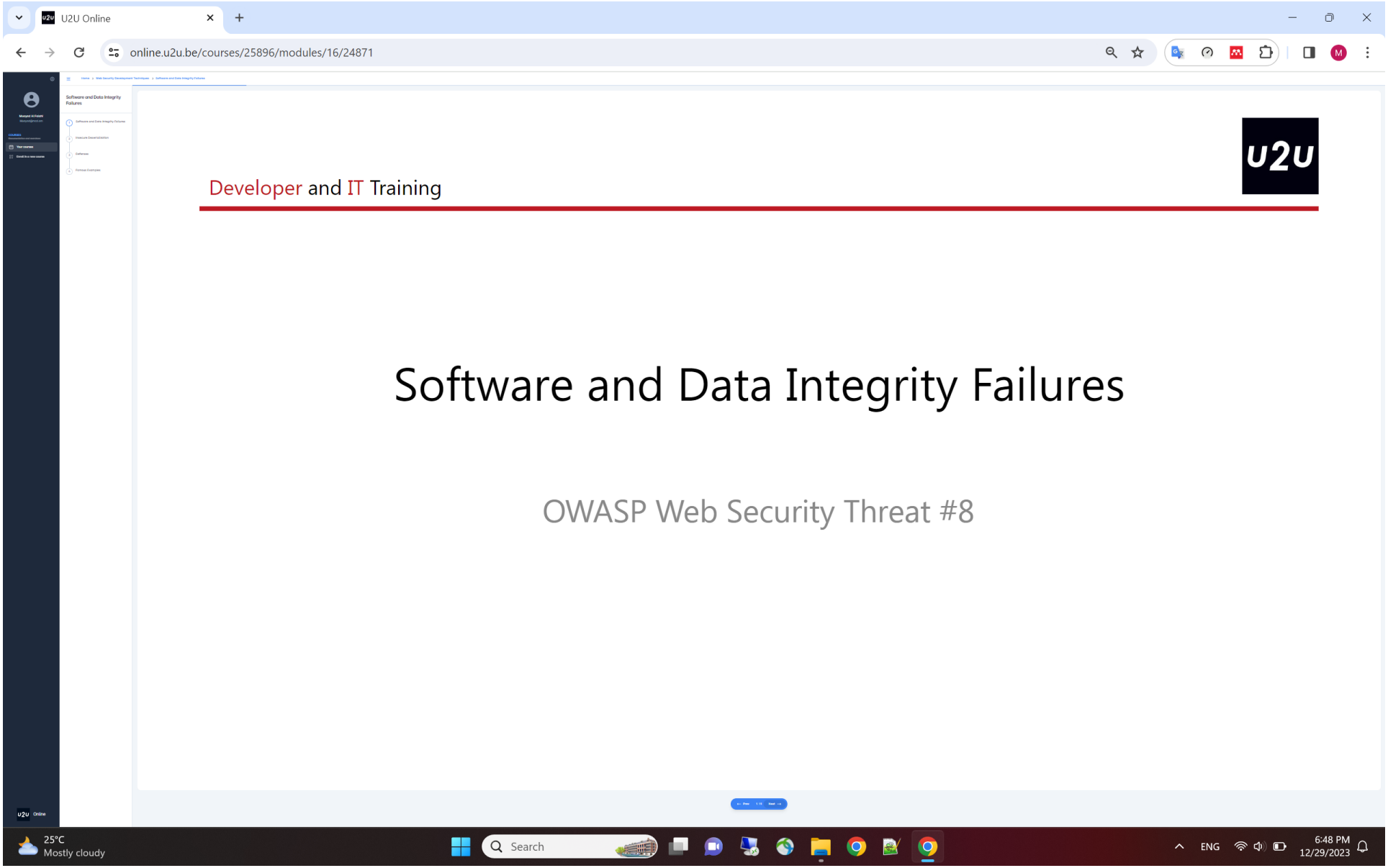
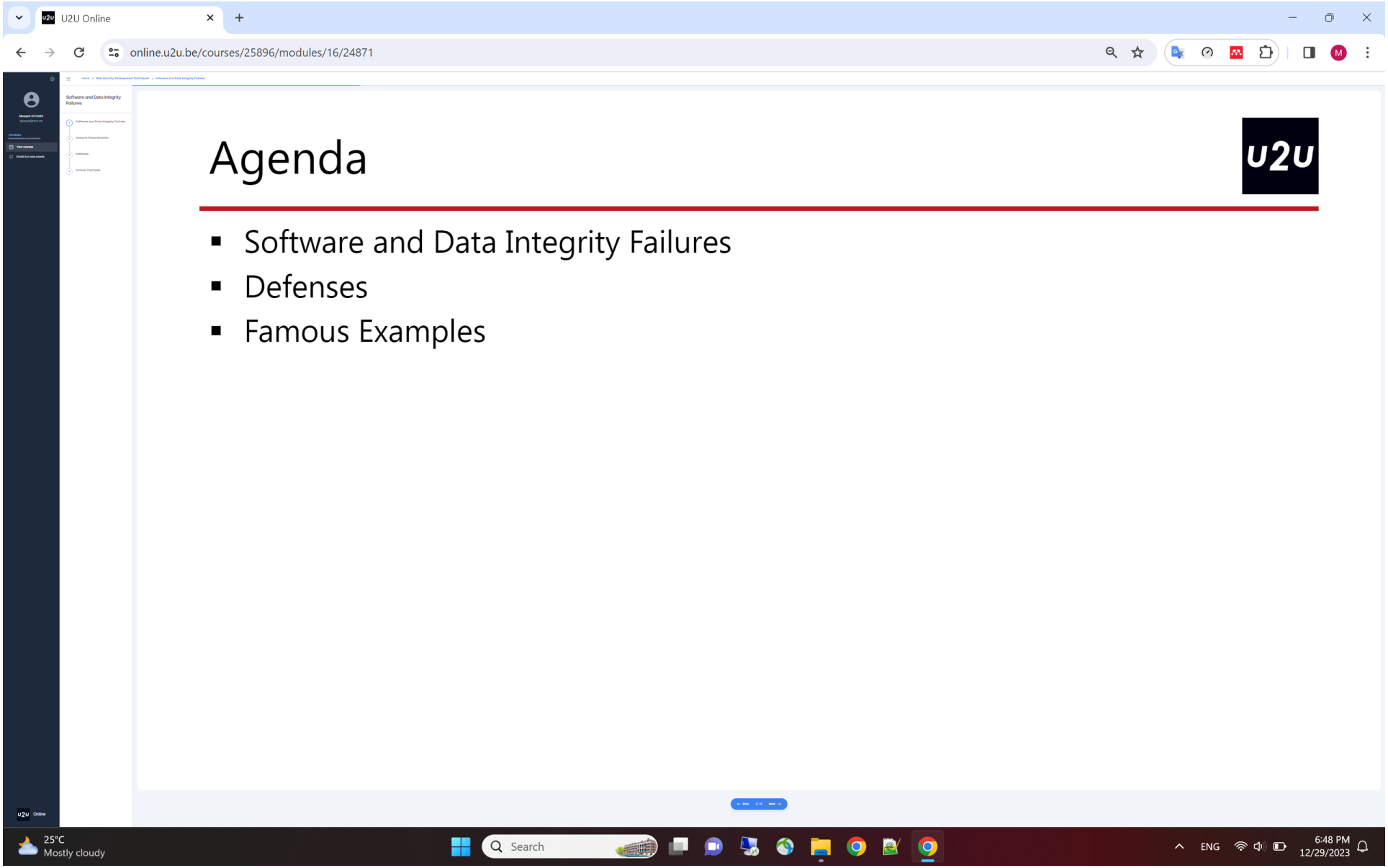
