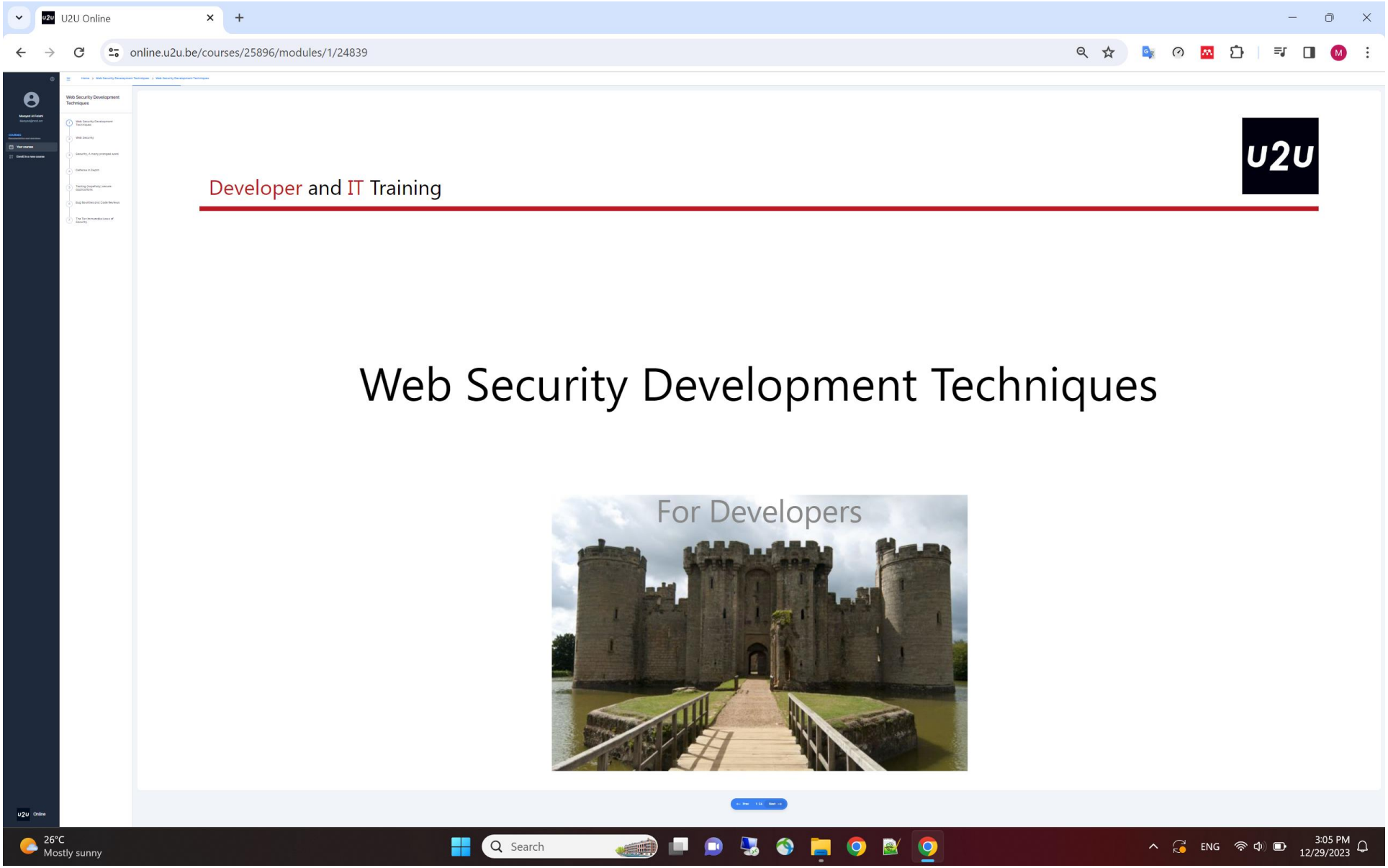
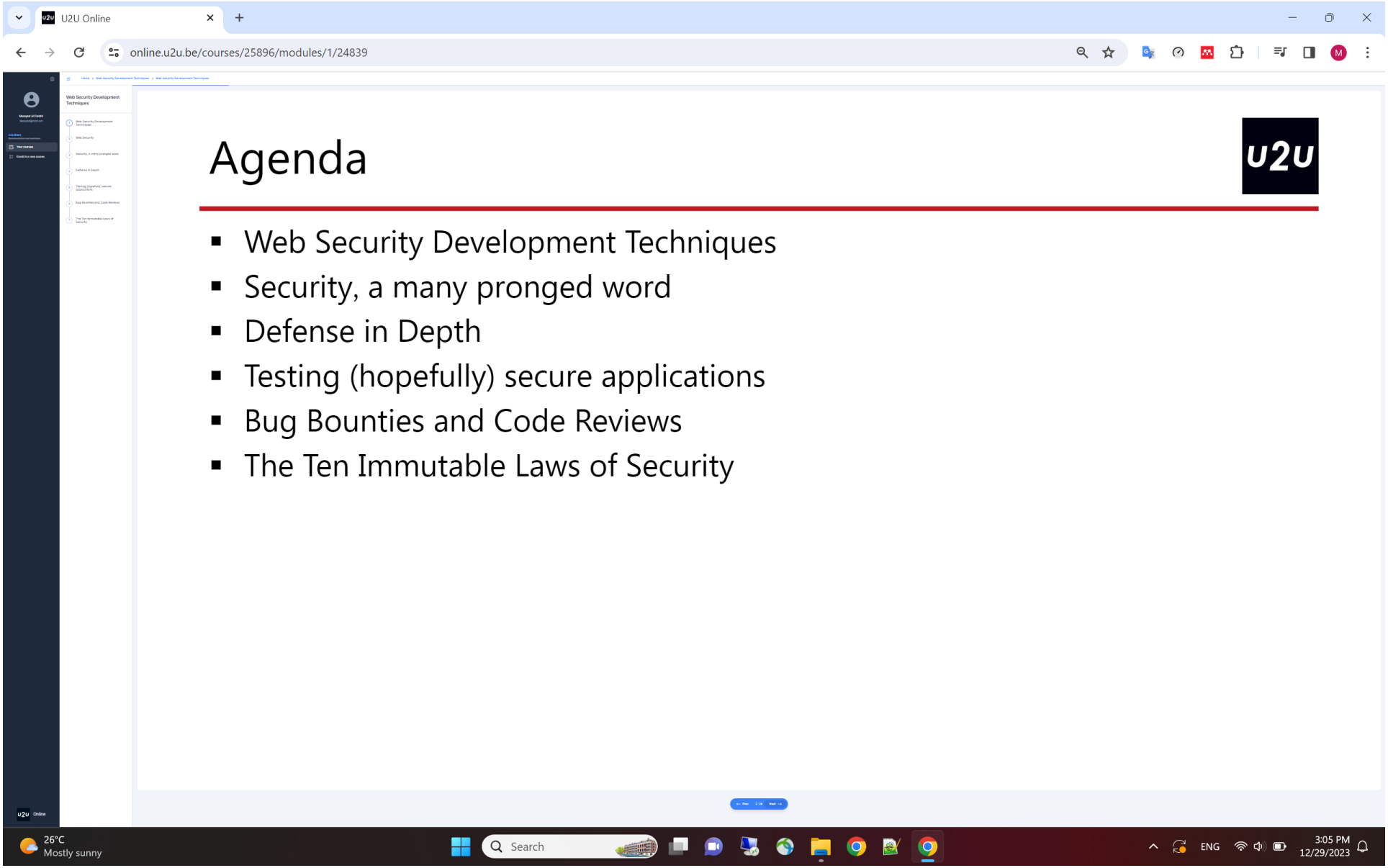
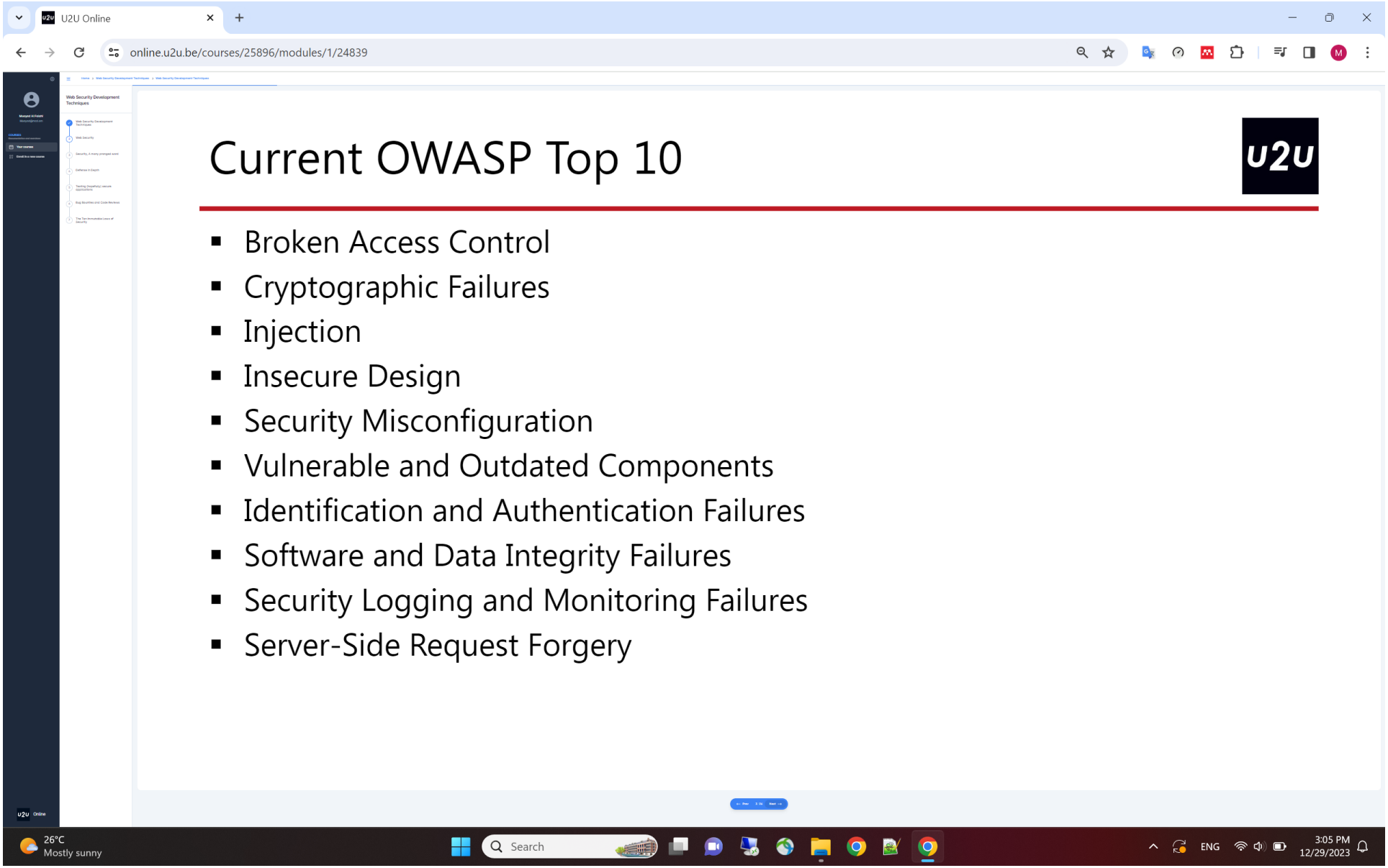

