

Lab 10 – Using Curl Tool

Lab Objective:

Using the Curl tool for manual information gathering.

Lab Purpose:

Curl stands for Client URL. It is a command line tool for getting and sending data including files using URL syntax.

Lab Tool:

Kali Linux

Lab Topology:

Used Kali Linux for this lab.

STEP 1:

The general syntax for using curl is the following:

Curl [options] URL

This is a basic syntax that makes the tool quite simple to use. To get some more information on curl and how it is used, type `curl --help` to display the information screen.

Curl can be installed on Linux using the following command:

```
sudo apt-get install curl
```

STEP 2:

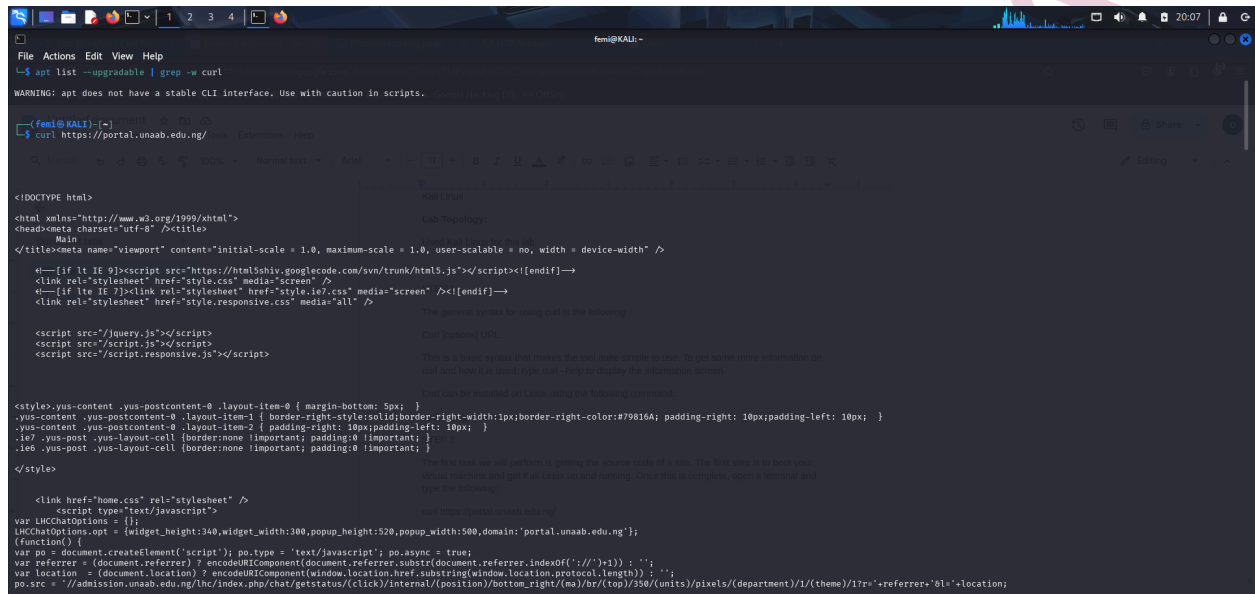
The first task we will perform is getting the source code of a site. The first step is to boot your virtual machine and get Kali Linux up and running. Once this is complete, open a terminal and type the following:

```
curl https://portal.unaab.edu.ng/
```

Some websites redirect you—`-L` ensures `curl` follows them.e.g Facebook.com

So use the command;

