

USING THE CURL TOOL

Project Objective: Learn how to use the CURL tool to gather information

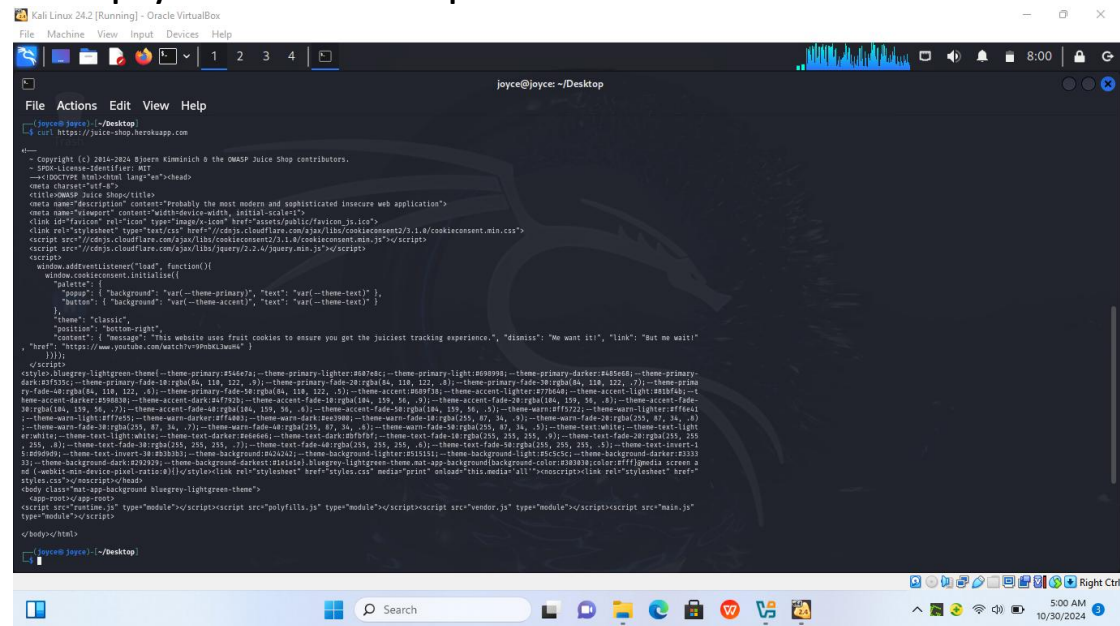
Curl(Client URL). It is a command line tool for getting and sending data including files using URL syntax.

Tool: Kali Linux

Project-site:<https://juice-shop.herokuapp.com>(OWASP Juice Shop)

curl <https://juice-shop.herokuapp.com>

This displayed the raw HTML output of the above site.