U2U Online
online.u2u.be/courses/25896/modules/1/24839
Developer and IT Training
u2u
Web Security Development Techniques
For Developers
26°C
Mostly sunny
Search
ENG
3:05 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Agenda
U2U
Web Security Development Techniques
Security, a many pronged word
Defense in Depth
Testing (hopefully) secure applications
Bug Bounties and Code Reviews
The Ten Immutable Laws of Security
26°C
Mostly sunny
Search
ENG
3:05 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Current OWASP 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Vulnerable and Outdated Components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
26°C
Mostly sunny
Search
ENG
3:05 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/1/24839

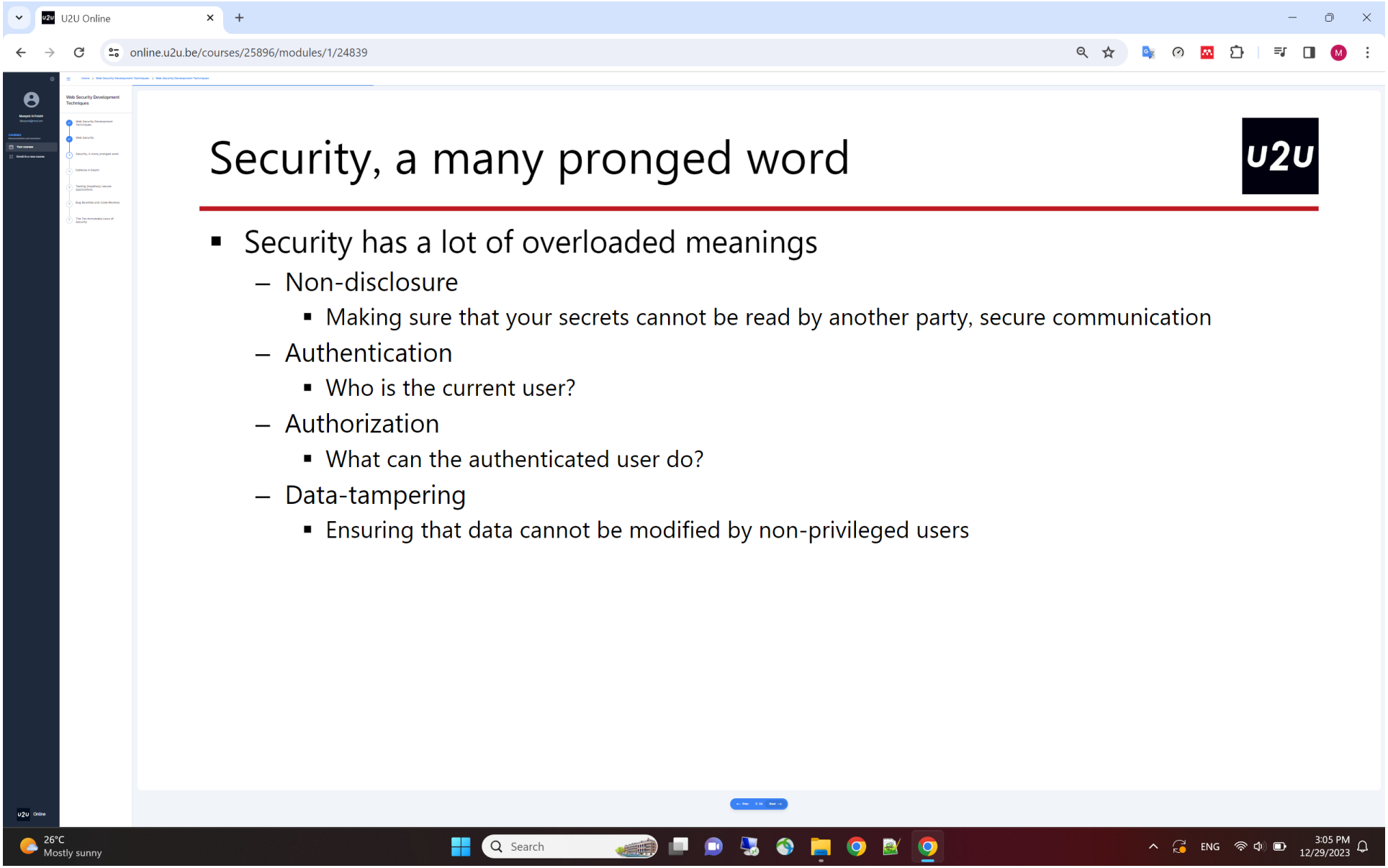
Types of hackers

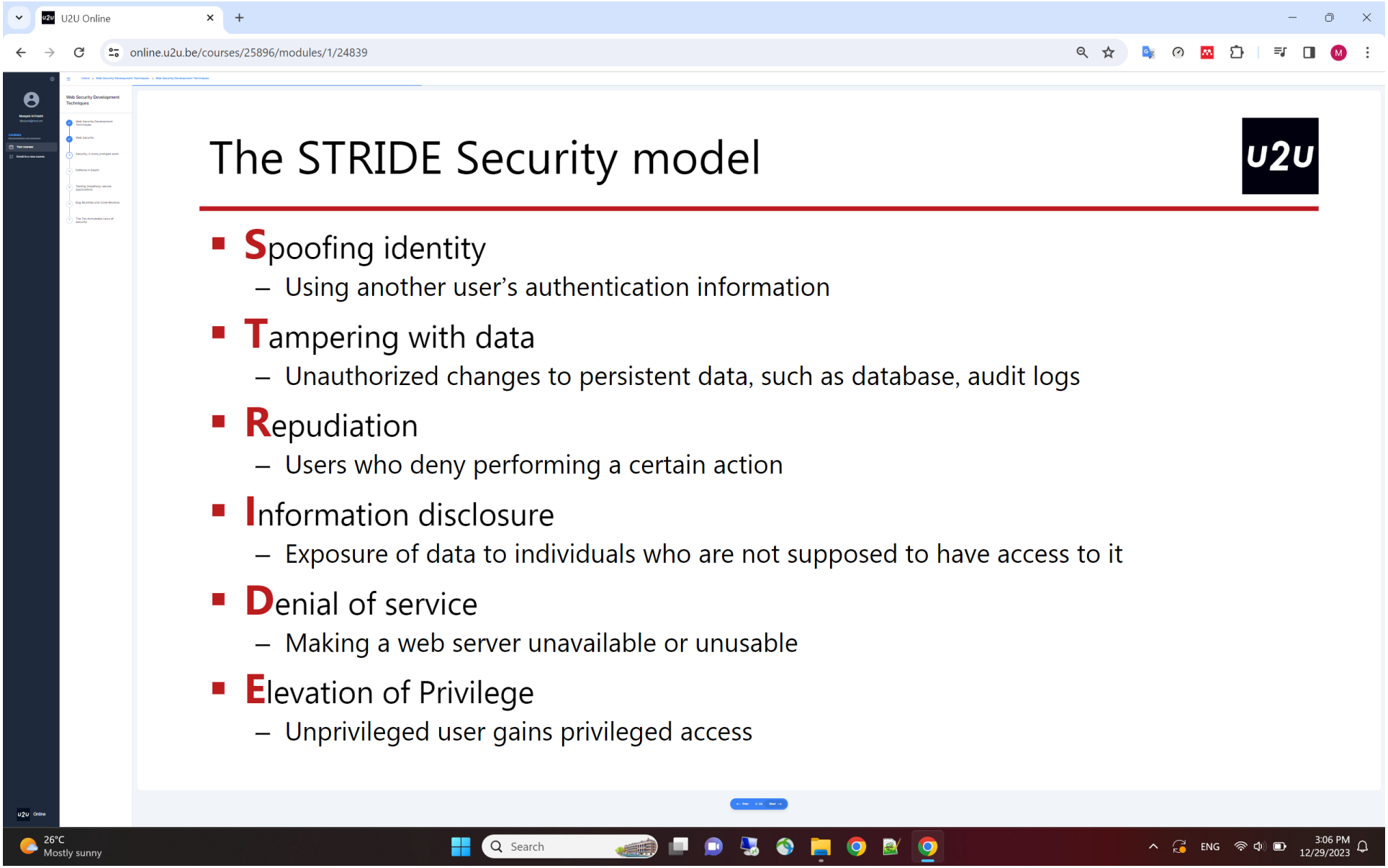
- Script Kiddies
  - No hacking skills
  - Run scripts downloaded from internet
  - In it for the fun of it
- Hacktivist (Anonymous, LulzSec)
  - Varying degrees of skills
  - Politically motivated
- Cyber Criminals
  - For gain $$$, €€€, ¥¥¥, ฿฿฿
  - Ransomware
- Cyber warfare
  - Government funded
  - Presidential election 2016 ☺

