

Práctica 3

Redes de computadoras

Emmanuel Peto Gutiérrez

22 de octubre de 2020

1. Pasos para realizar la práctica

Se realizó un fork del repositorio del profesor para tenerlo en mi cuenta de git.

<https://gitlab.com/nehnemini/redes-2021-1/-/tree/master/lab3>

En la carpeta `lab3` se encuentra una página web. Tiene un formulario donde se pide un nombre de usuario y una contraseña.

La página se modificó, añadiendo código al archivo `style.css` y añadiendo una imagen (el escudo de la facultad de ciencias).

Para conectarse con AWS primero hay que iniciar la instancia creada en la práctica 2. Para esto hay que ir a la consola de AWS, entrar a la opción EC2, en el menú de la izquierda ir a *Instancias/Instancias*, dar click en el id de la instancia y finalmente dar click en *Acciones/iniciar instancia*.

Una vez iniciada la instancia, me conecté desde mi equipo mediante el comando `ssh -i "practica2.pem ubuntu@ec2-54-166-88-197.compute-1.amazonaws.com`

```
ubuntu@ip-172-31-81-18: ~  
emmanuel@emmanuel-VPCS845FL:~$ ssh -i "practica2.pem" ubuntu@ec2-54-166-88-197.c  
ompute-1.amazonaws.com  
The authenticity of host 'ec2-54-166-88-197.compute-1.amazonaws.com (54.166.88.1  
97)' can't be established.  
ECDSA key fingerprint is SHA256:6hKRH/HCCXRIYo1QYjPN4VbXfN+aiBapxk1dJEXBKyw.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-54-166-88-197.compute-1.amazonaws.com,54.166.88.  
197' (ECDSA) to the list of known hosts.  
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1028-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Wed Oct 21 03:08:40 UTC 2020  
  
System load:  0.0          Processes:            103  
Usage of /:   24.3% of 7.69GB Users logged in:      0  
Memory usage: 21%         IPv4 address for eth0: 172.31.81.18  
Swap usage:   0%  
  
* Introducing autonomous high availability clustering for MicroK8s  
production environments! Super simple clustering, hardened Kubernetes,  
with automatic data store operations. A zero-ops HA K8s for anywhere.
```

Luego, me cambié al directorio `/var/www/html/`. Al dar `ls` se muestra el archivo `index.html` que se creó en la práctica 2.

```
ubuntu@ip-172-31-81-18:~$ cd /var/www/html/  
ubuntu@ip-172-31-81-18:/var/www/html$ ls  
index.html  
ubuntu@ip-172-31-81-18:/var/www/html$
```

En este directorio cloné el repositorio `redes-2021-1`. Si se ejecuta el comando `ls` se debe mostrar la carpeta.

```
ubuntu@ip-172-31-81-18:~$ cd /var/www/html/  
ubuntu@ip-172-31-81-18:/var/www/html$ ls  
index.html  
ubuntu@ip-172-31-81-18:/var/www/html$ sudo git clone https://gitlab.com/Peto626/  
redes-2021-1.git  
Cloning into 'redes-2021-1'...  
remote: Enumerating objects: 124, done.  
remote: Counting objects: 100% (124/124), done.  
remote: Compressing objects: 100% (68/68), done.  
remote: Total 124 (delta 45), reused 112 (delta 43), pack-reused 0  
Receiving objects: 100% (124/124), 1.02 MiB | 17.49 MiB/s, done.  
Resolving deltas: 100% (45/45), done.  
ubuntu@ip-172-31-81-18:/var/www/html$ ls  
index.html  redes-2021-1  
ubuntu@ip-172-31-81-18:/var/www/html$
```

Hay que cambiar de dirección a `/etc/apache2/`. De aquí hay que entrar a `sites-available`. Se copia el archivo `000-default.conf` con el nuevo nombre `redesfc.conf`. El archivo recién copiado se abre con un editor de texto (`vi` en este caso).

```

ubuntu@ip-172-31-81-18:/var/www/html$ ls
index.html  redes-2021-1
ubuntu@ip-172-31-81-18:/var/www/html$ cd /etc/apache2/
ubuntu@ip-172-31-81-18:/etc/apache2$ ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
ubuntu@ip-172-31-81-18:/etc/apache2$ cd sites-available
ubuntu@ip-172-31-81-18:/etc/apache2/sites-available$ ls
000-default.conf  default-ssl.conf
ubuntu@ip-172-31-81-18:/etc/apache2/sites-available$ sudo cp -a 000-default.conf
redesfc.conf
ubuntu@ip-172-31-81-18:/etc/apache2/sites-available$ sudo vi redesfc.conf

