

# Report on Sublist3r

Course No: CSE 406

Course Title: Computer Security Sessional

Presented By:

Sadia Tabassum - 1905091

Mayesha Rashid - 1905103

Subsection: B2

# Table of Contents

1. [Subdomain Enumeration](#)
  - (a) [Importance](#)
  - (b) [Techniques](#)
  - (c) [Challenges](#)
  - (d) [Security Implications](#)
  - (e) [Mitigation](#)
2. [Sublist3r](#)
  - (a) [SubBrute](#)
3. [High level Overview of Sublist3r](#)
  - (a) [Brute Force](#)
  - (b) [Search Engine](#)
  - (c) [DNS Resolution](#)
4. [Documentation to run each Feature](#)
  - (a) [Installing the tool](#)
    - i. [Cloning from github](#)
    - ii. [Installation on Linux](#)
  - (b) [Running the tool](#)
    - i. [Download and apply patch from github](#)
    - ii. [Setting the environment variable](#)
  - (c) [To list all the basic options and switches use -h switch:](#)
  - (d) [To enumerate subdomains of specific domain:](#)
  - (e) [To enumerate subdomains of specific domain and show only subdomains which have open ports 80 and 443:](#)
  - (f) [To enumerate subdomains of specific domain and show the results in realtime:](#)

- (g) To enumerate subdomains and use specific engines such Google, Yahoo and Virustotal engines :
- (h) textTo enumerate subdomains and enable the bruteforce module:
- (i) Usage
- (j) Using Sublist3r as a module in python scripts:
- (k) Additional tools for attempting dictionary attack
  - i. Scout installation
  - ii. Chrome driver download
  - iii. Chrome driver installation
  - iv. Burp suite Installation

## 5. Exploring Sublist3r

- (a) Subdomain Enumeration
- (b) Specific Subdomains Enumeration
- (c) Attempting a dictionary attack
  - i. Subdomain Enumeration of vulnweb
  - ii. Finding login page of [testphp.vulnweb.com](http://testphp.vulnweb.com)
  - iii. Exploring the login page [testphp.vulnweb.com/login](http://testphp.vulnweb.com/login)
  - iv. Running the attack
  - v. Attack becomes successful

## 6. Conclusion

# 1 Subdomain Enumeration

Subdomain enumeration is the process of identifying and cataloging the subdomains associated with a particular domain. Subdomains are subdivisions or additional components of a domain, typically represented as prefixes to the main domain name. It plays a crucial role in vulnerability analysis and web security.

## 1.1 Importance

- **Discovery:** Identifying all possible subdomains associated with a domain.
- **Analysis:** Analyzing the structure and organization of subdomains to gain insights into the architecture of the target domain.
- **Security Assessment:** Subdomain enumeration helps security professionals identify potential points of entry, weaknesses, or misconfigurations in a domain's infrastructure.
- **Asset Management:** Maintaining an up-to-date inventory of all subdomains is essential for effective asset management. This ensures that organizations have a comprehensive understanding of their online presence and can take appropriate measures to secure it.

## 1.2 Techniques

- **DNS (Domain Name System) Interrogation:** Querying DNS records to identify subdomains associated with a domain.
- **Brute Force:** Systematically generating and testing possible subdomain names to discover valid ones.
- **Search Engine Scrutiny:** Leveraging search engines to identify publicly indexed subdomains.
- **Certificate Transparency Logs:** Analyzing certificate transparency logs to identify subdomains associated with SSL/TLS certificates.

## 1.3 Challenges

- **Incomplete Results:** DNS (Domain Name System) records may be cached, leading to incomplete or outdated information during subdomain enumeration. Some DNS servers may implement rate limiting, preventing exhaustive enumeration within a short time frame.
- **False Positives and Negatives:** Brute force techniques may yield false positives or negatives, leading to inaccurate results. The sheer

volume of possible subdomains makes it challenging to ensure comprehensive coverage.

