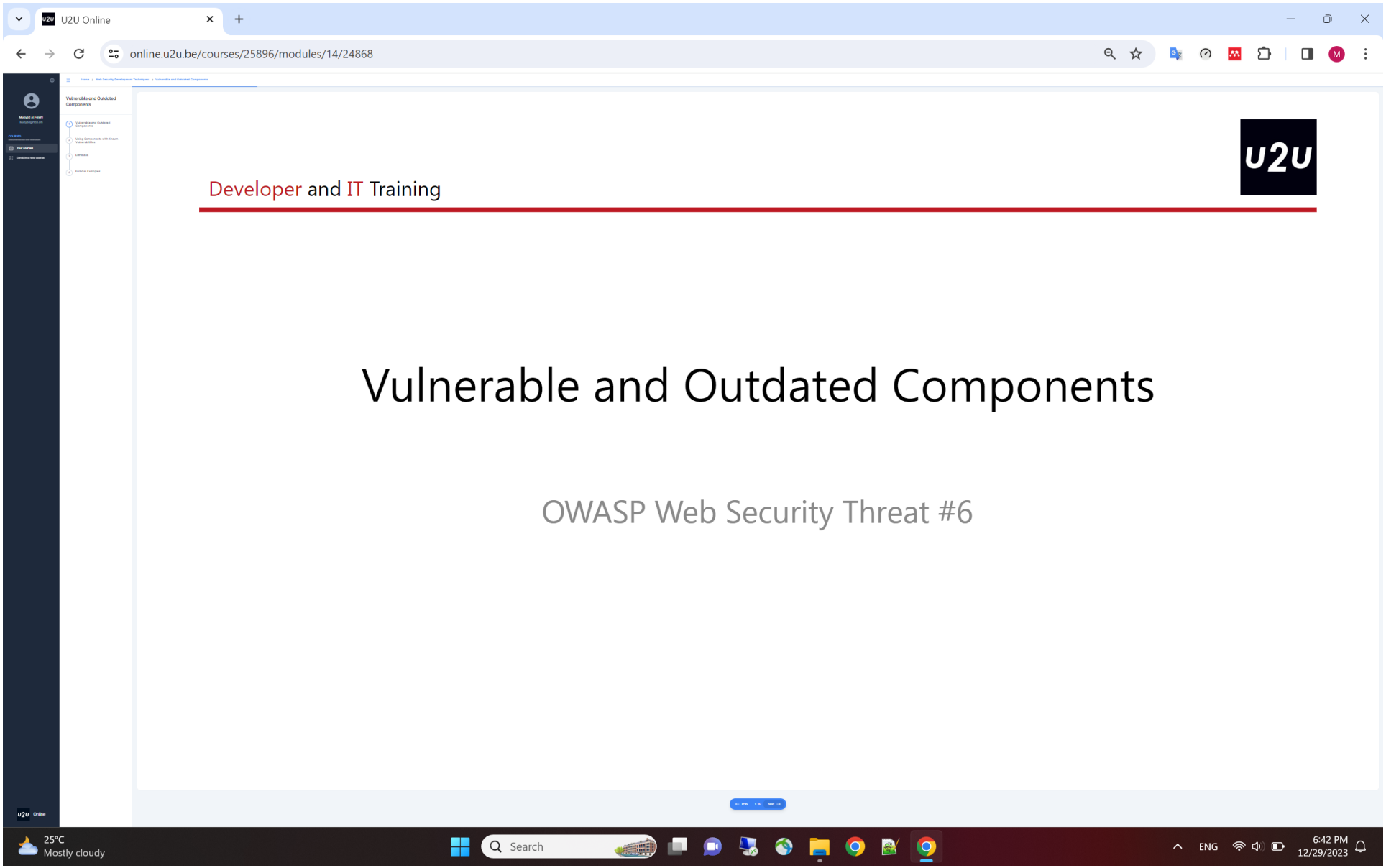
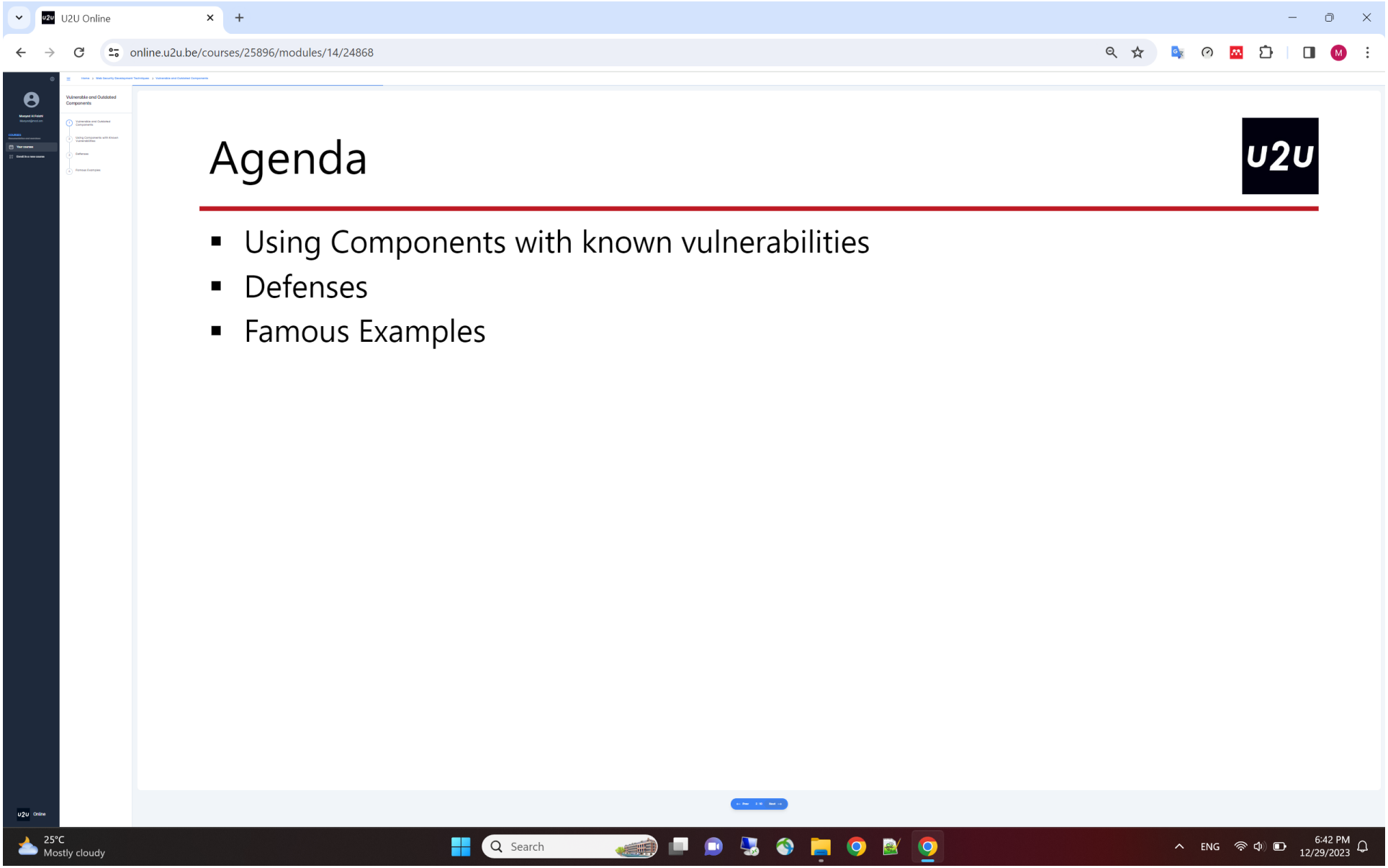
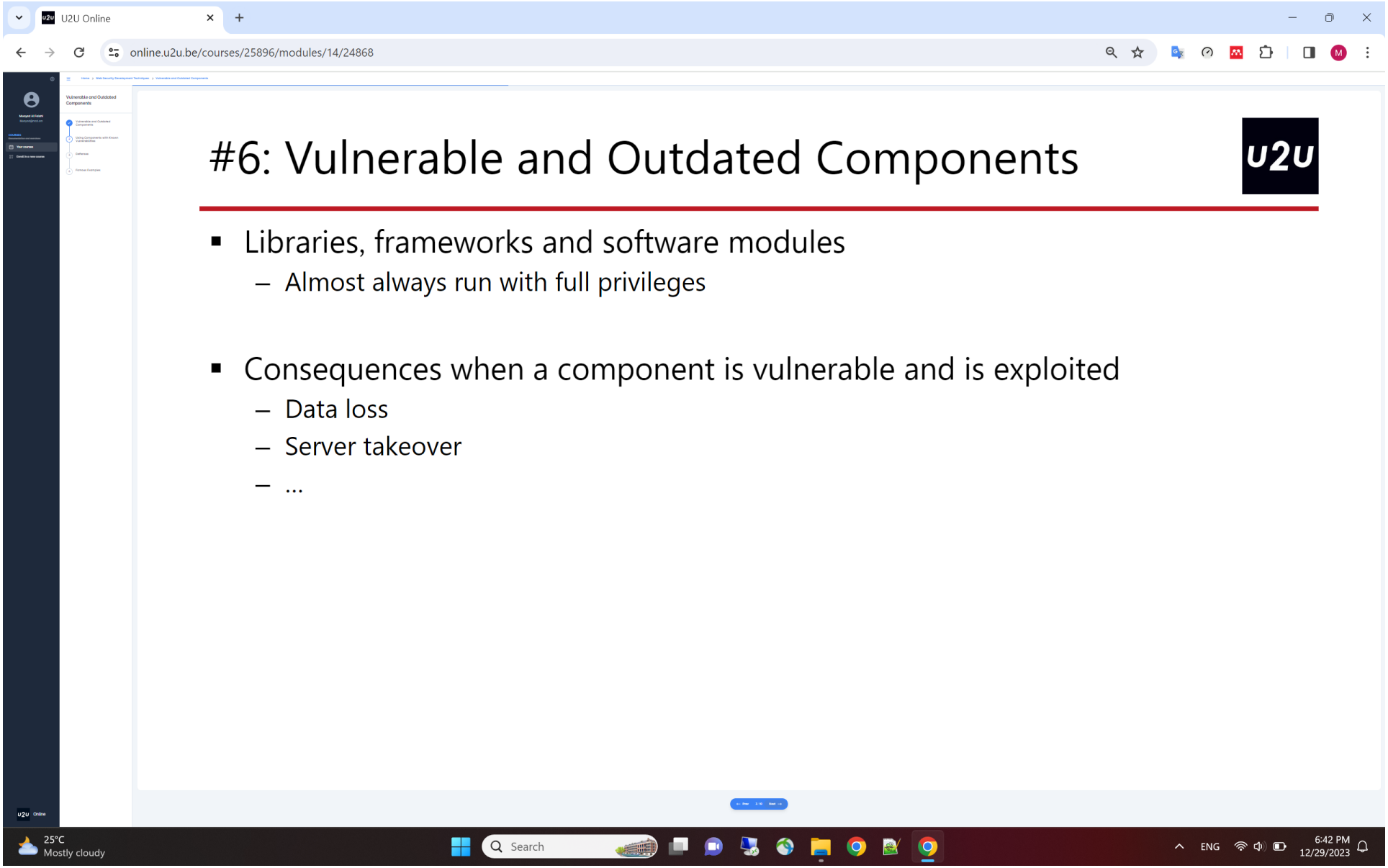
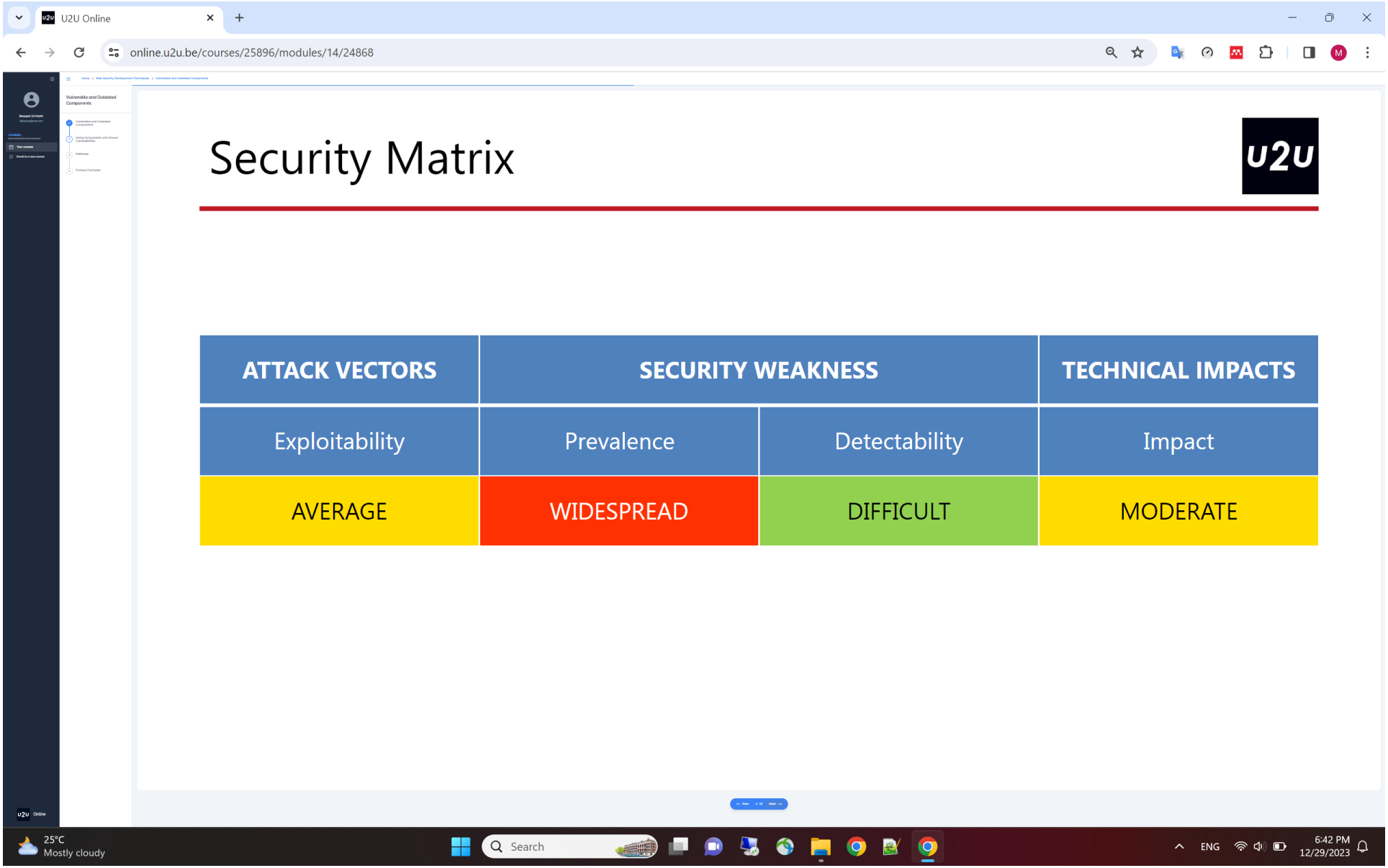
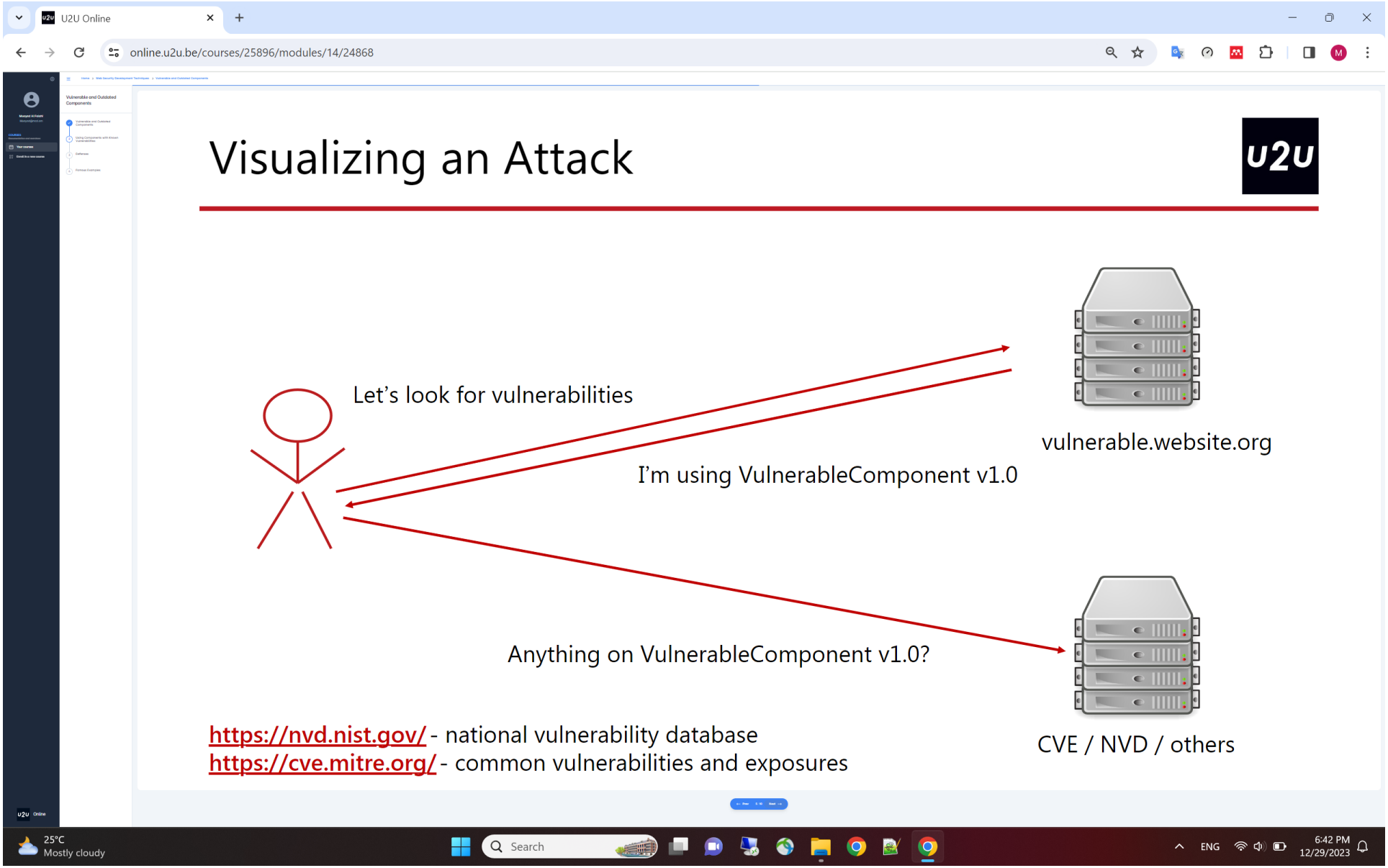
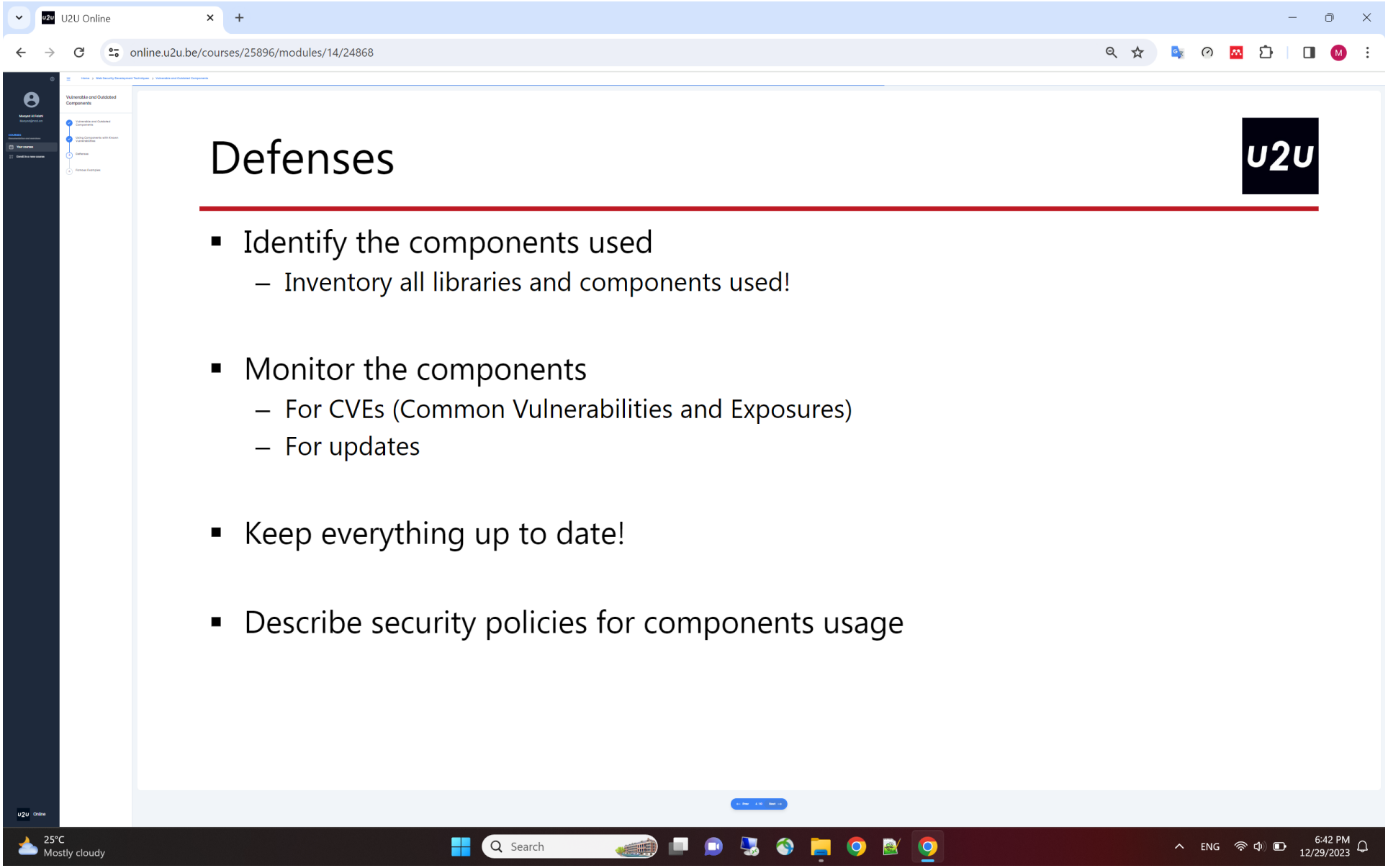

U2U Online
online.u2u.be/courses/25896/modules/14/24868
