConnectionError:
        pass


target_url = "google.com"
with open("/root/Downloads/subdomain_wordlist.txt", "r") as wordlist_file:
    for line in wordlist_file:
        word = line.strip()
```

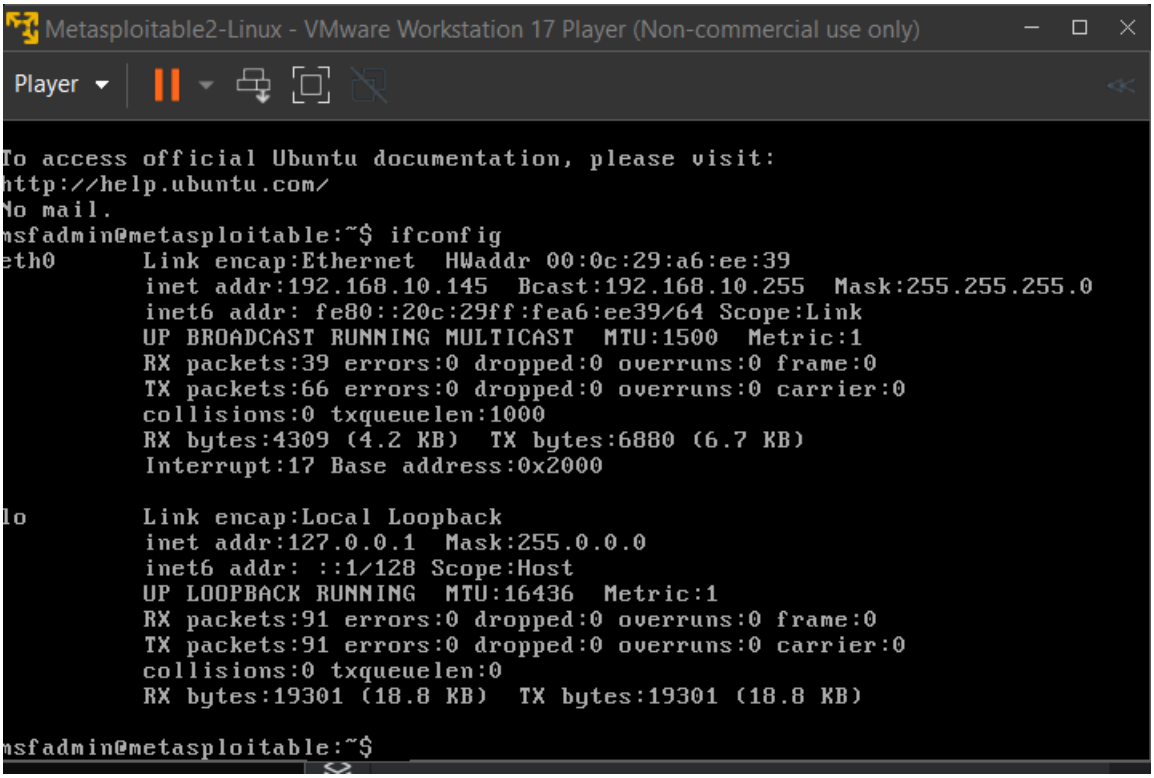
```
test_url = word + "." + target_url

response = request(test_url)

if response:

   print("[+] Discovered subdomain --> " + test_url)
```

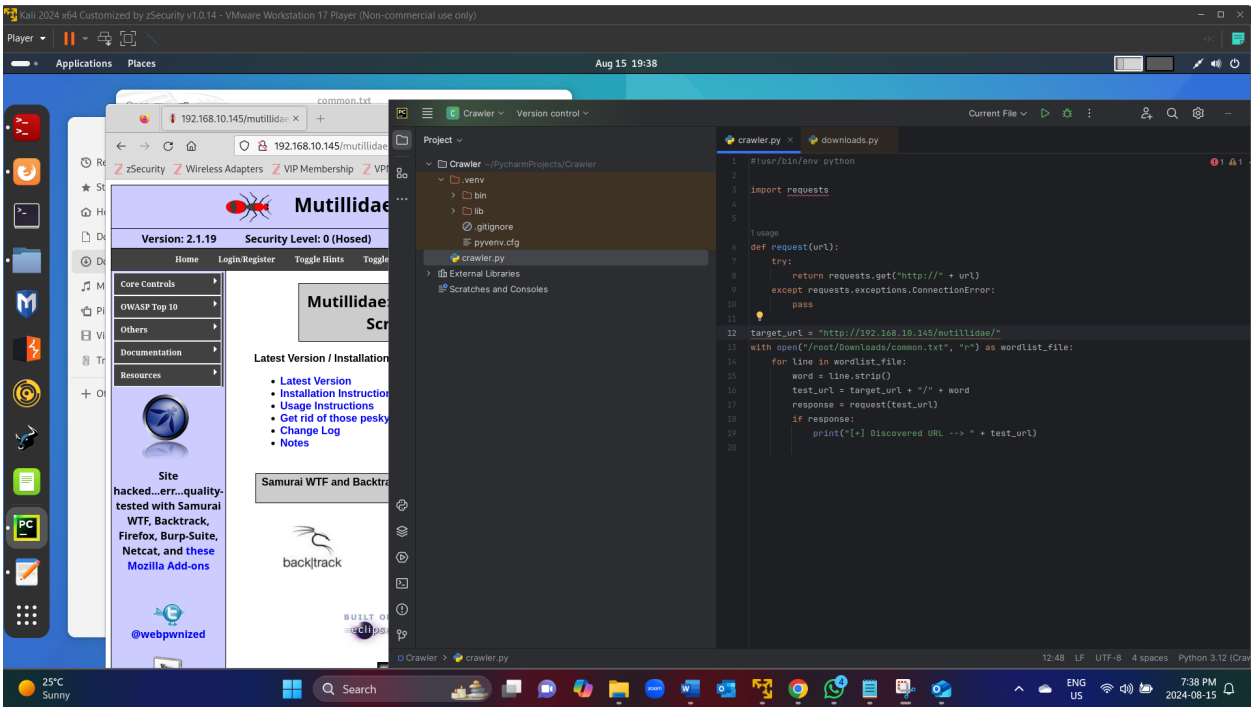


Discovering Hidden Paths in Websites:



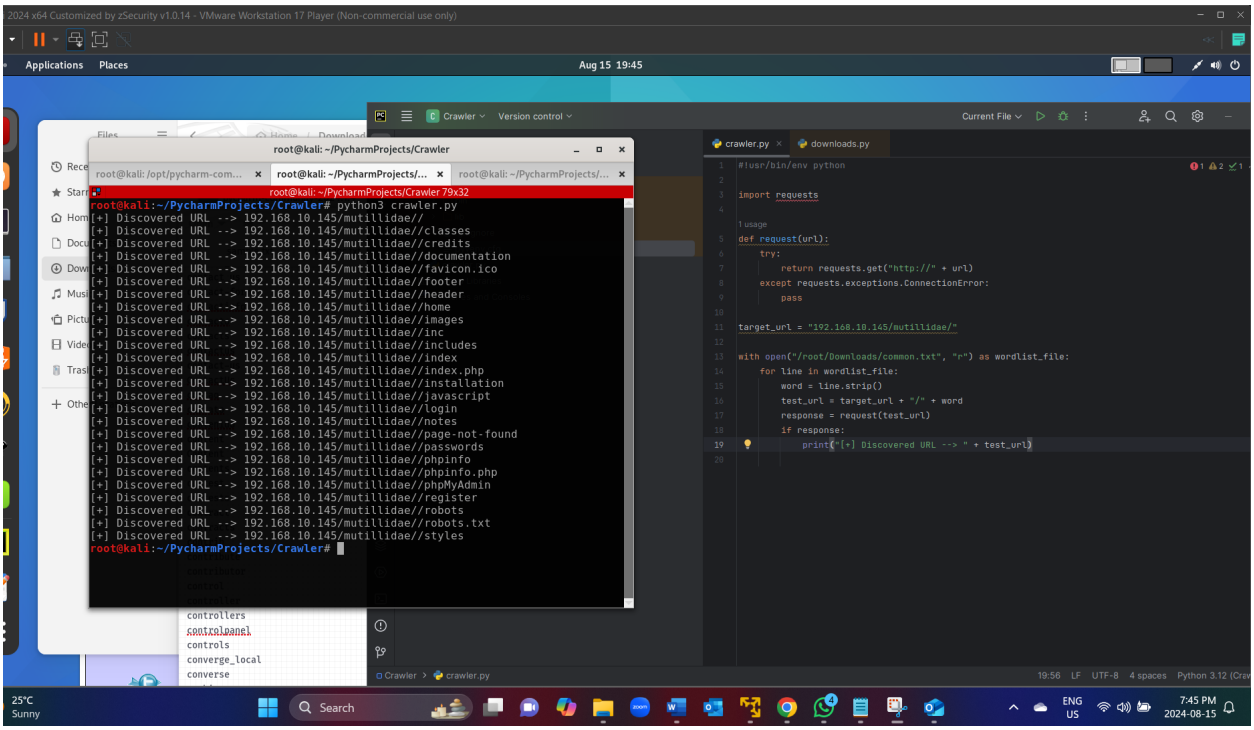


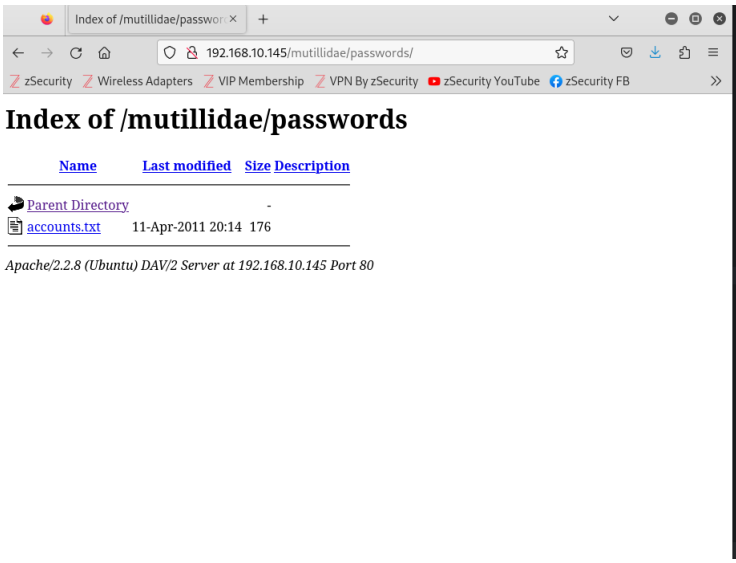

Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:a6:ee:39
inet addr:192.168.10.145 Bcast:192.168.10.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fea6:ee39/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:39 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4309 (4.2 KB) TX bytes:6880 (6.7 KB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$

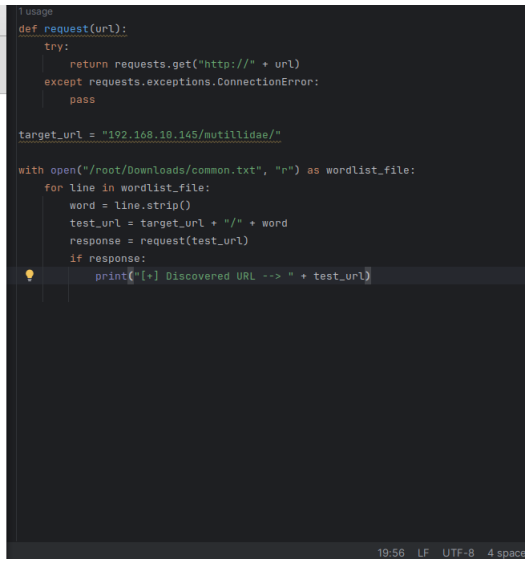

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Applications
Places
Aug 15 19:38
Mutillidae
Version: 2.1.19