- **Dynamic Infrastructure:** Modern web applications and cloud-based services often have dynamic infrastructure, making it difficult to maintain an accurate and up-to-date inventory of subdomains.

## 1.4 Security Implications

Inability to accurately identify all subdomains may expose an organization to potential security threats, as attackers could target overlooked subdomains that lack robust security measures.

## 1.5 Mitigation

- **Regular Enumeration:** Organizations should conduct regular subdomain enumeration to maintain an accurate inventory of their online assets.
- **Automation:** Leveraging automated tools and scripts to perform subdomain enumeration can help streamline the process and ensure comprehensive coverage.
- **Monitoring and Alerting:** Implementing mechanisms to detect changes in subdomain structure.
- **Security Measures:** Implementing robust security measures across all subdomains, including proper SSL/TLS configuration, secure coding practices, and regular vulnerability assessments, can help mitigate potential risks.

## 2 Sublist3r

Sublist3r is a subdomain enumeration tool written in python, designed to enumerate subdomains of a specific domain using OSINT. It is capable of leveraging multiple search engines, including Google, Yahoo, Bing, Baidu, and Ask, to identify subdomains associated with a target domain. Sublist3r also supports brute force enumeration using a wordlist, allowing users to discover additional subdomains that may not be indexed by search engines.

It also uses Netcraft, Virustotal, DNSdumpster, and ReverseDNS to gather additional information about the target domain.

## **2.1 SubBrute**

SubBrute is a free and open-source tool available on GitHub. It uses DNS Scan for finding subdomains of the target domain. It comes with Sublist3r by default. Sublist3r uses SubBrute for doing bruteforce search.

# **3 High level Overview of Sublist3r**

Sublist3r collects information of subdomains from various sources and then combines the results to provide a comprehensive list of subdomains. It uses the following techniques to gather information:

## **3.1 Brute Force**

Sublist3r uses a wordlist to perform a brute force search for subdomains. It generates possible subdomain names and checks their existence by querying DNS records. This method is quite time consuming and may not always gather results due to rate limiting and other restrictions. The subbrute package is used for this method.

## **3.2 Search Engine**

Sublist3r leverages multiple search engines, including Google, Yahoo, Bing, Baidu, and Ask, to identify subdomains associated with a target domain. It queries these search engines and scrapes the results to extract subdomains.

## **3.3 DNS Resolution**

Sublist3r performs DNS resolution to verify the existence of subdomains. It queries DNS servers to resolve subdomain names and gather information about their IP addresses. It includes Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS engines.

## 4 Documentation to run each Feature

### 4.1 Installing the tool

#### 4.1.1 Cloning from github

git clone <https://github.com/about3la/Sublist3r.git>

#### 4.1.2 Installation on Linux

pip3 install -r requirements.txt

### 4.2 Running the tool

Virustotal engine of the tool doesn't work the way it used to during the creation of Sublist3r. To make it work, we need to update the base url of Virustotal. VirusTotal currently requires API key from their official website. We can get that by creating an account on their website. After getting the API key, we need to apply the patch from the github repository of Sublist3r.

#### 4.2.1 Download and apply patch from github

Patch link: [click here](#)

#### 4.2.2 Setting the environment variable

The environment variable name has to be VT\_APIKEY. In Linux, open the .bashrc file in home directory and add the following line at the end of the file:

```
export VT_APIKEY=your_API_key
```

Then save the file and run the following command in the terminal:

```
source ~/.bashrc
```

### 4.3 To list all the basic options and switches use -h switch:

```
python3 sublist3r.py -h
```

#### 4.4 To enumerate subdomains of specific domain:

`python3 sublist3r.py -d example.com`

```
winterdark@tabu:~/software_stuff/Sublist3r$ python3 sublist3r.py -d google.com

Sublist3r

# Coded By Ahmed Aboul-Ela - @aboul31a

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Vtrustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Vtrustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 451
www.google.com
accounts.google.com
Freezone.accounts.google.com
console.actions.google.com
admanager.google.com
admin.google.com
admob.google.com
ads.google.com
adsense.google.com
adservice.google.com
```

