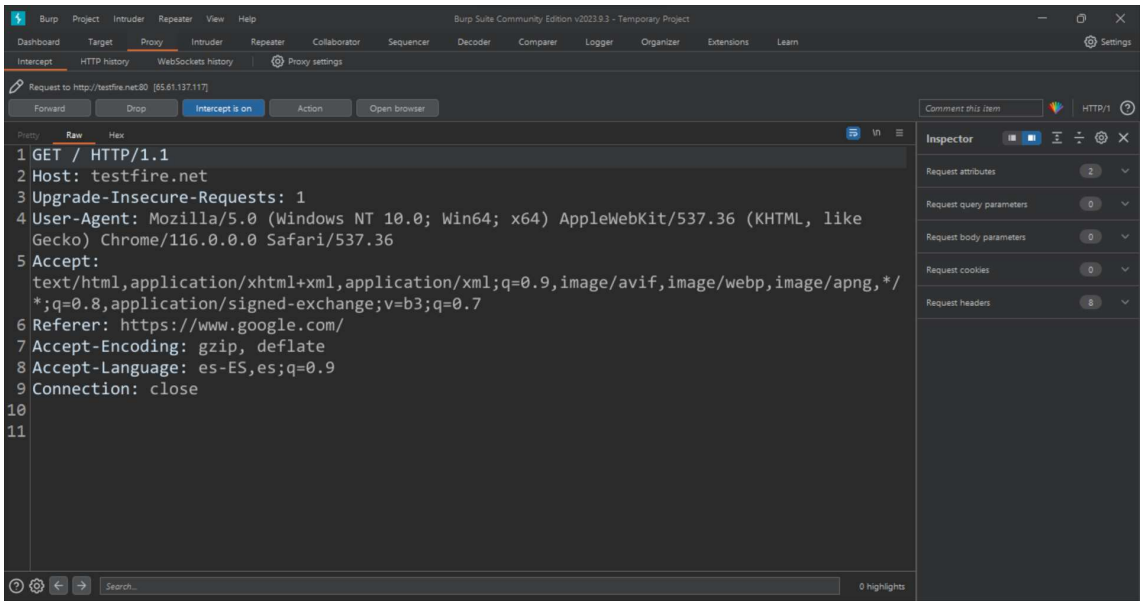


GET: Es el método para solicitar algún recurso por parte del cliente hacia el servidor
Un método HTTP permite solicitar recursos en general. El recurso puede ser lo que sea.
El 1.1 es la versión, casi todas las páginas utilizan la 1.
Host: Es el servidor. De cambiarlo, puede que no pase nada o que falle la conexión.
User Agent: Tiene que ver con el navegador, el tipo y la versión. Vienen el software, el sistema operativo, la versión y el tipo.
Accept: Vienen varios de los parámetros que puede enviar la página (texto, imágenes, etc)
Accept Languaje: Los idiomas que acepta la página
Accept Encoding: Las codificaciones aceptadas por la página
Referer: La aplicación o página web anterior. Puede explotarse una vulnerabilidad aquí
Connection: El estado de la transferencia de datos
Cookie: El identificador que ayuda a mantener la sesión entre intercambios de conexión.

Códigos de estado más comunes

Código de estado 200: Este es el código de estado estándar “OK” para una solicitud HTTP correcta. La respuesta que se devuelve depende de la solicitud. Por ejemplo, para una solicitud GET, la respuesta se incluirá en el cuerpo del mensaje. Para una solicitud PUT/POST, la respuesta incluirá el recurso que contiene el resultado de la acción.

Código de estado 204: La petición fue completada con éxito pero no hay nada que devolver. Entre los ejemplos de este código de estado se incluyen las solicitudes de eliminación o si se ha enviado una solicitud a través de un formulario y la respuesta no debe hacer que se actualice el formulario o que se cargue una nueva página.

Código de estado 301: La url ha cambiado permanentemente. Por ejemplo, el sitio se movió de http a https.
Código de estado 302: La url ha cambiado temporalmente

Código de estado 304: El código de estado que se utiliza para el almacenamiento en caché del explorador. Si la respuesta no se ha modificado, el cliente/usuario puede seguir

utilizando la misma versión de respuesta/caché. Por ejemplo, un explorador puede solicitar si un recurso se ha modificado desde una hora específica. Si no lo ha hecho, se envía el código de estado 304. Si se ha modificado, se envía un código de estado 200, junto con el recurso.
Puede pasar que al cargar una página, tengamos parte de la página en el caché, y al intentar atacarla, sólo estamos atacando el caché. Eliminar el caché o las cabeceras caché (If non cach) sirve para solucionarlo.

Código de estado 400: Sintaxis inválida (Bad request).

