Informe de análisis de las principales llamadas de red

Alberto van Oldenbarneveld

September 20, 2024

Informe de análisis de las principales llamadas de red

Página web analizada: Reddit.com

Llamada 1: Solicitud GET

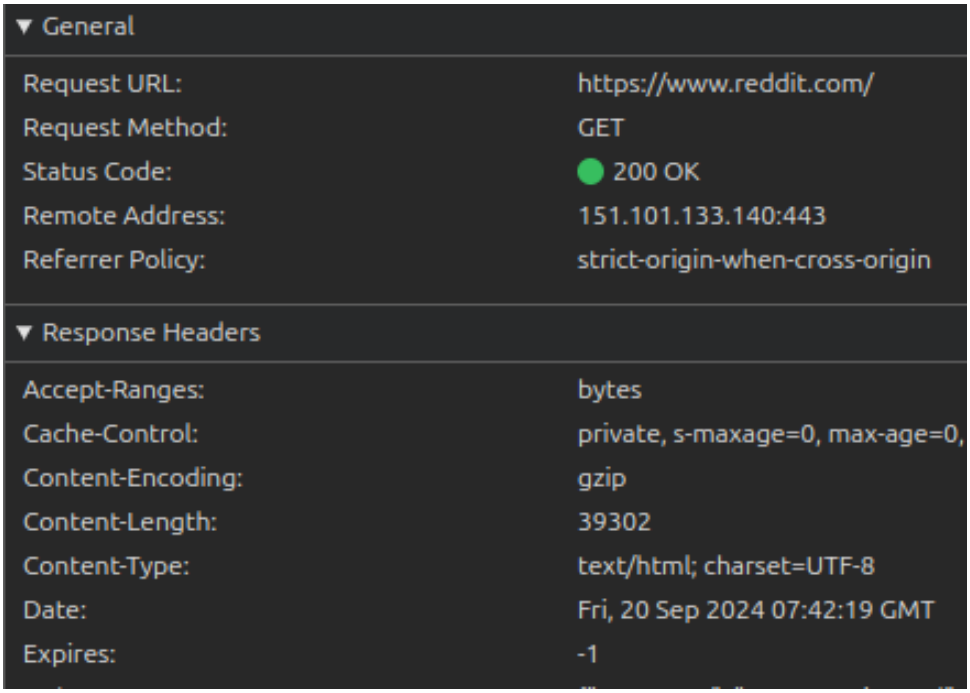

Figure 1: Captura de la solicitud GET

Método: GET
Status: 200 OK
URL: `https://www.reddit.com/`

Esta solicitud GET obtiene el documento HTML principal de la página principal de Reddit. Incluye la estructura HTML inicial que los navegadores renderizan para mostar el contenido con enlaces a recursos adicionales (como imágenes, scripts, y hojas de estilo) que el navegador cargará posteriormente para completar la visualización de la página.

Las principales cabeceras son:

- Host: www.reddit.com
- User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ exchange;v=b3;q=0.7
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: en-US,en;q=0.9
- Cookie: (varias cookies, incluyendo session_tracker, reddit_session, edgebucket)
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: none
- Sec-Fetch-User: ?1

Especifican el nombre del servidor al que se hace la solicitud, el navegador y el sistema operativo, así como los tipos de contenido que acepta el cliente, así como los algoritmos de compresión. También define los idiomas preferidos del cliente, los cookies almacenados y el tipo de documento solicitado, y que ha sido iniciado por interacción del usuario.