Developer and IT Training
u2u
Vulnerable and Outdated Components
OWASP Web Security Threat #6
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/14/24868
Agenda
U2U
Using Components with known vulnerabilities
Defenses
Famous Examples
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/14/24868
#6: Vulnerable and Outdated Components
U2U
Libraries, frameworks and software modules
Almost always run with full privileges
Consequences when a component is vulnerable and is exploited
Data loss
Server takeover
...
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023

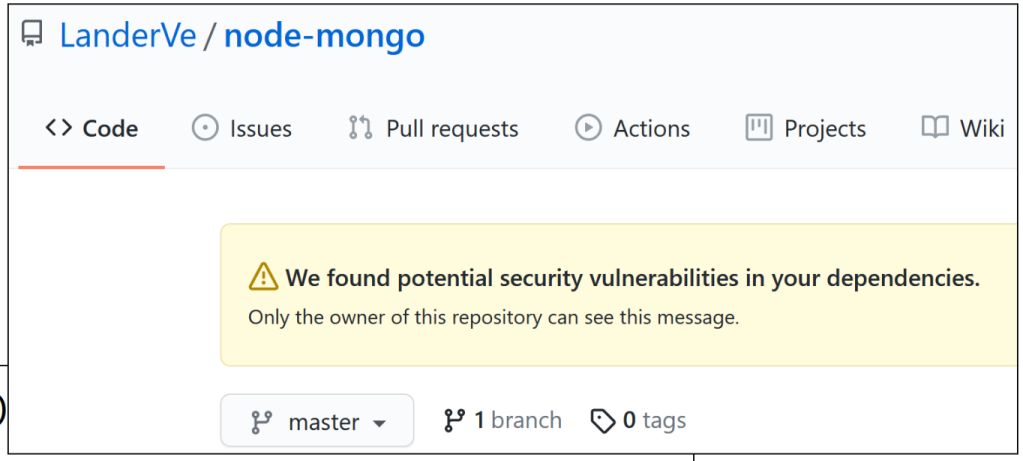

U2U Online
online.u2u.be/courses/25896/modules/14/24868
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
AVERAGE
WIDESPREAD
DIFFICULT
MODERATE
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023

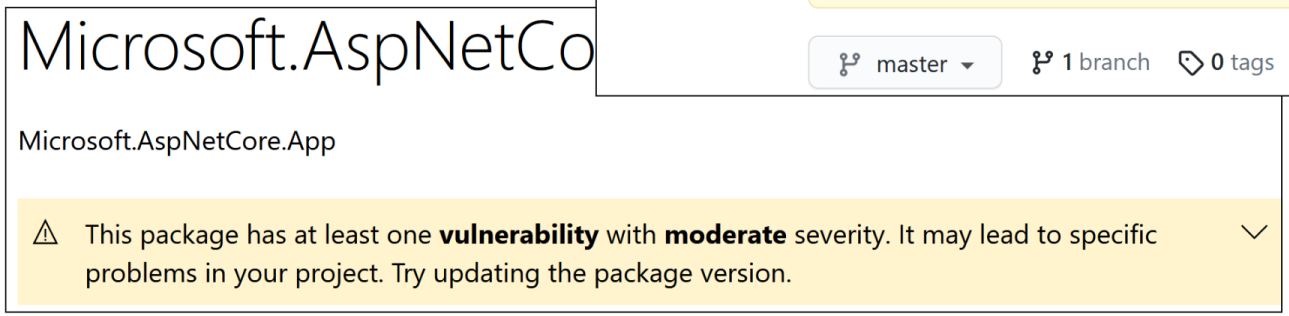

U2U Online
