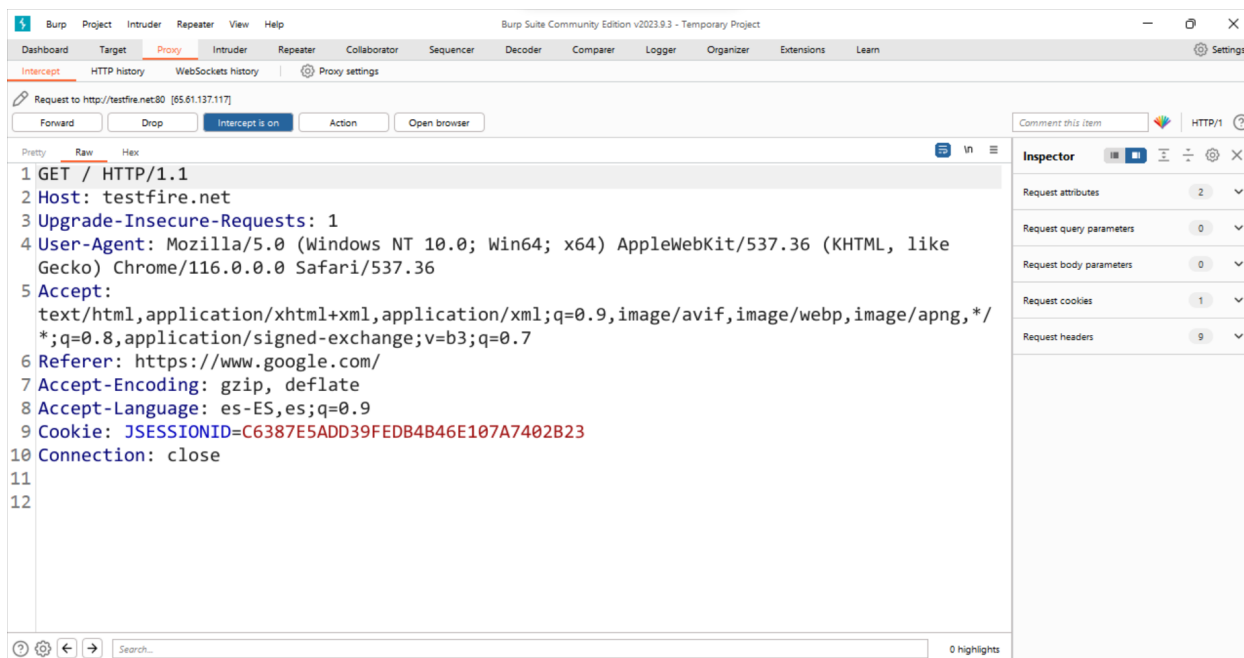


# Burp - Cabeceras

Por medio de Burp, al momento de realizar una interceptación en Altoro Mutual, nos arroja lo siguiente:



En la línea 1, obtenemos información del método HTTP que realiza la solicitud, el recurso al cual va dirigido y la versión que se utiliza.

En la línea 2, tenemos la información del Host, que en este caso es testfire.net, el cual es el servidor huésped de la dirección a la que queremos ingresar.

Si fuéramos a modificar la información del HOST, podríamos acceder a un servicio en particular.

En la línea 4, existe toda la información referente a la descripción del software utilizado para ingresar al sitio, su versión y demás características.

Si modificáramos la información de aquí, el sitio nos mostraría una versión diferente.