```

En la sección `DocumentRoot` se debe poner la dirección completa de la página web que se desea desplegar (debe haber un archivo `index.html`). En este caso es `/var/www/html/redes-2021-1/lab3/codigo_ejemplo`. Hay que guardar los cambios en el archivo y salir (`:x` en `vi`).

```

Actividades  Terminal  20 de oct 23:03
ubuntu@ip-172-31-81-18: /etc/apach

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/redes-2021-1/lab3/codigo_ejemplo

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

Hay que regresar al directorio `/var/www/html`. Actualmente, todos los cambios sólo pueden ser realizados por el administrador, así que hay que cambiar los permisos de la carpeta `redes-2021-1` para que el usuario `ubuntu:ubuntu` pueda hacer modificaciones. Claramente en otra situación el usuario puede tener otro nombre, pero en esta práctica es así. Para cambiar los permisos se ejecuta el comando `sudo chown -R ubuntu:ubuntu redes-2021-1/`

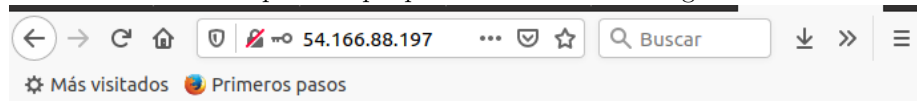
Una vez hecho esto, se debe deshabilitar el sitio de la práctica anterior (archivo `000-default.conf`) y habilitar el sitio de esta práctica (archivo `redesfc.conf`).

Se ejecutan los comandos: `sudo a2dissite 000-default.conf` y `sudo a2ensite redesfc.conf`.

Luego, para aplicar los cambios, hay que reiniciar el servidor apache con el comando `sudo systemctl restart apache2.service`.

```
ubuntu@ip-172-31-81-18:/var/www/html$ sudo chown -R ubuntu:ubuntu redes-2021-1
/
ubuntu@ip-172-31-81-18:/var/www/html$ sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@ip-172-31-81-18:/var/www/html$ sudo a2ensite redesfc.conf
Enabling site redesfc.
To activate the new configuration, you need to run:
    systemctl reload apache2
ubuntu@ip-172-31-81-18:/var/www/html$ sudo systemctl restart apache2.service
ubuntu@ip-172-31-81-18:/var/www/html$
```

Se puede comprobar que la página que se muestra ahora es la de esta práctica, poniendo la dirección IP pública que provee AWS en un navegador.



Iniciar sesión

User:





Pass:



Si se coloca la IP seguida de un directorio se va a mostrar el contenido. En este caso, se está mostrando el contenido de *images*. Para que no se muestre el contenido de los directorios hay que cambiar el archivo `redesfc.conf`.

← → ↻ 🏠 54.166.88.197/images/ Más visitados Primeros pasos

Index of /images

Name	Last modified	Size	Description
 Parent Directory			-
 ciencias.png	2020-10-21 03:19	74K	
 santas_bibliotecas_batman.png	2020-10-21 03:19	824K	
 tiburon.jpg	2020-10-21 03:19	39K	

Apache/2.4.41 (Ubuntu) Server at 54.166.88.197 Port 80

En la dirección `/etc/apache2/sites-available` se encuentra el archivo `redesfc.conf`, hay que abrirlo con `vi`. Para que no indexe el contenido hay que colocar el siguiente texto en el archivo:

```
<Directory /var/www/html/redes-2021-1/lab3/codigo_ejemplo>  
    Options -Indexes  
</Directory>
```

```
Actividades Terminal 21 de oct 07:52
ubuntu@ip-172-31-81-18: /etc/apache2

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/redes-2021-1/lab3/codigo_ejemplo

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    <Directory /var/www/html/redes-2021-1/lab3/codigo_ejemplo>
        Options -Indexes
    </Directory>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
-- INSERT --
```

Para que se apliquen los cambios hay que reiniciar apache con `sudo systemctl restart apache2.service` (en la misma dirección en la que está `redesfc.conf`).

Ahora, si se intenta acceder a un directorio desde un navegador se mostrará un mensaje diciendo que no tengo permiso de acceder a ese recurso.



En la carpeta `cgi-bin` del código ejemplo se encuentra un script en Python que sirve para manejar los datos de entrada (usuario y contraseña). Hay que configurar el servidor para que ejecute el script. Para eso, en el directorio `/etc/apache2/sites-available`, hay que ejecutar el comando `sudo a2enmod cgid`. Para aplicar los cambios hay que reiniciar el servicio con `sudo systemctl restart apache2`.

Después, hay que abrir otra vez el archivo `redesfc.conf` y colocar las siguientes líneas:

```
ScriptAlias /cgi-bin/ /var/www/html/redes-2021-1/lab3/codigo_ejemplo/cgi-bin/
```

```
<IfModule cgid-module>
  <Directory /var/www/html/redes-2021-1/lab3/codigo_ejemplo/cgi-bin/>
    Options -Indexes
    Options +ExecCGI
    AddHandler cgi-script .py
  </Directory>
</IfModule>
```

```
Actividades Terminal 21 de oct 18:29
ubuntu@ip-172-31-81-18: /etc/apache2/sites

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/redes-2021-1/lab3/codigo_ejemplo

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

<Directory /var/www/html/redes-2021-1/lab3/codigo_ejemplo>
    Options -Indexes
</Directory>

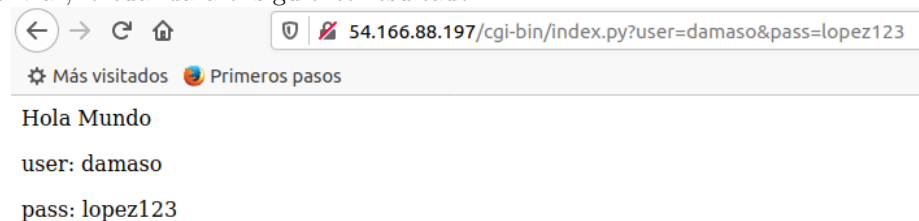
ScriptAlias /cgi-bin/ /var/www/html/redes-2021-1/lab3/codigo_ejemplo/cgi-bin/

<IfModule cgid-module>
    <Directory /var/www/html/redes-2021-1/lab3/codigo_ejemplo/cgi-bin/>
        Options -Indexes
        Options +ExecCGI
        AddHandler cgi-script .py
    </Directory>
</IfModule>
</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

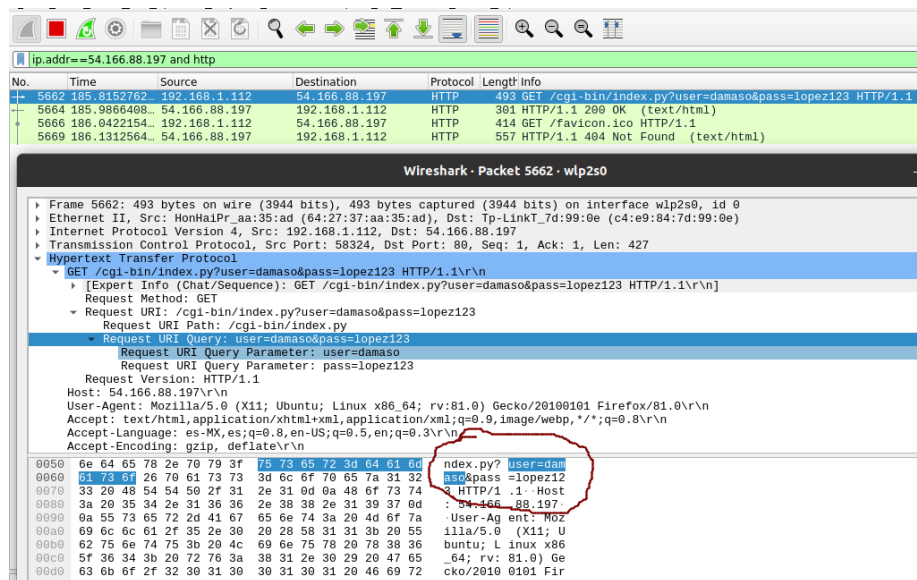
Una vez más, hay que aplicar los cambios con `sudo systemctl restart apache2.service`.

Para ver el tráfico entre mi computadora y la página que se acaba de crear se utiliza wireshark. Se coloca el filtro `ip.addr==54.166.88.197 and http`, que es la dirección de la página web y el protocolo que se desea filtrar.

Se coloca información de usuario y contraseña en el formulario y se da click a enviar, lo cual dará el siguiente resultado.



Y el tráfico en wireshark es el siguiente.



Como se notará, el resultado se envía mediante la url y es texto plano; es decir, no está cifrado.

