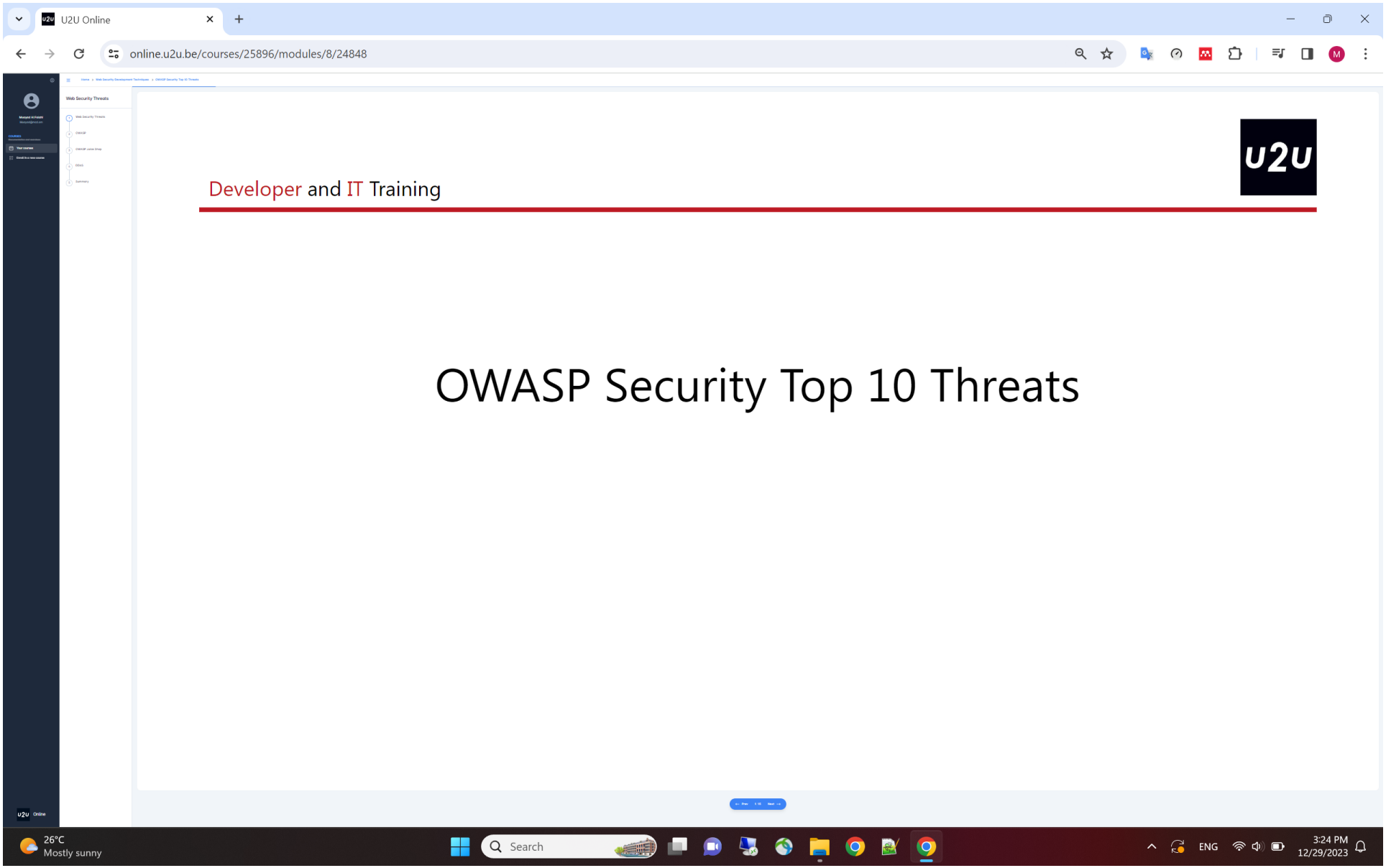
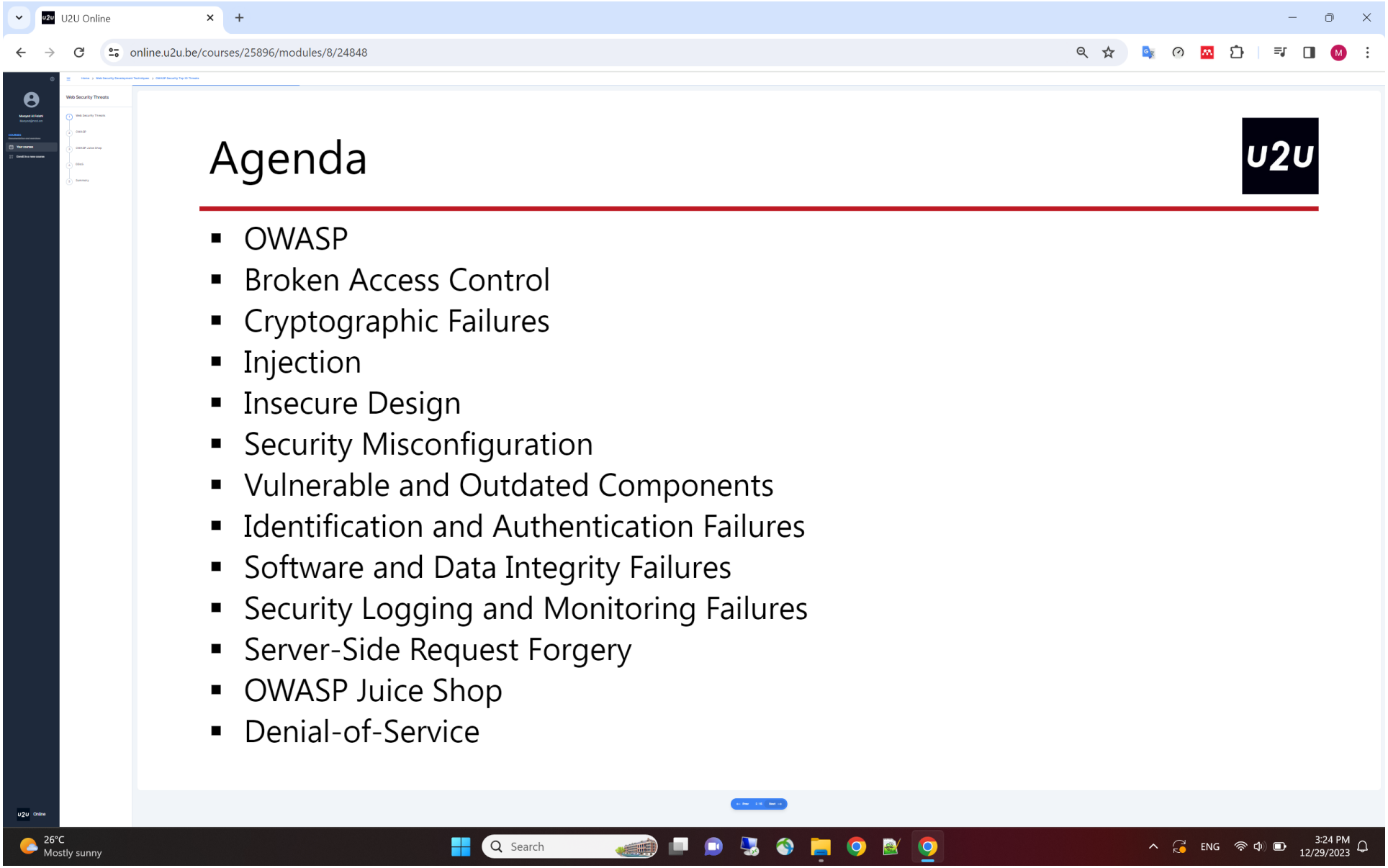