En la línea 5, podemos ver todas aquellas entradas que puede aceptar el servidor del cliente

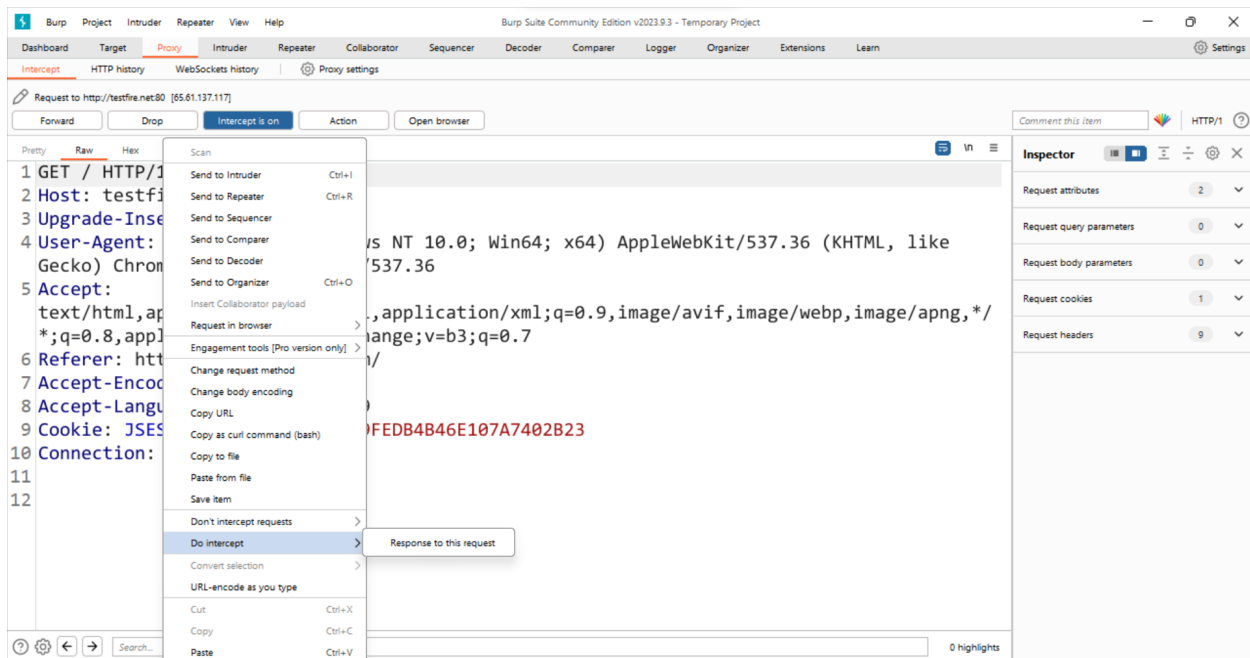
En la línea 6, tenemos lo que es el Referer, que nos muestra el lugar anterior desde el cual accedamos a la url de destino.

La línea 7 y 8 no son tan importantes por el momento. No obstante, nos indican el tipo de encriptación que se utiliza y los lenguajes aceptados.

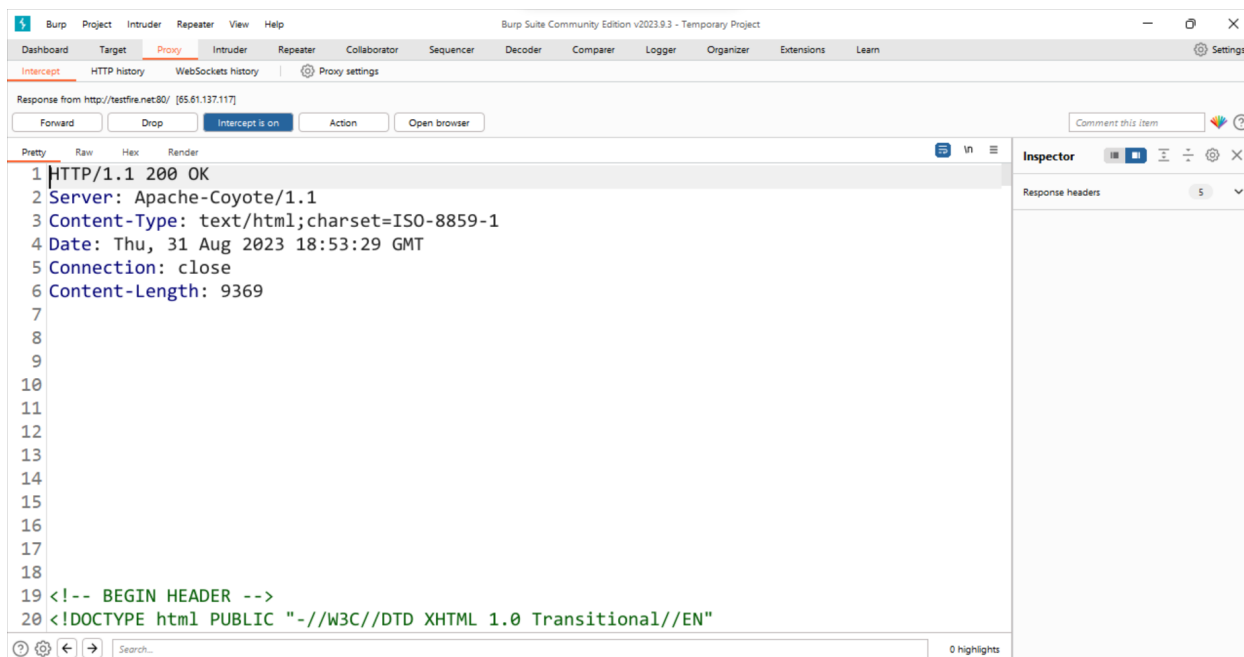
En la línea 9 podemos observar la Cookie, la cual nos identifica dentro del servidor.