#### 4.5 To enumerate subdomains of specific domain and show only subdomains which have open ports 80 and 443:

`python3 sublist3r.py -d example.com -p 80,443`



```
winterdark@tabu:~/software_stuff/Sublist3r$ python3 sublist3r.py -d google.com -p 80,443
```




```
# Coded By Ahmed Aboul-Ela - @aboul3la
```

```
[*] Enumerating subdomains now for google.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[*] Total Unique Subdomains Found: 97
[*] Start port scan now for the following ports: 80,443
www.google.com - Found open ports: 80, 443
answers.google.com - Found open ports: 80, 443
audioloads.google.com - Found open ports: 80, 443
accounts.google.com - Found open ports: 80, 443
adwords.google.com - Found open ports: 80, 443
proxyconfig.corp.google.com - Found open ports: 80, 443
login.corp.google.com - Found open ports: 80, 443
n.gutsdev.corp.google.com - Found open ports: 80, 443
n.guts.corp.google.com - Found open ports: 80, 443
uberproxy.corp.google.com - Found open ports: 80, 443
gmail.google.com - Found open ports: 80, 443
jmt0.google.com - Found open ports: 80, 443
twi-da-ext.google.com - Found open ports: 443
```

#### 4.6 To enumerate subdomains of specific domain and show the results in realtime:

python3 sublist3r.py -d example.com -v

```
winterdark@tabu:~/software_stuff/Sublist3r$ python3 sublist3r.py -v -d google.com
```



```
# Coded By Ahmed Aboul-Ela - @aboul3la
```

```
[*] Enumerating subdomains now for google.com
[*] verbosity is enabled, will show the subdomains results in realtime
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
SSL Certificates: onex.wifi.google.com
SSL Certificates: accounts.google.com
SSL Certificates: hosted-id.google.com
SSL Certificates: adwords.google.com
SSL Certificates: wifi.google.com
SSL Certificates: jnt0.google.com
SSL Certificates: upload.video.google.com
SSL Certificates: eggroll.ext.google.com
SSL Certificates: sandbox.google.com
SSL Certificates: cod.ext.google.com
SSL Certificates: glass.ext.google.com
SSL Certificates: ice.ext.google.com
SSL Certificates: www.google.com
SSL Certificates: checkout.google.com
SSL Certificates: mail.google.com
SSL Certificates: vp.video.l.google.com
SSL Certificates: glass-eur.ext.google.com
SSL Certificates: glass-ntv.ext.google.com
SSL Certificates: glass-tw2.ext.google.com
SSL Certificates: services.google.com
```

## 4.7 To enumerate subdomains and use specific engines such Google, Yahoo and Virustotal engines :

```
python3 sublist3r.py -d example.com -e google,yahoo,virustotal
```

## 4.8 To enumerate subdomains and enable the brute-force module:

```
python3 sublist3r.py -d example.com -b
```

## 4.9 Usage

Short Form	Long Form	Description
-h	-help	show this help message and exit
-d	-domain	Domain name to enumerate subdomains of
-b	-bruteforce	Enable the subbrute bruteforce module
-v	-verbose	Enable the verbose mode
-p	-ports	Scan subdomains against specific tcp ports
-e	-engines	Give a comma-separated list of search engines

## 4.10 Using Sublist3r as a module in python scripts:

```
import sublist3r
subdomains = sublist3r.main(domain, no_threads, savefile, ports, silent, verbose, enable_bruteforce, engines)
```

The main function will return a set of unique subdomains found by Sublist3r.

## 4.11 Additional tools for attempting dictionary attack

Scout is a URL fuzzer for discovering undisclosed files and directories on a web server.

Hatch is a tool that is used to brute force most websites.

