navln.com

Infosec articles, Hack The Box and Try Hack Me writeups, CTF articles and ethical hacking.

ACTIVE / HACK THE BOX / LINUX / OSCP / TRYHACKME

TryHackMe DailyBugle Writeup – Exploiting Joomla Version 3.7.0

by Navin May 8, 2020

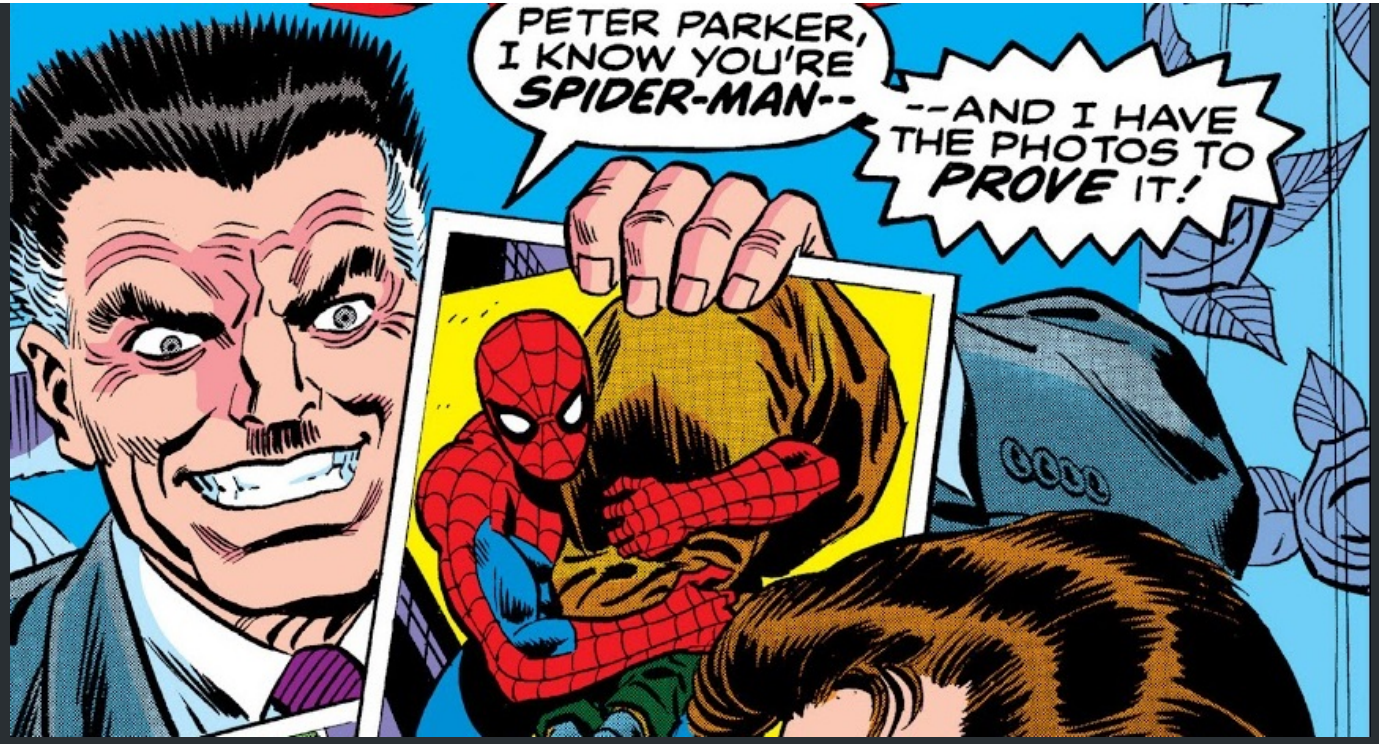
I'm working on the Offensive Pentesting Learning Path on TryHackme, I've already reached 3rd level by exploiting 7 machines on my way. Yesterday I was working on a machine called "DailyBugle" - a Joomla CMS based machine with Joomla version 3.7.0 related exploit. Here is my writeup and my way of exploiting the machine. Hope you enjoy reading it.

The machine Dailybugle is fairly straight-forward. One need a basic knowledge of CMS exploitation and fairly basic knowledge of cracking hashes and getting the password. As this machine is part of TryHackMe OSCP learning path one is not allowed to use SQLMAP, apart from that this is a medium hard machine.