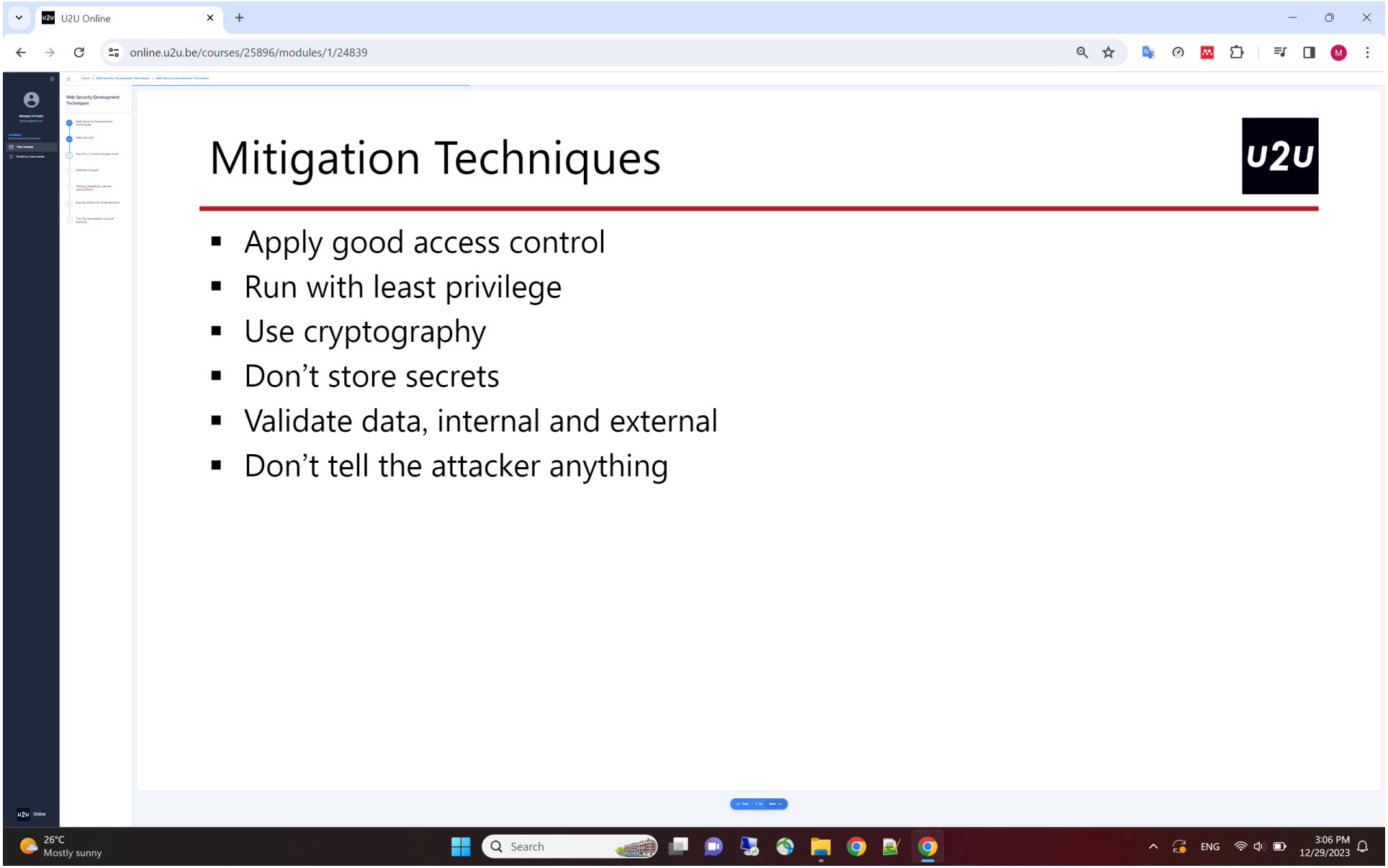
26°C Mostly sunny

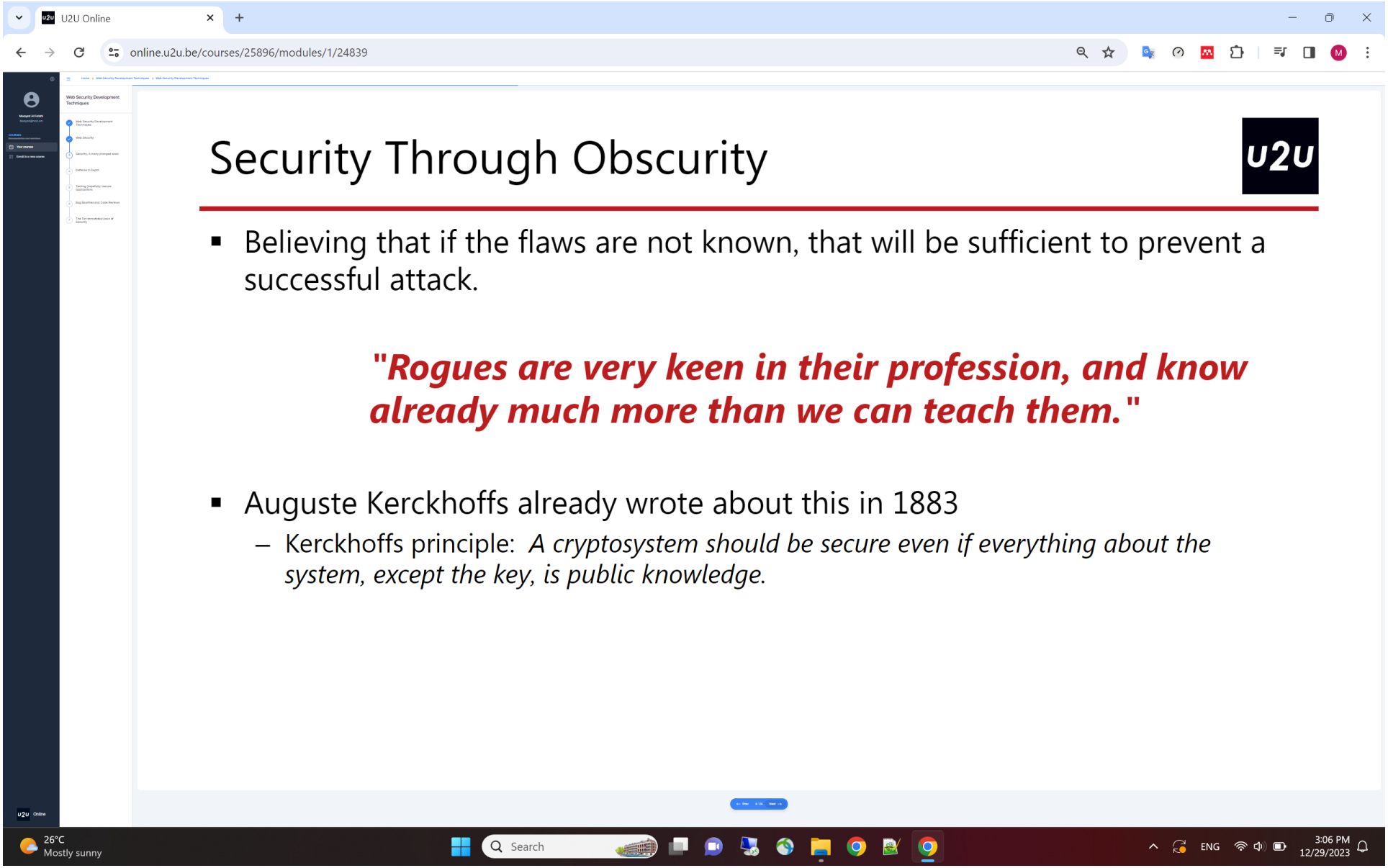
Search

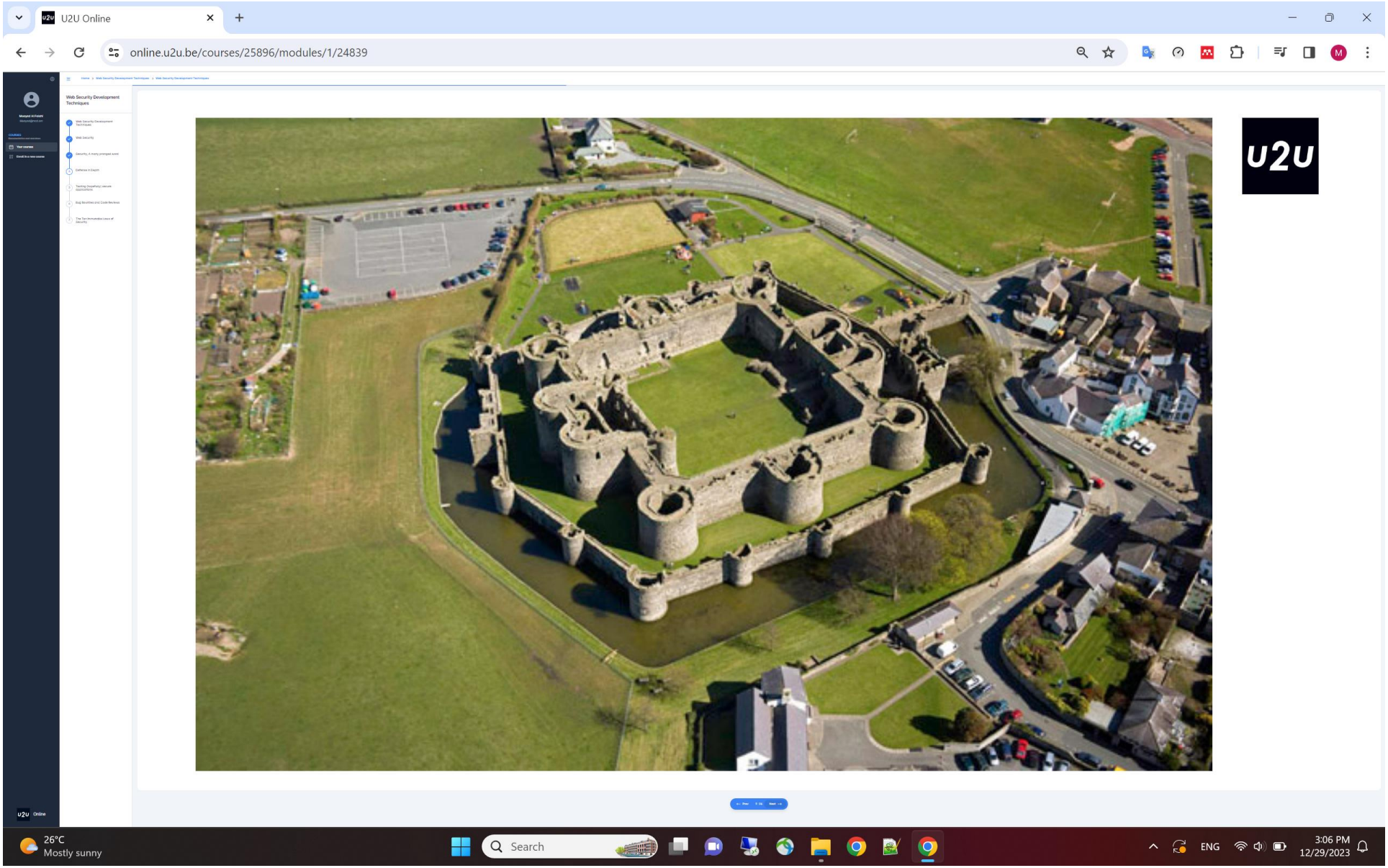
ENG 3:05 PM 12/29/2023

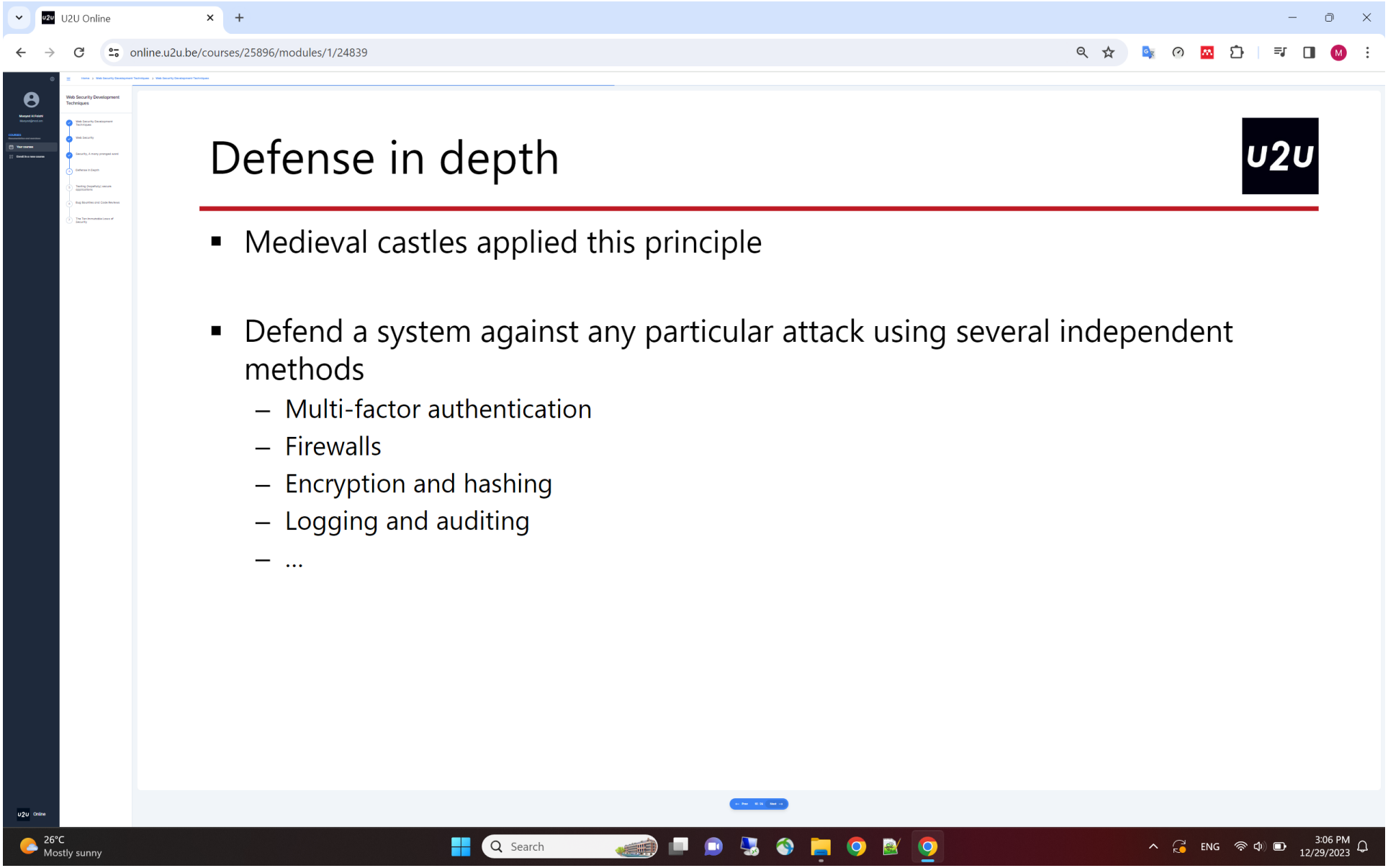

U2U Online
online.u2u.be/courses/25896/modules/1/24839
Security, a many pronged word
U2U
Security has a lot of overloaded meanings
Non-disclosure
Making sure that your secrets cannot be read by another party, secure communication
Authentication
Who is the current user?
Authorization
What can the authenticated user do?
Data-tampering
Ensuring that data cannot be modified by non-privileged users
26°C
Mostly sunny
Search
ENG
3:05 PM
12/29/2023

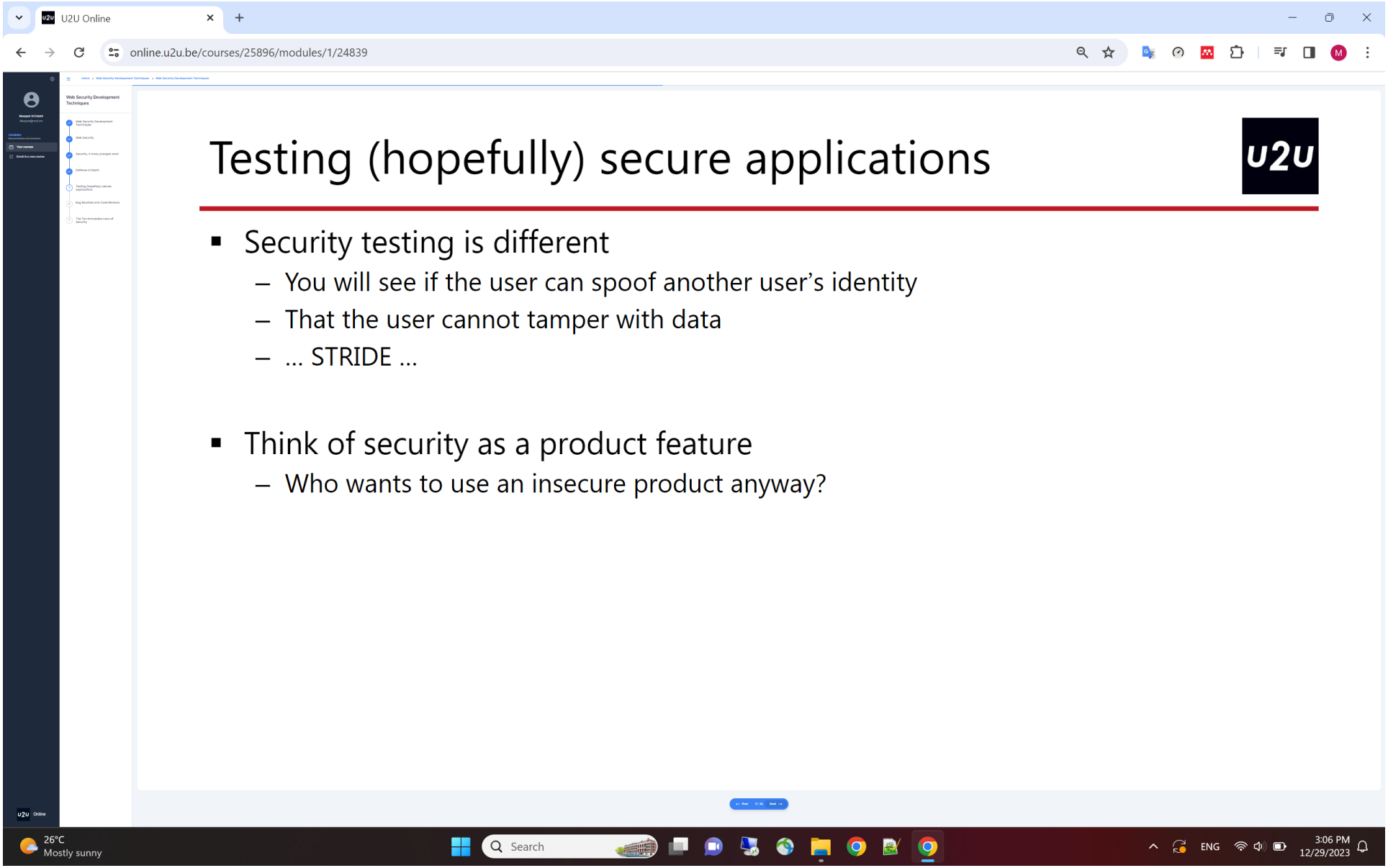

U2U Online
online.u2u.be/courses/25896/modules/1/24839
The STRIDE Security model
U2U
Spoofing identity
– Using another user's authentication information
Tampering with data
– Unauthorized changes to persistent data, such as database, audit logs
Repudiation
– Users who deny performing a certain action
Information disclosure
– Exposure of data to individuals who are not supposed to have access to it
Denial of service
– Making a web server unavailable or unusable
Elevation of Privilege
– Unprivileged user gains privileged access
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Mitigation Techniques
U2U
Apply good access control
Run with least privilege
Use cryptography
Don’t store secrets
Validate data, internal and external
Don’t tell the attacker anything
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Security Through Obscurity
U2U
Believing that if the flaws are not known, that will be sufficient to prevent a successful attack.
"Rogues are very keen in their profession, and know already much more than we can teach them."
Auguste Kerckhoffs already wrote about this in 1883
Kerckhoffs principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Web Security Development Techniques
u2u
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Defense in depth
U2U
Medieval castles applied this principle
Defend a system against any particular attack using several independent methods
Multi-factor authentication
Firewalls
Encryption and hashing
Logging and auditing
...
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Testing (hopefully) secure applications
U2U
Security testing is different
You will see if the user can spoof another user's identity
That the user cannot tamper with data
… STRIDE …
Think of security as a product feature
Who wants to use an insecure product anyway?
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023