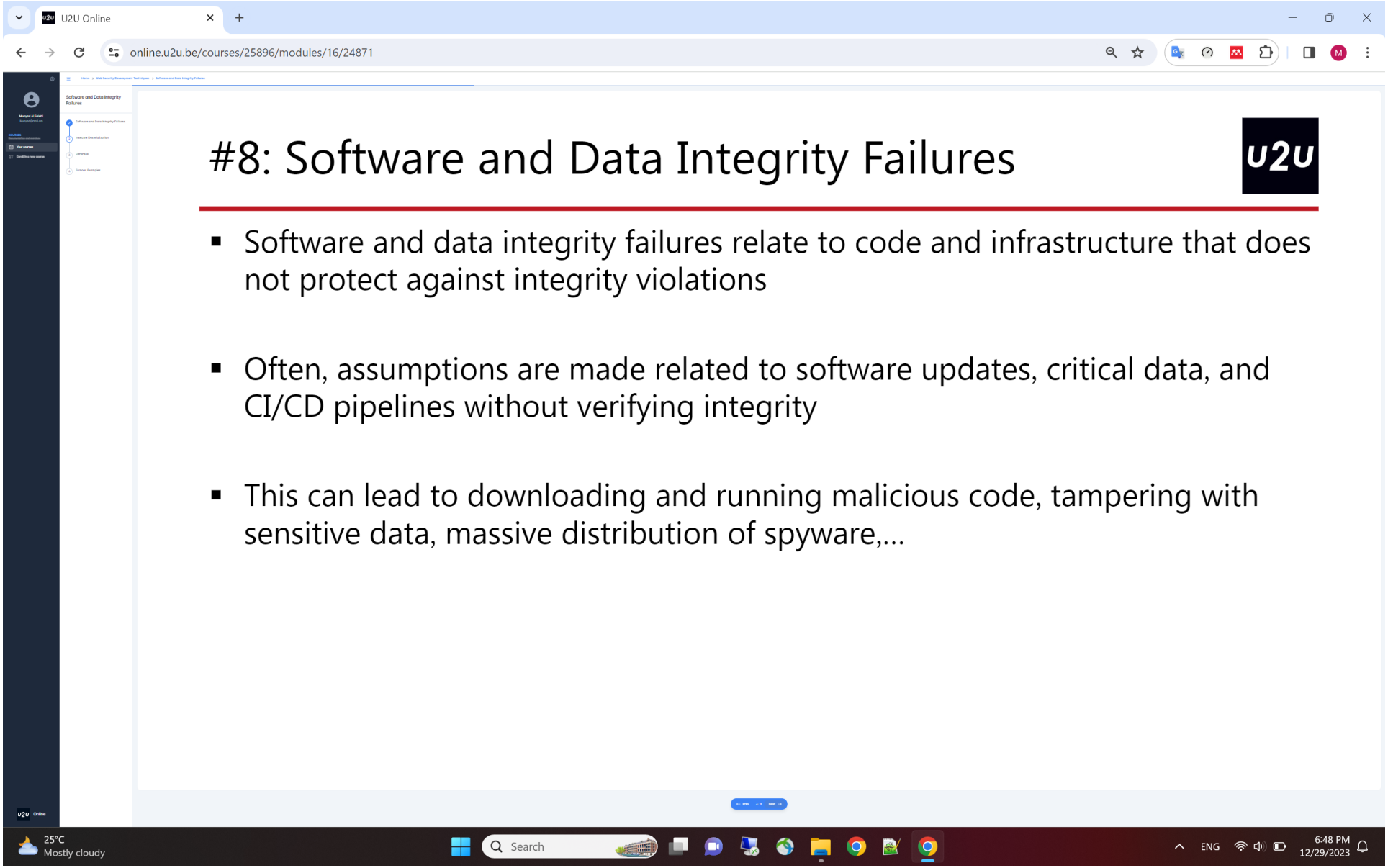