online.u2u.be/courses/25896/modules/14/24868
Visualizing an Attack
u2u
Let's look for vulnerabilities
I'm using VulnerableComponent v1.0
vulnerable.website.org
Anything on VulnerableComponent v1.0?
https://nvd.nist.gov/ - national vulnerability database
https://cve.mitre.org/ - common vulnerabilities and exposures
CVE / NVD / others
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023

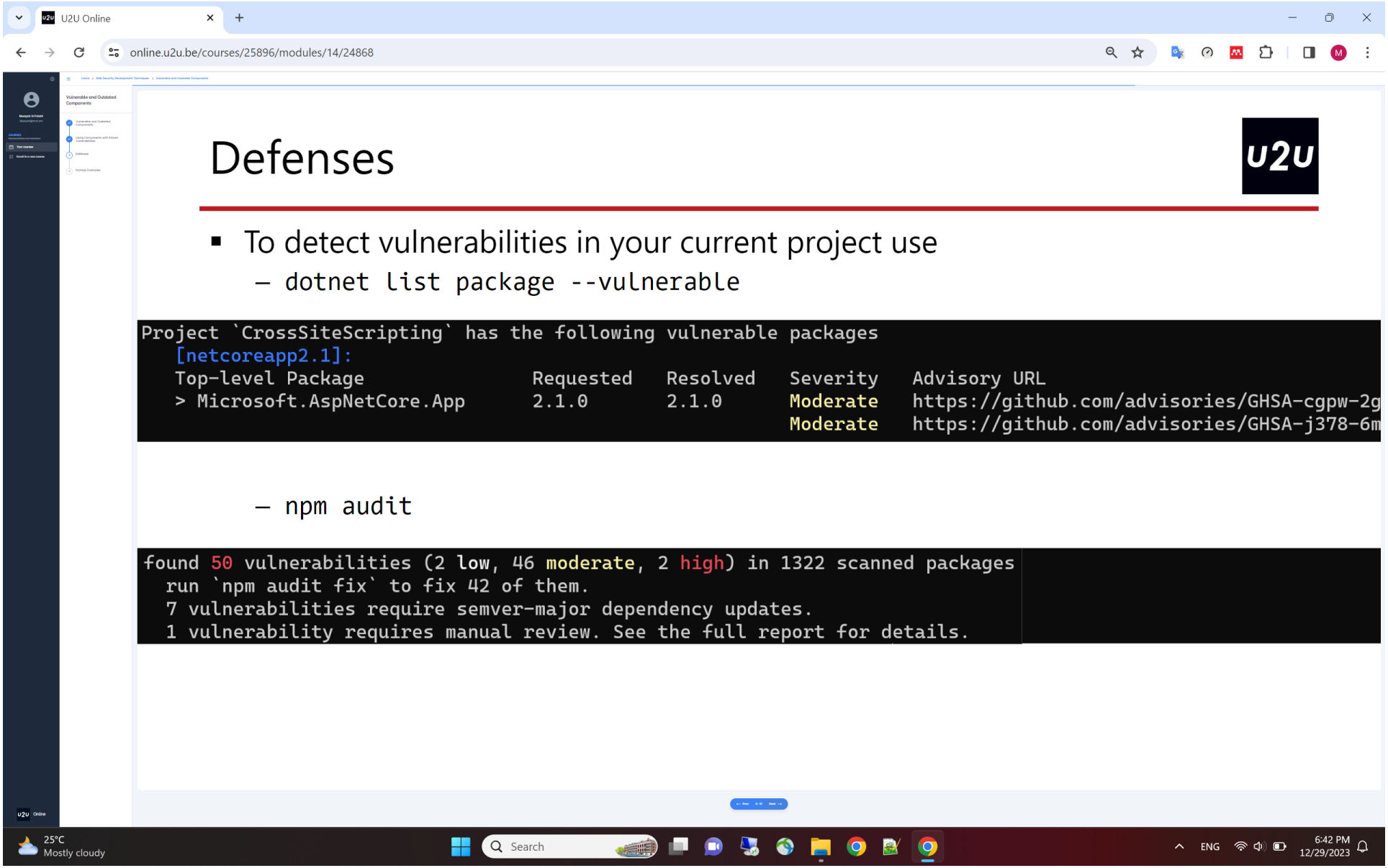

U2U Online
online.u2u.be/courses/25896/modules/14/24868
Vulnerable and Outdated Components
Defenses
u2u
Identify the components used
Inventory all libraries and components used!