### 4.11.1 Scout installation

```
curl -s "https://raw.githubusercontent.com/liamg/scout/master/scripts/install.sh" | bash
```

### 4.11.2 Chrome driver download

Download chromedriver according to operating system from [here](#)

### 4.11.3 Chrome driver installation

Unzip the folder and add the directory to path variable. For Ubuntu, we have to add the following line to .bashrc file in home folder considering chromedriver folder is in home directory:

```
export PATH="$PATH:/home/username/chromedriver/"
```

### 4.11.4 Burp suite Installation

Download link: <https://portswigger.net/burp/communitydownload>

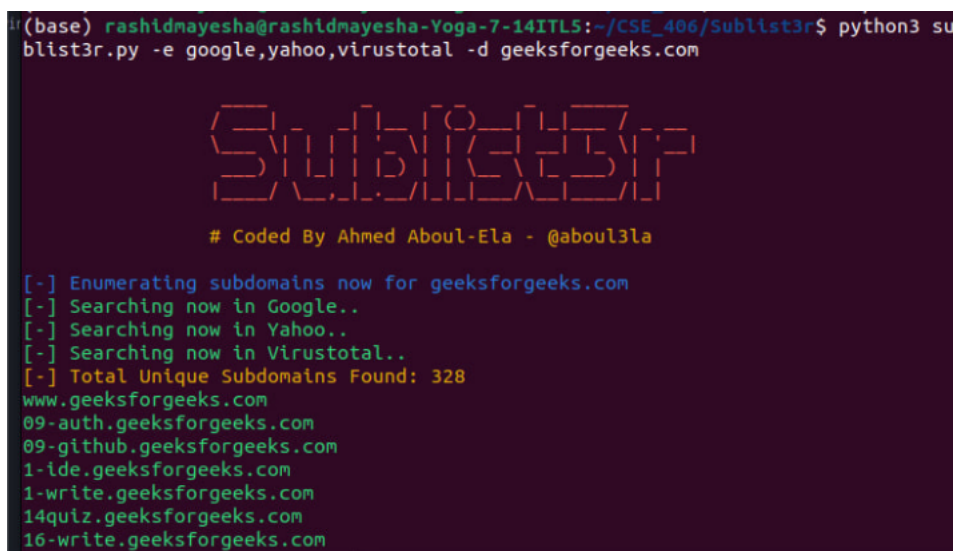
## 5 Exploring Sublist3r

### 5.1 Subdomain Enumeration

To enumerate subdomains of [geeksforgeeks.com](https://www.geeksforgeeks.com) using Google, Yahoo, and Virustotal engines, we can use the following command:

```
python3 sublist3r.py -d geeksforgeeks.com -e google,yahoo,virustotal
```

Running the command gives us the following output:



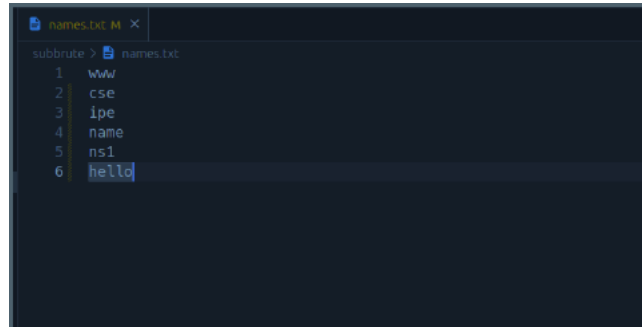
```
(base) rashidmayesha@rashidmayesha-Yoga-7-14ITL5:~/CSE_406/Sublist3r$ python3 su
blist3r.py -e google,yahoo,virustotal -d geeksforgeeks.com

  Sublist3r
  # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for geeksforgeeks.com
[-] Searching now in Google..
[-] Searching now in Yahoo..
[-] Searching now in Virustotal..
[-] Total Unique Subdomains Found: 328
www.geeksforgeeks.com
09-auth.geeksforgeeks.com
09-github.geeksforgeeks.com
1-ide.geeksforgeeks.com
1-write.geeksforgeeks.com
14quiz.geeksforgeeks.com
16-write.geeksforgeeks.com
```