Por ultimo, tenemos Connection, la cual menciona el estado de la conexión actual.

Una vez que sabemos que hace la mayoría de líneas, haremos clic derecho en la sección de “Raw” y daremos clic en “Do intercept → Response to this request”



Le seguiremos dando clic en forward hasta que nos aparezca el “200 OK” en la línea 1



Los códigos HTTP más utilizados son:

Los 200

- **200 – OK.** Se utiliza cuando la petición fue completada de manera exitosa. Como este código indica que “todo está bien” no suele mostrarse al usuario final.
- **201 – Created.** La petición del navegador se completó correctamente y se creó un nuevo recurso.
- **203 – Non-Authoritative Information.** La petición del navegador se completó correctamente, pero el contenido corresponde a un servidor diferente al que se ha realizado la petición.
- **204 – No Content.** La petición del navegador se completó correctamente, pero la respuesta no muestra ningún tipo de contenido.
- **205 – Reset Content.** Se utiliza cuando la petición del usuario se completa, pero es necesario volver a cargar la página. Es muy habitual cuando se envían datos a través de un formulario de contacto y se recarga la página.
- **206 – Partial Content.** Se utiliza cuando la petición se completa, pero solo se devuelve parte del contenido solicitado.
- **207 – Multi-Status.** Se devuelve un archivo XML que contiene varias respuestas diferentes, en función de las peticiones realizadas.

## Los 300

- **300 – Multiple Choices.** Ante una solicitud, existe más de una opción para acceder al mismo recurso.
- **301 – Moved Permanently.** El recurso solicitado se movió de forma permanente y el navegador es redirigido automáticamente a la nueva ubicación. Las redirecciones 301 son una buena opción para que Google no nos penalice si tenemos demasiados errores 404 en nuestra web.
- **302 – Moved Temporarily.** El recurso solicitado se movió de forma temporal y el navegador es redirigido automáticamente a esa nueva ubicación.
- **303 – See Other.** Este código indica que el recurso solicitado se movió, pero no hay ninguna redirección hecha.
- **304 – Not Modified.** Este código de estado se da cuando el navegador pregunta al servidor si el recurso ha sido movido desde la última vez que lo consultó, y este no ha sido cambiado.
- **305 – Use Proxy.** Este código HTTP se utiliza cuando el recurso solicitado debe obtenerse a través de un proxy Location situado en la cabecera.
- **306 – Switch Proxy.** En la actualidad este código de estado HTTP ya no se utiliza, pero se reserva para futuros casos.
- **307 – Temporary Redirect.** El recurso que solicita el navegador se puede obtener en otro lugar, pero únicamente para esta petición. Para próximas peticiones se puede utilizar la ubicación original.
- **308 – Permanent Redirect.** El recurso que solicita el navegador se encuentra en otra ubicación y el cambio es permanente. A diferencia del código HTTP 301, no se cambia el método HTTP para la nueva petición.