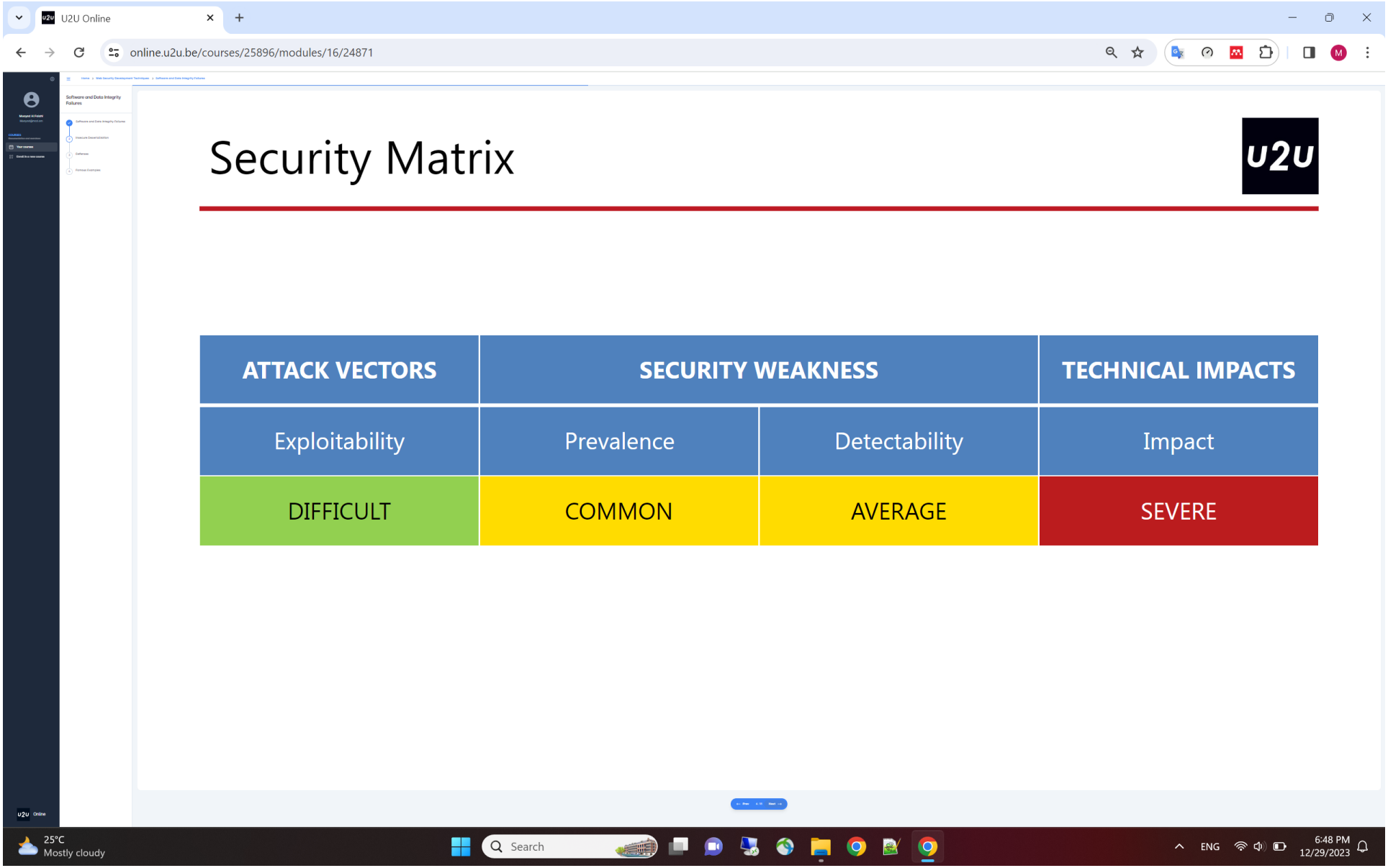
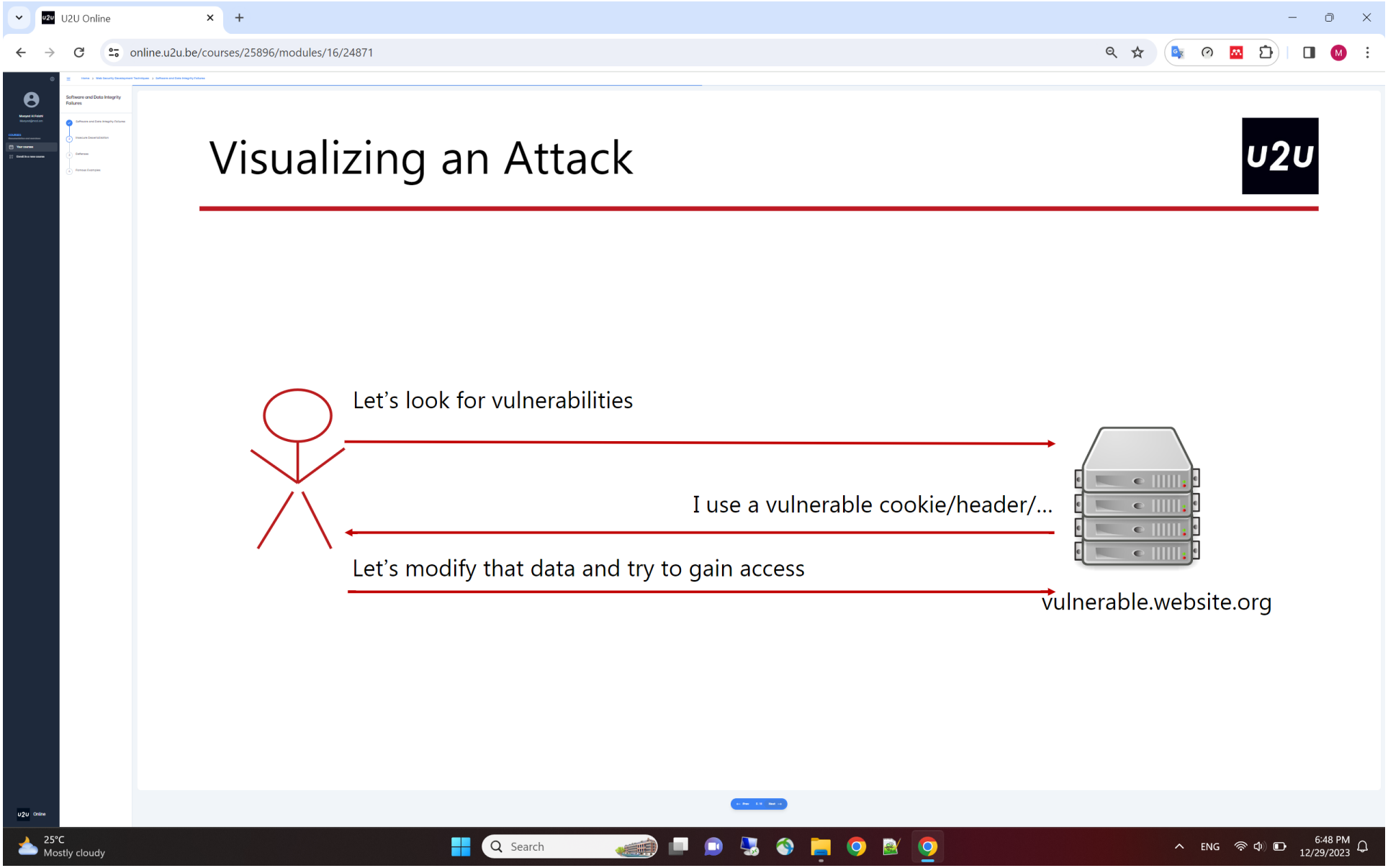
