# CYBERSECURITY LAB

Alessandro Renda

Dipartimento di Ingegneria e Architettura, Università degli Studi di Trieste

## AITM – LAB 1

Academic Year 2025/2026

**Exam**
Folder name for material submission **06_AITM_1**

# Tasks and delivery

# Preliminary "class" activity

*Let's see what comes out!*

- Someone creates a Google Form (or any equivalent) and share it with the entire class
- Everyone goes on some interesting (*) websites and checks whether it supports HSTS
  - Browser developer tools or `curl -I http://example.com`
- Insert URL and relevant information in the form

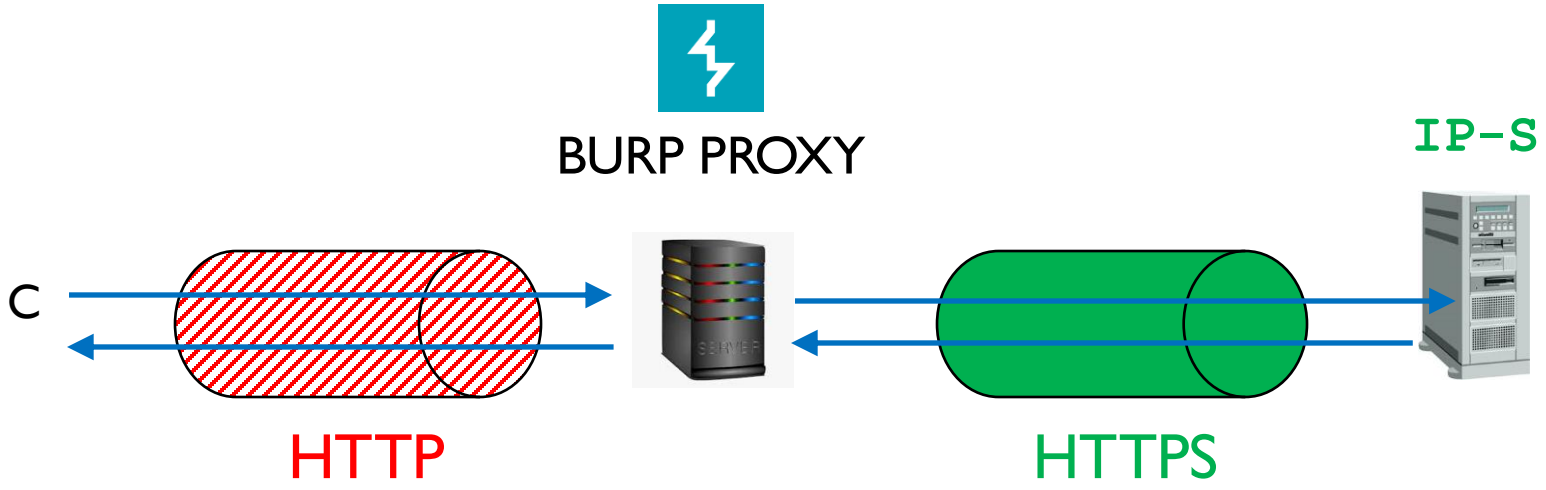
| | HTTP | | | HTTPS | | |
|---|---|---|---|---|---|---|
| | **Status code** | **Header** | **HSTS** | **Status code** | **Header** | **HSTS** |
| A.com | HTTP/1.1 302 Found | ... | X | HTTP/1.1 200 OK | ... | X |
| B.com | HTTP/1.1 302 Found | ... | X | HTTP/1.1 200 OK | ... | V |

- Include the link to the results in your submission folder
- *(*) banks, insurance, trading platforms, public administration, e-commerce, education, social … … …*

# Optional (not mandatory) activity

- You may want to analyze and discuss the results of the survey
  - Preprocessing:
    - Handling / removing duplicates
    - …
  - Analyzing:
    - Fraction of websites configured to listen only on HTTPS
    - Fraction of websites configured to listen only on HTTP
    - Fraction of websites configured to listen on HTTP, with redirection to HTTPS
    - Fraction of websites with HSTS active
    - …

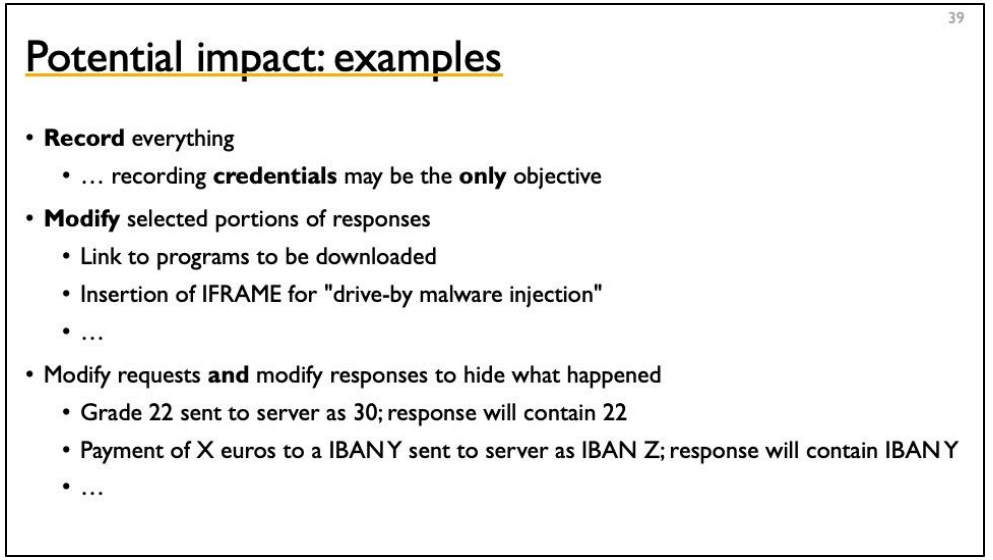
# Individual Lab activity




- Overall idea
  - **Configure BURP for SSLStrip**
  - Use Chromium embedded browser
  - Analyze **two cases**. Details follow

# SSLStrip on BURP Proxy – Case A

A. Choose a website, say `a.com`, that **does not use** Strict Transport Security
   - Configure BURP for SSLStrip
     - Force BURP to use TLS for requests
       - Settings → Proxy listeners → Edit the only interface → Request handling → …
     - Set the proper rules for carrying out the attack
   - Point your browser on `http://a.com`
   - Try to apply changes to requests/ responses →



# SSLStrip on BURP Proxy – Case B

B. Choose a website, say `b.com`, that **does use** Strict Transport Security
   - Check the HSTS status of `b.com`: `chrome://net-internals/#hsts`
   - Configure BURP for SSLStrip (as before)
   - Point your browser on `http://b.com`
   - Discuss the outcome of the attack depending on the HSTS status
   - Also:
     - If present, *delete from* the HSTS set to check the behavior in "before 1st visit" window
     - If absent, *add to* the HSTS set to check the behavior outside vulnerability windows

# Exam: report required

- You are expected to produce a report for this lab

- The report should describe and discuss the following aspects:
  - The needed configuration steps for carrying out the attack
  - The outcome of the attacks
    - In both cases (A and B), take screenshots of the website while browsing, showing access on HTTP
  - The differences with respect to the "normal" usage of BURP Proxy
  - Any other relevant observation you see fit