Security Level: 0 (Hosed)
Core Controls
OWASP Top 10
Others
Documentation
Resources
Latest Version / Installation
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
back|track
Crawler
Version control
crawler.py
downloads.py
#!usr/bin/env python
import requests
def request(url):
try:
return requests.get("http://" + url)
except requests.exceptions.ConnectionError:
pass
target_url = "http://192.168.10.145/mutillidae/"
with open("/root/Downloads/common.txt", "r") as wordlist_file:
for line in wordlist_file:
word = line.strip()
test_url = target_url + "/" + word
response = request(test_url)
if response:
print("[+] Discovered URL --> " + test_url)
25°C
Sunny
Search
ENG
US
7:38 PM
2024-08-15

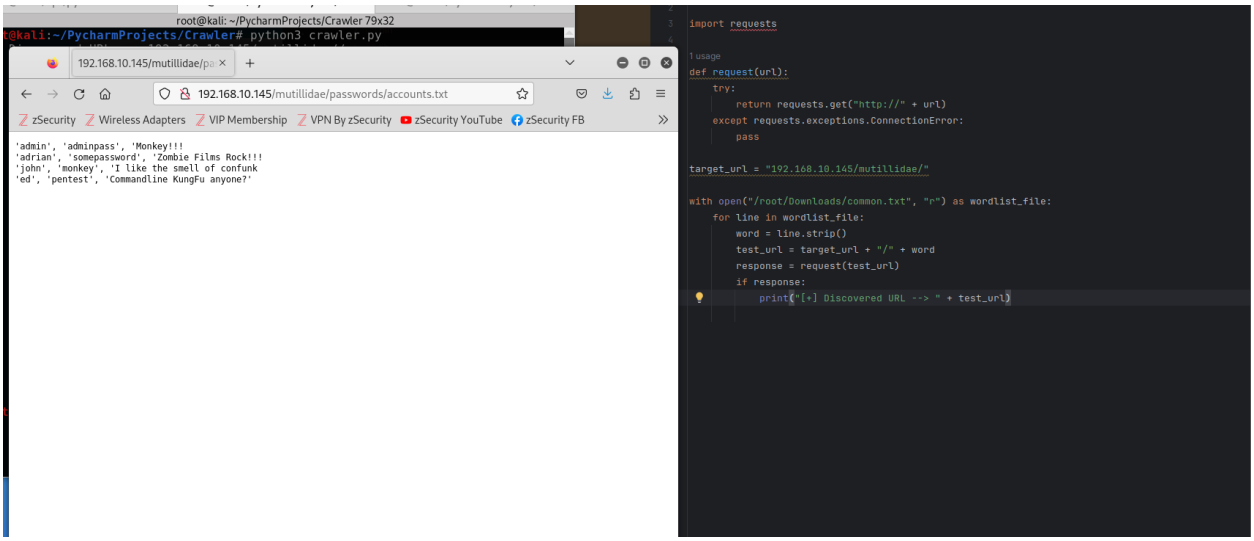
Crawler.py()