Subscribe To Nav1n.Com Via Email

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Email Address



TryHackMe DailyBugle Writeup - Exploiting Joomla V. 3.7.0

Enumeration

As usual, I'm going to perform an initial NAMP scan to find open ports, to find running services, get more information on OS version and if possible to find the applications running.

```
$ nmap -O -v 10.10.255.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 13:04 +03
Scanning 10.10.255.15 &#91;1000 ports]
Discovered open port 80/tcp on 10.10.255.15
Discovered open port 22/tcp on 10.10.255.15
Discovered open port 3306/tcp on 10.10.255.15
```


Disclaimer

All the information provided on **https://www.nav1n.com** is for educational purposes only. This web site and the authors of the website are no way responsible for any misuse of the information.

https://www.nav1n.com or the authors of this blog writes on the topics which are related to information security, Penetration Testing and computer security, **https://www.nav1n.com** does not promote or

```
Increasing send delay for 10.10.255.15 from 0 to 5 due to 289 out of 961 dropped probes since last increase.
Completed SYN Stealth Scan at 13:04, 7.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against 10.10.255.15
Retrying OS detection (try #2) against 10.10.255.15
Retrying OS detection (try #3) against 10.10.255.15
Retrying OS detection (try #4) against 10.10.255.15
Retrying OS detection (try #5) against 10.10.255.15
Nmap scan report for 10.10.255.15
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/8%OT=22%CT=1%CU=33863%PV=Y%DS=2%DC=I%G=Y%TM=5EB52EB0
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10B%TI=Z%II=I%TS=A)SEQ(SP=FF%
OS:GCD=1%ISR=10B%TI=Z%CI=I%TS=A)SEQ(SP=FF%GCD=1%ISR=10B%TI=Z%TS=A)OPS(O1=M5
OS:08ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O
OS:6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%D
OS:F=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%I
OS:PL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Fri May  8 13:03:43 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

encourage computer Hacking (unethical), cracking or any other illegal activity.

```
Nmap done: 1 IP address (1 host up) scanned in 23.17 seconds
           Raw packets sent: 1448 (67.738KB) | Rcvd: 1080 (46.694KB)
```

The NMAP port scan shows, SSK on port 22, a web server is running on the default port 80 and MySQL on its default port 3306.

I found-out a website “Dailybugle” is running on the Apache web server. Upon going through the website we noticed “Spider-Man” has robbed a bank 🙂

Enumerating Hidden Directories

I proceed forward after find the website to enumerate the directories. I used GoBuster and found following hidden directories along with an interesting /administrator/

```
# root @ ns09 in ~/thm/dailybugle &#91;14:04:43] C:1
$ gobuster dir -u http://10.10.166.36/ -w /usr/share/wordlists/dirb/common.tx
t
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) &amp; Christian Mehlmauer (@_FireFart_)
===============================================================
&#91;+] Url:            http://10.10.166.36/
&#91;+] Threads:        10
&#91;+] Wordlist:       /usr/share/wordlists/dirb/common.txt
&#91;+] Status codes:   200,204,301,302,307,401,403
&#91;+] User Agent:     gobuster/3.0.1
&#91;+] Timeout:        10s
===============================================================
2020/05/08 14:52:32 Starting gobuster
```