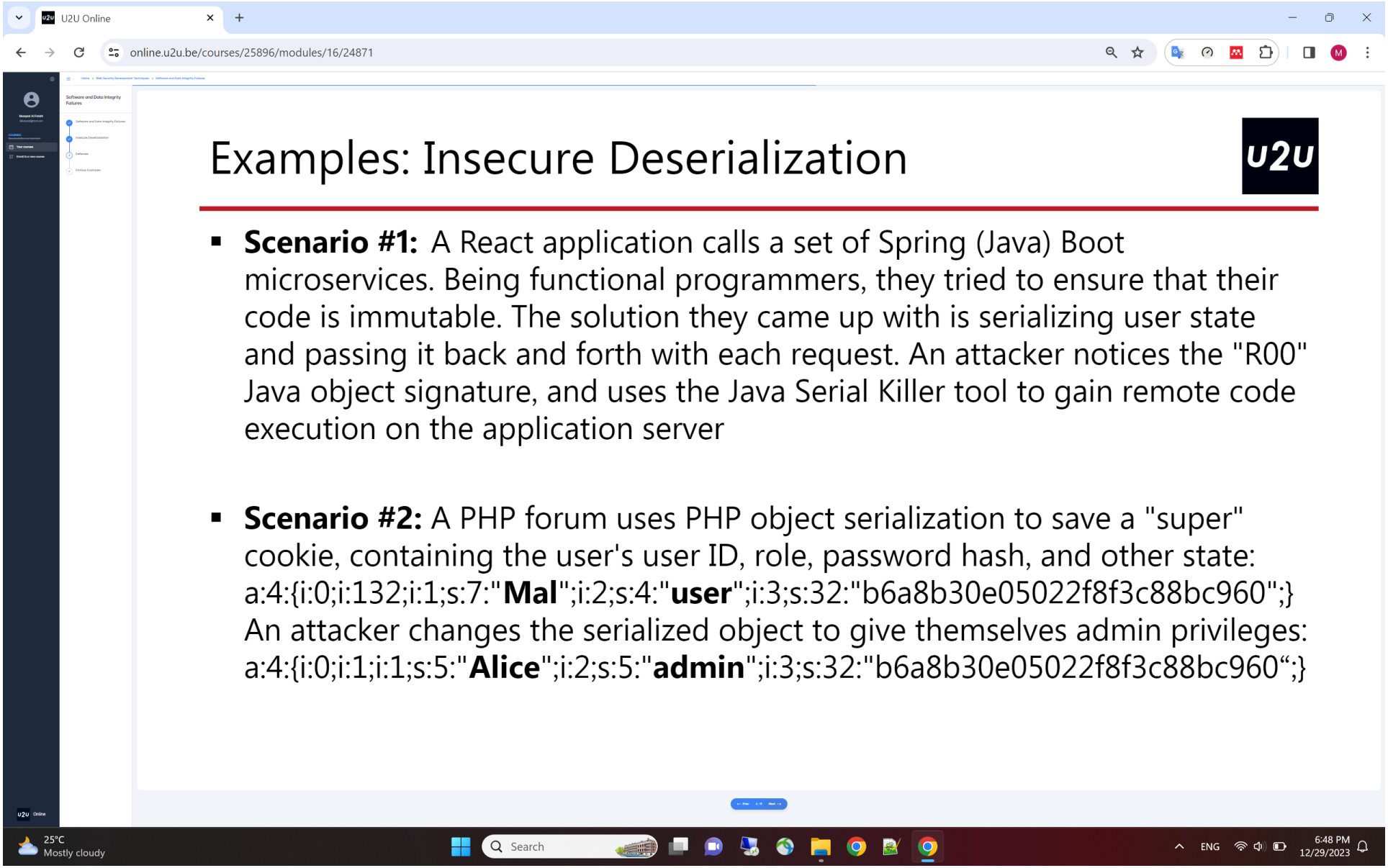