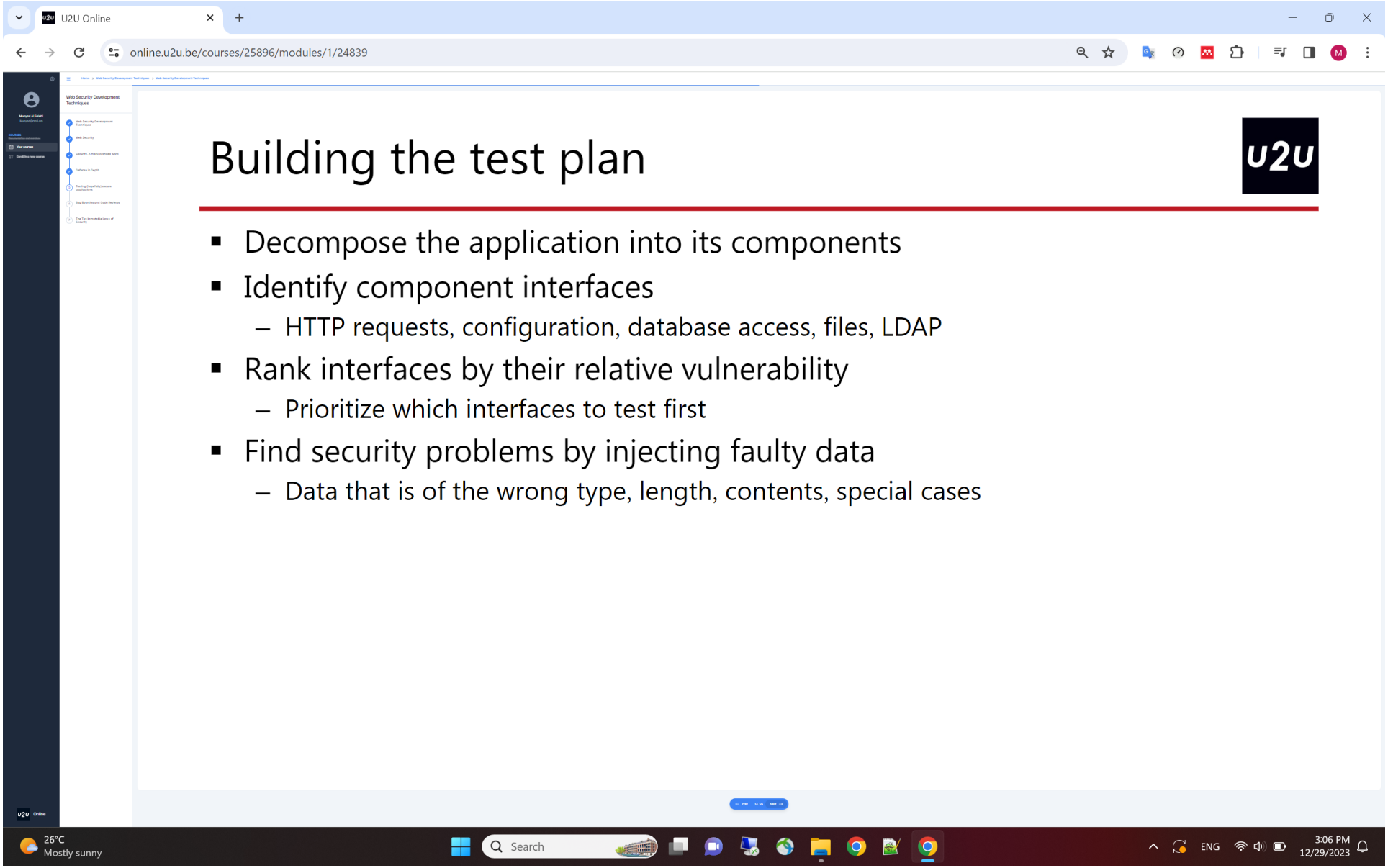
Role playing Marge, Homer and Bart

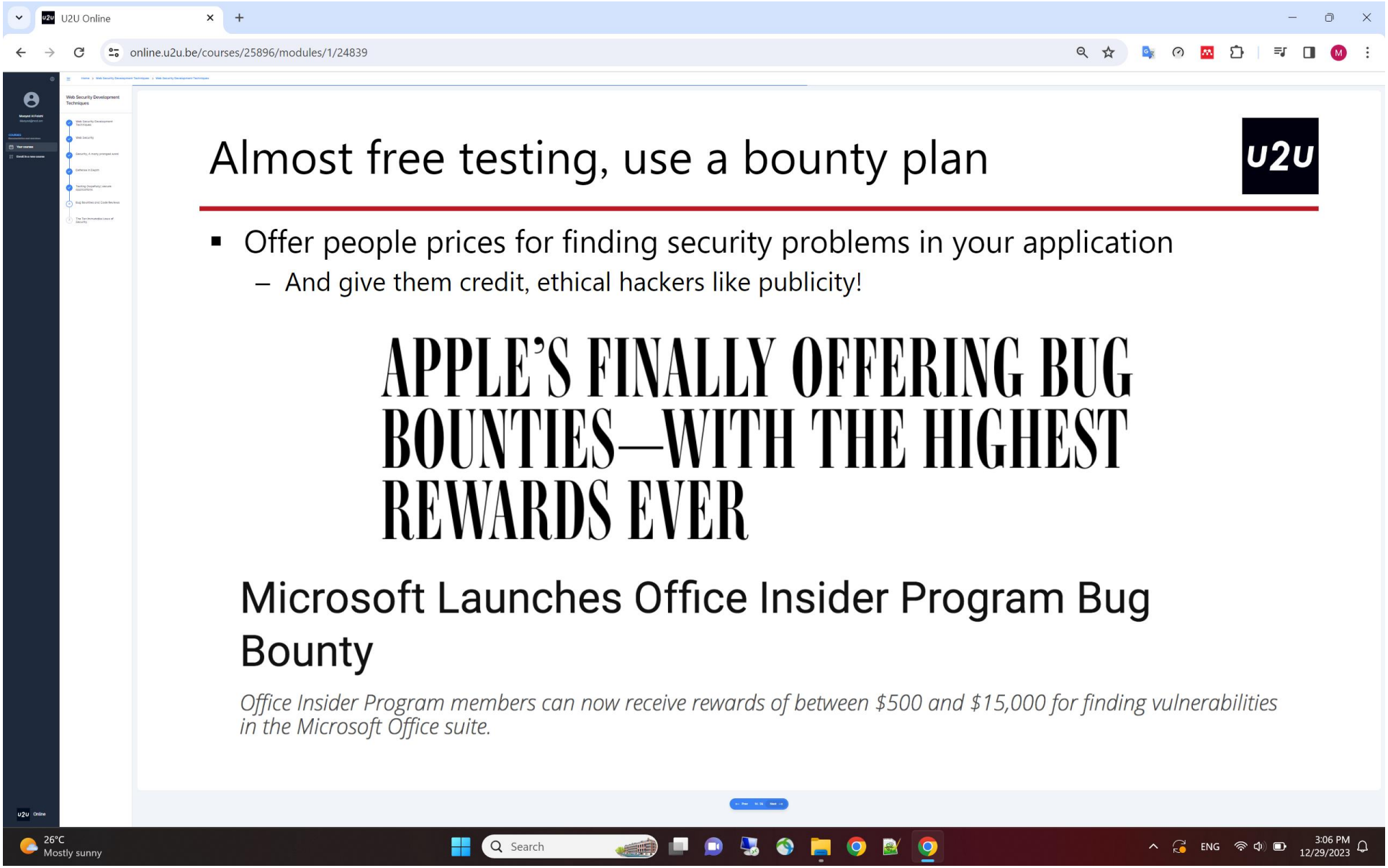
- You need to **assume three roles** while testing

