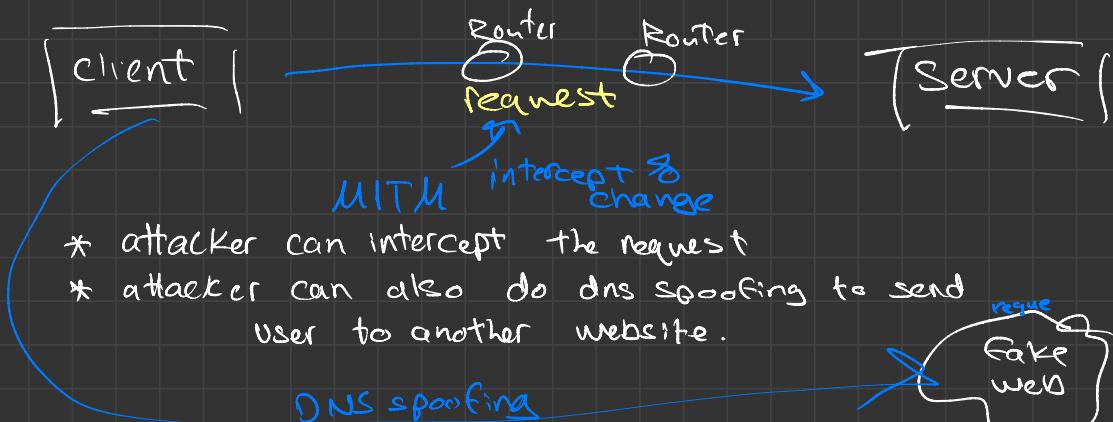


Missing HTTP Strict Transport Security (HSTS) Header



* attacker can intercept the request

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

* How does HSTS help us?

HSTS policy enforces 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 = expiresIn (in seconds); includeSubdomain`

② When browser access the website, the server reply with HSTS header.

③ after receiving 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 / SSL Test](https://www.ssllabs.com/ssltest)

Put target host and search for HSTS header.

⑧ hseccscan tool from github.
this tool will give you Missing Response Headers

SecWe example

```
CWE: CWE-693: Protection Mechanism Failure
CWE URL: https://cwe.mitre.org/data/definitions/693.html
HTTPS: N

Header Field Name: Content-Security-Policy-Report-Only
Reference: http://www.w3.org/TR/CSP/
Security Description: Like Content-Security-Policy, but only reports. Useful d
using implementation, tuning and testing efforts.
Security Reference: https://www.owasp.org/index.php>List_of_useful_HTTP_header
s
Recommendations: Read the reference http://www.w3.org/TR/CSP/ and set accordin
g to your case. This is not an easy job.
CWE: CWE-708: Header Neutralization of Input During Web Page Generation ('Cro
ss-site Scripting')
CWE URL: https://cwe.mitre.org/data/definitions/799.html
HTTPS: N

bash-3.2# curl -s -D https://www.dell.com/en-in/ | grep -i Strict
bash-3.2# curl -s -D https://www.dell.com/en-in/ | grep -i Strict
bash-3.2# curl -s -D https://www.dell.com/ | grep -i Strict
bash-3.2# curl -s -D https://www.apple.com/ | grep -i Strict
bash-3.2# curl -s -D https://secure1.store.apple.com/ | grep -i Strict
Strict-Transport-Security: max-age=31536000; includeSubDomains
bash-3.2#
```

```
1 User credentials are sent in clear
text
2
3 if any application is having http
4 they are accepting password over http
protocol
5
6
7 how to hunt ths bug
8
9 1. find login page
10 2.if you can force that login page
to browse with http
11 then there is a vulnerability
12
13
14
```