```
#!usr/bin/env python


import requests


def request(url):
  try:
    return requests.get("http://" + url)
  except requests.exceptions.ConnectionError:
    pass


target_url = "http://192.168.10.145/mutillidae/"
with open("/root/Downloads/common.txt", "r") as wordlist_file:
  for line in wordlist_file:
    word = line.strip()
    test_url = target_url + "/" + word
    response = request(test_url)
    if response:
      print("[+] Discovered URL --> " + test_url)
```


root@kali: ~/PycharmProjects/Crawler
root@kali:~/PycharmProjects/Crawler# python3 crawler.py
[+] Discovered URL --> 192.168.10.145/mutillidae//
[+] Discovered URL --> 192.168.10.145/mutillidae//classes
[+] Discovered URL --> 192.168.10.145/mutillidae//credits
[+] Discovered URL --> 192.168.10.145/mutillidae//documentation
[+] Discovered URL --> 192.168.10.145/mutillidae//favicon.ico
[+] Discovered URL --> 192.168.10.145/mutillidae//footer
[+] Discovered URL --> 192.168.10.145/mutillidae//header
[+] Discovered URL --> 192.168.10.145/mutillidae//home
[+] Discovered URL --> 192.168.10.145/mutillidae//images
[+] Discovered URL --> 192.168.10.145/mutillidae//inc
[+] Discovered URL --> 192.168.10.145/mutillidae//includes
[+] Discovered URL --> 192.168.10.145/mutillidae//index
[+] Discovered URL --> 192.168.10.145/mutillidae//index.php
[+] Discovered URL --> 192.168.10.145/mutillidae//installation
[+] Discovered URL --> 192.168.10.145/mutillidae//javascript
[+] Discovered URL --> 192.168.10.145/mutillidae//login
[+] Discovered URL --> 192.168.10.145/mutillidae//notes
[+] Discovered URL --> 192.168.10.145/mutillidae//page-not-found
[+] Discovered URL --> 192.168.10.145/mutillidae//passwords
[+] Discovered URL --> 192.168.10.145/mutillidae//phpinfo
[+] Discovered URL --> 192.168.10.145/mutillidae//phpinfo.php
[+] Discovered URL --> 192.168.10.145/mutillidae//phpMyAdmin
[+] Discovered URL --> 192.168.10.145/mutillidae//register
[+] Discovered URL --> 192.168.10.145/mutillidae//robots
[+] Discovered URL --> 192.168.10.145/mutillidae//robots.txt
[+] Discovered URL --> 192.168.10.145/mutillidae//styles
root@kali:~/PycharmProjects/Crawler#
crawler.py
downloads.py
#!usr/bin/env python
import requests
def request(url):
try:
return requests.get("http://" + url)
except requests.exceptions.ConnectionError:
pass
target_url = "192.168.10.145/mutillidae/"
with open("/root/Downloads/common.txt", "r") as wordlist_file:
for line in wordlist_file:
word = line.strip()
test_url = target_url + "/" + word
response = request(test_url)
if response:
print("[+] Discovered URL --> " + test_url)

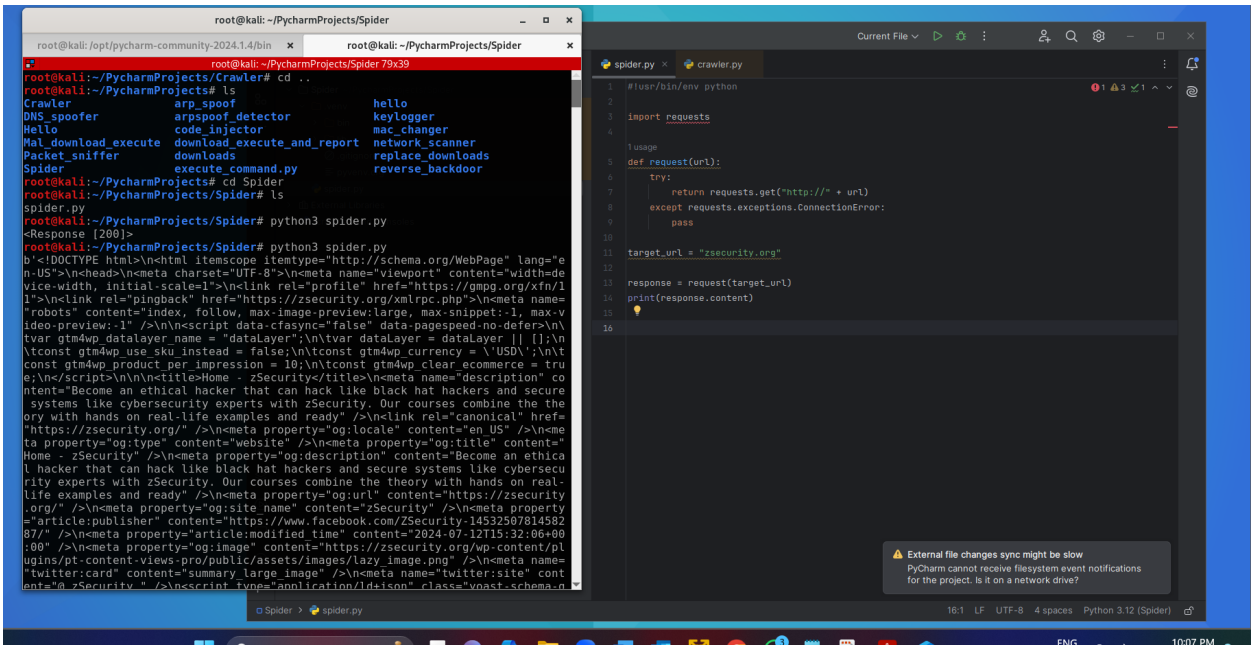

Index of /mutillidae/passwords
192.168.10.145/mutillidae/passwords/
zSecurity
Wireless Adapters
VIP Membership
VPN By zSecurity
zSecurity YouTube
zSecurity FB
Index of /mutillidae/passwords
Name
Last modified
Size
Description
Parent Directory
accounts.txt
11-Apr-2011 20:14
176
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.145 Port 80


def request(url):
try:
return requests.get("http://" + url)
except requests.exceptions.ConnectionError:
pass
target_url = "192.168.10.145/mutillidae/"
with open("/root/Downloads/common.txt", "r") as wordlist_file:
for line in wordlist_file:
word = line.strip()
test_url = target_url + "/" + word
response = request(test_url)
if response:
print("[+] Discovered URL --> " + test_url)


root@kali: ~/PycharmProjects/Crawler 79x32
@kali:~/PycharmProjects/Crawler# python3 crawler.py
192.168.10.145/mutillidae/pa
192.168.10.145/mutillidae/passwords/accounts.txt
zSecurity
Wireless Adapters
VIP Membership
VPN By zSecurity
zSecurity YouTube
zSecurity FB
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
import requests
1 usage
def request(url):
try:
return requests.get("http://" + url)
except requests.exceptions.ConnectionError:
pass
target_url = "192.168.10.145/mutillidae/"
with open("/root/Downloads/common.txt", "r") as wordlist_file:
for line in wordlist_file:
word = line.strip()
test_url = target_url + "/" + word
response = request(test_url)
if response:
print("[+] Discovered URL --> " + test_url)

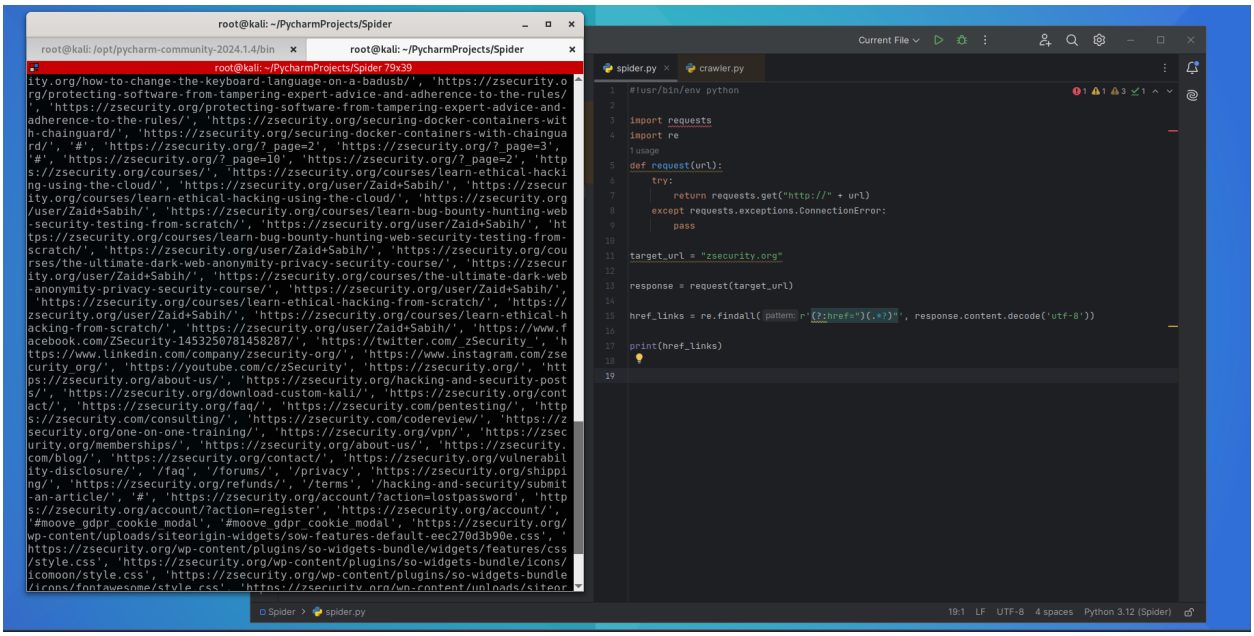
Reading Response Content