## 5.2 Specific Subdomains Enumeration

To show if some specific subdomains are available under a particular domain, we have to keep the list of desired subdomains in `/subbrute/names.txt`. For testing, we are keeping these six entries:



Then we can run the following command to check if these subdomains are available under [buet.ac.bd](http://buet.ac.bd):

```
python3 sublist3r.py -d buet.ac.bd -b
```

The output is as follows:

```
(base) rashidmayesha@rashidmayesha-Yoga-7-14ITL5:~/CSE_406/Sublist3r$ python3 su
blist3r.py -b -v -e google -d buet.ac.bd

          SUBLIST3R
          # Coded By Ahmed Aboul-Ela - @aboul3la

[+] Enumerating subdomains now for buet.ac.bd
[+] verbosity is enabled, will show the subdomains results in realtime
[+] Searching now in Google..
[+] Starting bruteforce module now using subbrute..
buet.ac.bd
www.buet.ac.bd
cse.buet.ac.bd
ipe.buet.ac.bd
name.buet.ac.bd
ns1.buet.ac.bd
[+] Total Unique Subdomains Found: 6
buet.ac.bd
www.buet.ac.bd
cse.buet.ac.bd
ipe.buet.ac.bd
name.buet.ac.bd
ns1.buet.ac.bd
```

Subbrute lists domains and nameservers so we can see [buet.ac.bd](http://buet.ac.bd). Additionally, we can see that all other subdomains except hello is listed as it does not exist.

## 5.3 Attempting a dictionary attack

### 5.3.1 Subdomain Enumeration of vulnweb

Now we are going to attempt a dictionary attack on a vulnerable website. For safety reasons, we are running it on a safe website named vulnweb.

```
python3 sublist3r.py -e virustotal -d vulnweb.com
```

The output is as follows:

```
(base) rashidmayesha@rashidmayesha-Yoga-7-14ITL51:~/CSE_406/sublist3r$ python3 s
sublist3r.py -e virustotal -d vulnweb.com

          SUBLIST3R
# Coded By Ahmed Aboul-El* - @aboul3la

[-] Enumerating subdomains now for vulnweb.com
[-] Searching now in Virustotal..
[-] Total Unique Subdomains Found: 979
www.vulnweb.com
0.vulnweb.com
0000-00-00testasp.vulnweb.com
0000-00-00testasp.vulnweb.com
0000-00-00testaspalias.vulnweb.com
0707.vulnweb.com
097efeb9221037d3c4b350100ba723.vulnweb.com
01.vulnweb.com
011-177-dev0-testphp-descargas.vulnweb.com
01192521404251httpstestaspnet.vulnweb.com
01192521404254-neller2.vulnweb.com
01192521404256-viruswall.vulnweb.com
01205521401240httpstestaspnet.vulnweb.com
01205521401242testphp.vulnweb.com
01205521401250-printer2.vulnweb.com
01290521402551-printer2.vulnweb.com
01290521402565dealer.vulnweb.com
01290521402566testphp.vulnweb.com
02109-testphp-tavaux.vulnweb.com
```

