

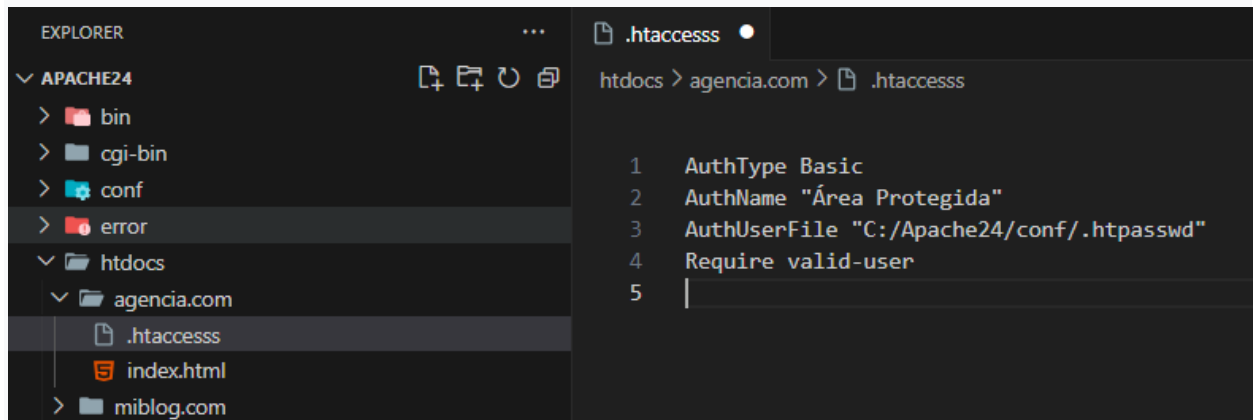
Enunciado

Utiliza la práctica P.1 para incluir restricciones de acceso:

1. Crea un usuario con tu nombre y contraseña 123456 y restringe el acceso a :
`agencia.com`

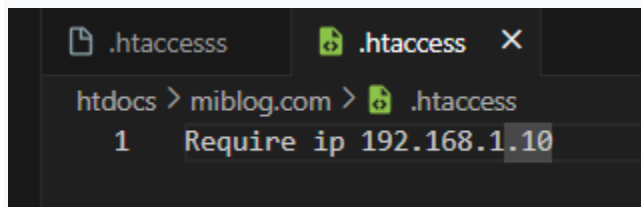
```
PS C:\WINDOWS\system32> cd C:\Apache24\bin\  
PS C:\Apache24\bin> .\htpasswd.exe -c "C:\Apache24\conf\.htpasswd" usuario1  
New password: ****  
Re-type new password: ****  
Adding password for user usuario1  
PS C:\Apache24\bin>
```

// En mi caso usare un archivo .htaccess en el subdirectoroi de /agencia.com:

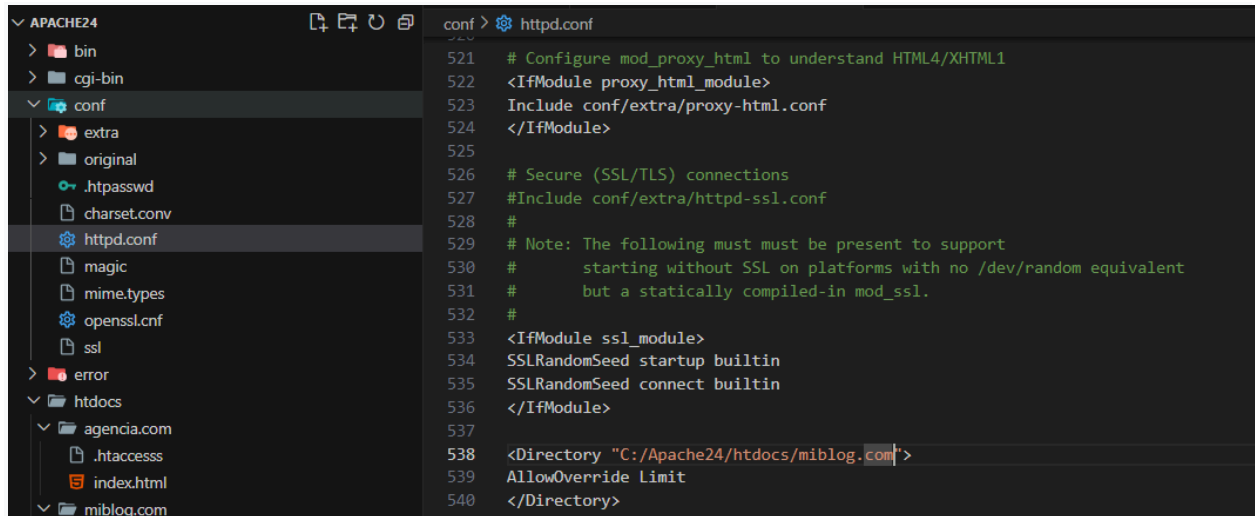


2. Configura Apache para que solo la IP 192.168.1.10 pueda acceder a `miblog.com`

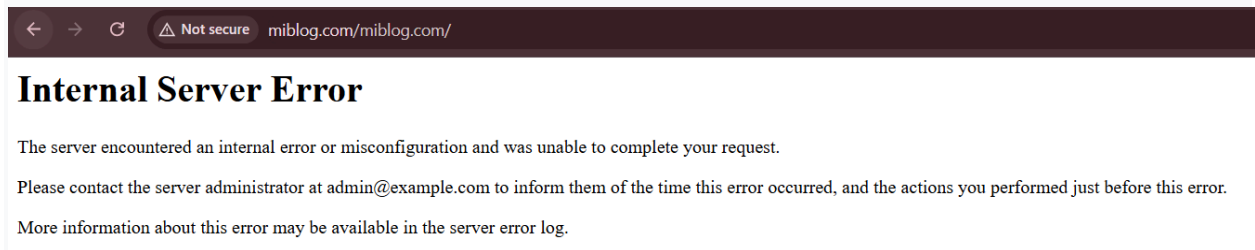
// creamos otro archivo htaccess dentro de /miblog.com con la siguiente directiva:



// Y a continuación editamos el fisher httpd.conf para habilitar esta directiva con `AllowOverride Limit`



// Ahora no nos permite ingresar en miblog.com ya que no pertenecemos a la ip requerida



// pero si nos deja ingresar en las demás





3. Investigación. Busca como se puede restringir el acceso por múltiples rangos de red. Explica como se haría y pon la ruta a la fuente que has utilizado.

// Es sencillo, en el archivo htaccess podríamos hacer lo siguiente:

```
Require ip rango_ip./24
```

```
Require ip otro_rango./16
```

```
Require ip otro_rango./24
```

```
Require ip otro_rango./8
```

... etc

Consideraciones

- Recuerda que el usuario se genera utilizando un aplicación específica de Apache..
- Puedes hacer el ejercicio en Windows, Linux (WSL u otra distribución) o con Docker
- Recuerda que para probar si funciona tendrás que acceder a cada dominio por lo que modifica tu fichero hosts para redireccionar el nombre de dominio a localhost/127.0.0.1 (Si ya lo hiciste para el ejercicio anterior no tendrás que modificar nada más)

Entrega

- Un zip con la configuración y código generado.
- Un pdf con los pasos realizados con una pequeña descripción sobre los mismos.