Las principales cabeceras de respuesta son:

- Cache-Control: private, s-maxage=0, max-age=0, must-revalidate, no-store
- Content-Encoding: gzip
- Content-Length: 39302
- Content-Type: text/html; charset=UTF-8
- Date: Fri, 20 Sep 2024 07:42:19 GMT
- Expires: -1
- NEL (Network Error Logging): "report_to": "w3-reporting-nel", "max_age": 14400, "include_subdomains": false, "success_fraction": 1.0, "failure_fraction": 1.0
- Set-Cookie: session_tracker=kjpbpeilornbcolphd...; Max-Age=7199; Path=/; expires=Fri, 20-Sep-2024 09:42:19 GMT; secure; SameSite=None
- Strict-Transport-Security: max-age=31536000; includeSubdomains
- Vary: accept-encoding

Las cabeceras de respuesta contienen información sobre la prohibición de guardar el contenido en caché, que el contenido ha sido comprimido con gzip, el tamaño del mismo, y que es HTML con codificación UTF-8, así como la fecha, dónde se deben loguear los errores de red, un cookie de seguimiento y la conexión a través de HTTPS.

El cuerpo de la respuesta contiene un documento HTML con la estructura básica de la página, con enlaces a otros recursos, como son las hojas de estilo CSS, scripts de JavaScript, y el favicon.

Llamada 2: Solicitud GET

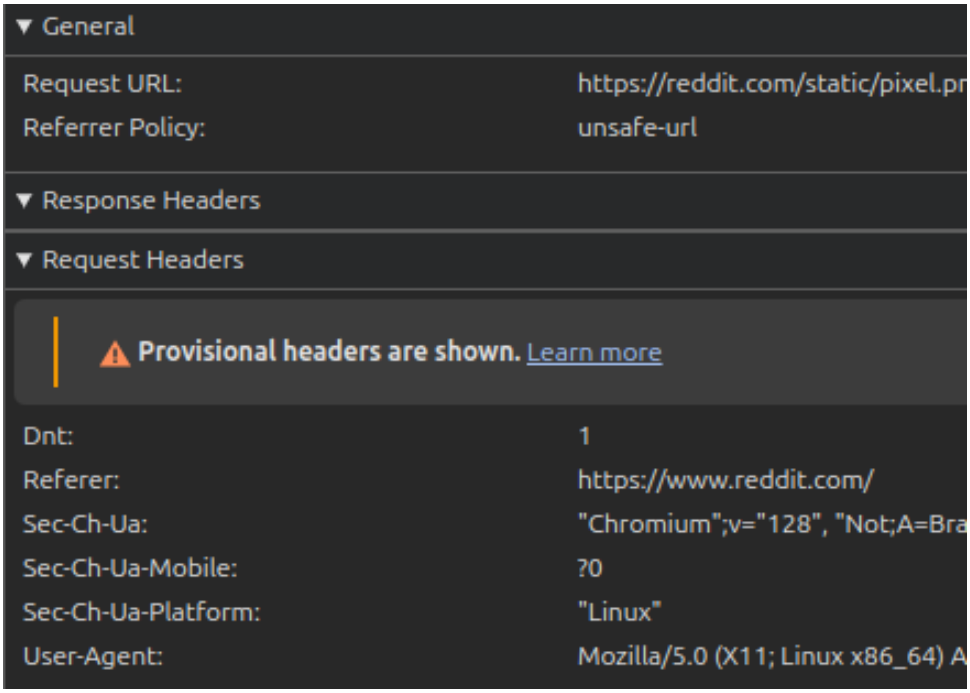

Figure 2: Captura de la solicitud GET fallida

Método: GET
Status: Failed
URL: `https://reddit.com/static/pixel.png`

Esta solicitud GET ha intentado obtener una imagen llamada pixel.png, lo que solicita en el documento HTML cargado en la primera llamada. Se realiza a través de la siguiente línea de código:

```
<img id="hsts_pixel" src="//reddit.com/static/pixel.png">
```

Esta imagen se utiliza para hacer seguimiento y analíticas de los sitios visitados. Al tener instalada la extensión Ublock Origin, se ha bloqueado la carga de esta imagen. Si nos metemos en la consola podremos ver la siguiente información:

```
GET https://reddit.com/static/pixel.png net::ERR_BLOCKED_BY_CLIENT
```

Quiere decir que la llamada fue bloqueada por el navegador antes de que la solicitud se envíe al servidor.

