

## Autenticación en Nginx:

Deberemos instalar la herramienta openssl para crear contraseñas. En este caso la tenemos instalada, si no la tuviéramos tendríamos que instalarla.

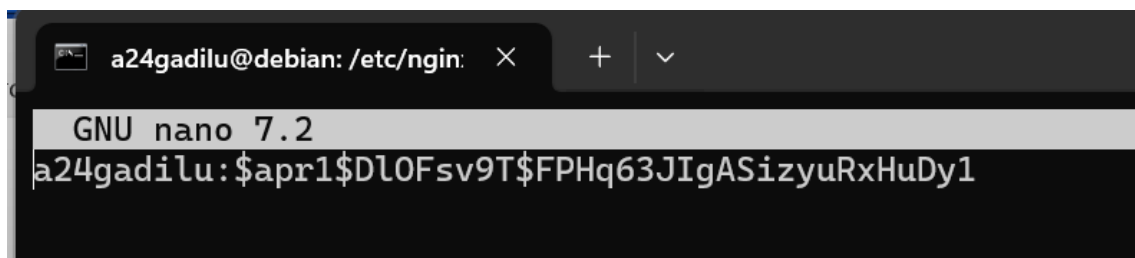
```
a24gadilu@debian:~$ sudo dpkg -l | grep openssl
ii  openssl                 3.0.14-1~deb12u2      amd64      Secure Sockets Layer toolkit - cryptographic utility
a24gadilu@debian:~$
```

Ahora crearemos los usuarios y las claves para el acceso web, para ello deberemos crear el archivo llamado .htpasswd en el directorio /etc/nginx.

```
"sudo sh -c "echo -n 'a24gadilu:' >> /etc/nginx/.htpasswd""
```

Creamos la clave con el siguiente comando:

```
"sudo sh -c "openssl passwd -apr1 >> /etc/nginx/.htpasswd""
```

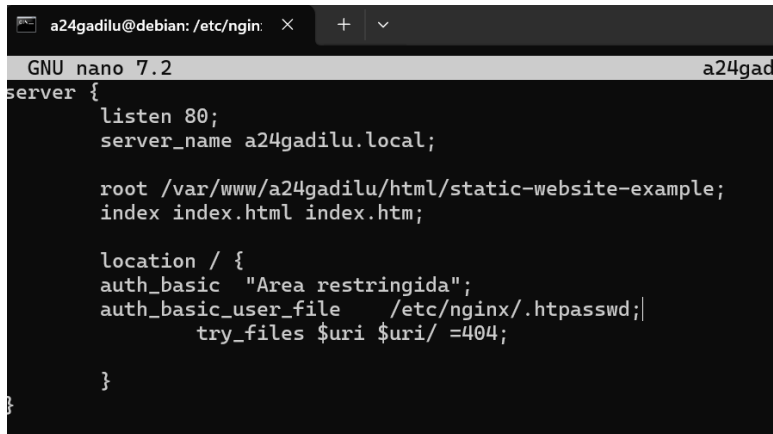


```
a24gadilu@debian: /etc/nginx/ X + v
GNU nano 7.2
a24gadilu:$apr1$Dl0Fsv9T$FPHq63JIgASizyuRxHuDy1
```

Editaremos la configuración del server sobre el cual queremos aplicar la restricción de acceso. Para ello usaremos nuestro sitio web. Editamos el archivo de nuestra web:

```
"sudo nano /etc/nginx/sites-available/a24gadilu"
```

Deberemos añadir la localización de nuestro archivo .htpasswd



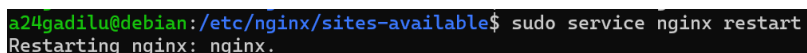
```
a24gadilu@debian: /etc/nginx/ X + v
GNU nano 7.2 a24gad
server {
    listen 80;
    server_name a24gadilu.local;

    root /var/www/a24gadilu/html/static-website-example;
    index index.html index.htm;

    location / {
        auth_basic "Area restringida";
        auth_basic_user_file /etc/nginx/.htpasswd;|
        try_files $uri $uri/ =404;
    }
}
```