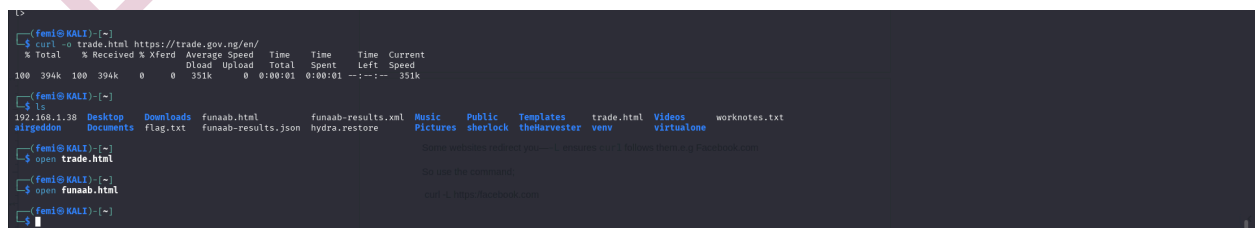
```
curl -L https://facebook.com
```



```
femi@KALI:~$ curl https://portal.unaab.edu.ng/
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
  <head><meta charset="utf-8" /><title>
    Main
  </title><meta name="viewport" content="initial-scale = 1.0, user-scalable = no, width = device-width" />
  <!--[if lt IE 9]><script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
  <link rel="stylesheet" href="style.css" media="screen" />
  <!--[if lte IE 7]><link rel="stylesheet" href="style.ie7.css" media="screen" /><![endif]-->
  <link rel="stylesheet" href="style.responsive.css" media="all" />
  <script src="//jquery.js"></script>
  <script src="//script.js"></script>
  <script src="//script.responsive.js"></script>
  <style>.yus-content .yus-postcontent-0 .layout-item-0 { margin-bottom: 5px; }
.yus-content .yus-postcontent-0 .layout-item-1 { border-right-style:solid;border-right-width:1px;border-right-color:#79816A; padding-right: 10px;padding-left: 10px; }
.yus-content .yus-postcontent-0 .layout-item-2 { padding-right: 10px;padding-left: 10px; }
.ie7 .yus-post .yus-layout-cell {border:none !important; padding:0 !important; }
.ie6 .yus-post .yus-layout-cell {border:none !important; padding:0 !important; }
</style>
  <link href="home.css" rel="stylesheet" />
  <script type="text/javascript">
    var LHCChatOptions = {widget_height:340,widget_width:300,popup_height:520,popup_width:500,domain:'portal.unaab.edu.ng'};
    (function() {
      var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
      var referrer = (document.referrer) ? encodeURIComponent(document.referrer.substr(document.referrer.indexOf('/:')+1)) : '';
      var location = (document.location) ? encodeURIComponent(window.location.href.substring(window.location.protocol.length)) : '';
      po.src = '//admission.unaab.edu.ng/lhc/index.php/chat/getstatus?click/internal&position/bottom_right&ma/hr/top/350/(units)/pixels/(department)/1/(theme)/1?r='+referrer+'&l='+location;
    })();
  </script>
</html>
```

To save this output to a file, we will use either the `-o` or `-O` option. The lowercase option saves the file with a predefined filename, while the uppercase option saves the file with its original filename. Basically, the lowercase option allows us to specify a file name. This is a useful option if the webpage we are trying to inspect is preventing us from right clicking on the page to view the source code in the browser. Type the following to save your output:

```
curl -o funaab.html https://portal.unaab.edu.ng/
```



```
femi@KALI:~$ curl -o trade.html https://trade.gov.ng/en/
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 394k 100 394k 0 0 551k 0 0:00:01 0:00:01 --:--:-- 551k

femi@KALI:~$ ls
192.168.1.38 Desktop Downloads funaab.html funaab-results.xml funaab Public Templates trade.html Videos worknotes.txt
airgeddon Documents flag.txt funaab-results.json hydra.restore Pictures sherlock theharvester veno virtualbox

femi@KALI:~$ cat trade.html
femi@KALI:~$ cat funaab.html
```

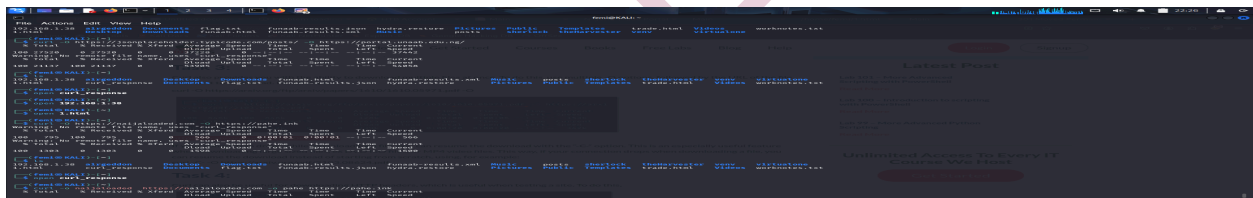
STEP 3:

Curl also provides you with the ability to download multiple files at once. To do this, use multiple -O options, followed by the URL of the file you want to download. For example:

```
$ curl -O https://naijaloaded.com -O https://pahe.in
```

If your connection drops while downloading a file, you can resume the download with the “-C-” option. This is an especially useful feature when downloading large sized files, ex DVD ISO files, or MP4 video files. This way, if your connection drops when downloading a file, you can resume the download instead of starting from scratch, using, for example:

```
curl -C- -O https://arxiv.org/pdf/2103.08624.pdf
```