Monitor the components
For CVEs (Common Vulnerabilities and Exposures)
For updates
Keep everything up to date!
Describe security policies for components usage
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023

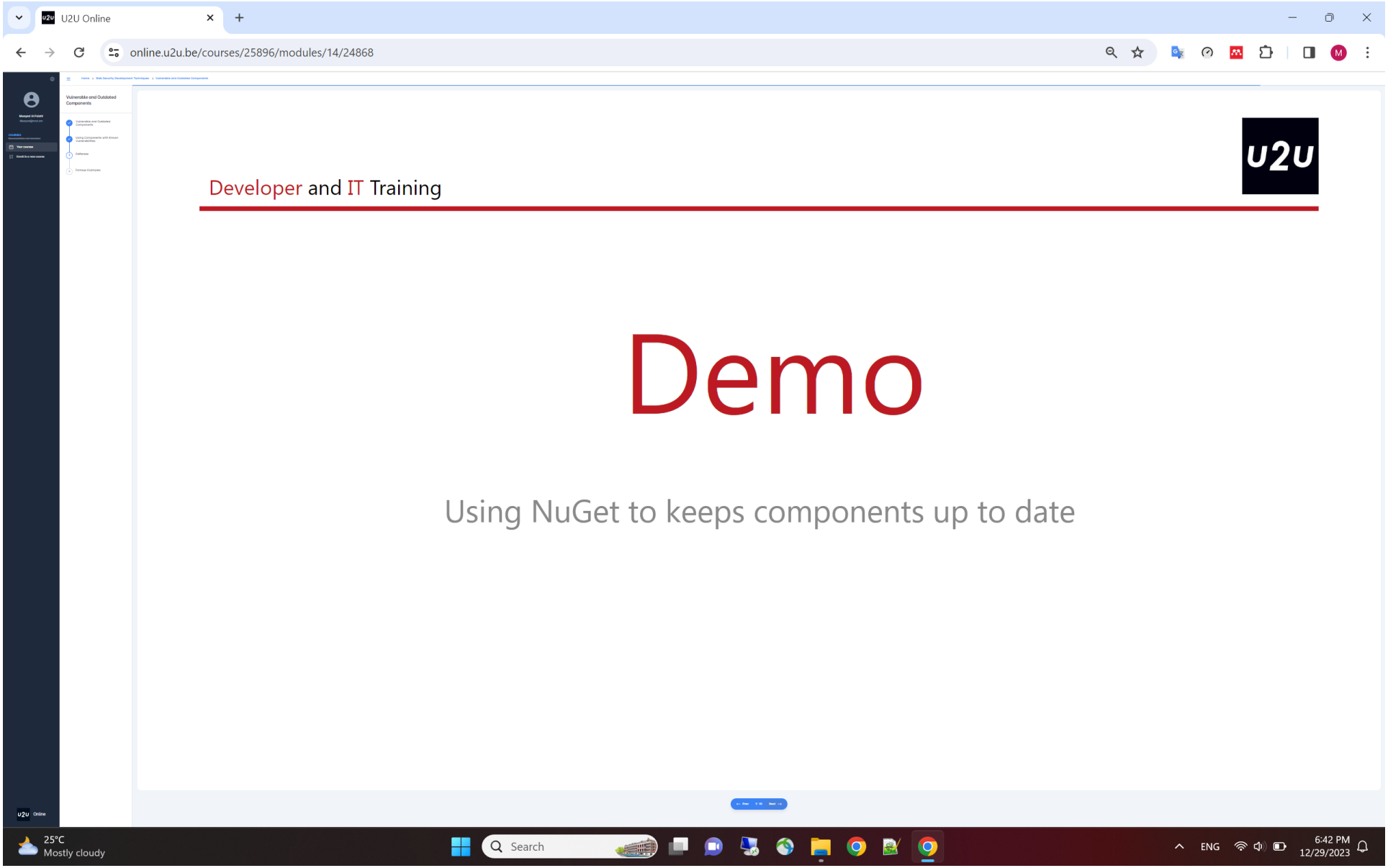
Defenses

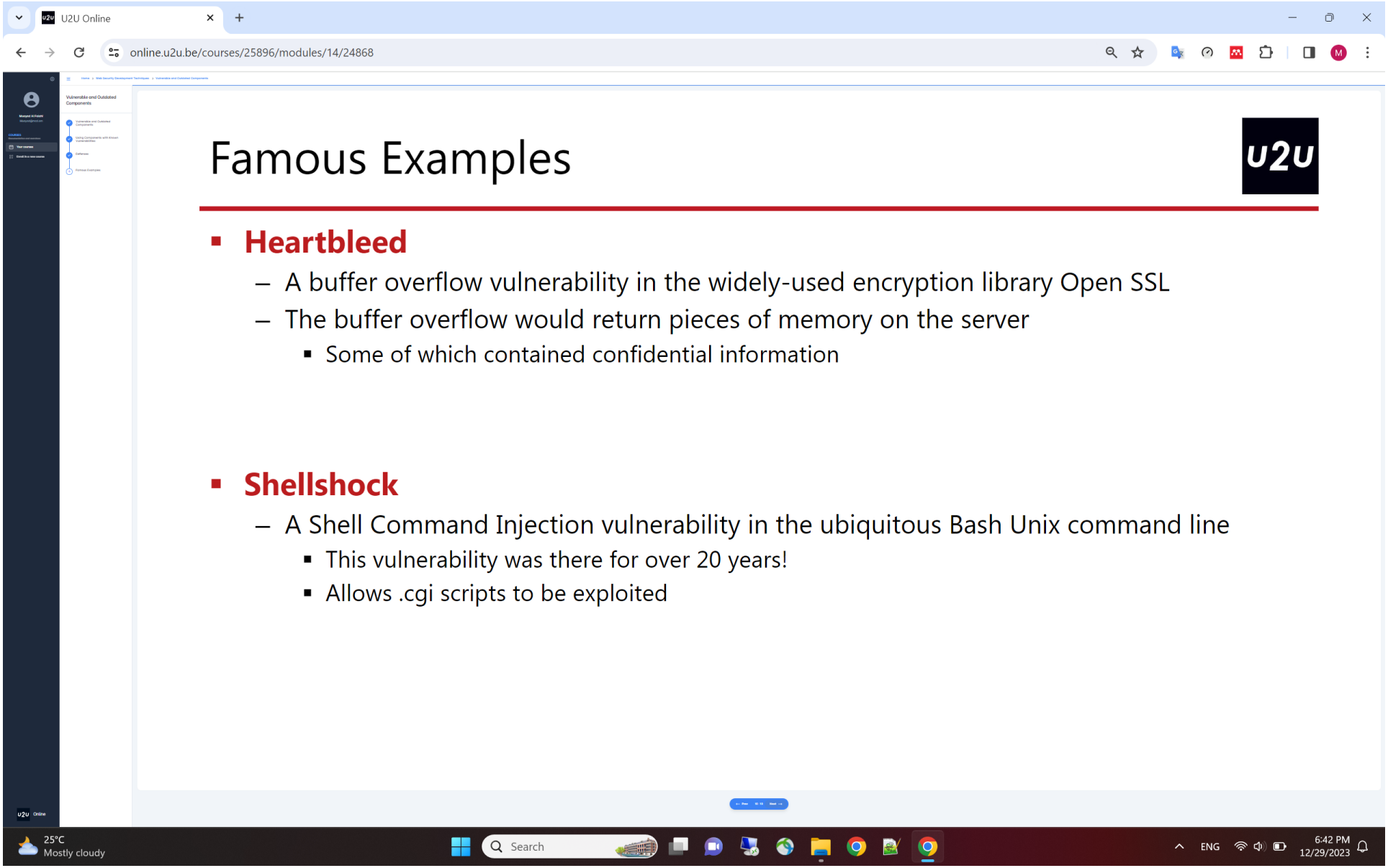
- Modern tools help detecting vulnerabilities
  - E.g., GitHub
  - E.g., NuGet.org






U2U Online
online.u2u.be/courses/25896/modules/14/24868
Defenses
u2u
To detect vulnerabilities in your current project use
dotnet list package --vulnerable
Project `CrossSiteScripting` has the following vulnerable packages
[netcoreapp2.1]:
Top-level Package Requested Resolved Severity Advisory URL
> Microsoft.AspNetCore.App 2.1.0 2.1.0 Moderate https://github.com/advisories/GHSA-cgpw-2g
Moderate https://github.com/advisories/GHSA-j378-6m
npm audit
found 50 vulnerabilities (2 low, 46 moderate, 2 high) in 1322 scanned packages
run `npm audit fix` to fix 42 of them.
7 vulnerabilities require semver-major dependency updates.
1 vulnerability requires manual review. See the full report for details.
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/14/24868
Developer and IT Training
Demo
Using NuGet to keeps components up to date
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/14/24868
Famous Examples
u2u
Heartbleed
A buffer overflow vulnerability in the widely-used encryption library Open SSL
The buffer overflow would return pieces of memory on the server
Some of which contained confidential information
Shellshock
A Shell Command Injection vulnerability in the ubiquitous Bash Unix command line
This vulnerability was there for over 20 years!
Allows .cgi scripts to be exploited
25°C
Mostly cloudy
Search
ENG
6:42 PM
12/29/2023