

# Technique

```
import os
import requests
import sys

file = f"{sys.argv[1]}"
path = os.getcwd() + file

sub_list = open(file).read()
subdoms = sub_list.splitlines()

for sub in subdoms:
    sub_domains = f"http://{sub}.{sys.argv[2]}"
    ``

'''The script iterates through each subdomain in the list and

try:
    requests.get(sub_domains)
except requests.ConnectionError:
    pass

else:
    print("Valid domain: ", sub_domains)
```

## Import Statements:

- `import os`  
`import requests`  
`import sys`

These statements import necessary modules for file handling (`os`), making HTTP requests (`requests`), and accessing command-line arguments (`sys`).

## • Command-Line Arguments:

- `file = f"{sys.argv[1]}"`  
`path = os.getcwd() + file`

Our command will be `python3 python_file_name mainfile.txt domain` . For this to be happened

we have to use `sys.argv[1]` this is only for the mainfile.txt that we have selected. We are using `file = f"{sys.argv[1]}"`  
`path = os.getcwd() + file`

only for the commands.

- `sys.argv` is a list in Python that contains the command-line arguments passed to the script.
- `sys.argv[0]` is the script name itself, so `sys.argv[1]` refers to the first command-line argument provided by the user.
- The `file` variable holds the value of the first command-line argument, which is expected to be a file name.
- **File Path Construction:**
- `path = os.getcwd() + file`
  - This line attempts to construct an absolute file path by concatenating the current working directory ( `os.getcwd()` ) with the provided file name.
- **Reading Subdomains from File:**
- `sub_list = open(file).read()`  
`subdoms = sub_list.splitlines()`
  - The script opens the file specified by the user (or provided as a command-line argument), reads its contents, and splits them into a list of subdomains ( `subdoms` ) using `splitlines()` .
- **Iterating through Subdomains:**
- `for sub in subdoms: sub_domains = f"http://{sub}.{sys.argv[2]}" ```  
- The script iterates through each subdomain in the list and constructs a full URL by combining it with the  
second command-line argument ( `sys.argv[2]` ), which is expected to be a domain.
- **HTTP Request and Exception Handling:**
- `try: requests.get(sub_domains)`  
`except requests.ConnectionError: pass`

- The script attempts to make an HTTP GET request to the constructed URL using `requests.get()`.
- If a `requests.ConnectionError` occurs (indicating a failed connection), it is caught and ignored.

### • Printing Valid Domains:

1. `else: print("Valid domain: ", sub_domains)`
  - If the HTTP request is successful (no exception is raised), it prints the message "Valid domain" along with the constructed URL.

In summary, this script reads a list of subdomains from a file, combines each subdomain with a provided domain, and checks if the resulting URLs are reachable by making HTTP requests. If a connection is successful, it prints a message indicating a valid domain.

The screenshot shows a VS Code editor with a file named `lab-1_webacademy_sqli.py`. The script's content is as follows:

```

1  import os
2  import requests
3  import sys
4
5  file = f"{sys.argv[1]}"
6  path = os.getcwd() + file
7  sub_list = open(file).read()
8  subdoms = sub_list.splitlines()
9
10 for sub in subdoms:
11     sub_domains = f"http://{sub}.{sys.argv[2]}"
12
13     try:
14         requests.get(sub_domains)
15
16     except requests.ConnectionError:

```

Below the editor, the terminal shows the execution of the script. It starts with an error because the file was not found in the current directory. Then, the user runs the script with the correct file path and domain, resulting in the following output:

```

PS C:\Users\alruh> python3 lab-1_webacademy_sqli.py
Python was not found; run without arguments to install from the Microsoft Store, or disable this shortcut from Settings > Manage App Execution Aliases.
PS C:\Users\alruh> python lab-1_webacademy_sqli.py
C:\Users\alruh\AppData\Local\Programs\Python\Python312\python.exe: can't open file 'C:\Users\alruh\lab-1_webacademy_sqli.py': [Errno 2] No such file or directory
PS C:\Users\alruh> python lab-1_webacademy_sqli.py F:\Scripts\wordlist2.txt google.com
C:\Users\alruh\AppData\Local\Programs\Python\Python312\python.exe: can't open file 'C:\Users\alruh\lab-1_webacademy_sqli.py': [Errno 2] No such file or directory
PS C:\Users\alruh> python F:\Scripts\lab-1_webacademy_sqli.py F:\Scripts\wordlist2.txt google.com
Valid domain: http://video.google.com
Valid domain: http://movie.google.com
Valid domain: http://time.google.com
Valid domain: http://music.google.com
PS C:\Users\alruh>

```

This screenshot shows a terminal window where the script is executed from the directory `F:\Scripts`. The command is `python F:\Scripts\lab-1_webacademy_sqli.py F:\Scripts\wordlist2.txt google.com`, and the output is:

```

PS C:\Users\alruh> python F:\Scripts\lab-1_webacademy_sqli.py F:\Scripts\wordlist2.txt google.com
Valid domain: http://video.google.com
Valid domain: http://movie.google.com
Valid domain: http://time.google.com
Valid domain: http://music.google.com

```

here look i'm not in the directory of the python file so i had to define the files directory