```
#!usr/bin/env python

import requests

def request(url):
    try:
        return requests.get("http://" + url)
    except requests.exceptions.ConnectionError:
        pass

target_url = "zsecurity.org"

response = request(target_url)
print(response.content)
```



Extracting Useful Data From Response

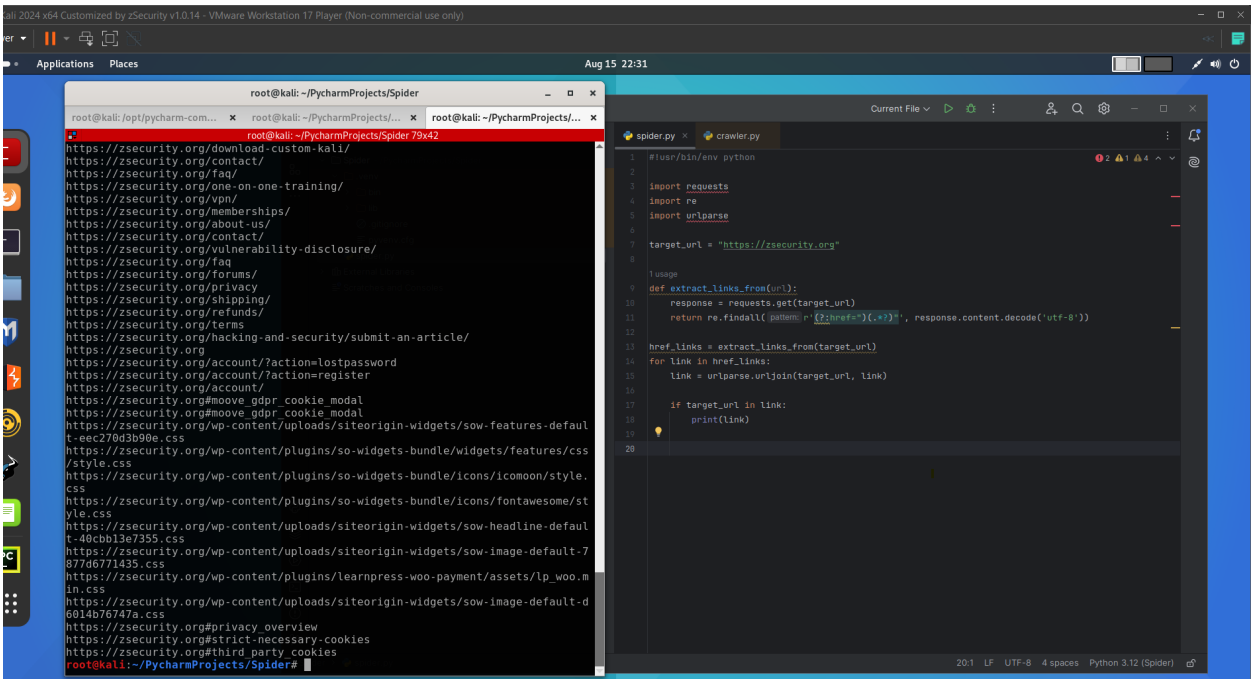
```
#!usr/bin/env python

import requests
import re
def request(url):
  try:
    return requests.get("http://" + url)
  except requests.exceptions.ConnectionError:
    pass

target_url = "zsecurity.org"

response = request(target_url)

href_links = re.findall(r'(?:href=")(.*?)"', response.content.decode('utf-8'))

print(href_links)
```


root@kali: ~/PycharmProjects/Spider
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/Spider
root@kali: ~/PycharmProjects/Spider 79x39
ity.org/how-to-change-the-keyboard-language-on-a-badusb/', 'https://zsecurity.org/protecting-software-from-tampering-expert-advice-and-adherence-to-the-rules/', 'https://zsecurity.org/protecting-software-from-tampering-expert-advice-and-adherence-to-the-rules/', 'https://zsecurity.org/securing-docker-containers-with-chainguard/', 'https://zsecurity.org/securing-docker-containers-with-chainguard/', '#', 'https://zsecurity.org/?_page=2', 'https://zsecurity.org/?_page=3', '#', 'https://zsecurity.org/?_page=10', 'https://zsecurity.org/?_page=2', 'https://zsecurity.org/courses/', 'https://zsecurity.org/courses/learn-ethical-hacking-using-the-cloud/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/learn-ethical-hacking-using-the-cloud/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/learn-bug-bounty-hunting-web-security-testing-from-scratch/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/learn-bug-bounty-hunting-web-security-testing-from-scratch/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/the-ultimate-dark-web-anonymity-privacy-security-course/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/the-ultimate-dark-web-anonymity-privacy-security-course/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/learn-ethical-hacking-from-scratch/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://zsecurity.org/courses/learn-ethical-hacking-from-scratch/', 'https://zsecurity.org/user/Zaid+Sabih/', 'https://www.facebook.com/ZSecurity-1453250781458287/', 'https://twitter.com/_zSecurity_', 'https://www.linkedin.com/company/zsecurity-org/', 'https://www.instagram.com/zsecurity_org/', 'https://youtube.com/c/zSecurity', 'https://zsecurity.org/', 'https://zsecurity.org/about-us/', 'https://zsecurity.org/hacking-and-security-posts/', 'https://zsecurity.org/download-custom-kali/', 'https://zsecurity.org/contact/', 'https://zsecurity.org/faq/', 'https://zsecurity.com/pentesting/', 'https://zsecurity.com/consulting/', 'https://zsecurity.com/codereview/', 'https://zsecurity.org/one-on-one-training/', 'https://zsecurity.org/vpn/', 'https://zsecurity.org/memberships/', 'https://zsecurity.org/about-us/', 'https://zsecurity.com/blog/', 'https://zsecurity.org/contact/', 'https://zsecurity.org/vulnerability-disclosure/', '/faq', '/forums/', '/privacy', 'https://zsecurity.org/shipping/', 'https://zsecurity.org/refunds/', '/terms', '/hacking-and-security/submit-an-article/', '#', 'https://zsecurity.org/account/?action=lostpassword', 'https://zsecurity.org/account/?action=register', 'https://zsecurity.org/account/', '#moove_gdpr_cookie_modal', '#moove_gdpr_cookie_modal', 'https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-features-default-eec270d3b90e.css', 'https://zsecurity.org/wp-content/plugins/so-widgets-bundle/widgets/features/css/style.css', 'https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/icomoon/style.css', 'https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/fontawesome/style.css', 'https://zsecurity.org/wp-content/uploads/siteor
Current File
spider.py
crawler.py
#!usr/bin/env python
import requests
import re
1 usage
def request(url):
try:
return requests.get("http://" + url)
except requests.exceptions.ConnectionError:
pass
target_url = "zsecurity.org"
response = request(target_url)
href_links = re.findall(pattern: r'(?:href=")(.*?)"', response.content.decode('utf-8'))
print(href_links)
Spider
spider.py
19:1
LF
UTF-8
4 spaces
Python 3.12 (Spider)

Filtering Results

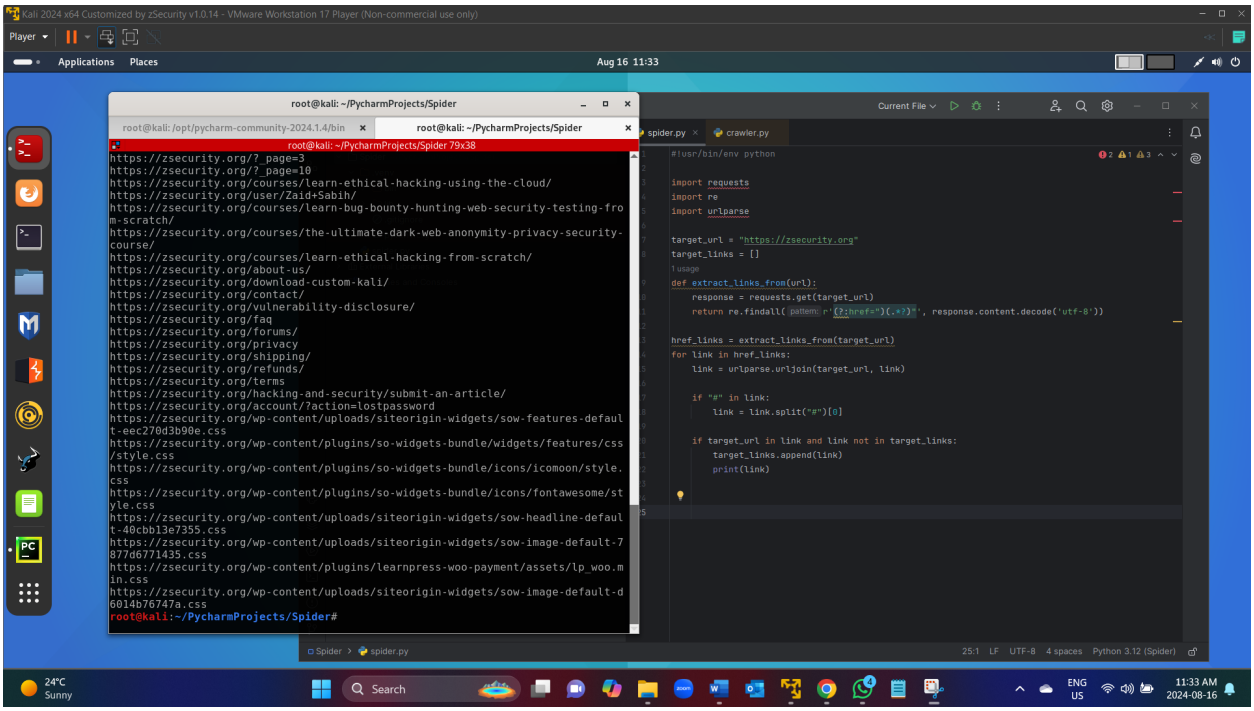
Spider.py