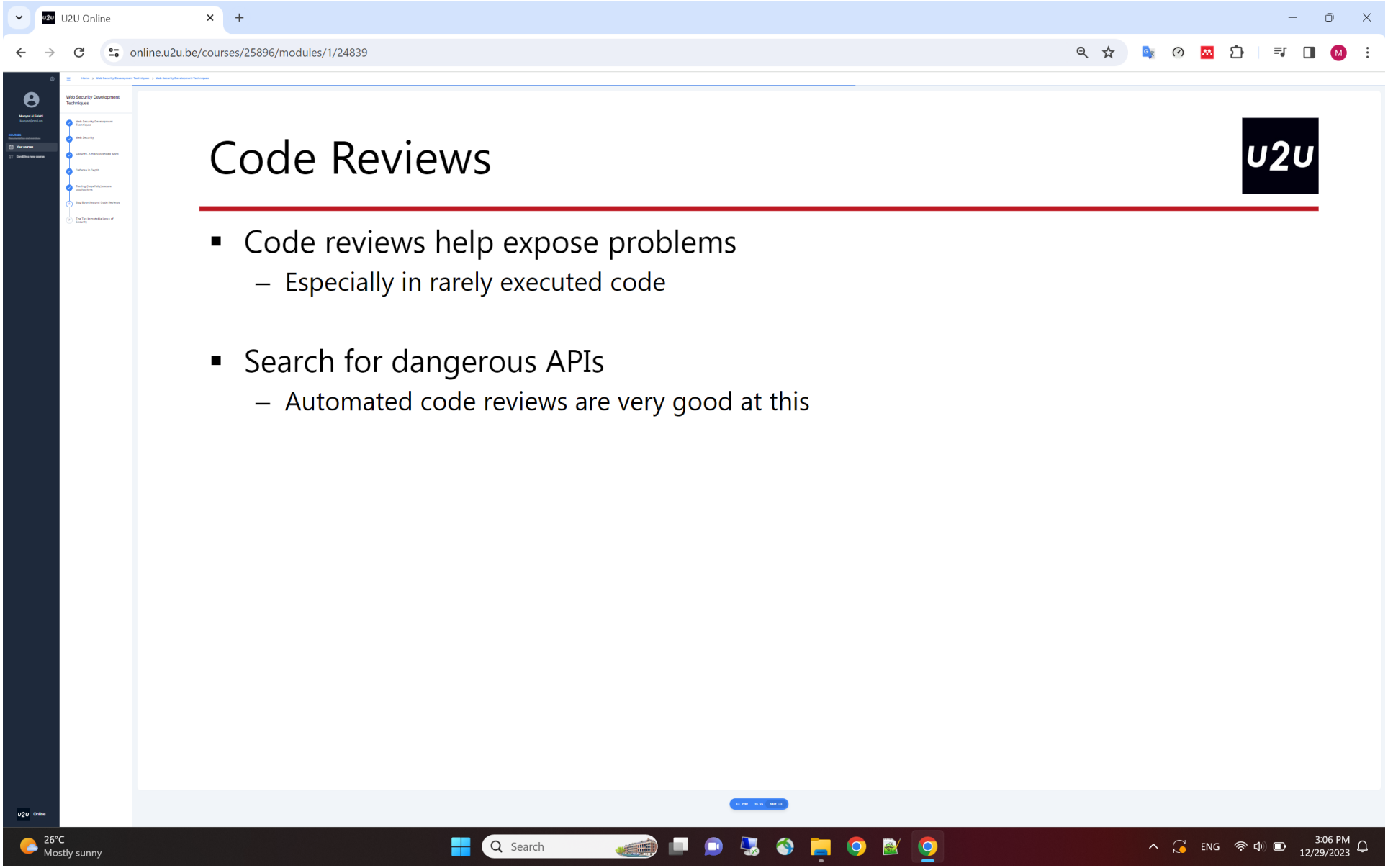
Marge is the user who does her job correctly and uses the system for its intended purposes

Homer is the user who fills in data you would never suspect out of laziness/stupidity

Bart is the user who tries to exploit the system, either out of plain evilness, or for gain


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Building the test plan
u2u
Decompose the application into its components
Identify component interfaces
HTTP requests, configuration, database access, files, LDAP
Rank interfaces by their relative vulnerability
Prioritize which interfaces to test first
Find security problems by injecting faulty data
Data that is of the wrong type, length, contents, special cases
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Almost free testing, use a bounty plan
U2U
Offer people prices for finding security problems in your application
And give them credit, ethical hackers like publicity!
APPLE'S FINALLY OFFERING BUG BOUNTIES—WITH THE HIGHEST REWARDS EVER
Microsoft Launches Office Insider Program Bug Bounty
Office Insider Program members can now receive rewards of between $500 and $15,000 for finding vulnerabilities in the Microsoft Office suite.
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
Code Reviews
u2u
Code reviews help expose problems
Especially in rarely executed code
Search for dangerous APIs
Automated code reviews are very good at this
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/1/24839

The Ten Immutable Laws of Security

- Break any of these laws and you will be pwned!

26°C
Mostly sunny

Search

ENG

3:06 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/1/24839

#1

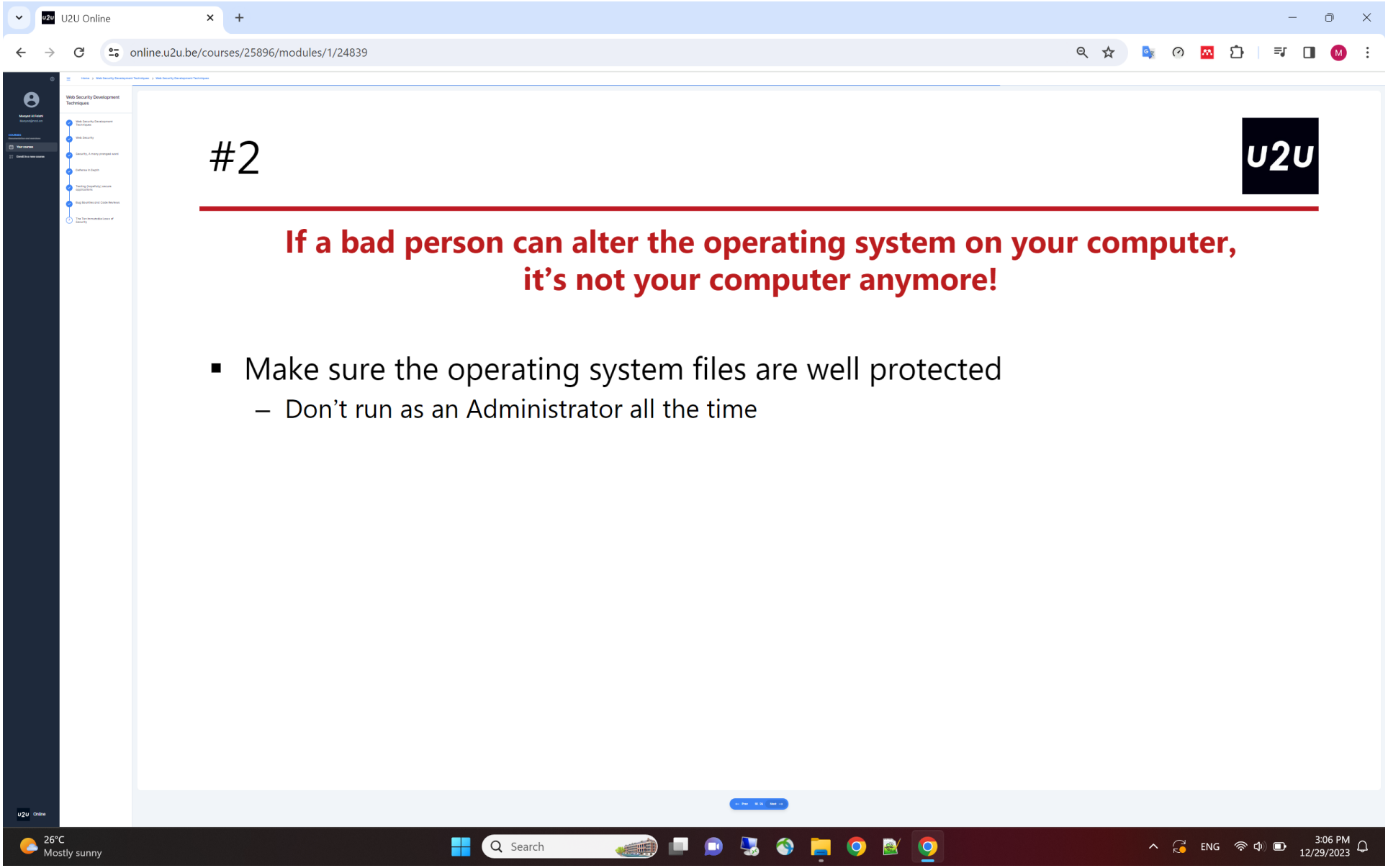
If a bad person can persuade you to run a program on your computer, it's not your computer anymore!

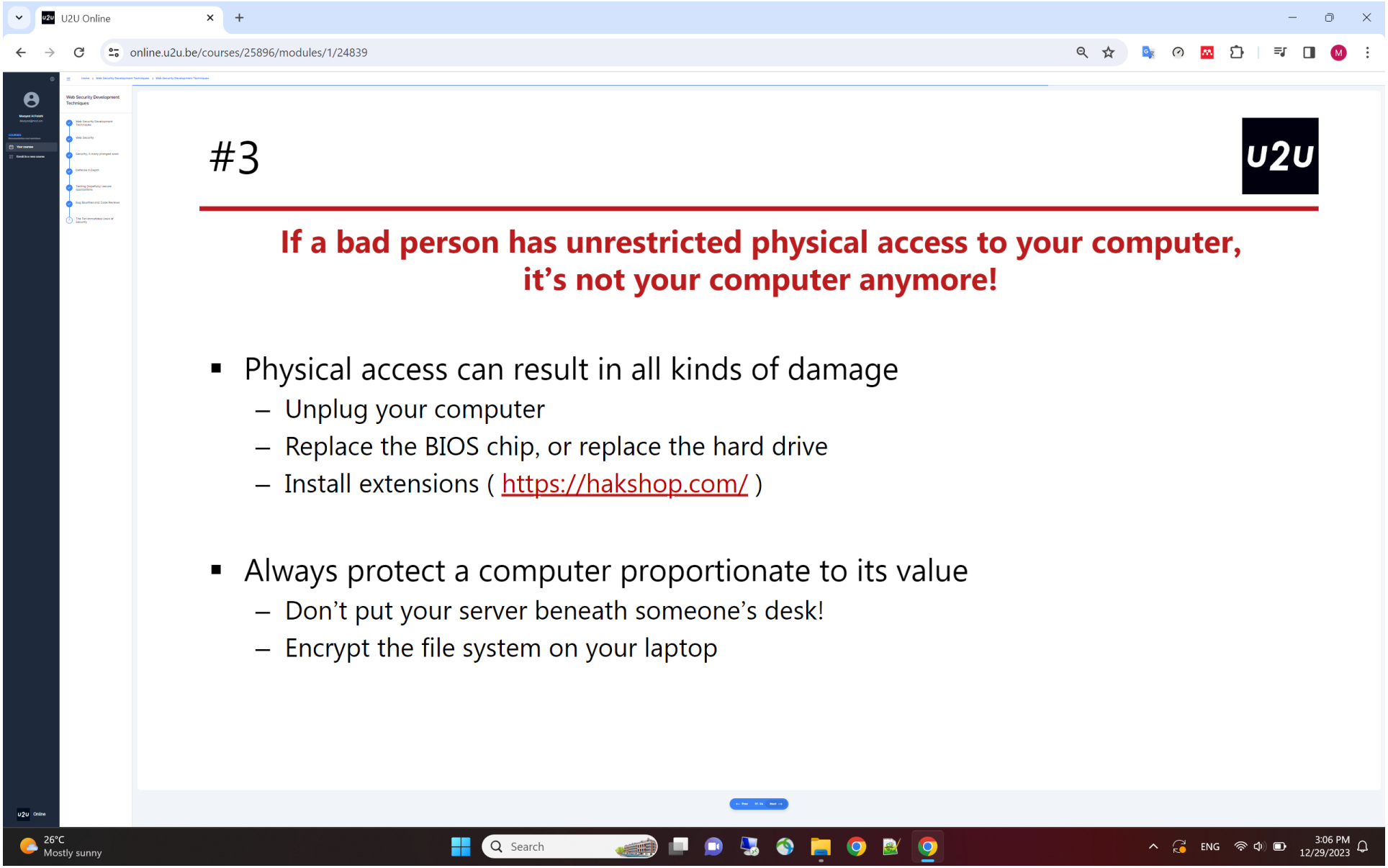
- A program running on your computer can do a lot of things
  - Install a virus (even ransomware), or a backdoor
  - Send rude messages
  - Install a keylogger
  - …
- Never run (or even download) a program from an untrusted source!