U2U Online
online.u2u.be/courses/25896/modules/8/24848
Developer and IT Training
U2U
OWASP Security Top 10 Threats
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
Agenda
u2u
OWASP
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery
OWASP Juice Shop
Denial-of-Service
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/8/24848

What is OWASP?

- The Open Web Application Security Project
  - Publishes a top 10 security issues every couple of years
- Open community dedicated to help organizations
  - Non-profit organization
  - Technology agnostic
- OWASP publishes free and open
  - Application security tools
  - Complete books on security testing, development, …
  - Cutting edge research
  - …

- https://www.owasp.org

26°C Mostly sunny

Search

ENG 3:24 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/8/24848

Top 10 OWASP Security Issues

- First Released in 2003
  - Updates in 2003, 2004, 2007, 2010, 2013, 2017 and 2021

- Goals
  - Raise awareness about application security
  - Identify some of the most critical risks facing organizations

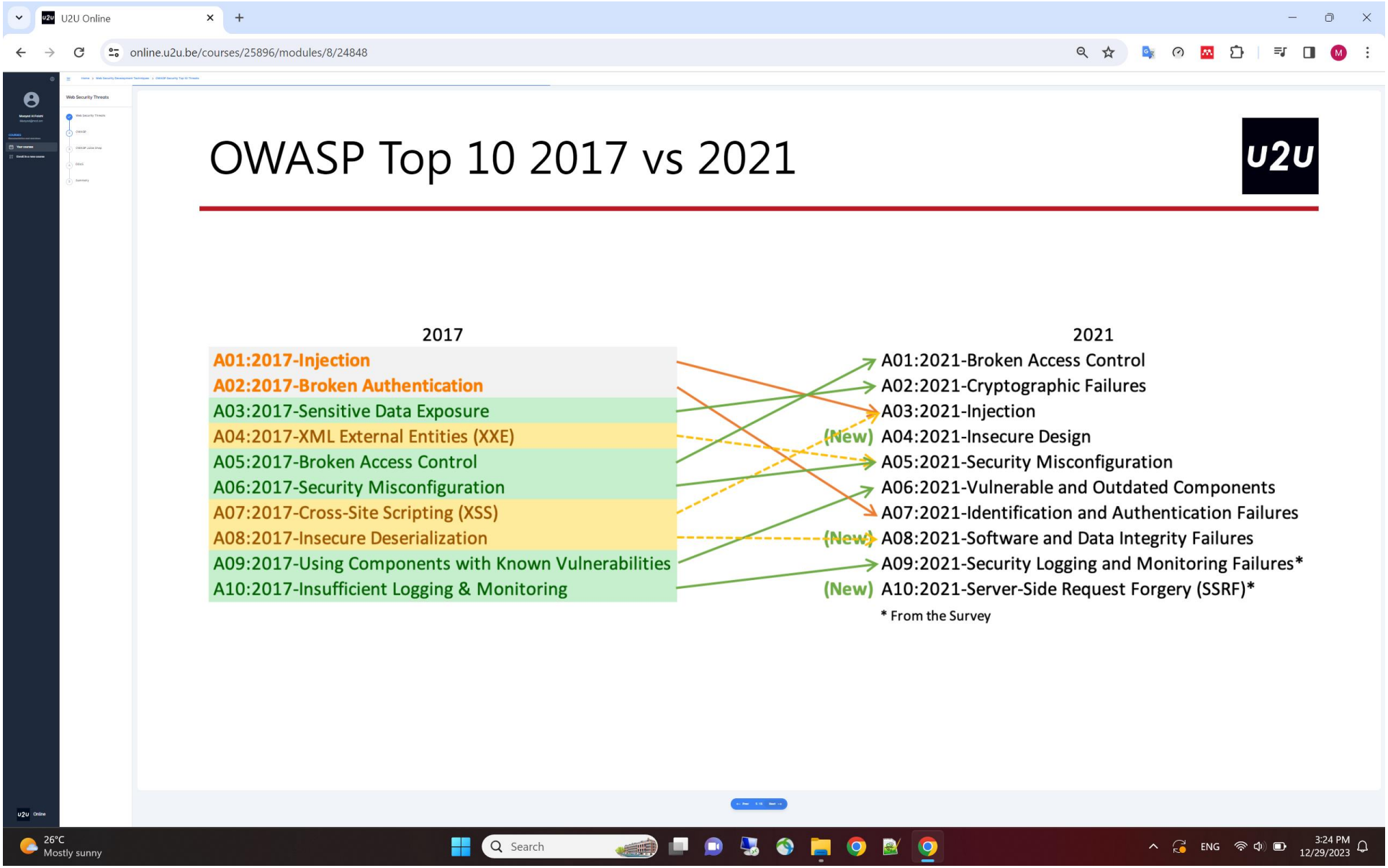
OWASP Top 10

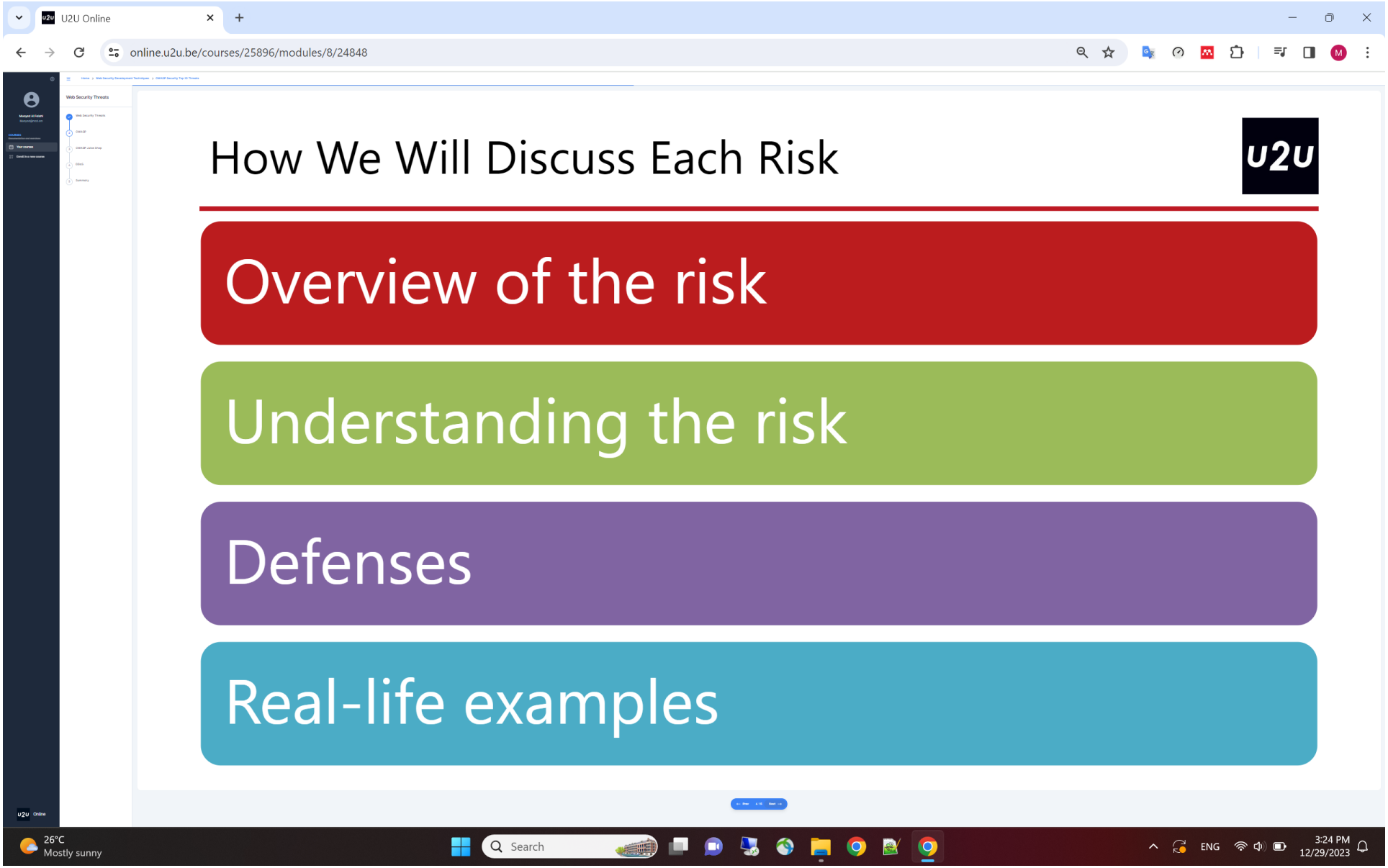
The Ten Most Critical Web Application Security Risks