U2U Online
online.u2u.be/courses/25896/modules/16/24871
Developer and IT Training
u2u
Software and Data Integrity Failures
OWASP Web Security Threat #8
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023

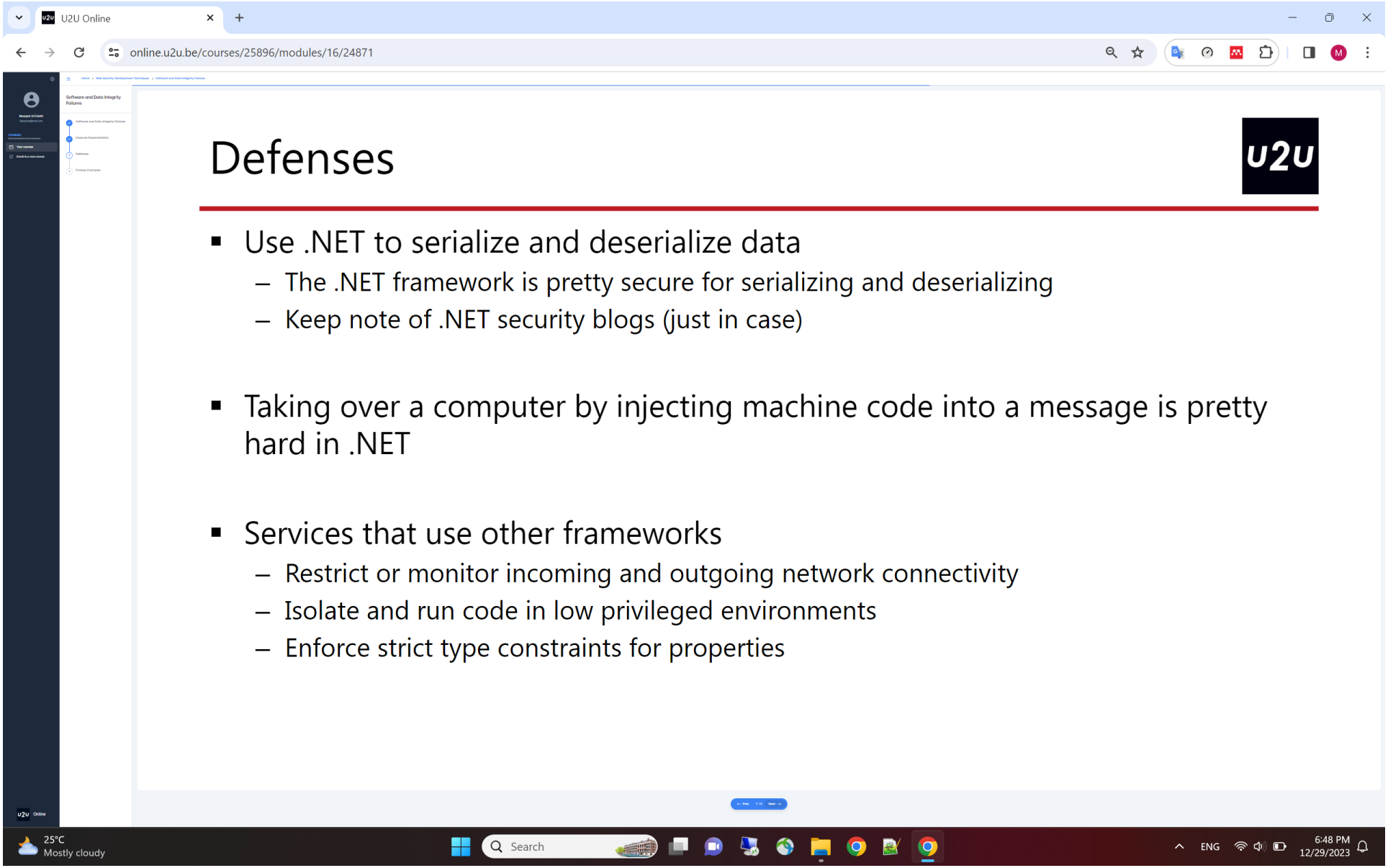

U2U Online
online.u2u.be/courses/25896/modules/16/24871
Agenda
U2U
Software and Data Integrity Failures
Defenses
Famous Examples
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023