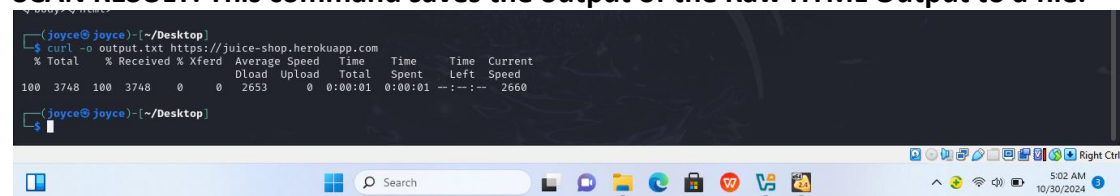


```
joyce@kali: ~/Desktop
$ curl https://juice-shop.herokuapp.com

<!--
  Copyright (c) 2014-2024 Björn Kimminich & the OWASP Juice Shop contributors.
  SPDX-License-Identifier: MIT
-->
<!DOCTYPE html><html lang="en"><head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticated insecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="static/favicon.ico?c=2">
  <link rel="stylesheet" type="text/css" href="/css/cdnjs.cloudflare.com/ajax/libs/cookieconsent/3.1.0/cookieconsent.min.css">
  <script src="/cdnjs.cloudflare.com/ajax/libs/cookieconsent/3.1.0/cookieconsent.min.js"></script>
  <script src="/cdnjs.cloudflare.com/ajax/libs/jquery/3.2.0/jquery.min.js"></script>
  <script>
    window.addEventListener("load", function() {
      window.cookieconsent.initialise({
        "palette": {
          "popup": { "background": "var(--theme-primary)", "text": "var(--theme-text)" },
          "button": { "background": "var(--theme-accent)", "text": "var(--theme-text)" }
        },
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message": "This website uses fruit cookies to ensure you get the juiciest tracking experience.", "dismiss": "We want it!", "link": "But no wait!" },
        "href": "https://www.youtube.com/watch?v=smk8hume"
      });
    });
  </script>
  <style>
    :root {
      --theme-primary: #444;
      --theme-primary-lighter: #888;
      --theme-primary-light: #ccc;
      --theme-primary-darker: #222;
      --theme-primary-darkest: #000;
      --theme-primary-fade-10: rgba(68, 119, 122, 0.1);
      --theme-primary-fade-20: rgba(68, 119, 122, 0.2);
      --theme-primary-fade-30: rgba(68, 119, 122, 0.3);
      --theme-primary-fade-40: rgba(68, 119, 122, 0.4);
      --theme-primary-fade-50: rgba(68, 119, 122, 0.5);
      --theme-primary-fade-60: rgba(68, 119, 122, 0.6);
      --theme-primary-fade-70: rgba(68, 119, 122, 0.7);
      --theme-primary-fade-80: rgba(68, 119, 122, 0.8);
      --theme-primary-fade-90: rgba(68, 119, 122, 0.9);
      --theme-primary-fade-100: rgba(68, 119, 122, 1.0);
      --theme-accent: #f7941d;
      --theme-accent-lighter: #f9c99d;
      --theme-accent-light: #fde4b1;
      --theme-accent-darker: #f4792e;
      --theme-accent-darkest: #e66a00;
      --theme-accent-fade-10: rgba(247, 156, 29, 0.1);
      --theme-accent-fade-20: rgba(247, 156, 29, 0.2);
      --theme-accent-fade-30: rgba(247, 156, 29, 0.3);
      --theme-accent-fade-40: rgba(247, 156, 29, 0.4);
      --theme-accent-fade-50: rgba(247, 156, 29, 0.5);
      --theme-accent-fade-60: rgba(247, 156, 29, 0.6);
      --theme-accent-fade-70: rgba(247, 156, 29, 0.7);
      --theme-accent-fade-80: rgba(247, 156, 29, 0.8);
      --theme-accent-fade-90: rgba(247, 156, 29, 0.9);
      --theme-accent-fade-100: rgba(247, 156, 29, 1.0);
      --theme-warn: #ff7f50;
      --theme-warn-lighter: #ffccbc;
      --theme-warn-light: #ffe4c4;
      --theme-warn-darker: #ff4500;
      --theme-warn-darkest: #ff0000;
      --theme-warn-fade-10: rgba(255, 127, 80, 0.1);
      --theme-warn-fade-20: rgba(255, 127, 80, 0.2);
      --theme-warn-fade-30: rgba(255, 127, 80, 0.3);
      --theme-warn-fade-40: rgba(255, 127, 80, 0.4);
      --theme-warn-fade-50: rgba(255, 127, 80, 0.5);
      --theme-warn-fade-60: rgba(255, 127, 80, 0.6);
      --theme-warn-fade-70: rgba(255, 127, 80, 0.7);
      --theme-warn-fade-80: rgba(255, 127, 80, 0.8);
      --theme-warn-fade-90: rgba(255, 127, 80, 0.9);
      --theme-warn-fade-100: rgba(255, 127, 80, 1.0);
      --theme-text: #fff;
      --theme-text-lighter: #eee;
      --theme-text-light: #ddd;
      --theme-text-darker: #bbb;
      --theme-text-darkest: #888;
      --theme-text-fade-10: rgba(255, 255, 255, 0.1);
      --theme-text-fade-20: rgba(255, 255, 255, 0.2);
      --theme-text-fade-30: rgba(255, 255, 255, 0.3);
      --theme-text-fade-40: rgba(255, 255, 255, 0.4);
      --theme-text-fade-50: rgba(255, 255, 255, 0.5);
      --theme-text-fade-60: rgba(255, 255, 255, 0.6);
      --theme-text-fade-70: rgba(255, 255, 255, 0.7);
      --theme-text-fade-80: rgba(255, 255, 255, 0.8);
      --theme-text-fade-90: rgba(255, 255, 255, 0.9);
      --theme-text-fade-100: rgba(255, 255, 255, 1.0);
      --theme-background-dark: #222;
      --theme-background-darker: #000;
      --theme-background-lighter: #444;
      --theme-background-light: #ccc;
      --theme-background-fade-10: rgba(34, 34, 34, 0.1);
      --theme-background-fade-20: rgba(34, 34, 34, 0.2);
      --theme-background-fade-30: rgba(34, 34, 34, 0.3);
      --theme-background-fade-40: rgba(34, 34, 34, 0.4);
      --theme-background-fade-50: rgba(34, 34, 34, 0.5);
      --theme-background-fade-60: rgba(34, 34, 34, 0.6);
      --theme-background-fade-70: rgba(34, 34, 34, 0.7);
      --theme-background-fade-80: rgba(34, 34, 34, 0.8);
      --theme-background-fade-90: rgba(34, 34, 34, 0.9);
      --theme-background-fade-100: rgba(34, 34, 34, 1.0);
      --theme-media-screen-a: #fff;
      --theme-media-screen-b: #000;
    }
  </style>
  <script>
    <!--
      app-root=~/app-root
      script src="/main.js" type="module"></script>
      script src="/polyfills.js" type="module"></script>
      script src="/vendor.js" type="module"></script>
      script src="/main.js" type="module"></script>
    </script>
  </body></html>
</pre>
```