26°C Mostly sunny

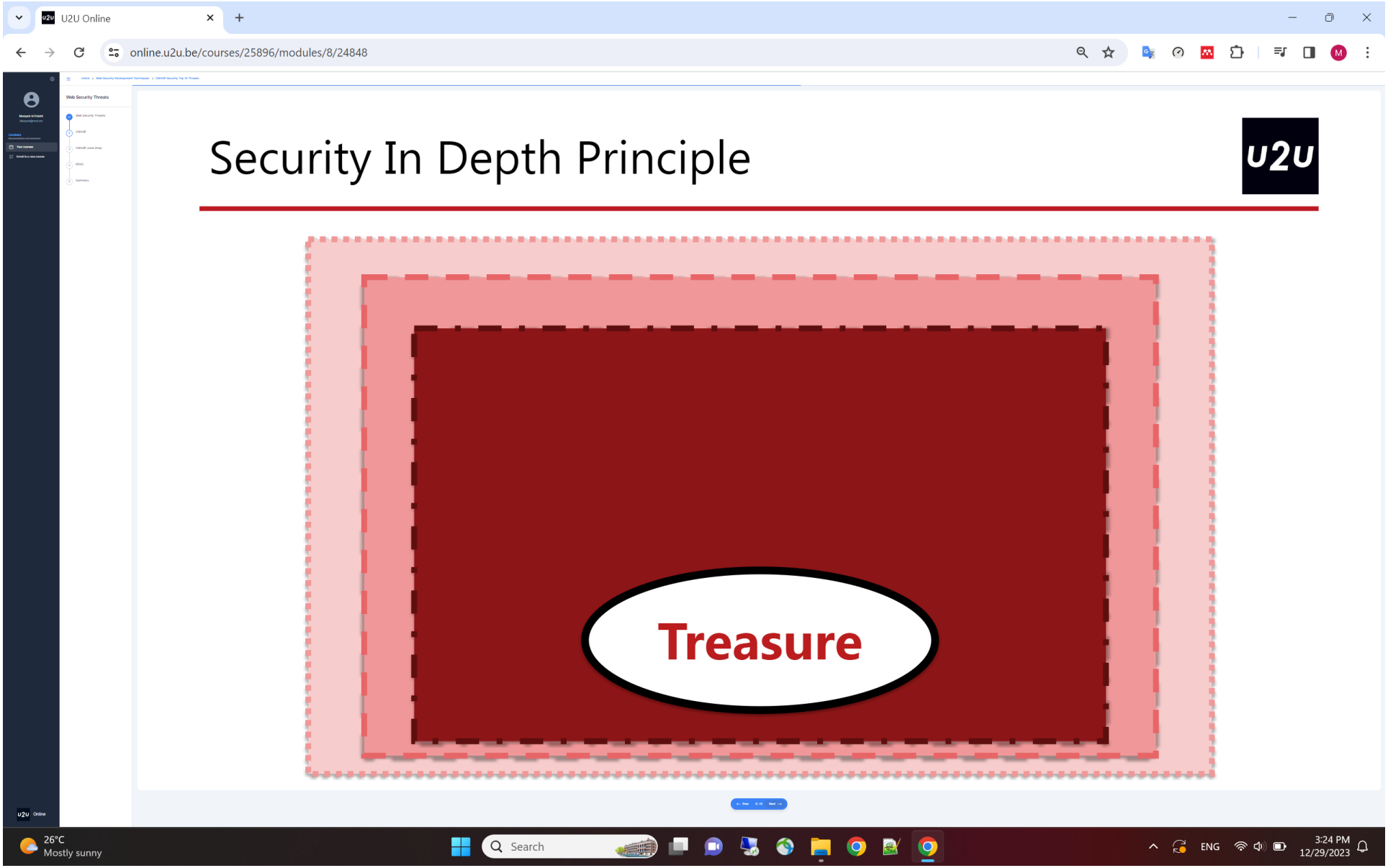
Search

ENG 3:24 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
OWASP Top 10 2017 vs 2021
U2U
2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023

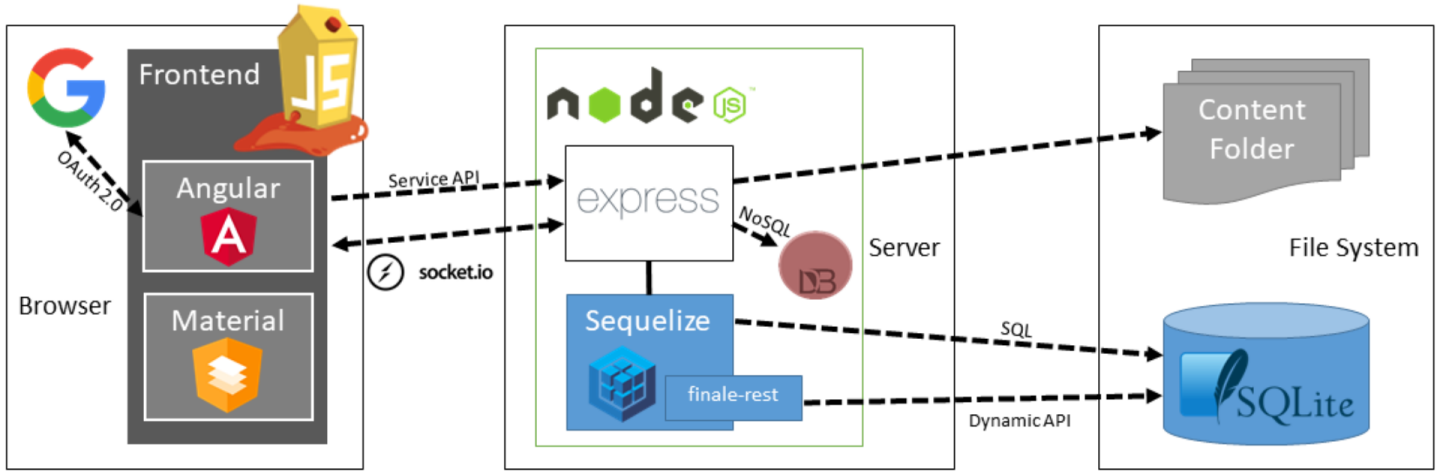

U2U Online
online.u2u.be/courses/25896/modules/8/24848
How We Will Discuss Each Risk
U2U
Overview of the risk
Understanding the risk
Defenses
Real-life examples
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023