Se procede a modificar el archivo `index.html` que se encuentra en el directorio `/var/www/html/redes-2021-1/lab3/codigo_ejemplo`. En la acción del formulario ahora se va a usar el método `post` (antes se usaba el `get`); sólo hay que comentar una línea y quitarle el comentario a la otra.

```

Actividades  Terminal 21 de oct 19:02
ubuntu@ip-172-31-81-18: /var/www/html/redes-20

<html>
<head>
<title>Práctica 3</title>
<link rel="stylesheet" href="css/style.css">
<meta charset="UTF-8"/>
<script src="js/script.js"></script>
</head>

<body>
<div id="midiv">
<h1 class="centrado" id="mih1">Iniciar sesión</h1>
</div>

<!-- <form action="/cgi-bin/index.py" method="get" class="centrado"> -->
<form action="/cgi-bin/index.py" method="post">
  User: <input type="text" name="user" ></br>
  Pass: <input type="password" name="pass" ></br>
  <input type="submit" value="enviar">
</form>


</body>
</html>

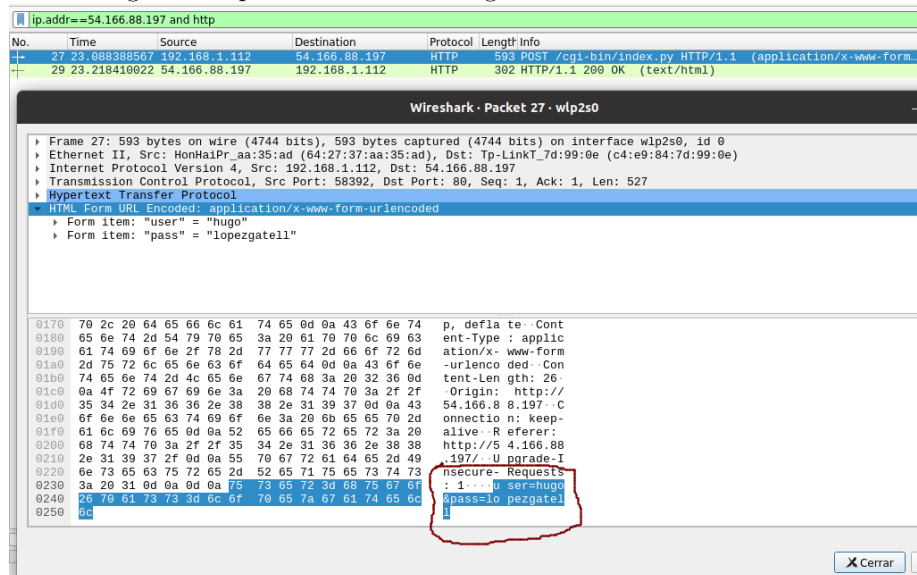
```

Otra vez hay que enviar los datos en el formulario. Ahora los datos de usuario

y contraseña ya no se muestran en la url.



El tráfico generado por wireshark es el siguiente.



Como se nota, el nombre de usuario y contraseña se envían en texto plano de todas formas con el método post.

2. Cuestionario

1. Menciona con tus propias palabras las ventajas que tiene centralizar el código fuente con git sin trabajar directamente en el servidor.

La primera ventaja notada es que, en nuestras computadoras, podemos usar el editor de textos que queramos, mientras que en un servidor se debe trabajar en la terminal; también cambiar de un directorio a otro es más fácil en nuestras computadoras.

Al usar git es más fácil trabajar en equipo, pues se pueden crear ramas, tener

control de versiones y notificar errores. Una vez terminado un proyecto, después de hacer pruebas, se puede clonar al servidor.

2. ¿Para qué se usa la directiva Options -Indexes?

Se usa para desindexar las carpetas y archivos de una aplicación web montada en un servidor. Así, las carpetas ya no son visibles para las personas que accedan a la página desde un navegador.

3. Menciona algún concepto que no te haya quedado del todo claro (opcional).

Sobre “Apache” (aunque no es un concepto): no entendi por qué no se puede abrir una página web en el servidor sin haber instalado Apache en éste.