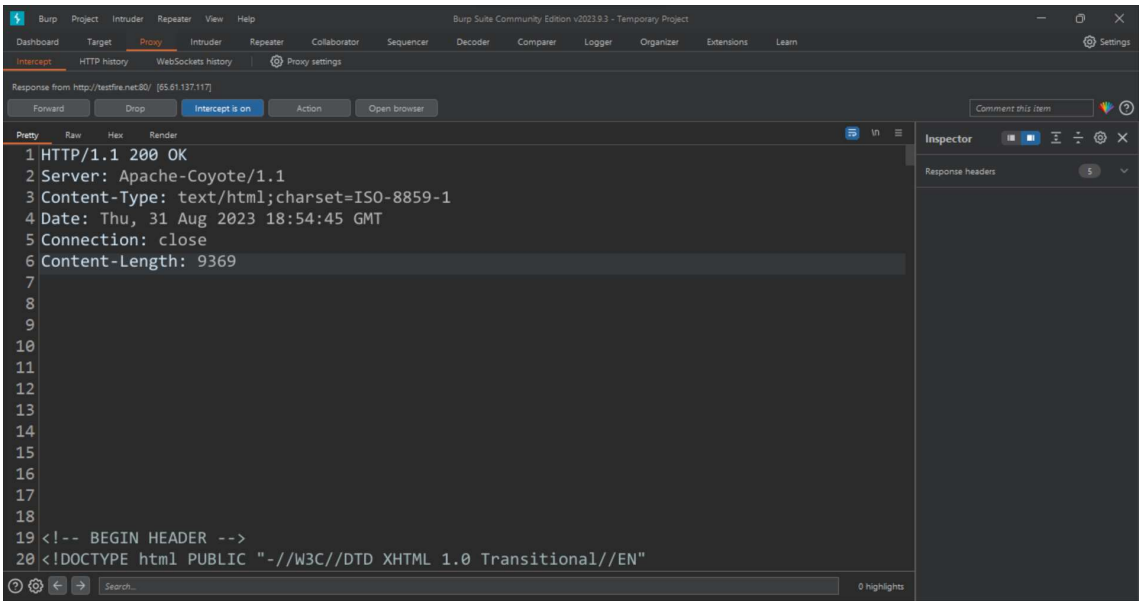
Código de estado 401: Esta solicitud de código de estado se produce cuando se requiere autenticación, pero se ha producido un error o no se ha proporcionado.

Código de estado 403: No se tienen los permisos adecuados.

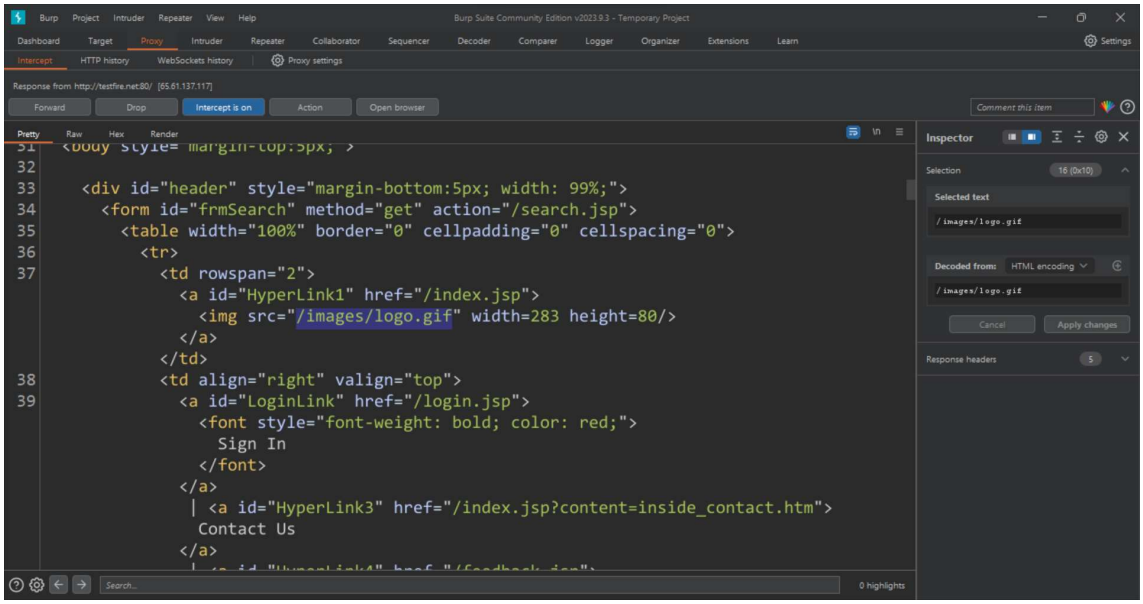
Código de estado 404: Se produce cuando la solicitud es válida, pero el recurso no se encuentra en el servidor. Aunque estos se agrupan en el “bucket” de errores de cliente, a menudo se deben a una redirección de URL incorrecta.
Código de estado 405: Las peticiones no están bien hechas (Cambiar de GET a POST o viceversa)

Código de estado 409: Se envía un código de estado 409 cuando una solicitud entra en conflicto con el estado actual del recurso. Esto suele ser un problema con actualizaciones simultáneas, o versiones, que entran en conflicto entre sí.

Código de estado 410: El recurso solicitado ya no está disponible y no volverá a estar disponible.
Código de estado 500: Error interno del servidor.
Código de estado 501: El servidor va a morir XD
Código de estado 503: Hubo un error interno que provocó un fallo.



Server: Gracias a su información, podemos buscar vulnerabilidades y exploits de acuerdo a su versión.
Set-Cookie: Es nuestra sesión asignada por el servidor como clientes.
Content-Type: El tipo de código que te regresa el servidor. Regresa código html de tipo texto
Date: La fecha de la response
Content-Length: Largo de los caracteres



Crawling: Usar los enlaces mostrados en ese código para acceder a ellos de la siguiente manera:
http://testfire.com/images/ logo.gif + login