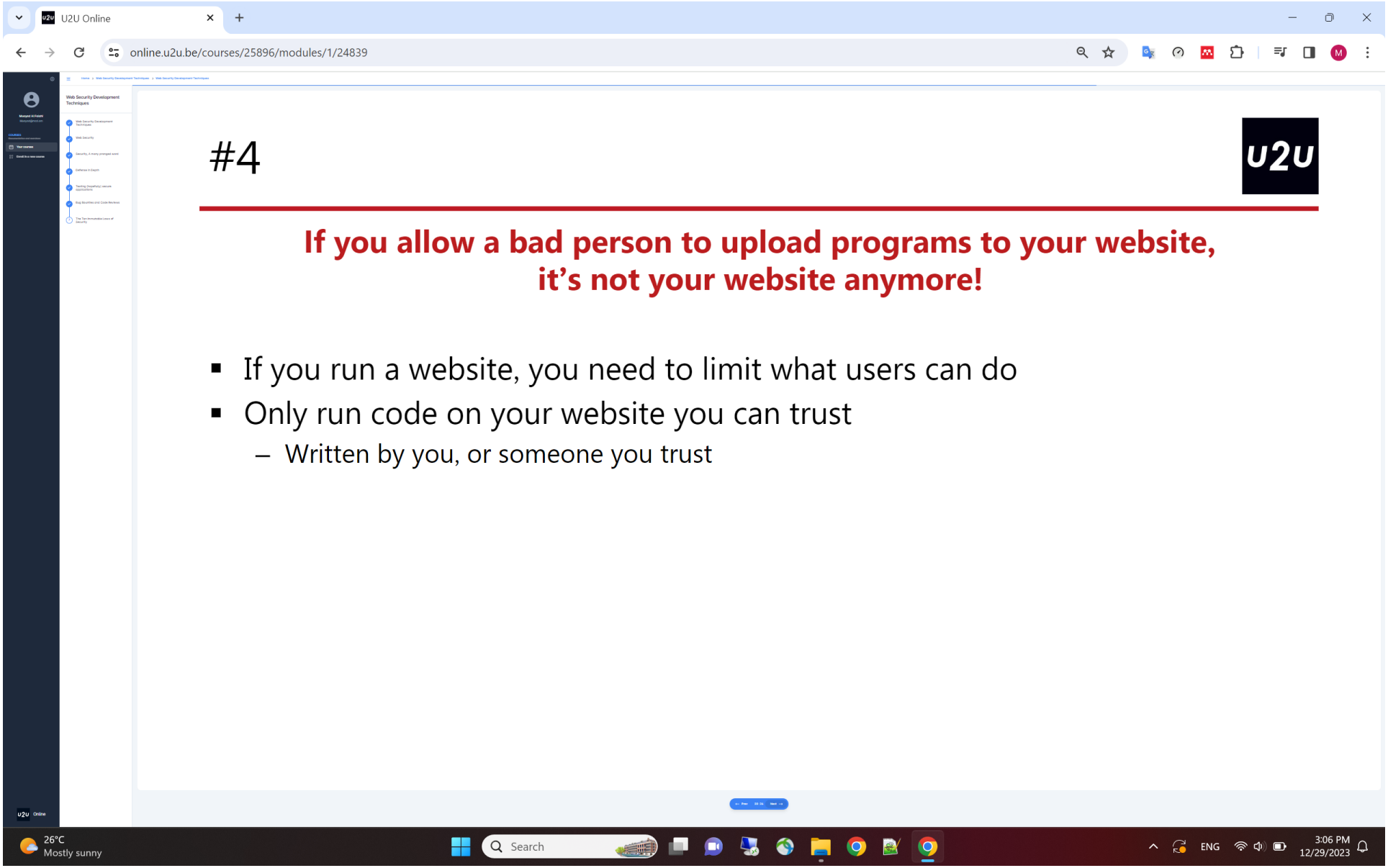
26°C Mostly sunny

Search

ENG 3:06 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#2
u2u
If a bad person can alter the operating system on your computer, it's not your computer anymore!
Make sure the operating system files are well protected
Don't run as an Administrator all the time
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#3
U2U
If a bad person has unrestricted physical access to your computer, it's not your computer anymore!
Physical access can result in all kinds of damage
Unplug your computer
Replace the BIOS chip, or replace the hard drive
Install extensions (https://hakshop.com/)
Always protect a computer proportionate to its value
Don't put your server beneath someone's desk!
Encrypt the file system on your laptop
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#4
U2U
If you allow a bad person to upload programs to your website, it's not your website anymore!
If you run a website, you need to limit what users can do
Only run code on your website you can trust
Written by you, or someone you trust
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023

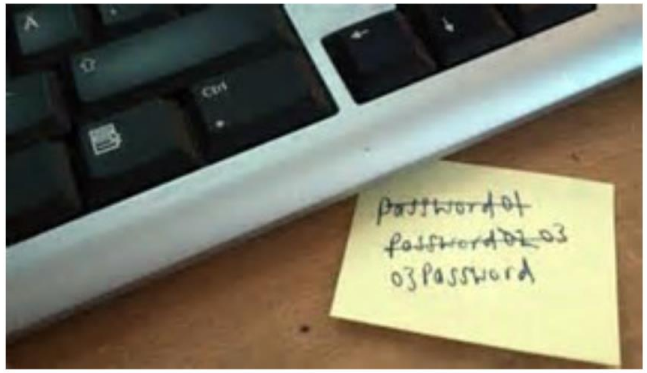
U2U Online

online.u2u.be/courses/25896/modules/1/24839

#5

Weak passwords trump strong security

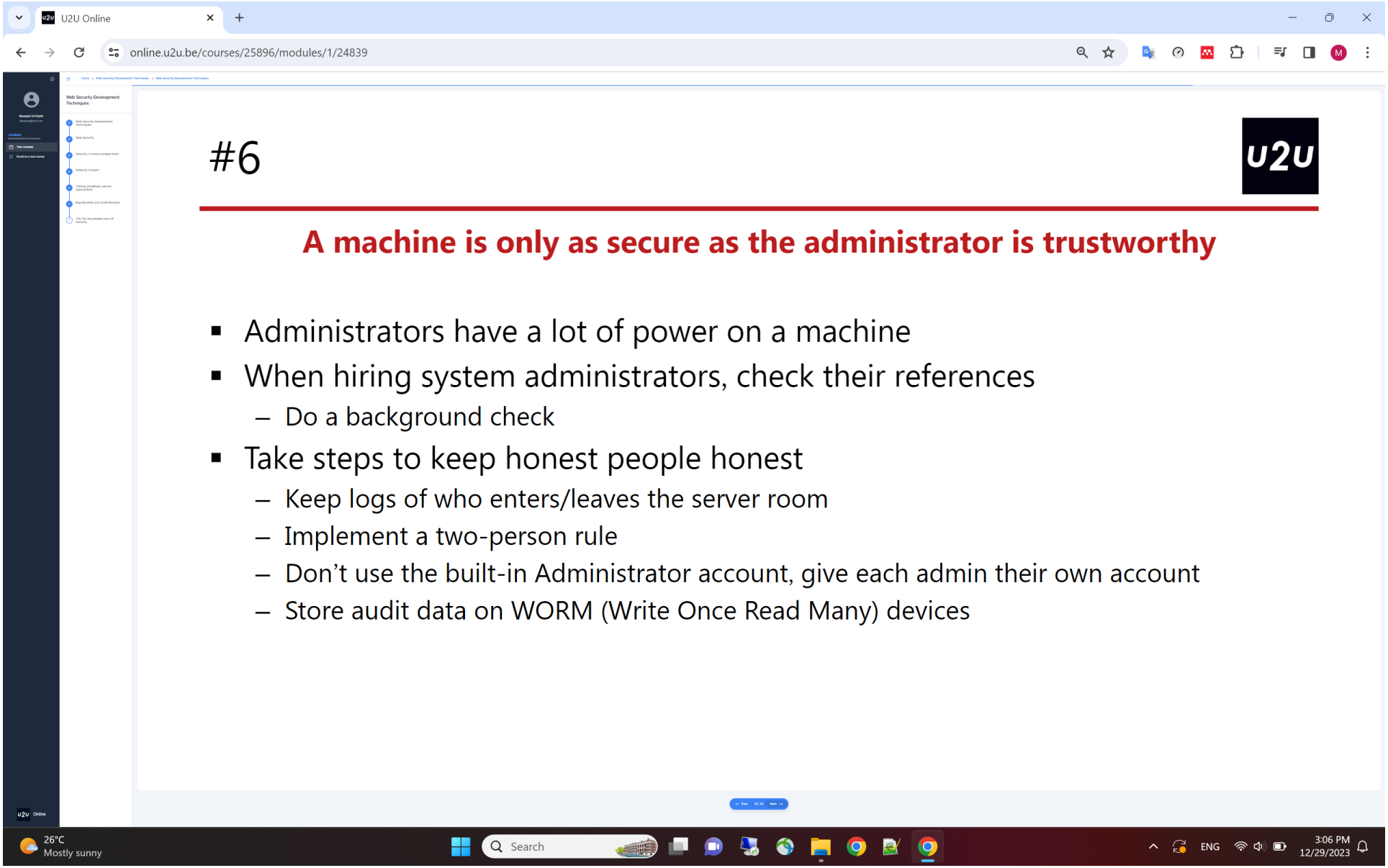
- Any bad person who gets your password can do anything you can
  - And it will be in your name!
- Always use strong passwords that are complex
  - And have a different password for each account
    - Use a password manager to help with this
  - Don't write it down!
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf(ch 5.1.1)



