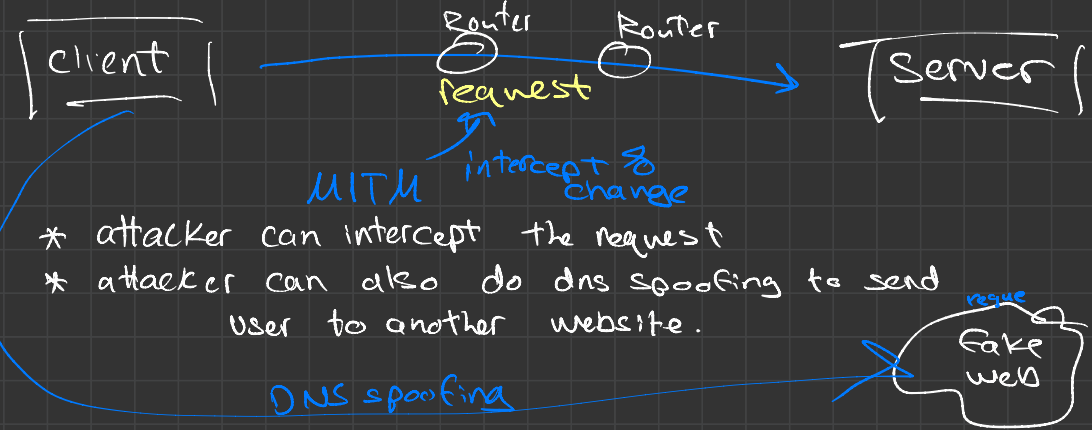
Missing Http strict transport Security (HSTS) Header



* attacker can intercept the request
* attacker can also do dns spoofing to send user to another website.

* How does HSTS help us?
  HSTS policy enforce all the request to pass through only Https instead of plain text.

① you have to add HSTS response header
  ↳ Strict-Transport-security - max-age = expireTim (in seconds);
  include subdomain
② when browser access the website, the server reply with HSTS header.
③ after recieving HSTS header browser sends an Https request

* if application do not have HSTS header, then anyone can make an MITM attack on network side

* How to find ?
  ① curl -s -D- any.com | grep -i Strict
run the command if you did not get anything, it means it is vulnerable
↳ secure response should contain HSTS response header.

② ssllabs.com/ssltest
put target host and search for HSTS header.

③ hsecscan tool from github.

this tool will give you Missing Response headers

Secure example