```
#!usr/bin/env python

import requests
import re
import urlparse

target_url = "https://zsecurity.org"

def extract_links_from(url):
    response = requests.get(target_url)
    return re.findall(r'(?:href=")(.*?)"', response.content.decode('utf-8'))

href_links = extract_links_from(target_url)
for link in href_links:
    link = urlparse.urljoin(target_url, link)

    if target_url in link:
        print(link)
```


Applications
Places
Aug 15 22:31
root@kali: ~/PycharmProjects/Spider
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/Spider 79×42
https://zsecurity.org/download-custom-kali/
https://zsecurity.org/contact/
https://zsecurity.org/faq/
https://zsecurity.org/one-on-one-training/
https://zsecurity.org/vpn/
https://zsecurity.org/memberships/
https://zsecurity.org/about-us/
https://zsecurity.org/contact/
https://zsecurity.org/vulnerability-disclosure/
https://zsecurity.org/faq
https://zsecurity.org/forums/
https://zsecurity.org/privacy
https://zsecurity.org/shipping/
https://zsecurity.org/refunds/
https://zsecurity.org/terms
https://zsecurity.org/hacking-and-security/submit-an-article/
https://zsecurity.org
https://zsecurity.org/account/?action=lostpassword
https://zsecurity.org/account/?action=register
https://zsecurity.org/account/
https://zsecurity.org#moove_gdpr_cookie_modal
https://zsecurity.org#moove_gdpr_cookie_modal
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-features-default-eec270d3b90e.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/widgets/features/css/style.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/icomoon/style.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/fontawesome/style.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-headline-default-40cbb13e7355.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-image-default-7877d6771435.css
https://zsecurity.org/wp-content/plugins/learnpress-woo-payment/assets/lp_woo.min.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-image-default-d6014b76747a.css
https://zsecurity.org#privacy_overview
https://zsecurity.org#strict-necessary-cookies
https://zsecurity.org#third_party_cookies
root@kali:~/PycharmProjects/Spider#
Current File
spider.py
crawler.py
#!usr/bin/env python
import requests
import re
import urlparse
target_url = "https://zsecurity.org"
1 usage
def extract_links_from(url):
response = requests.get(target_url)
return re.findall(pattern: r'(?:href=")(.*?)"', response.content.decode('utf-8'))
href_links = extract_links_from(target_url)
for link in href_links:
link = urlparse.urljoin(target_url, link)
if target_url in link:
print(link)
20:1 LF UTF-8 4 spaces Python 3.12 (Spider)

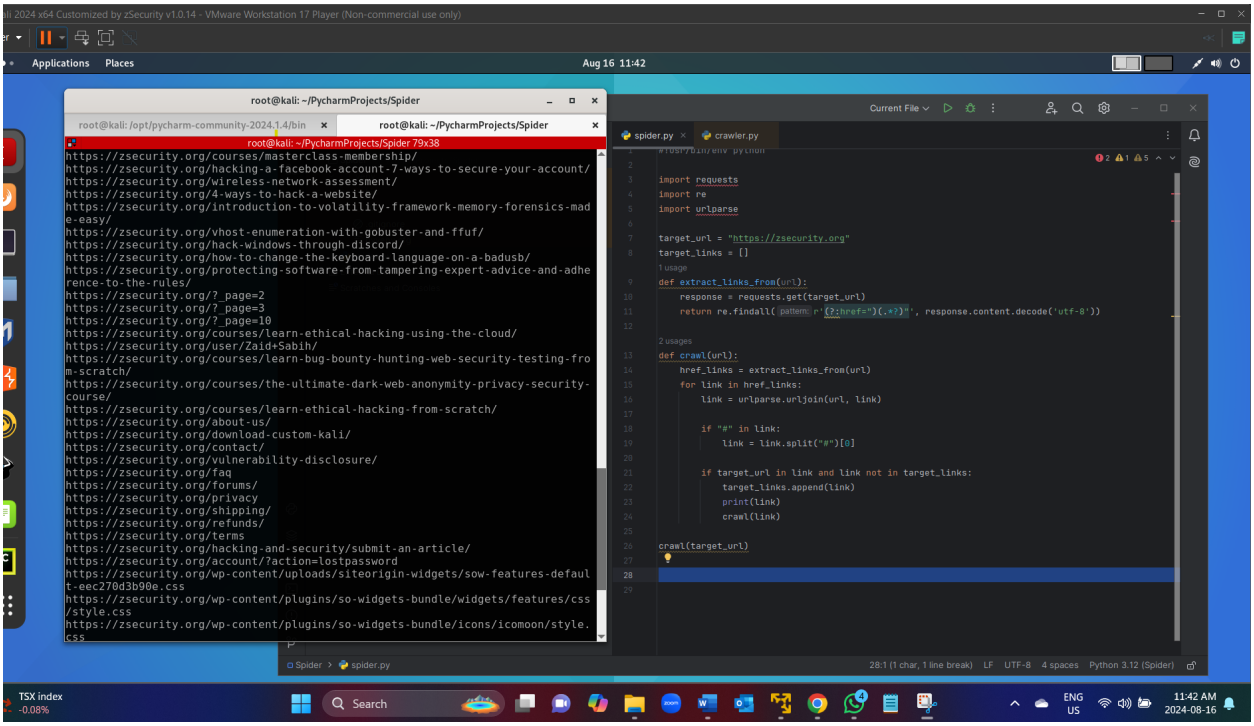
Extracting Unique Links & Storing Them In a List:

```
#!usr/bin/env python

import requests
import re
import urlparse

target_url = "https://zsecurity.org"
target_links = []
def extract_links_from(url):
  response = requests.get(target_url)
  return re.findall(r'(?:href=")(.*?)"', response.content.decode('utf-8'))

href_links = extract_links_from(target_url)
for link in href_links:
  link = urlparse.urljoin(target_url, link)

  if "#" in link:
    link = link.split("#")[0]

  if target_url in link and link not in target_links:
    target_links.append(link)
    print(link)
```


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 16 11:33
root@kali: ~/PycharmProjects/Spider
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/Spider
root@kali: ~/PycharmProjects/Spider 79x38
https://zsecurity.org/?_page=3
https://zsecurity.org/?_page=10
https://zsecurity.org/courses/learn-ethical-hacking-using-the-cloud/
https://zsecurity.org/user/Zaid+Sabih/
https://zsecurity.org/courses/learn-bug-bounty-hunting-web-security-testing-from-scratch/
https://zsecurity.org/courses/the-ultimate-dark-web-anonymity-privacy-security-course/
https://zsecurity.org/courses/learn-ethical-hacking-from-scratch/
https://zsecurity.org/about-us/
https://zsecurity.org/download-custom-kali/
https://zsecurity.org/contact/
https://zsecurity.org/vulnerability-disclosure/
https://zsecurity.org/faq
https://zsecurity.org/forums/
https://zsecurity.org/privacy
https://zsecurity.org/shipping/
https://zsecurity.org/refunds/
https://zsecurity.org/terms
https://zsecurity.org/hacking-and-security/submit-an-article/
https://zsecurity.org/account/?action=lostpassword
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-features-default-eec270d3b90e.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/widgets/features/css/style.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/icomoon/style.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/fontawesome/style.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-headline-default-40cbb13e7355.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-image-default-7877d6771435.css
https://zsecurity.org/wp-content/plugins/learnpress-woo-payment/assets/lp_woo.min.css
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-image-default-d6014b76747a.css
root@kali:~/PycharmProjects/Spider#
Current File
spider.py
crawler.py
#!usr/bin/env python
import requests
import re
import urlparse
target_url = "https://zsecurity.org"
target_links = []
1 usage
def extract_links_from(url):
response = requests.get(target_url)
return re.findall(pattern: r'(?:href=")(.*?)"', response.content.decode('utf-8'))
href_links = extract_links_from(target_url)
for link in href_links:
link = urlparse.urljoin(target_url, link)
if "#" in link:
link = link.split("#")[0]
if target_url in link and link not in target_links:
target_links.append(link)
print(link)
Spider > spider.py
25:1 LF UTF-8 4 spaces Python 3.12 (Spider)
24°C
Sunny
Search
ENG
US
11:33 AM
2024-08-16

Recursively Discovering All Paths On a Target Website

```
#!usr/bin/env python

import requests
import re
import urlparse

target_url = "https://zsecurity.org"
target_links = []
def extract_links_from(url):
  response = requests.get(target_url)
  return re.findall(r'(?:href=")(.*?)"', response.content.decode('utf-8'))

def crawl(url):
  href_links = extract_links_from(url)
  for link in href_links:
    link = urlparse.urljoin(url, link)

    if "#" in link:
      link = link.split("#")[0]

    if target_url in link and link not in target_links:
      target_links.append(link)
      print(link)
      crawl(link)