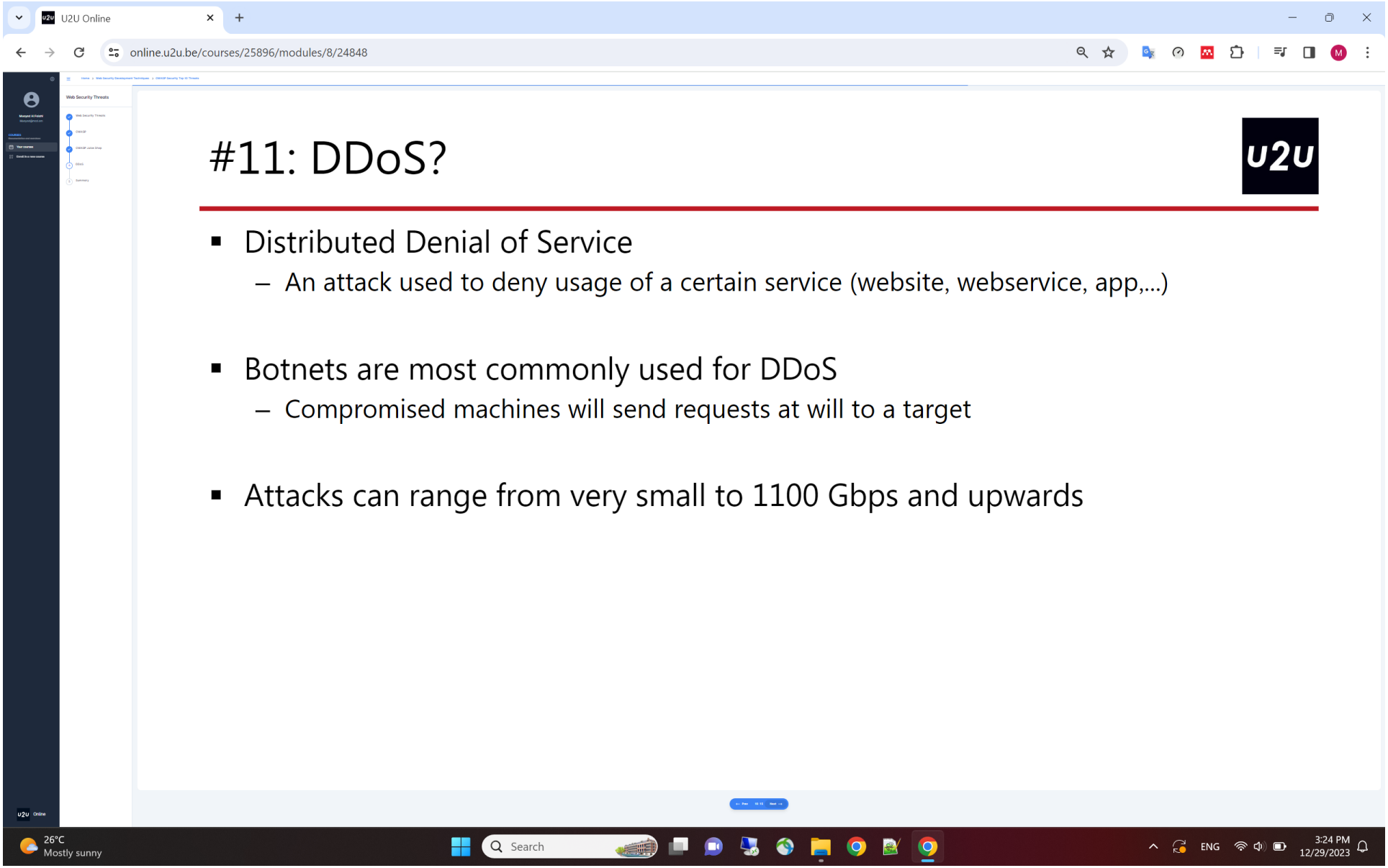

U2U Online
online.u2u.be/courses/25896/modules/8/24848
Current Top 10
U2U
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery
Bonus: Denial-of-Service
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023