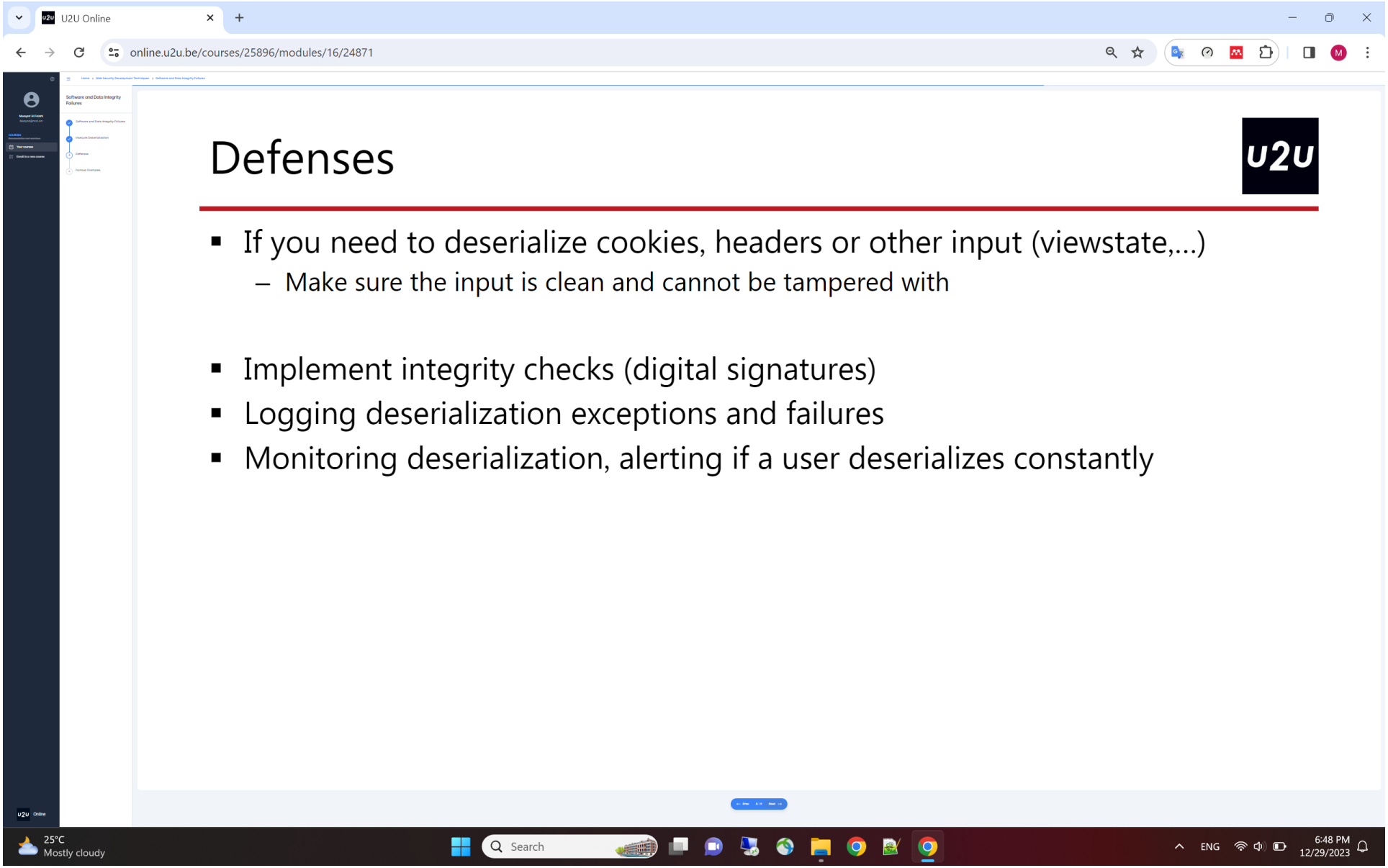

U2U Online
online.u2u.be/courses/25896/modules/16/24871
#8: Software and Data Integrity Failures
U2U
Software and Data Integrity Failures relate to code and infrastructure that does not protect against integrity violations
Often, assumptions are made related to software updates, critical data, and CI/CD pipelines without verifying integrity
This can lead to downloading and running malicious code, tampering with sensitive data, massive distribution of spyware,…
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023