STEP 4:

Curl can also be useful for downloading HTTP headers, which is useful when testing a site. To do this, use the following command:

```
curl -I https://portal.unaab.edu.ng
```

```
(femi@KALI) [-]
$ curl -i https://portal.unaab.edu.ng
HTTP/2 200
cache-control: private
content-length: 21137
content-type: text/html; charset=utf-8
server: Microsoft-IIS/10.0
x-aspnet-version: 4.0.30319
x-powered-by: ASP.NET
date: Sun, 30 Mar 2025 21:31:54 GMT

(femi@KALI) [-]
$ curl -i https://pahe.in
HTTP/2 307
date: Sun, 30 Mar 2025 21:32:16 GMT
content-type: text/html
x-sucuri-id: 13017
x-ssr-protection: is mode:block
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
strict-transport-security: max-age=31536000
content-security-policy: upgrade-insecure-requests;
server: Scuri/Cloudproxy
alt-svc: h3="443", ma=2592000, h3-29="443", ma=2592000

(femi@KALI) [-]
$ curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me
193.50.135.12
```

STEP 5:

When attempting to download a file or gather other information using curl, you may discover that the target site may be designed to block curl. In this case, it is useful to emulate a browser, such as Firefox, to return the information you are looking for. To do this, use the following command:

```
curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me
```

```
femi@KALI -
File Actions Edit View Help

(femi@KALI) [-]
$ curl https://ifconfig.me
105.112.11.59

(femi@KALI) [-]
$ curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me
zsh: parse error near `)'

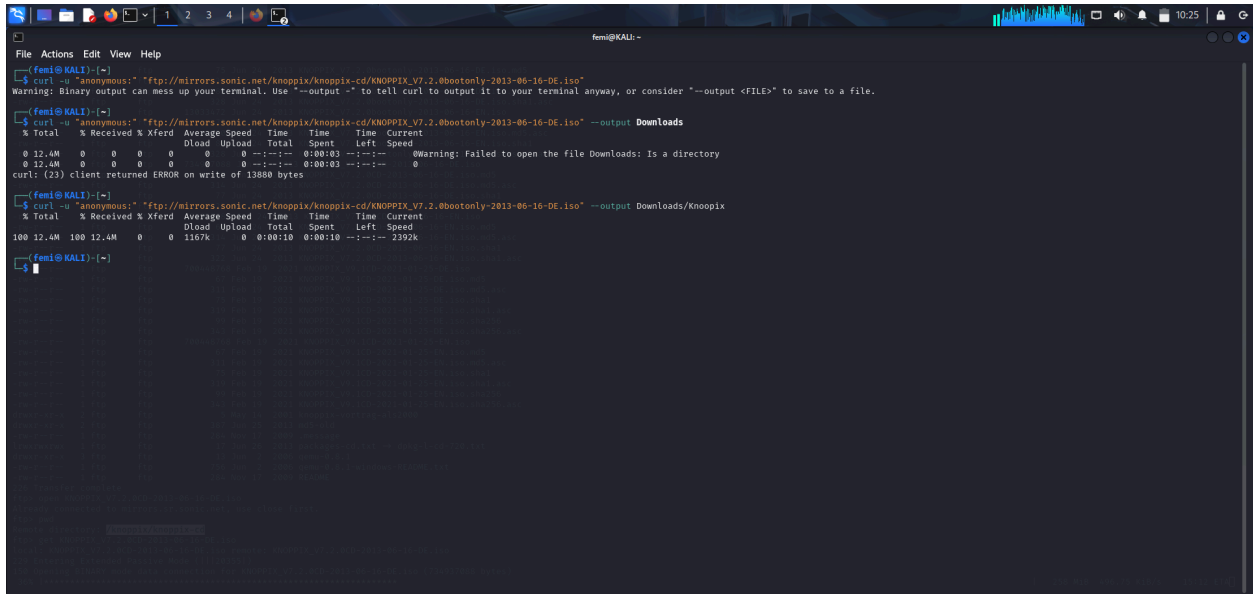
(femi@KALI) [-]
$ curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me

<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta http-equiv="Content-Style-Type" content="text/css" />
  <meta http-equiv="Content-Script-Type" content="text/javascript" />
  <meta http-equiv="Content-Language" content="en" />
  <meta http-equiv="pragma" content="no-cache" />
  <meta http-equiv="cache-control" content="no-cache" />
  <meta name="description" content="Get my IP Address" />
  <meta name="keywords" content="ip address ifconfig ifconfig.me" />
  <meta name="author" content="" />
  <link rel="shortcut icon" href="https://ifconfig.me/" />
  <title>What Is My IP Address? - ifconfig.me</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="/static/style/style.css" rel="stylesheet" type="text/css">
  <link href="https://fonts.googleapis.com/css?family=Open+Sans&display=swap" rel="stylesheet">
</head>
<body>
  <div id="ad-container">
    <div class="ad">
      Need a robust API to Geolocate IPs and fetch other crucial information? Try
      <a href="https://ipinfo.io/?utm_source=ifconfig.me&utm_medium=referral&utm_campaign=supsell_sister_sites">IPinfo.io</a>.
    </div>
  </div>
  <div id="container" class="clearfix">
    <div id="header">
      <table>
        <tr>
          <td>
            <h1><a href="http://ifconfig.me">What Is My IP Address? - ifconfig.me</a></h1>
          </td>
        </tr>
      </table>
    </div>
  </div>
</body>
</html>
```