We see a subdomain with [testphp.vulnweb.com](http://testphp.vulnweb.com).

```
stphp.vulnweb.com
support.vulnweb.com
svn.vulnweb.com
svn-compute-1.vulnweb.com
syslog.vulnweb.com
taiyangchengyulewang818.vulnweb.com
tc.vulnweb.com
technologyservicesmetric-testtestphp-pay.vulnweb.com
tera-oculus-verts-shv-02-sin16.vulnweb.com
tesasp.vulnweb.com
testphp.vulnweb.com
test.vulnweb.com
test1.vulnweb.com
test2.vulnweb.com
testadministrator-chdtestphp.vulnweb.com
testadministrator-chdtestphpsps.vulnweb.com
testarsp.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
testaspnet-chronos.vulnweb.com
testaspv.vulnweb.com
testclienttestphpstaff.vulnweb.com
testphp.vulnweb.com
testforantivirus1.vulnweb.com
testthphp.vulnweb.com
testthn1.vulnweb.com
testthn13.vulnweb.com
testthn14.vulnweb.com
testthn15.vulnweb.com
testjsp.vulnweb.com
testmetasploitable.vulnweb.com
testnet.vulnweb.com
testoho.vulnweb.com
```

We are going to attempt a dictionary attack on this subdomain.

### 5.3.2 Finding login page of [testphp.vulnweb.com](http://testphp.vulnweb.com)

We use scout to find out all the directories, subdirectories and files of [testphp.vulnweb.com](http://testphp.vulnweb.com). The command is as follows:

scout url http://testphp.vulnweb.com

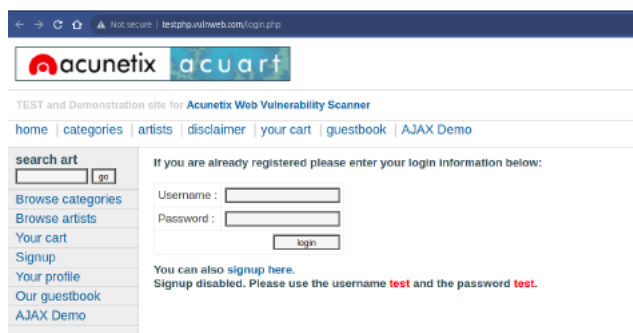
The output will look like:

```
(base) rashidmayesha@rashidmayesha-Yoga-7-14ITL5:~$ scout url http://testphp.vulnweb.com
[+] Target URL      http://testphp.vulnweb.com
[+] Routines        10
[+] Extensions      php,htm,html,txt
[+] Positive Codes   200,400,500,405,204,401,403,302,301
[+] Spider          false

[200] [4958] http://testphp.vulnweb.com/
[301] [169] http://testphp.vulnweb.com/vendor
[200] [268] http://testphp.vulnweb.com/vendor/
[301] [169] http://testphp.vulnweb.com/images
[200] [377] http://testphp.vulnweb.com/images/
[301] [169] http://testphp.vulnweb.com/admin
[200] [262] http://testphp.vulnweb.com/admin/
[301] [169] http://testphp.vulnweb.com/CVS
[200] [595] http://testphp.vulnweb.com/CVS/
[200] [4732] http://testphp.vulnweb.com/search.php
[200] [5523] http://testphp.vulnweb.com/login.php
```

We see that there is a login page at [testphp.vulnweb.com/login](http://testphp.vulnweb.com/login). We are going to attempt a dictionary attack on this page.

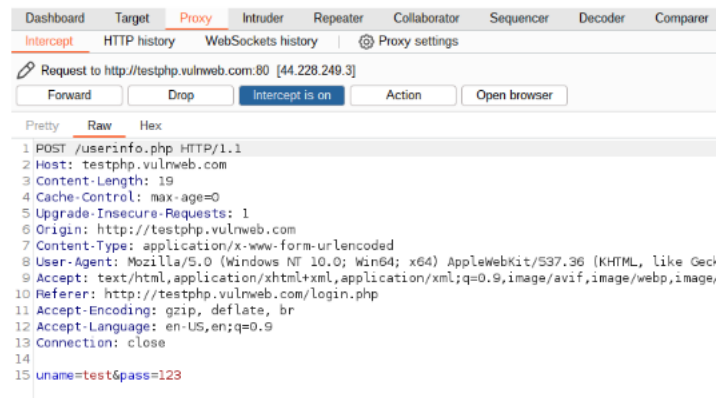
### 5.3.3 Exploring the login page [testphp.vulnweb.com/login](http://testphp.vulnweb.com/login)