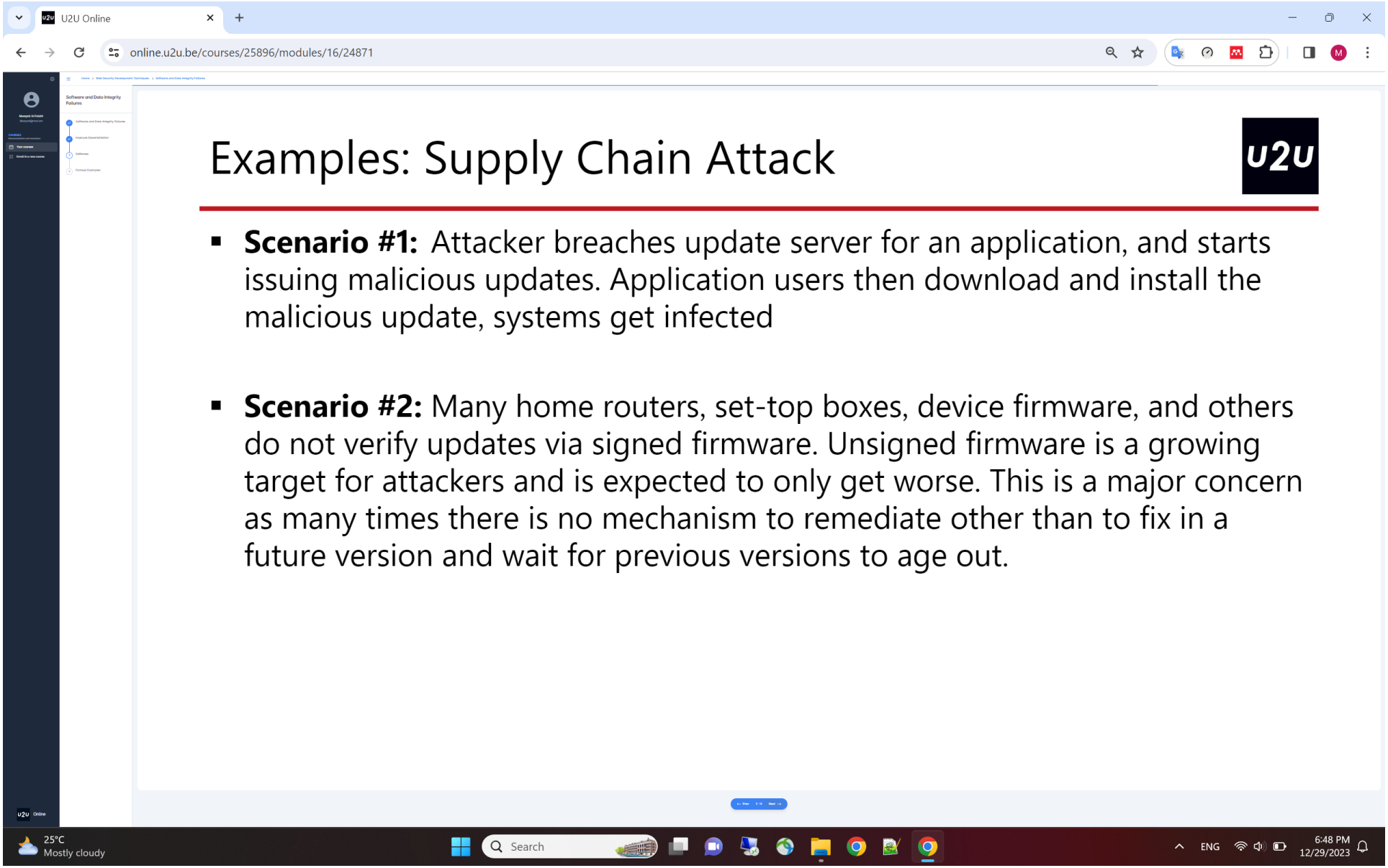

U2U Online
online.u2u.be/courses/25896/modules/16/24871
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
DIFFICULT
COMMON
AVERAGE
SEVERE
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023