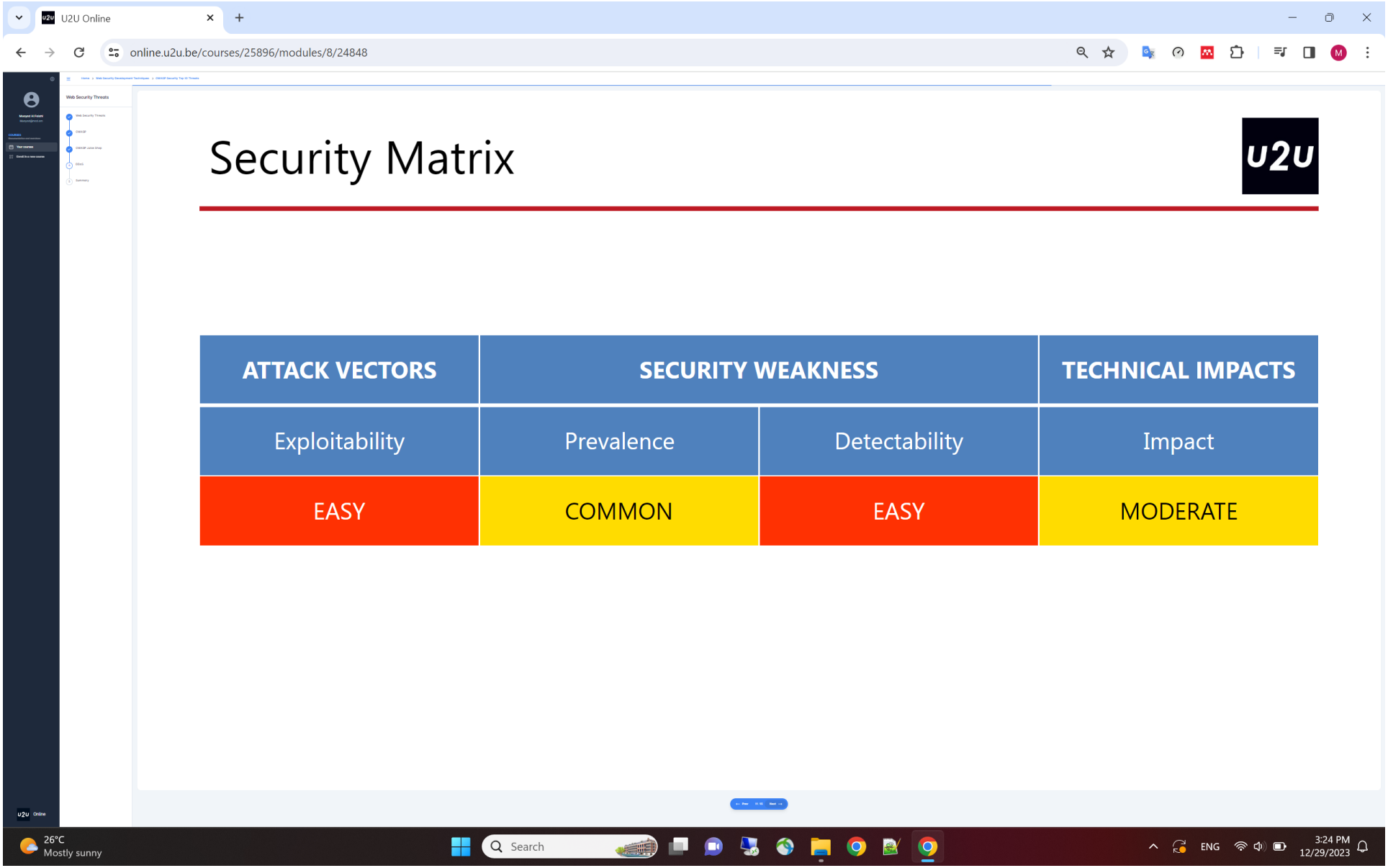

U2U Online
online.u2u.be/courses/25896/modules/8/24848
Web Security Threats
Security In Depth Principle
U2U
Treasure
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023