STEP 6:

Another important feature of curl is its ability to transfer files. This is useful when interacting with servers through the command line, particularly if you are trying to take advantage of potential vulnerabilities. To access a protected FTP server, use the -u option to specify the username and password:

```
curl -u "anonymous:"  
"ftp://mirrors.sonic.net/knoppix/knoppix-cd/KNOPPIX_V7.2.0bootonly-2013-06-16-DE.iso"  
-output Downloads/Knoppix
```

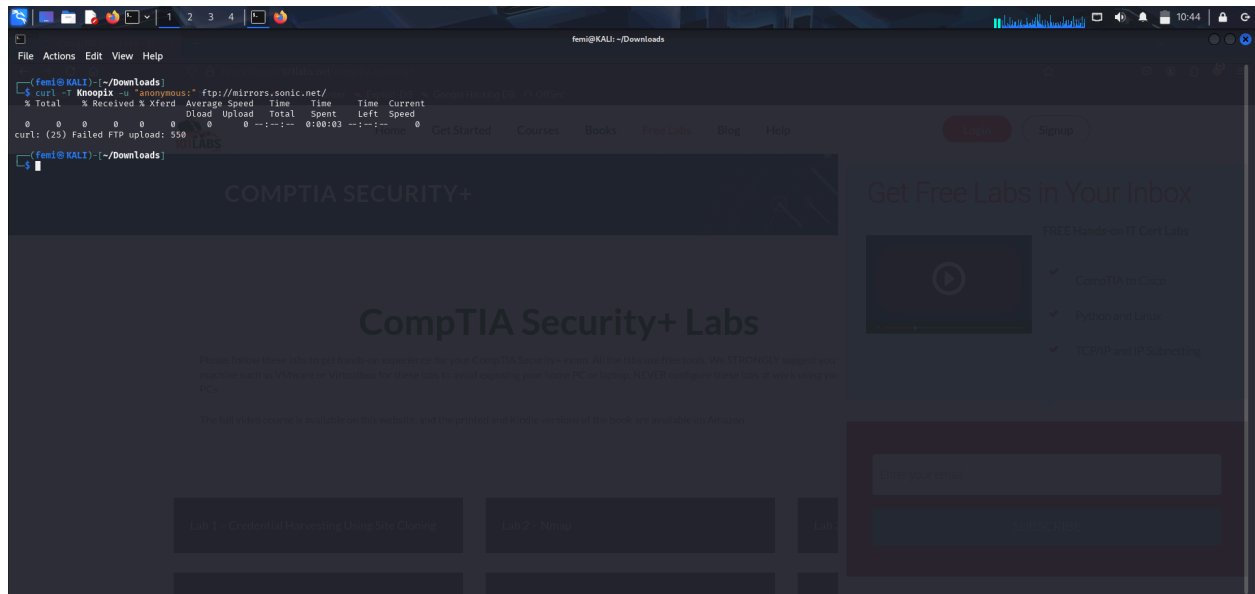


```
femi@KALI:~$ curl -u "anonymous:" "ftp://mirrors.sonic.net/knoppix/knoppix-cd/KNOPPIX_V7.2.0bootonly-2013-06-16-DE.iso"  
Warning: Binary output can mess up your terminal. Use "--output -" to tell curl to output it to your terminal anyway, or consider "--output <FILE>" to save to a file.  
  
femi@KALI:~$ curl -u "anonymous:" "ftp://mirrors.sonic.net/knoppix/knoppix-cd/KNOPPIX_V7.2.0bootonly-2013-06-16-DE.iso" --output Downloads  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
0 12.4M    0     0    0      0      0      0      0  0:00:03  0:00:03  0:00:03  0  
0 12.4M    0     0    0      0      0      0      0  0:00:03  0:00:03  0:00:03  0  
curl: (23) client returned ERROR on write of 13880 bytes  
  
femi@KALI:~$ curl -u "anonymous:" "ftp://mirrors.sonic.net/knoppix/knoppix-cd/KNOPPIX_V7.2.0bootonly-2013-06-16-DE.iso" --output Downloads/Knoppix  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
100 12.4M  100 12.4M    0    1167k    0      0      0  0:00:10  0:00:10  0:00:10 2392k  
  
femi@KALI:~$
```

