

Actividad 2. Descripción de cabeceras de Burp Suite.

Get: nos muestra el recurso y la versión del HTTP.

Host: nos dice el dominio web.

User-Agent: nos dice el tipo de servidor, sistema operativo, la versión, etc.

Accept: nos dice lo que puede aceptar el cliente (texto, imagen, etc.)

Accept-Language: tipo de idioma.

Accept-Encoding: tipo de formato de archivo.

Referer: nos da la información de la página web anterior.

Server: si nos dice la versión, si esta desactualizada, la podemos vulnerar.

Set cookie: indica nuestra sesión, le dice al usuario que podemos autenticarnos en el sistema, nos asigna la autenticación.

Cookie: sesiones guardadas.

Content-type: nos regresa código html de tipo texto, u otros códigos.

Content- Length: longitud del carácter de la petición.

Date: Fecha de la request.

Forward: sirve para cargar los cambios que se hacen y demás peticiones existentes, cargando lo anterior.

Drop: es cuando tira el paquete, lo elimina.

Intruder: herramienta para hacer ataques de fuerza bruta

Proxy: para capturar la request y response.

Repeater: abre dos pantallas y copia la petición del proxy y la podemos manipular sin utilizar el navegador web.

Target: mapeo de la aplicación web de lo que se ha hecho, de las peticiones que se hacen, de forma automatizada.

Código de estados más comunes.

Códigos de estado HTTP 1xx: son informativos y la página se muestra sin problema, el código no aparece como tal.

Algunos de ellos son:

- **100.- Continue.** Este código de estado notifica que el servidor ha recibido la primera petición y está esperando recibir más instrucciones del navegador.
- **101.- Switching Protocols.** Se utiliza cuando el servidor acepta un cambio propuesto por el navegador. Por ejemplo, un cambio de HTTP 1.0 a HTTP 1.1.
- **102.- Processing.** El servidor ha recibido la petición, pero no la ha completado. Esto evita que el navegador interprete que la petición se ha perdido, si no que todavía no ha finalizado.
- **103.- Checkpoint.** Se utiliza para reanudar una petición que previamente fue perdida o cancelada.

Códigos de estado HTTP 2xx: son respuestas satisfactorias y dicen que la petición se realizó.

- **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.
- **204 – No Content.** La petición del navegador se completó correctamente, pero la respuesta no muestra ningún tipo de contenido.

Códigos de estado HTTP 3xx: Nos dice que realiza una redirección.

- **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.
- **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.

Códigos de estado HTTP 4xx: Son errores producidos por el navegador web.

- **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.
- **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.

Códigos de estado HTTP 5xx: son errores producidos por el servidor web.

- **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.