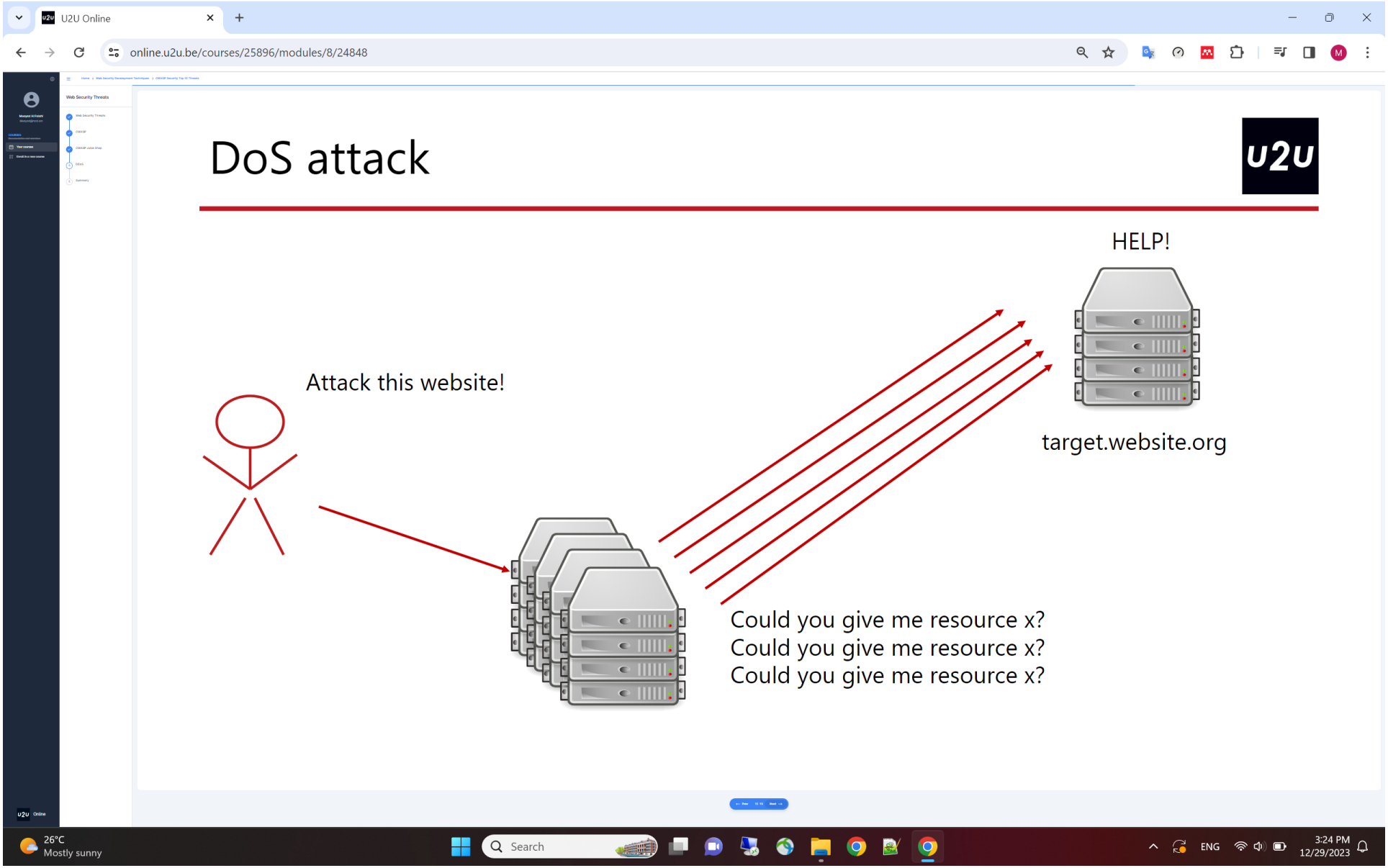
OWASP Juice Shop

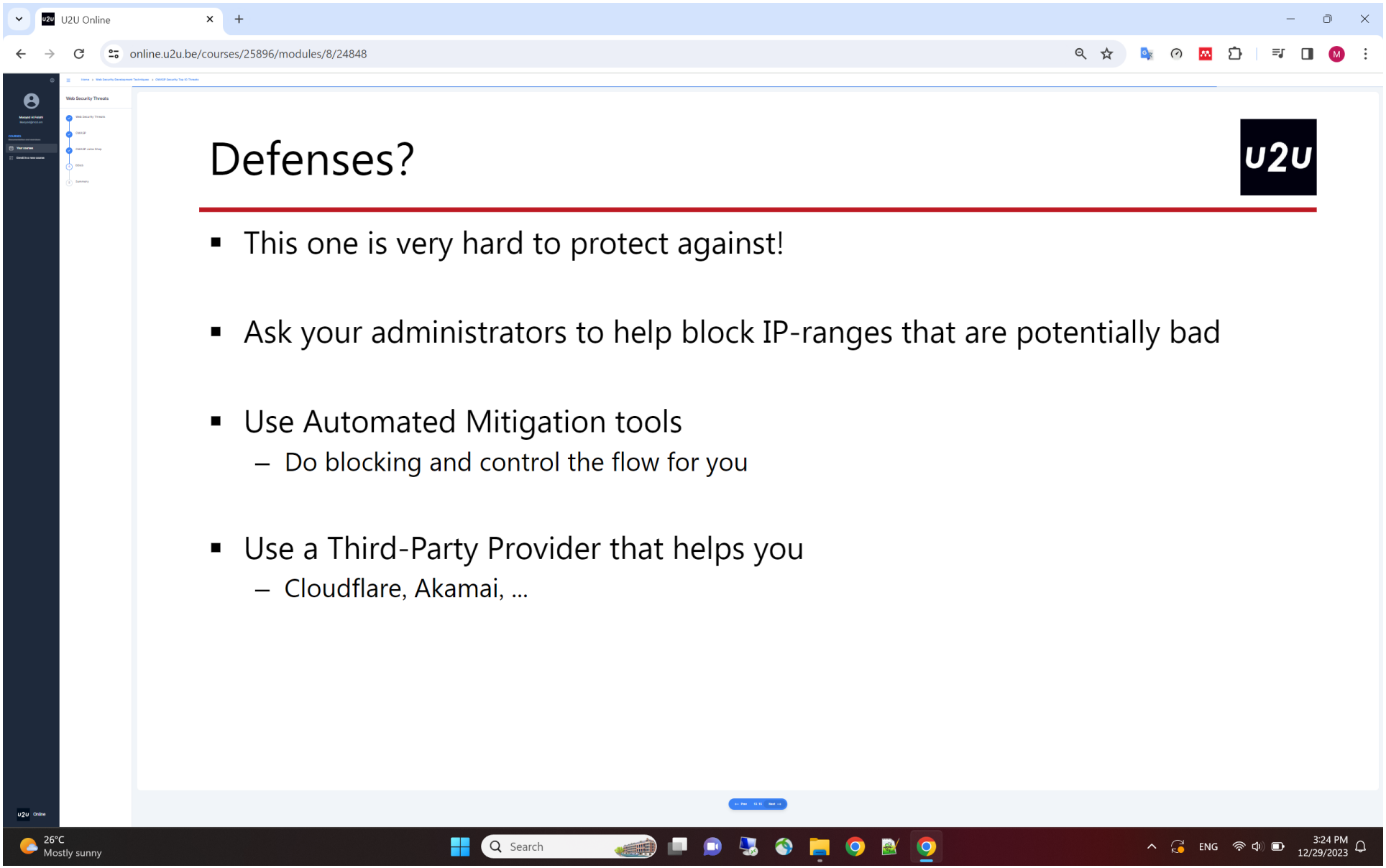
- Demo application containing tons of vulnerabilities
- Notifies you when you solved a challenge and keeps track on a scoreboard

