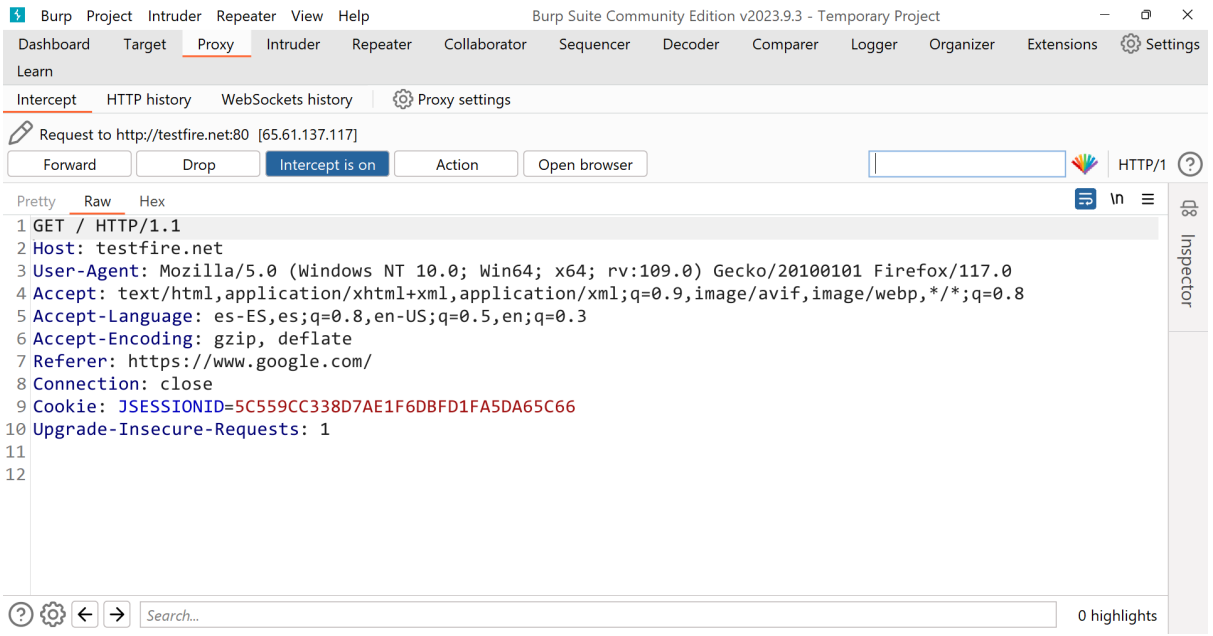
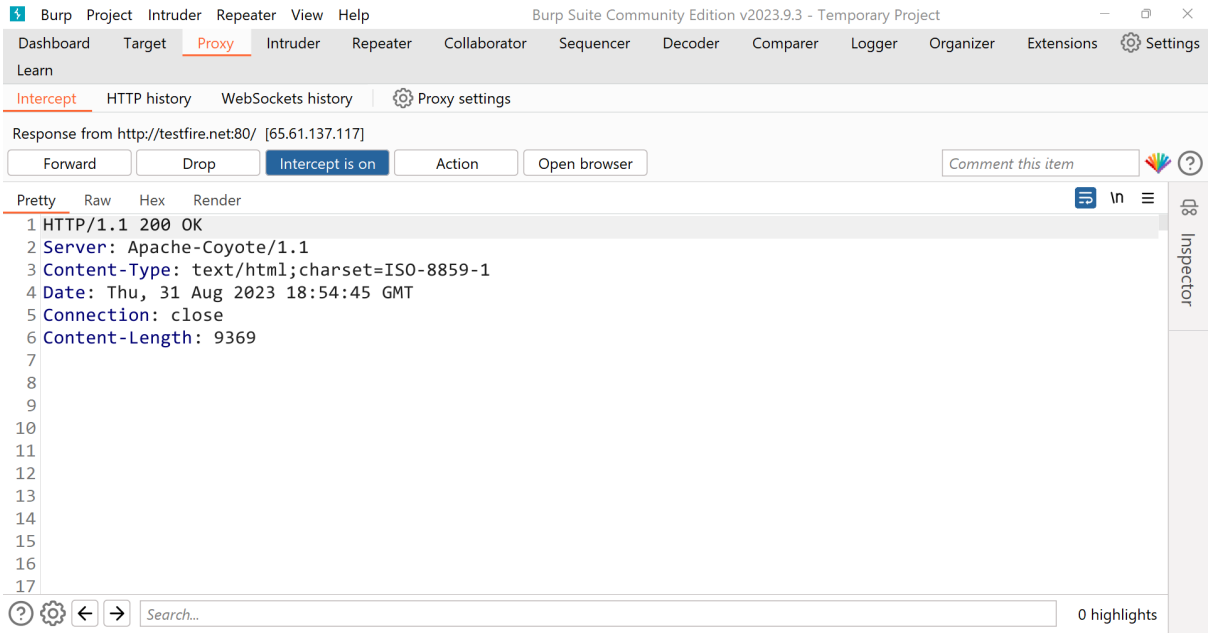
Analizando el request



GET -> Método utilizado
/ -> Recurso solicitado
HTTP/1.1 -> Versión de HTTP utilizado
Host -> Nombre del dominio que será buscado en la dirección IP
User-Agent -> Software que realiza la consulta, tipo y la versión
Accept -> Tipo de archivos que acepta el cliente
Accept-Language -> Lenguajes aceptados por el cliente
Accept-Encoding -> Que algoritmos de codificación acepta el cliente
Referer -> Es la aplicación web anterior
Connection -> Indica cómo debe comportarse la conexión entre el cliente y el servidor después de que se complete el request y el responde.
Cookie -> Se manejan las sesiones.
Content-Type -> Tipo de contenido que el cliente está enviando al servidor

- Si cambiamos el host podemos encontrar otros virtual host.
- Virtual host es cuando se cuentan con varias aplicaciones web en un servidor.
- Hay vulnerabilidades de CSRF. Esto nos permite evadir mecanismos de autenticación, Pondríamos testfire.net/admin y así el servidor podría pensar que eres un admin.

Response



Códigos de estado de respuesta HTTP

200 -> Es utilizado cuando la request tuvo éxito
301 -> El recurso que fue solicitado se movió de forma permanente y el servidor redireccionó a la nueva dirección
304 -> Regresa cabeceras de caché. Carga lo que se encuentra en el caché.
400 -> La sintaxis de la petición es incorrecta
401 -> La petición requiere una previa autorización para acceder al recurso
403 -> El servidor denegó el acceso al recurso solicitado
404 -> El recurso solicitado al servidor no existe o no está disponible.
405 -> El método utilizado por el navegador no es compatible con el servidor
500 -> Indica un error inesperado en el servidor
503 -> El servidor se encuentra saturado
504 -> Se agotó el tiempo de respuesta del servidor

Analizando la response

HTTP/1.1 -> Versión de HTTP utilizada
200 -> Codigo de estado
Server-> Tipo y versión del servicio usado en el servidor
Set-Cookie -> Se te asigna una cookie para autenticarte en el sistema.
Content-Type -> Tipo de contenido que está regresando el servidor
Date -> Fecha de la response/request
Content-Length -> Número de caracteres

- Posteriormente se encuentra código HTML.
- La cabecera Server puede dar información al atacante para explotar una vulnerabilidad.