

I5020 Computer Security

Coding 1: HTTPS secure server

This assessment evaluates the following competencies:

- *CS001 – Understand the CIA triad and use it to explain the key objectives of computer security*
- *CS003 – Identify weaknesses in a computer system or infrastructure and propose solutions*
- *CS201 – Discuss about general design principles for protection mechanisms*
- *CS202 – Understand software protections that can be installed on a computer system*
- *CS303 – Apply code design principles in developed software*
- *CS402 – Capture network traffic with Wireshark to perform basic analyses*
- *CS006 – Identify residual risks that come from a countermeasure*
- *CS304 – Program, configure and launch a secured HTTPS server*

For this assessment, you have to write a small web server that distributes one page with a form that can be filled by the user and whose data are sent back to the server. This server must be first served over HTTP and then modified to be served over HTTPS.

Pay attention to the following elements:

- The design and content of the website served is not important.
- Use a password input field in the form.

Prepare yourself for the following manipulations/questions:

- Show how data filled in the form can be eavesdropped with the HTTP server and are hidden with the HTTPS server, using the Wireshark tool.
- Explain the role of an HTTPS server regarding the CIA triad.
- Think about the residual risks of putting an HTTPS server in place, instead of a simpler HTTP server.