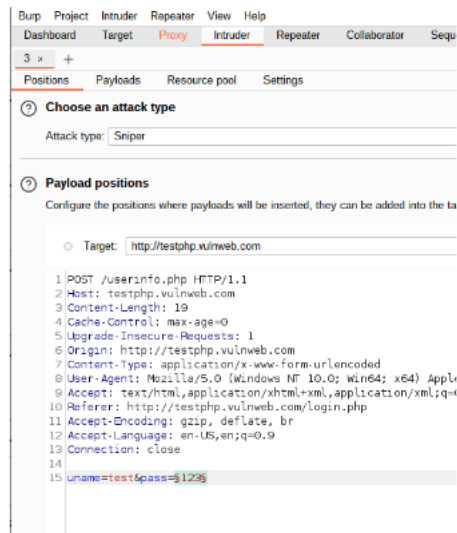
If we paste the link in browser, we can see that the page is alive.

### 5.3.4 Running the attack

Now let's create a new project in burp suite and turn the intercept on in proxy field. From there, we will click the open browser, which will open burp suite's browser. There we will open the login page and try to login with some random credentials. We will see the request in burp suite.



Now we will send this request to intruder and add password as payload by adding curly braces (§) on either side.



In payloads, we load our password lists file and click start attack.



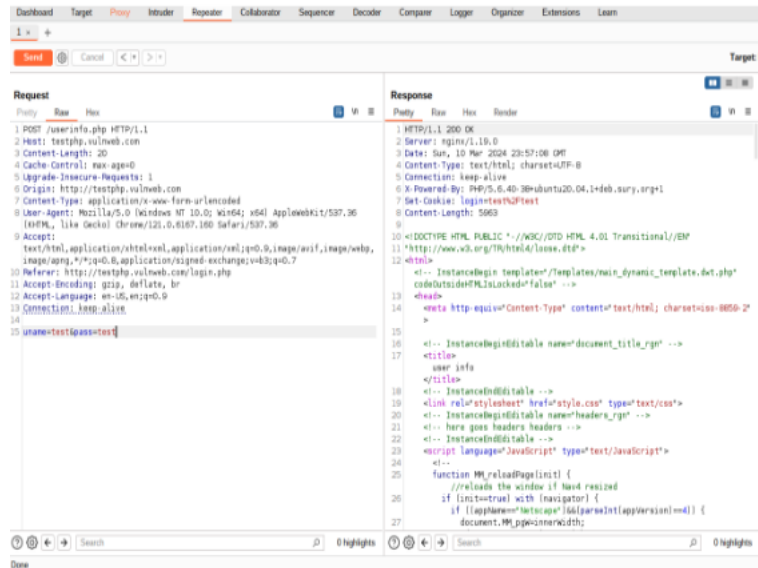
### 5.3.5 Attack becomes successful

From the attack we can see that, for password test we have got status code 200 and the length is different than others. We now select the request of test and forward it to repeater.

Payload	Status code	Response received	Error	Timeout	Length ^	Comment
JUT7rs6AFu	302	304			258	
PublicDeskBenefactor	302	350			258	
SxwDxUHaGbbgPm	302	306			258	
pqr	302	277			258	
testing123	302	307			258	
helloworld	302	328			258	
test	200	334			258	

If we click send at repeater, we will see that we get a webpage as a response. Now copying this request to proxy and forwarding it will load the logged in page in browser. Thus a successful dictionary attack has been done.





## 6 Conclusion

Therefore, we can say that Sublist3r is a powerful tool for subdomain enumeration. It can be used to find subdomains of a specific domain using various search engines and DNS resolution. It also supports brute force enumeration using a wordlist. Sublist3r can be used to identify potential points of

entry, weaknesses, or misconfigurations in a domain's infrastructure. It is an essential tool for vulnerability analysis and web security.