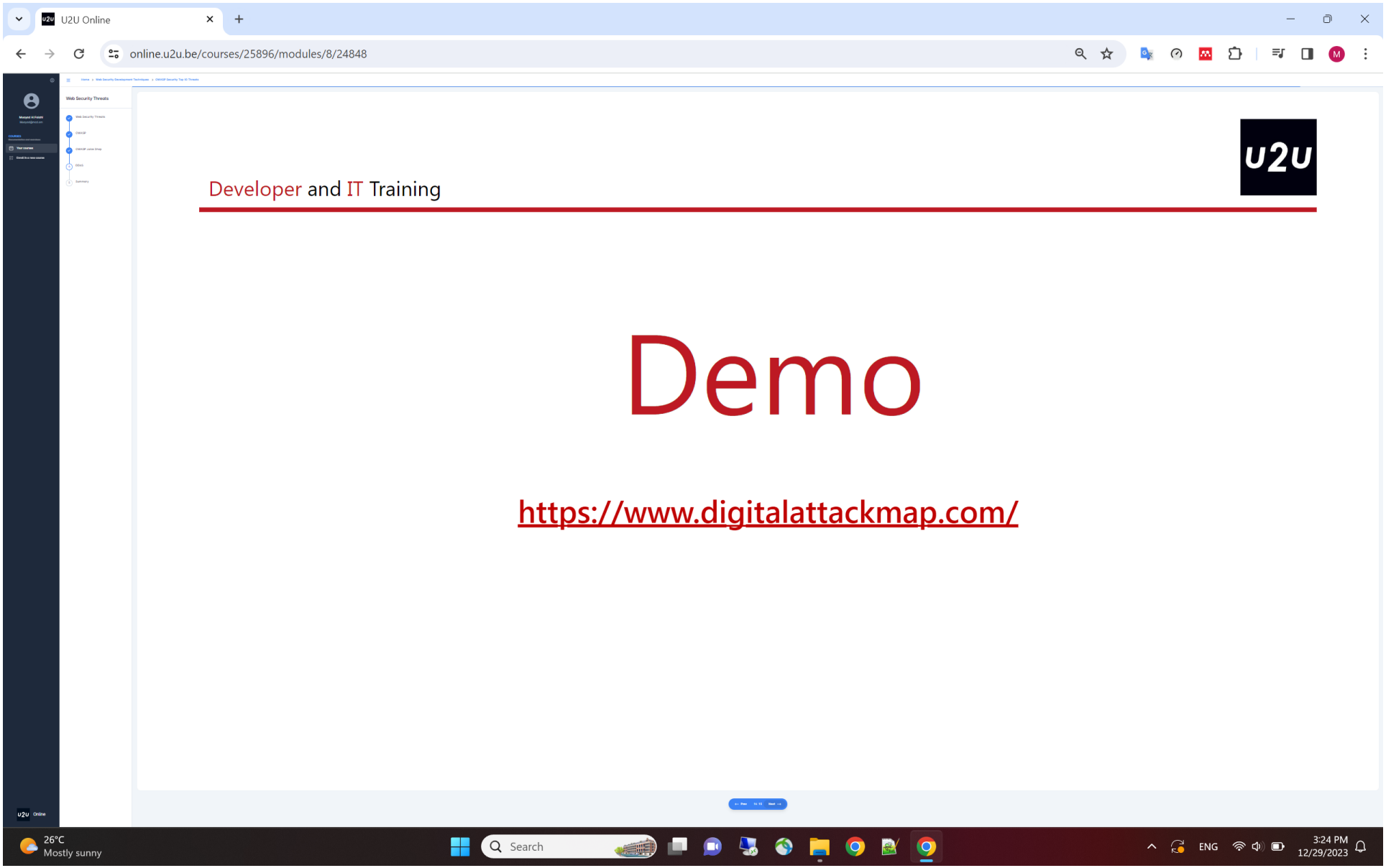


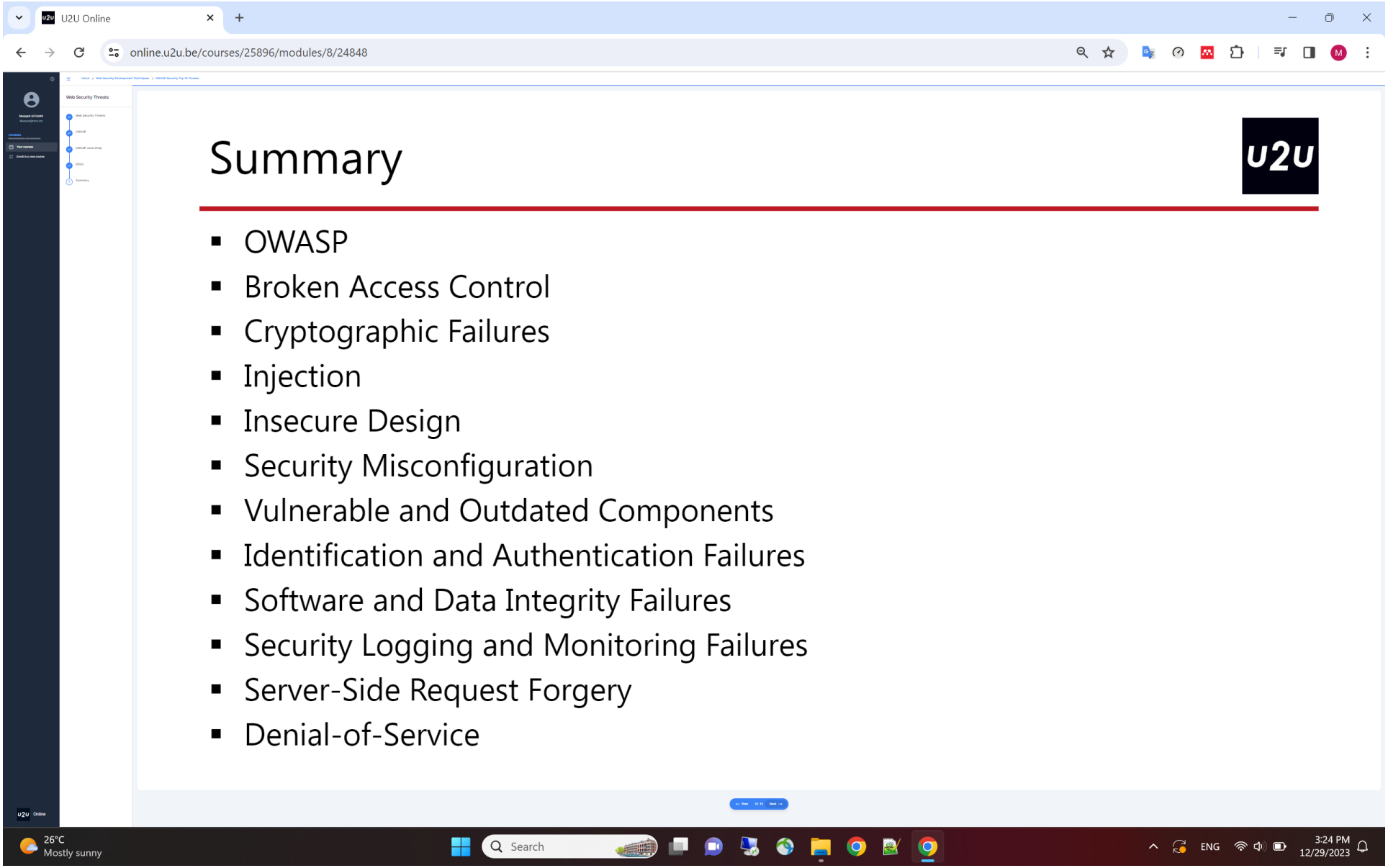

U2U Online
online.u2u.be/courses/25896/modules/8/24848
#11: DDoS?
U2U
Distributed Denial of Service
An attack used to deny usage of a certain service (website, webservice, app,...)
Botnets are most commonly used for DDoS
Compromised machines will send requests at will to a target
Attacks can range from very small to 1100 Gbps and upwards
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
EASY
COMMON
EASY
MODERATE
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
DoS attack
HELP!
target.website.org
Attack this website!
Could you give me resource x?
Could you give me resource x?
Could you give me resource x?
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
Defenses?
U2U
This one is very hard to protect against!
Ask your administrators to help block IP-ranges that are potentially bad
Use Automated Mitigation tools
Do blocking and control the flow for you
Use a Third-Party Provider that helps you
Cloudflare, Akamai, ...
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
Developer and IT Training
u2u
Demo
https://www.digitalattackmap.com/
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/8/24848
Summary
U2U
OWASP
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server-Side Request Forgery
Denial-of-Service
26°C
Mostly sunny
Search
ENG
3:24 PM
12/29/2023