crawl(target_url)
```

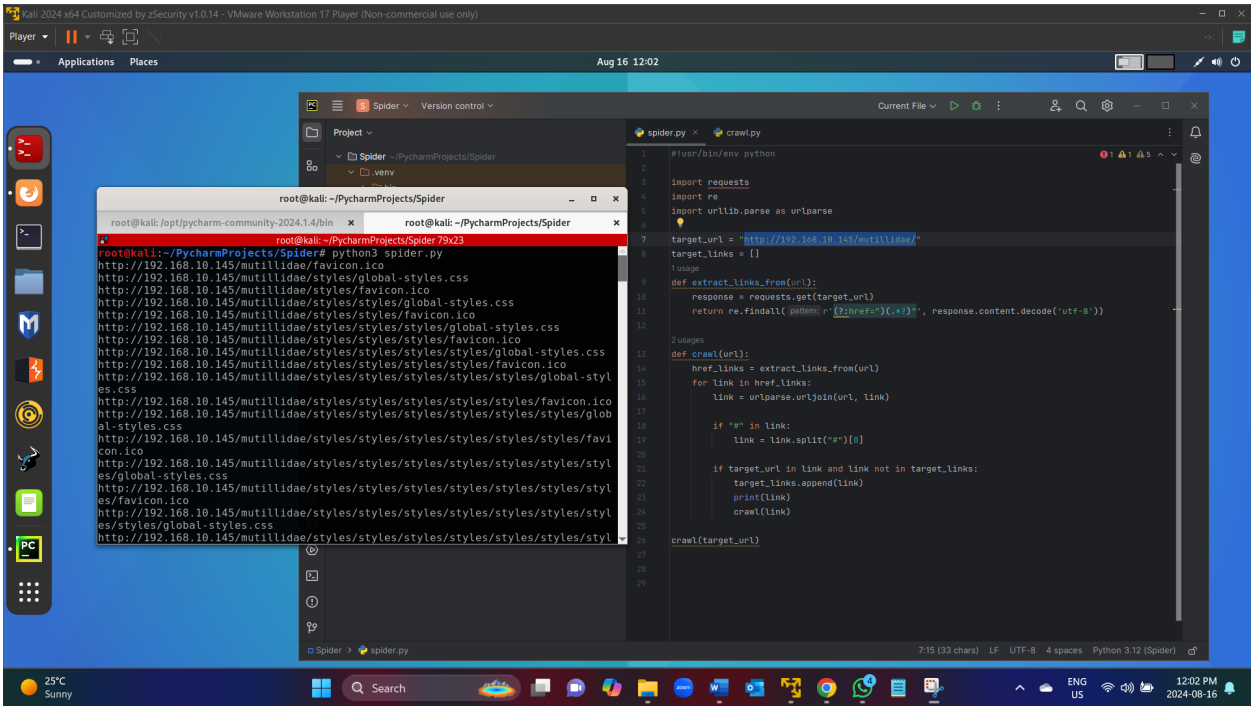

li 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Applications
Places
Aug 16 11:42
root@kali: ~/PycharmProjects/Spider
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/Spider
root@kali: ~/PycharmProjects/Spider 79x38
https://zsecurity.org/courses/masterclass-membership/
https://zsecurity.org/hacking-a-facebook-account-7-ways-to-secure-your-account/
https://zsecurity.org/wireless-network-assessment/
https://zsecurity.org/4-ways-to-hack-a-website/
https://zsecurity.org/introduction-to-volatility-framework-memory-forensics-made-easy/
https://zsecurity.org/vhost-enumeration-with-gobuster-and-ffuf/
https://zsecurity.org/hack-windows-through-discord/
https://zsecurity.org/how-to-change-the-keyboard-language-on-a-badusb/
https://zsecurity.org/protecting-software-from-tampering-expert-advice-and-adherence-to-the-rules/
https://zsecurity.org/?_page=2
https://zsecurity.org/?_page=3
https://zsecurity.org/?_page=10
https://zsecurity.org/courses/learn-ethical-hacking-using-the-cloud/
https://zsecurity.org/user/Zaid+Sabih/
https://zsecurity.org/courses/learn-bug-bounty-hunting-web-security-testing-from-scratch/
https://zsecurity.org/courses/the-ultimate-dark-web-anonymity-privacy-security-course/
https://zsecurity.org/courses/learn-ethical-hacking-from-scratch/
https://zsecurity.org/about-us/
https://zsecurity.org/download-custom-kali/
https://zsecurity.org/contact/
https://zsecurity.org/vulnerability-disclosure/
https://zsecurity.org/faq
https://zsecurity.org/forums/
https://zsecurity.org/privacy
https://zsecurity.org/shipping/
https://zsecurity.org/refunds/
https://zsecurity.org/terms
https://zsecurity.org/hacking-and-security/submit-an-article/
https://zsecurity.org/account/?action=lostpassword
https://zsecurity.org/wp-content/uploads/siteorigin-widgets/sow-features-default-eec270d3b90e.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/widgets/features/css/style.css
https://zsecurity.org/wp-content/plugins/so-widgets-bundle/icons/icomoon/style.css
Current File
spider.py
crawler.py
#!usr/bin/env python
import requests
import re
import urlparse
target_url = "https://zsecurity.org"
target_links = []
1 usage
def extract_links_from(url):
response = requests.get(target_url)
return re.findall(pattern: r'(?:href=")(.*?)"', response.content.decode('utf-8'))
2 usages
def crawl(url):
href_links = extract_links_from(url)
for link in href_links:
link = urlparse.urljoin(url, link)
if "#" in link:
link = link.split("#")[0]
if target_url in link and link not in target_links:
target_links.append(link)
print(link)
crawl(link)
crawl(target_url)
Spider
spider.py
28:1 (1 char, 1 line break)
LF
UTF-8
4 spaces
Python 3.12 (Spider)
TSX index
-0.08%
Search
ENG
US
11:42 AM
2024-08-16

Testing code with Python3:

Spider.py ()

```
#!usr/bin/env python


import requests
import re
import urllib.parse as urlparse


target_url = "http://192.168.10.145/mutillidae/"
target_links = []
def extract_links_from(url):
  response = requests.get(target_url)
  return re.findall(r'(?:href=")(.*?)"', response.content.decode('utf-8'))


def crawl(url):
  href_links = extract_links_from(url)
  for link in href_links:
    link = urlparse.urljoin(url, link)


    if "#" in link:
      link = link.split("#")[0]


  if target_url in link and link not in target_links:
      target_links.append(link)
      print(link)
      crawl(link)
```

crawl(target_url)



Crawl.py ()

```
#!usr/bin/env python


import requests


def request(url):
  try:
    return requests.get("http://" + url)
  except requests.exceptions.ConnectionError:
    pass


target_url = "192.168.10.145/mutillidae/"


with open("/root/Downloads/common.txt", "r") as wordlist_file:
  for line in wordlist_file:
```

```
word = line.strip()
test_url = target_url + "/" + word
response = request(test_url)
if response:
    print("[+] Discovered URL --> " + test_url)
```