To upload a file to the server, we can use the -T option:

Cd to the directory where the file is located, then input the command

```
curl -T Knoppix -u "anonymous:" ftp://mirrors.sonic.net/
```



STEP 7:

Normally, curl denies connection to sites which have invalid SSL certificates. To connect without blocking and getting a warning message, we can use the “-k” option, for example:

```
curl -k http://192.168.1.1/
```

STEP 8:

Curl can also be configured to use a proxy. To do this, use the -x option followed by the proxy URL. For example:

```
curl -x 192.168.0.1:8080 http://unaab.edu.ng
```

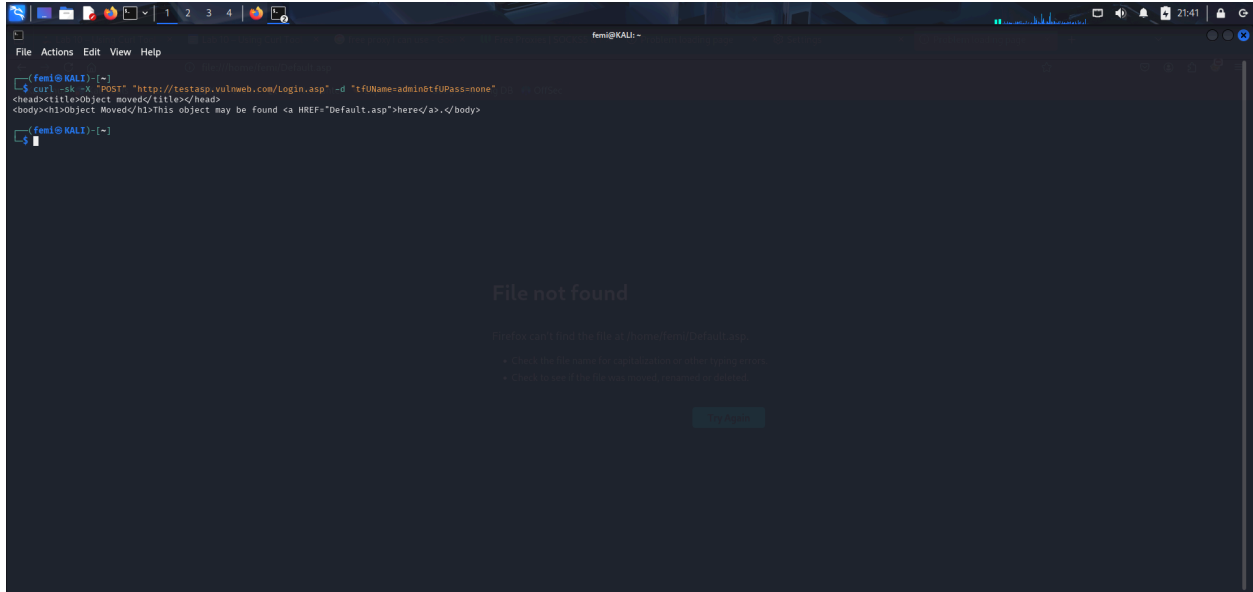
STEP 9:

Curl can also be used for sending HTTP POST data to FORM pages.

In this example, we are sending two parameters, “tfUName” and “tfUPass”, with attached values to “<http://testasp.vulnweb.com/Login.asp>”.

Use the code;

```
curl -sk -X "POST" "http://testasp.vulnweb.com/Login.asp" -d "tfUName=admin&tfUPass=none"
```



END