Llamadas 3-16: Solicitud GET para CSS

Método: GET
Status: 200 OK

Las siguientes llamadas son todas para cargar documentos CSS, hojas de estilo que definen la apariencia y diseño de la web:

- reddit.YXox_dqXzrc.css

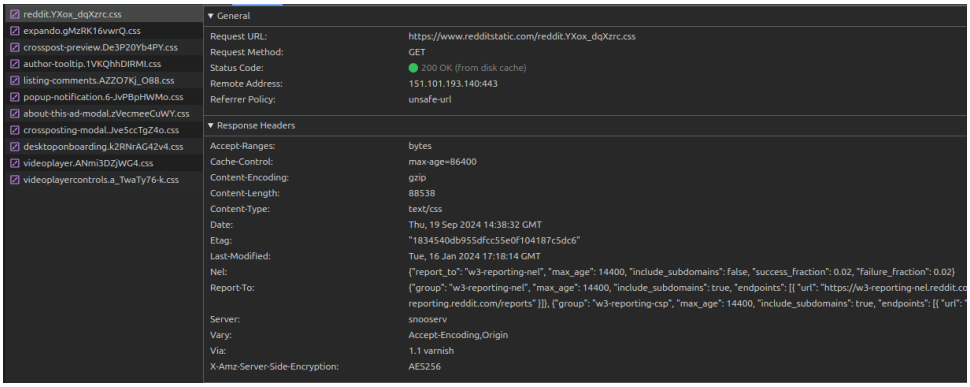

Figure 3: Carga de hojas de estilo CSS

- expando.gMzRK16vwrQ.css
- crosspost-preview.De3P20Yb4PY.css
- author-tooltip.1VKQhhDIRMI.css
- listing-comments.AZZO7Kj_O88.css
- popup-notification.6-JvPBpHWMo.css
- about-this-ad-modal.zVecmeeCuWY.css
- crossposting-modal.Jve5ccTgZ4o.css
- desktoponboarding.k2RNrAG42v4.css
- videoplayer.ANmi3DZjWG4.css
- videoplayercontrols.a_TwaTy76-k.css

Estas hojas de estilo definen el diseño y la estructura visual de la página. Contienen información sobre diseños que se aplican a toda la página web, elementos que se pueden expandir y contraer, la apariencia de comentarios, pop ups, el reproductor de video incrustado, así como los botones del mismo.

Llamadas 17 a 20: Solicitud GET para JavaScript

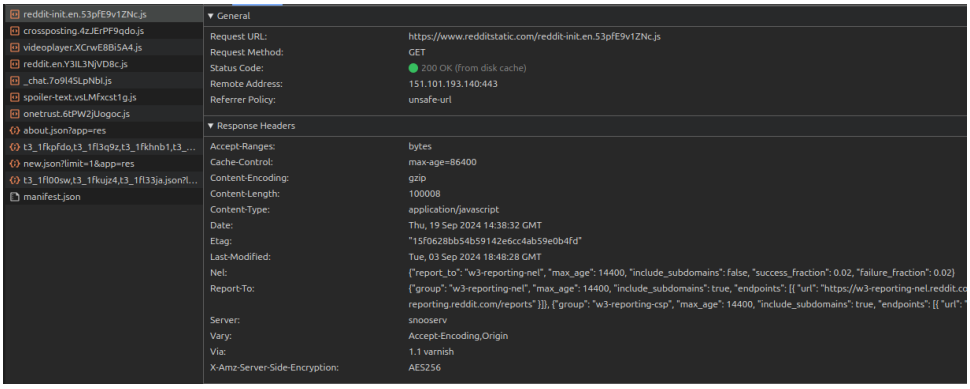

Figure 4: Carga de scripts JavaScript

Método: GET
Status: 200 OK
URL: `https://www.redditstatic.com/`

Estas llamadas se hacen a scripts de JavaScript que inician la configuración inicial de JavaScript, la funcionalidad de crossposting, y el reproductor de vídeo.