## Los 400

- **400 – Bad Request.** El servidor no entiende la petición del navegador porque la sintaxis no es correcta.
- **401 – Unauthorized.** La petición que realiza el navegador precisa autenticación.
- **402 – Payment Required.** Es un código HTTP reservado para futuros usos.

- **403 – Forbidden.** La petición que realiza el navegador es correcta, pero se ha denegado el acceso al recurso solicitado.
- **404 -Not Found.** El recurso que solicita el navegador no se encuentra o no está disponible en el servidor. No es posible detectar si esta ausencia es temporal o permanente.
- **405 – Method Not Allowed.** El navegador utiliza un método para obtener el recurso que no es aceptado por el servidor.
- **406 – Not Acceptable.** El recurso solicitado tiene un formato que no es aceptado por el navegador.
- **407 – Proxy Authentication Required.** Un código de estado similar al 401, pero en este caso el navegador debe autenticarse primero mediante un proxy.
- **408 – Request Timeout.** Este código HTTP se muestra cuando el navegador ha tardado tanto tiempo en realizar su petición que el servidor ya no la espera.
- **409 – Conflict.** No se pudo completar la petición porque se produjo un conflicto con el recurso solicitado.
- **410 – Gone.** No es posible encontrar el recurso solicitado y la ausencia se considera permanente. Si hay alguna posibilidad de que esta ausencia sea temporal, se debe utilizar el código HTTP 404.
- **411 – Length Required.** El servidor devuelve este código HTTP cuando la petición no incluye la cabecera Content-Length adecuada.
- **414 – Request-URI Too Long.** La URL que se corresponde con la petición realiza es demasiado larga para ser procesada. Esto ocurre cuando una dirección tiene muchos parámetros.
- **423 – Locked.** Se muestra este código HTTP cuando el recurso solicitado está bloqueado.
- **429 – Too Many Request.** El navegador realiza demasiadas peticiones en un período de tiempo determinado.

Los 500

- **500 – Internal Server Error.** No se puede completar la petición, ya que se ha producido un error inesperado en el navegador.

- **501 – Not implemented.** El servidor no soporta alguna funcionalidad necesaria para responder a la solicitud que realiza el navegador.
- **502 – Bad Gateway.** El servidor no puede responder con la petición del navegador, ya que este servidor está actuando como proxy o gateway, o tiene instalado un proxy inverso y ha recibido una respuesta no válida desde dicho servidor.
- **503 – Service Unavailable.** El servidor no puede responder a la petición del navegador porque está saturado o se están realizando tareas de mantenimiento en el mismo.
- **504 – Gateway Timeout.** El servidor no puede responder con la petición del navegador, ya que este servidor está actuando como proxy o gateway, o tiene instalado un proxy inverso y se ha agotado el tiempo de respuesta de dicho servidor.
- **505 – HTTP Version Not Supported.** El servidor no es compatible con la versión del protocolo HTTP utilizada en la petición del navegador.
- **509 – Bandwidth Limit Exceeded.** Es un código HTTP muy utilizado en cPanel y se muestra cuando se ha alcanzado el límite de ancho de banda y no se puede procesar la petición.
- **510 – Not Extended.** Este código se muestra cuando es necesario añadir más extensiones al servidor para que pueda procesar la petición.
- **511 – Network Authentication Required.** El navegador debe autenticarse para poder cumplir las peticiones.

Una vez visto lo anterior, podemos ver que la petición que enviamos fue correcta.

El set-Cookie nos menciona acerca de la galleta que va a ser ingresada y que representa nuestra sesión.

El Content-Type nos menciona el tipo de contenido que te regresa de respuesta el servidor.

Date nos da detalles de la respuesta / response de la solicitud.

Y el Content-Lenght nos menciona la cantidad de caracteres que hay.