Curl -o output.txt <https://juice-shop.herokuapp.com>

SCAN RESULT: This command saves the output of the Raw HTML Output to a file.



```
joyce@kali: ~/Desktop
$ curl -o output.txt https://juice-shop.herokuapp.com
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 3748 100 3748 0 0 2653 0 0:00:01 0:00:01 --:-- 2660
$
```

Curl -O researchgate.net/publication/375075414_Cyber_Security_

SCAN RESULT: It provides the ability to download multiple files at once.



```
joyce@kali: ~/Desktop
$ curl -O researchgate.net/publication/375075414_Cyber_Security_
rs
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:-- --:-- --:--
0 0 0 0 0 0 0 0 --:-- --:-- --:--
0 0 0 0 0 0 0 0 --:-- --:-- --:--
0 0 0 0 0 0 0 0 --:-- --:-- --:--
100 167 100 167 0 0 97 0 0:00:01 0:00:01 --:-- 9
$
```

Curl -C -O : This is useful in downloading HTTP headers,when testing a site.

```
(joyce@ joyce) - [~/Desktop]
$ curl -C- -O researchgate.net/publication/375075414_Cyber_Security_
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total       Spent    Left     Speed
100 167    100 167      0      0        176      0 --:--:-- --:--:-- --:--:-- 178

(joyce@ joyce) - [~/Desktop]
$ cp CyberSecurity.pdf ~/Documents
CyberSecurity.pdf
```