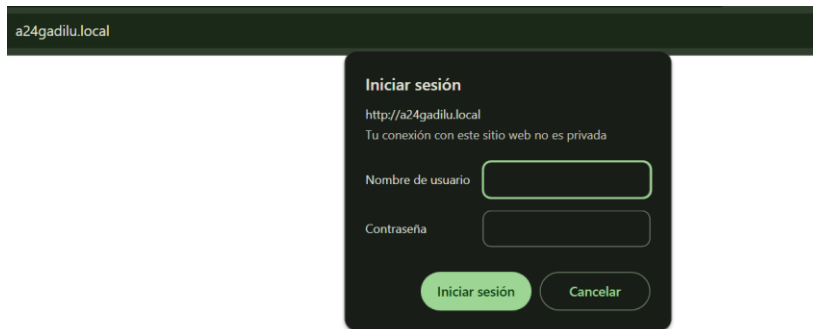
Una vez guardado reiniciamos el servicio:

```
"sudo service nginx restart"
```

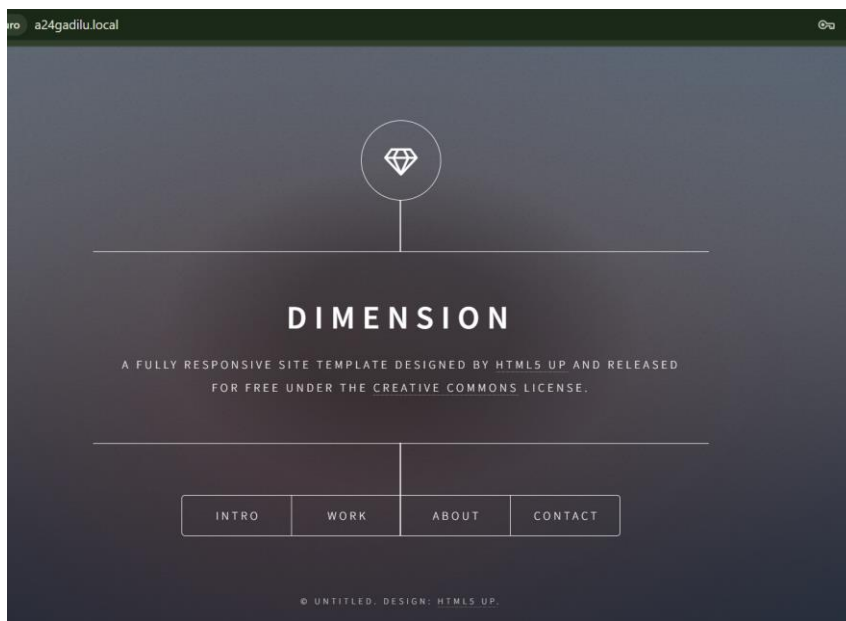


```
a24gadilu@debian:/etc/nginx/sites-available$ sudo service nginx restart
Restarting nginx: nginx.
```

Comprobamos que al entrar a nuestra página nos pide una autentificación:



Insertamos el usuario creado previamente con su contraseña y ya podremos acceder a nuestro sitio web:



Deberemos comprobar mediante los logs del servidor que la autenticación ha sido correcta, para ello deberemos ver el archivo Access.log:

“sudo tail -f /var/log/nginx/access.log”

```
192.168.116.207 - a24gadilu [01/Oct/2024:09:11:39 +0200] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36"
```

Con esto vemos que accedemos correctamente.

Para ver si ha habido un error en la autenticación usaremos el siguiente comando:

“sudo tail -f /var/log/nginx/error.log”

```
2024/10/01 09:16:10 [error] 2125#2125: *7 user "a24gadilu": password mismatch, client: 192.168.116.207, server: a24gadilu.local, request: "GET / HTTP/1.1", host: "a24gadilu.local"
```

Vemos que da error porque la contraseña introducida es incorrecta.