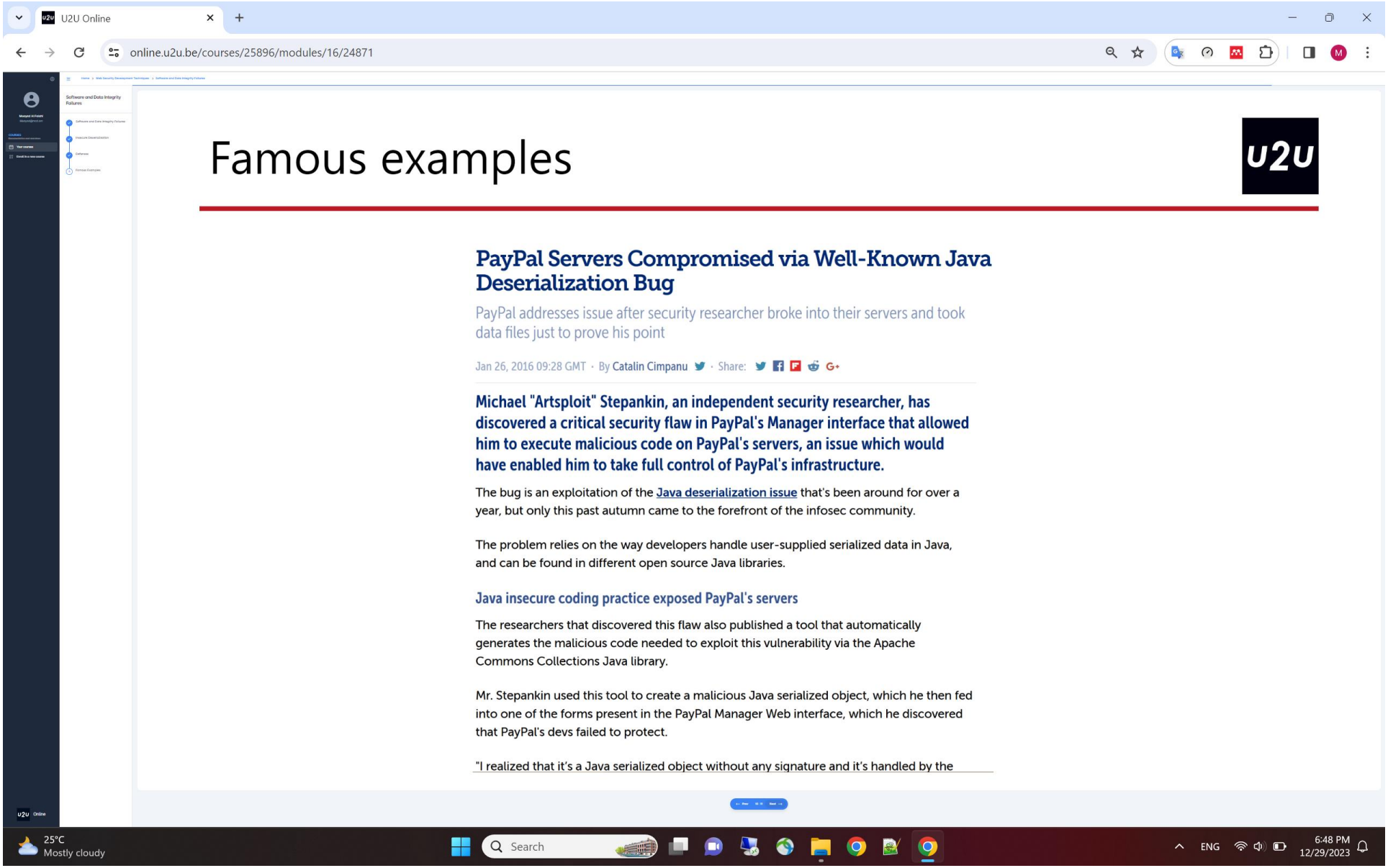

U2U Online
online.u2u.be/courses/25896/modules/16/24871
Visualizing an Attack
u2u
Let's look for vulnerabilities
I use a vulnerable cookie/header/...
Let's modify that data and try to gain access
vulnerable.website.org
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/16/24871
Examples: Insecure Deserialization
U2U
Scenario #1: A React application calls a set of Spring (Java) Boot microservices. Being functional programmers, they tried to ensure that their code is immutable. The solution they came up with is serializing user state and passing it back and forth with each request. An attacker notices the "R00" Java object signature, and uses the Java Serial Killer tool to gain remote code execution on the application server
Scenario #2: A PHP forum uses PHP object serialization to save a "super" cookie, containing the user's user ID, role, password hash, and other state:
a:4:{i:0;i:132;i:1;s:7:"Mal";i:2;s:4:"user";i:3;s:32:"b6a8b30e05022f8f3c88bc960";}
An attacker changes the serialized object to give themselves admin privileges:
a:4:{i:0;i:1;i:1;s:5:"Alice";i:2;s:5:"admin";i:3;s:32:"b6a8b30e05022f8f3c88bc960";}
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/16/24871
Defenses
u2u
Use .NET to serialize and deserialize data
The .NET framework is pretty secure for serializing and deserializing
Keep note of .NET security blogs (just in case)
Taking over a computer by injecting machine code into a message is pretty hard in .NET
Services that use other frameworks
Restrict or monitor incoming and outgoing network connectivity
Isolate and run code in low privileged environments
Enforce strict type constraints for properties
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/16/24871
Defenses
U2U
If you need to deserialize cookies, headers or other input (viewstate,...)
Make sure the input is clean and cannot be tampered with
Implement integrity checks (digital signatures)
Logging deserialization exceptions and failures
Monitoring deserialization, alerting if a user deserializes constantly
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/16/24871
Examples: Supply Chain Attack
U2U
Scenario #1: Attacker breaches update server for an application, and starts issuing malicious updates. Application users then download and install the malicious update, systems get infected
Scenario #2: Many home routers, set-top boxes, device firmware, and others do not verify updates via signed firmware. Unsigned firmware is a growing target for attackers and is expected to only get worse. This is a major concern as many times there is no mechanism to remediate other than to fix in a future version and wait for previous versions to age out.
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/16/24871
Famous examples
U2U
PayPal Servers Compromised via Well-Known Java Deserialization Bug
PayPal addresses issue after security researcher broke into their servers and took data files just to prove his point
Jan 26, 2016 09:28 GMT · By Catalin Cimpanu · Share:
Michael "Artsploit" Stepankin, an independent security researcher, has discovered a critical security flaw in PayPal's Manager interface that allowed him to execute malicious code on PayPal's servers, an issue which would have enabled him to take full control of PayPal's infrastructure.
The bug is an exploitation of the Java deserialization issue that's been around for over a year, but only this past autumn came to the forefront of the infosec community.
The problem relies on the way developers handle user-supplied serialized data in Java, and can be found in different open source Java libraries.
Java insecure coding practice exposed PayPal's servers
The researchers that discovered this flaw also published a tool that automatically generates the malicious code needed to exploit this vulnerability via the Apache Commons Collections Java library.
Mr. Stepankin used this tool to create a malicious Java serialized object, which he then fed into one of the forms present in the PayPal Manager Web interface, which he discovered that PayPal's devs failed to protect.
"I realized that it's a Java serialized object without any signature and it's handled by the
25°C
Mostly cloudy
Search
ENG
6:48 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Famous examples

Wide-ranging SolarWinds probe sparks fear in Corporate America

By Christopher Bing, Chris Prentice and Joseph Menn on Sep 11, 2021 11:28AM

Over liability for unreported cyber incidents.

A US Securities and Exchange Commission investigation into the SolarWinds Russian hacking operation has dozens of corporate executives fearful information unearthed in the expanding probe will expose them to liability, according to six people familiar with the inquiry.

25°C Mostly cloudy

Search

ENG 6:48 PM 12/29/2023