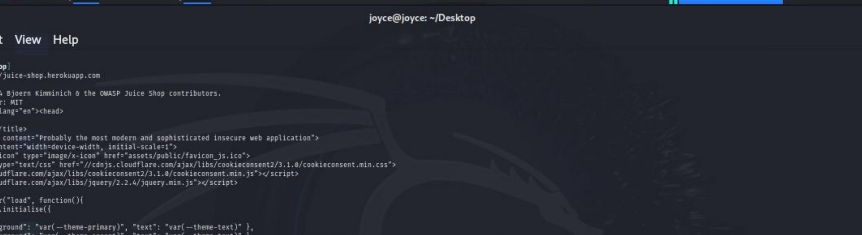
Curl -I: This displays information such as status code, server information, content, and content encoding.

```

(joyce@joyce) [~/Desktop]
$ curl -I https://juice-shop.herokuapp.com
HTTP/1.1 200 OK
Server: Cowboy
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1730312925&sid=812dcc77-0bd0-43b1-a5f1-b257503829596s-erCAYtrZSMJ3ctaUdpPkqsRwHfLntItaIHvKasyDUX3D"}]}
Reporting-Endpoints: heroku-nel-https://nel.heroku.com/reports?ts=1730312925&sid=812dcc77-0bd0-43b1-a5f1-b257503829596s-erCAYtrZSMJ3ctaUdpPkqsRwHfLntItaIHvKasyDUX3D
Nel: {"report-to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 30 Oct 2024 18:06:33 GMT
Etag: W/"ea4-192de9b9e73"
Content-Type: text/html; charset=UTF-8
Content-Length: 3748
Vary: Accept-Encoding
Date: Wed, 30 Oct 2024 18:28:45 GMT
Via: 1.1 vegur

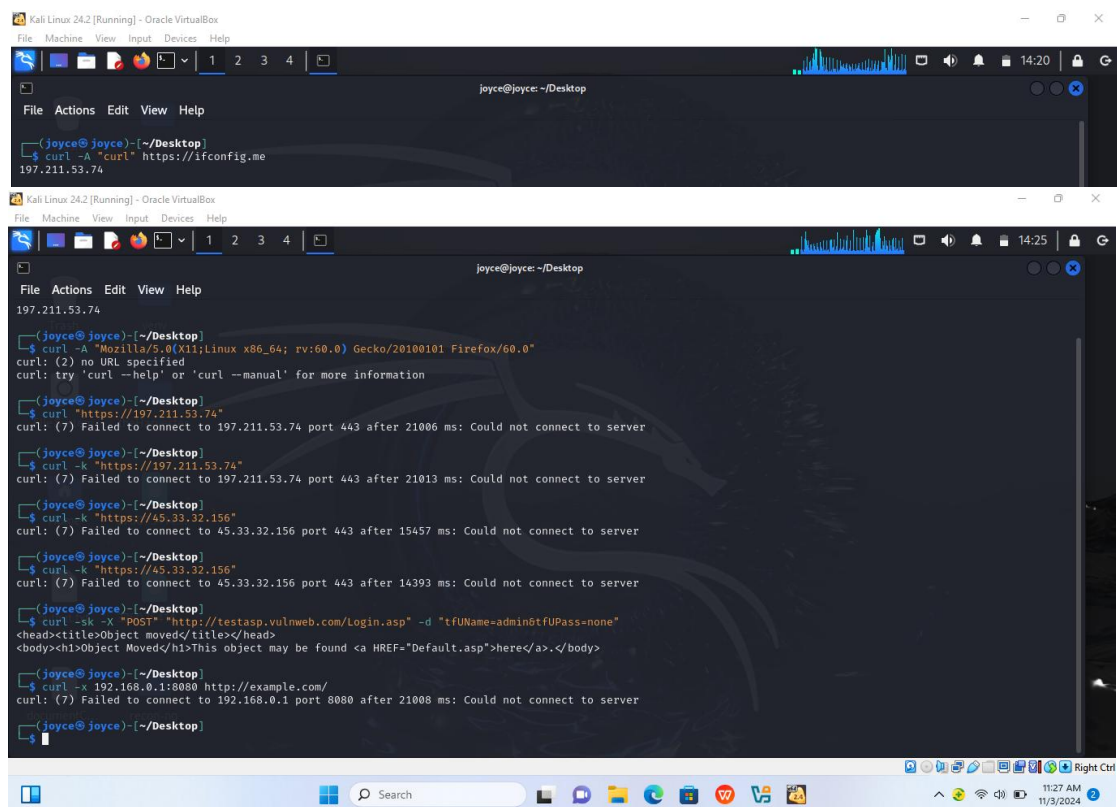
```

Curl -A : This gives full scan on the Target site HTML DOCUMENT.



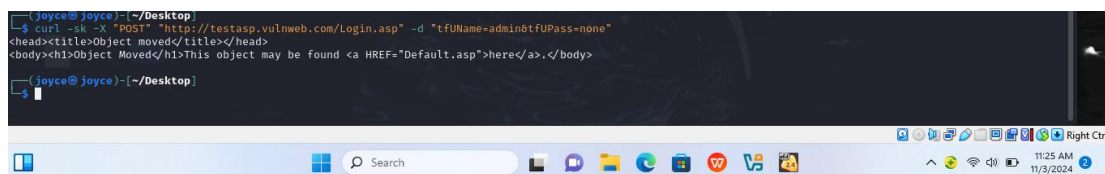
When attempting to download a file or gather other information using curl, you may discover that the target site may be designed to block curl. In this case, it is useful to emulate a browser, such as Firefox, to return the information you are looking for. To do this, use the following command:

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



The image shows two screenshots of a Kali Linux terminal window. The top screenshot shows the command `curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me` being executed, which returns the IP address `197.211.53.74`. The bottom screenshot shows a series of curl commands and their outputs. It starts with `curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me` returning `197.211.53.74`. Then, it shows `curl -k https://197.211.53.74` failing to connect. Next, it shows `curl -k https://45.33.32.156` failing to connect. Finally, it shows `curl -sk -X "POST" "http://testasp.vulnweb.com/Login.asp" -d "tfuname=admin&tfupass=none"` returning an HTML response: `<head><title>Object moved</title></head><body><h1>Object Moved</h1>This object may be found here.</body>`. The terminal window has a taskbar at the bottom with various icons and a search bar.

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”.



The image shows a screenshot of a Kali Linux terminal window. The terminal displays the command `curl -sk -X "POST" "http://testasp.vulnweb.com/Login.asp" -d "tfuname=admin&tfupass=none"` and its output: `<head><title>Object moved</title></head><body><h1>Object Moved</h1>This object may be found here.</body>`. The terminal window has a taskbar at the bottom with various icons and a search bar.