```
14 ===============================================================
15 /.hta (Status: 403)
16 /.htaccess (Status: 403)
17 /.htpasswd (Status: 403)
18 /administrator (Status: 301)
19 /bin (Status: 301)
20 /cache (Status: 301)
21 /cgi-bin/ (Status: 403)
22 /components (Status: 301)
23 /images (Status: 301)
24 /includes (Status: 301)
25 /index.php (Status: 200)
26 /language (Status: 301)
27 /layouts (Status: 301)
28 /libraries (Status: 301)
29 /media (Status: 301)
30 /modules (Status: 301)
31 /plugins (Status: 301)
32 /robots.txt (Status: 200)
33 /templates (Status: 301)
34 /tmp (Status: 301)
35 ===============================================================
36 2020/05/08 14:53:38 Finished
37 ===============================================================
38
```

Administrator Login Page

Sweet, when I see this login-page I know there is a vulnerability associated with it. The Joomla can be easily on top of the list of the highest vulnerability found CMS.

Finding Joomla Version and Exploits

In fact, it doesn't take much time to find exploits related to the Joomla, however each exploit works on particular version of CMS or any application, so I need to find the Joomla version first.

There is a very nice and frequently updating tool that every pen tester use at least once while testing and finding web application version in GitHub called "CMSeek" by Tuhinshubhra. I used it and the tool got me the information I was looking for. The Joomla version 3.7.0 is running in this machine.

Finding The Exploit For Joomla 3.7.0

As per the tasks in TryHackMe, we could use SQL injection to find user and the password however, they recommended using a Python script. I know a script which I recently used in one of the alignment which is called "JoomBLAH".

Finding The User

I copied the python script to my Dailybugle working directory and have the user "Jonah" and her hashed password. The interesting part is user Jonah seem to be a Super User, which is going to be more fun.

Cracking The Hash

The hashed password can't be used to log in the CMS, I'm going to use John and HashCat both using all-time favorite RockYou, so lets see which one cracks faster.

John, took around 0:29:54 minutes to crack the password.

Where Hashcat took just 0:07:00 minutes.

As I have a valid credential let us log in to the CMS.

Joomla
Administrator
Portal

Reverse Shelling The Box

I tried to use the credential to SSH the box it didn't work, so plan B was to have a reverse shell to the machine. There are a couple of reverse-shell that I could use, I chose to be with PenTestMonkey's PHP reverse shell which always works. I've used it extensively on different machines of HackTheBox.

The usage is always the same, find a template and edit the source and amend it with our reverse shell script, run a listener in local machine, run the script and boom, there you have the reverse shell and it is as simple as it sounds.

I open the default template and proceed to customize it. I used the index.php page of the default template, In the other hand I started my listener running on the port 9999.

And Update to this:

Once the amendment is done, I open the page by running it and my listener is activated and I have reverse shell as Apache.

Upon enumerating further I found the user JJameson, however I wasn't able to go to his home as the Apache user doesn't have permission.

As I'm not able to do anything unless I have a right password or right user, I started to enumerate further. I know as an Apache user I will be able to read files within www I proceed to do so. While reading contents of www folder I noticed `/var/www/html/configuration.php` some credentials.

ATM, I knew that it is the password of user JJameson and I will be able to SSH the box using it. I did the same and I'm logged in to the box as user JJameson.

Privilege Escalation

As usual, post exploitation I run sudo -l to see if the user is able to run anything as root. Luckily, yes he's able to run /usr/bin/yum as root. So the user have root privileges to yum which as well lets the root setUID executable. This privesc is the route for escalating user JJameson to root.

I used the exploit as mentioned in the article.

And ran my custom plugin exploit got the root shell and I found the root.txt in /root/ home folder.

That's all, thank you for reading.

Post Views: 764

Like this:

Loading...

TAGGED CMS EXPLOIT JOOMLA JOOMLA EXPLOIT SETUID SQLI YUM EXPLOIT

PREVIOUS POST
TryHackMe LFI Writeup

NEXT POST
HackTheBox Cache Writeup – 10.10.10.188

Navin

Hey there, I'm Navin, a passionate Info-Sec enthusiast from Bahrain. I started this blog to share my knowledge. I usually write on HackTheBox machines and challenges, cybersecurity-related articles and bug-bounty. If you are an HTB user and like my articles, please respect here: https://www.hackthebox.eu/home/users/profile/68523

View all posts by Navin →

YOU MIGHT ALSO LIKE

HackTheBox Endgame P.O.O Writeup Part 1 – Recon (Flag 01/05)

February 25, 2020

HackTheBox Blackfield Writeup – 10.10.10.192

June 11, 2020

HackTheBox Endgame Xen Writeup Part 4 – Owned (Flag 06 /06)

May 25, 2020

0

Article Rating

★★★★★

Subscribe

Login

Join the discussion

B I U S {} [+]

1 COMMENT

Oldest

HackTheBox Cache Writeup - 10.10.10.188 - nav1n.com

1 month ago

[…] Previous Post Previous post: TryHackMe DailyBugle Writeup – Exploiting Joomla Version 3.7.0 […]

0 Reply