En las cabeceras de solicitud se envía la información del navegador antes mencionada. Entre las cabeceras de respuesta se envía información sobre el rango de aceptación del tamaño del contenido, la compresión, el tipo de contenido, la fecha y hora de la respuesta, identificadores para el control del caché y el Network Error Logging.

En los cuerpos de respuesta de las llamadas se encuentran los módulos de JavaScript que contienen jQuery, una popular biblioteca que facilita la manipulación del DOM y otras funciones de JavaScript. El segundo fragmento está relacionado con la funcionalidad de crossposting, que permite a los usuarios republicar contenido en diferentes subreddits. El tercero es un cargador de módulos, que maneja dependencias de otros archivos o módulos dentro del entorno de JavaScript, lo que es común en sistemas de JavaScript modulares como Node.js o Webpack.

Llamada POST: Autenticación

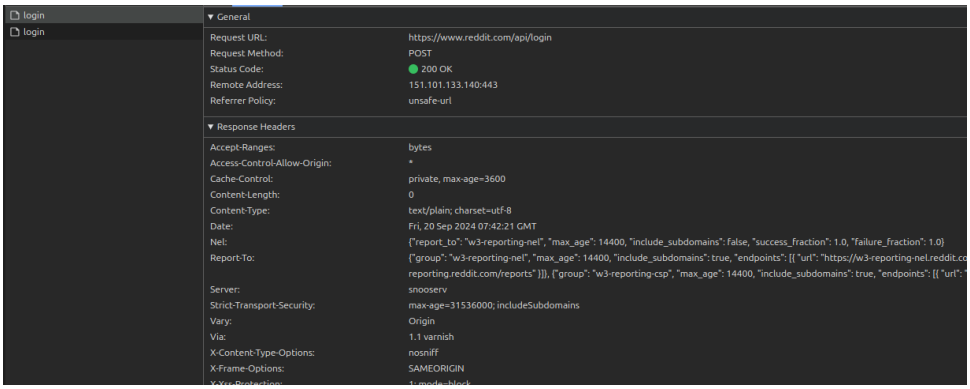

Figure 5: Solicitud POST de autenticación

Método: POST
Status: 200 OK
URL: `https://www.reddit.com/api/login`

Esta llamada POST solicita el endpoint `/api/login`, utilizado para autenticar al usuario.

Cabeceras de seguridad:

- Content-Type: application/x-www-form-urlencoded; charset=UTF-8
- x-modhash: ... (token de seguridad contra ataques CSRF)
- x-signature-v2: ... (firma criptográfica para asegurar la autenticidad de la solicitud)

Las cabeceras de respuesta contienen información sobre seguridad, caché, control de acceso y políticas de errores de red, asegurando la integridad de la conexión y gestionando cómo se entrega y almacena el contenido.

Conclusión

El análisis de las llamadas de red en Reddit.com revela una combinación de solicitudes GET y POST. Las solicitudes GET cargan el HTML principal, imágenes, hojas de estilo CSS y scripts de JavaScript necesarios para la correcta visualización y funcionamiento interactivo del sitio. Algunos recursos, como el *tracking pixel*, pueden ser bloqueados por extensiones de bloqueo de contenido como uBlock Origin.

Las solicitudes POST, como la de autenticación en `/api/login`, manejan el envío de datos al servidor, con medidas de seguridad como tokens de protección CSRF y firmas criptográficas para garantizar la autenticidad de las solicitudes. Las cabeceras de respuesta incluyen información sobre la gestión de caché, políticas de seguridad (como HSTS y XSS), y registro de errores de red (NEL).

En general, las llamadas GET y POST, junto con los recursos CSS y JavaScript, trabajan en conjunto para proporcionar una experiencia de usuario segura y eficiente, facilitando la navegación, la interactividad y la autenticación en la plataforma.