26°C Mostly sunny

Search

ENG 3:06 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#6
U2U
A machine is only as secure as the administrator is trustworthy
Administrators have a lot of power on a machine
When hiring system administrators, check their references
Do a background check
Take steps to keep honest people honest
Keep logs of who enters/leaves the server room
Implement a two-person rule
Don't use the built-in Administrator account, give each admin their own account
Store audit data on WORM (Write Once Read Many) devices
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023

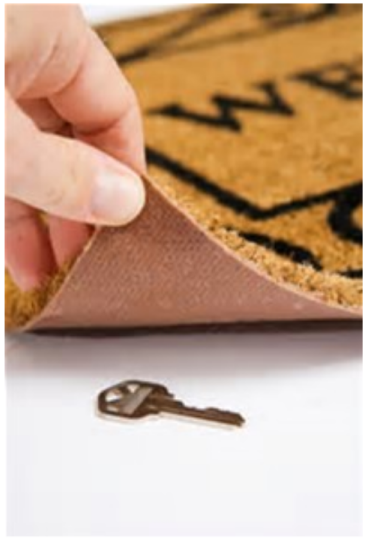
U2U Online

online.u2u.be/courses/25896/modules/1/24839

#7

Encrypted data is only as secure as the decryption key

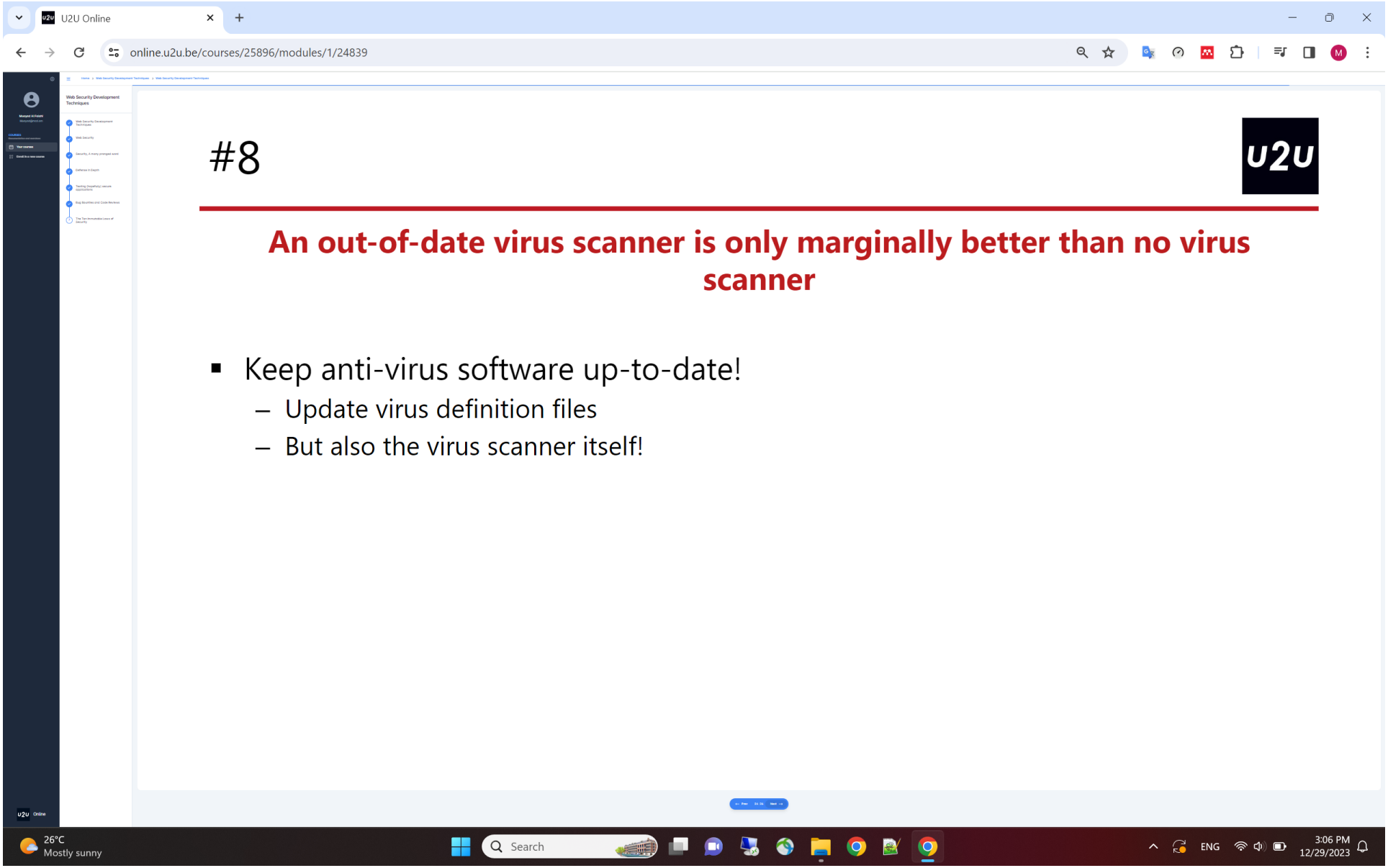
- Use offline storage for keys
  - Passwords used to generate keys should be very strong!
- Don't put the key under the doormat ☺

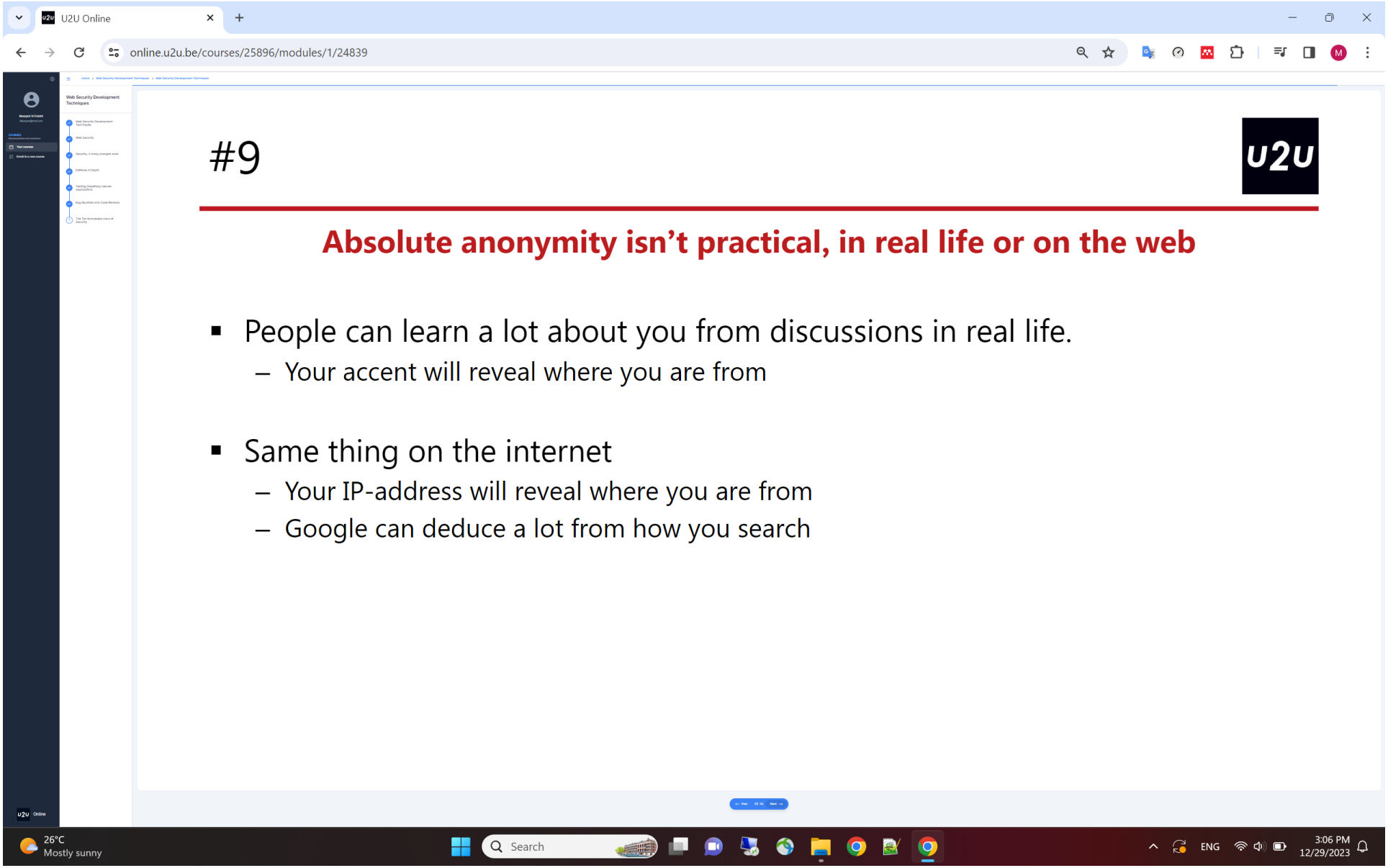


26°C Mostly sunny

Search

ENG 3:06 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#8
U2U
An out-of-date virus scanner is only marginally better than no virus scanner
Keep anti-virus software up-to-date!
Update virus definition files
But also the virus scanner itself!
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/1/24839
#9
u2u
Absolute anonymity isn't practical, in real life or on the web
People can learn a lot about you from discussions in real life.
Your accent will reveal where you are from
Same thing on the internet
Your IP-address will reveal where you are from
Google can deduce a lot from how you search
26°C
Mostly sunny
Search
ENG
3:06 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/1/24839

#10

Technology is not a panacea

- Technology does not offer a risk-free world
  - Perfect security does not exist
  - All software has bugs
- Sometimes hackers will fall back on social engineering

26°C Mostly sunny

Search

ENG 3:06 PM 12/29/2023