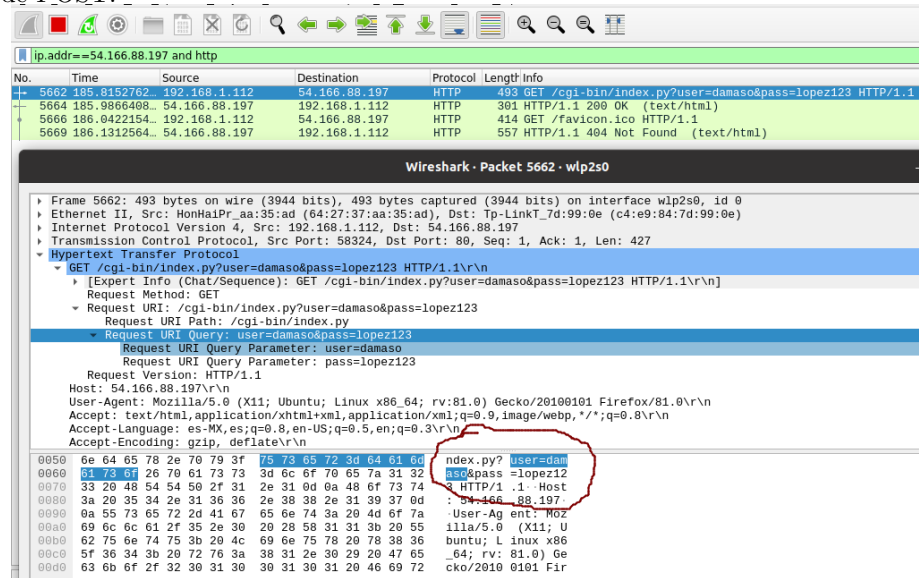
Por otra parte, no pude ejecutar el script de Python cuando probé el formulario en mi computadora.

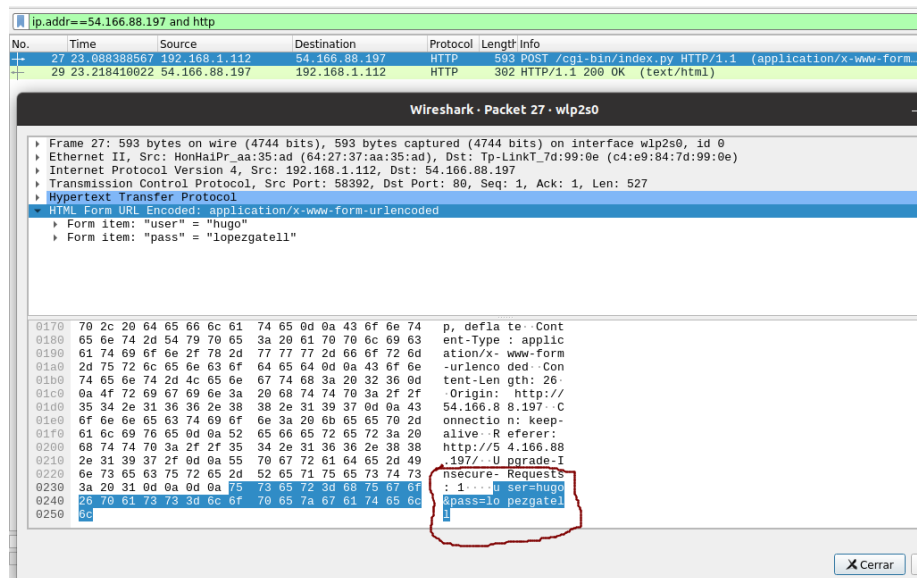
4. Liga del repositorio GitLab del repositorio con tus cambios.

<https://gitlab.com/Peto626/redes-2021-1>

5. Captura de pantalla del tráfico http (no seguro) con wireshark, marcando en dónde se envía la información en claro, tanto para el método GET como para el método POST.

En la región encerrada se encuentra la información de usuario y contraseña enviada en el mensaje. La primera imagen es la del método GET y la segunda la de POST.





6. ¿Cuál es la diferencia que se aprecia en Wireshark entre los mensajes que en donde se usó el método GET y los mensajes en donde se usa el método POST?, ¿cuál es la diferencia que se nota en el navegador web cuando se usa cada uno de estos métodos?

En wireshark:

En el método GET los datos aparecen en la sección de HTTP. Aquí se observa un Request URI Path, que es donde se encuentra el script de Python; también se ve un Request URI Query que es donde están los datos de user y pass, que en este caso son damaso y lopez123.

En el método POST los datos están contenidos en una sección llamada HTML Form URL Encoded. Los datos son items del formulario, donde las llaves son “user” y “pass” mientras que los valores asociados a esas llaves son “hugo” y “lopezgatell”.

En el navegador:

Para el método GET, los datos de usuario y contraseña aparecen en la URL de la página, después de la ruta del script, como user=damaso&pass=lopez123.

En cambio, en el método POST, no aparecen los datos de usuario y contraseña en la URL, sino que solo aparece la ruta del script: /cgi-bin/index.py.